



IST-2002-507932

ECRYPT

European Network of Excellence in Cryptology

Network of Excellence

Information Society Technologies

D.VAM.14
Performing Benchmarks

Due date of deliverable: 31. July 2007
Actual submission date: 31. July 2008

Start date of project: 1. February 2004 Duration: 4.5 years

Lead contractor: KUL

Revision 1.1

Project co-funded by the European Commission within the 6th Framework Programme		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission services)	
RE	Restricted to a group specified by the consortium (including the Commission services)	
CO	Confidential, only for members of the consortium (including the Commission services)	

Performing Benchmarks

Editor
Daniel Page (BRIS)

Contributors
Daniel J. Bernstein (UIC, visiting TUE)
Tanja Lange (TUE)

31. July 2008
Revision 1.1

The work described in this report has in part been supported by the Commission of the European Communities through the IST program under contract IST-2002-507932. The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Contents

1 Introduction **3**

2 Which primitives are measured? **5**
2.1 Introduction . . . 5
2.2 List of hash primitives measured . . . 5
2.3 List of stream-cipher primitives measured . . . 6
2.4 List of public-key-encryption primitives measured . . . 8
2.5 List of public-key-signature primitives measured . . . 8
2.6 List of public-key-secret-sharing primitives measured . . . 11

3 Which computers are used for measurements? **13**
3.1 Introduction . . . 13
3.2 Notes on multiple-core computers . . . 13
3.3 List of computers used for measurements . . . 14

4 Which compilers are used for measurements? **19**
4.1 Introduction . . . 19
4.2 Notes on multiple operations . . . 19
4.3 Notes on machine-specific compilers . . . 20
4.4 Notes on multiple ABIs . . . 20
4.5 List of compilers tested . . . 20

5 Which compilers produced the best results? **75**
5.1 Introduction . . . 75
5.2 amd64, 1403MHz, AMD Opteron 240 (f58), `nmisles8amd64` . . . 75
5.3 amd64, 2400MHz, Intel Core 2 Duo (6fb), `utrecht` . . . 82
5.4 amd64, 2800MHz, Intel Xeon (f41), `nmi0056` . . . 91
5.5 amd64, 2800MHz, Intel Xeon (f41), `nmi0057` . . . 98
5.6 amd64, 2800MHz, Intel Xeon (f41), `nmi0063` . . . 105
5.7 amd64, 3000MHz, Intel Pentium D (f64), `speed` . . . 112
5.8 amd64, 3000MHz, Intel Xeon (f4a), `nmi0090` . . . 121
5.9 amd64, 3392MHz, Intel Pentium D (f64), `nmi0104` . . . 127
5.10 amd64, 3392MHz, Intel Pentium D (f64), `nmi0161` . . . 135
5.11 amd64, 3392MHz, Intel Pentium D (f64), `nmi0241` . . . 143
5.12 ia64, 900MHz, HP Itanium II, `nmi0025` . . . 150
5.13 ia64, 997MHz, HP Itanium II, `nmi0020` . . . 153
5.14 ia64, 997MHz, HP Itanium II, `nmi0058` . . . 157

5.15 ia64, 1396MHz, HP Itanium II, nmi0065 . . . 161
5.16 ppc32, 400MHz, Motorola PowerPC G4 7400, nmi0042 . . . 165
5.17 ppc32, 2000MHz, IBM PowerPC G5 970, geespaz . . . 169
5.18 ppc32, 2097MHz, IBM POWER5, nmi0154 . . . 174
5.19 ppc32, 3192MHz, IBM Cell PPE, nmips3 . . . 177
5.20 ppc64, 2000MHz, IBM PowerPC G5 970, geespaz . . . 181
5.21 ppc64, 2097MHz, IBM POWER5, nmi0154 . . . 184
5.22 ppc64, 3192MHz, IBM Cell PPE, nmips3 . . . 187
5.23 sparcv9, 300MHz, Sun UltraSPARC IIi, nmi0096 . . . 189
5.24 sparcv9, 900MHz, Sun UltraSPARC III, nmi0051 . . . 193
5.25 sparcv9, 1200MHz, Sun UltraSPARC III, nmisolaris10 . . . 196
5.26 x86, 1196MHz, Intel Celeron (6b1), vieux . . . 199
5.27 x86, 1403MHz, AMD Opteron 240 (f58), nmisles8amd64 . . . 207
5.28 x86, 1833MHz, Intel Core Duo, nmi0068 . . . 215
5.29 x86, 2400MHz, Intel Pentium 4 (f24), nmitest4 . . . 220
5.30 x86, 2400MHz, Intel Core 2 Duo (6fb), utrecht . . . 228
5.31 x86, 2401MHz, Intel Pentium 4 (f24), nmi0086 . . . 235
5.32 x86, 2658MHz, Intel Xeon (f25), nmi0013 . . . 243
5.33 x86, 2658MHz, Intel Xeon (f25), nmibuild15 . . . 251
5.34 x86, 2658MHz, Intel Xeon (f25), nmibuild16 . . . 258
5.35 x86, 2658MHz, Intel Xeon (f25), nmibuild22 . . . 266
5.36 x86, 2659MHz, Intel Xeon (f25), nmibuild21 . . . 274
5.37 x86, 2659MHz, Intel Xeon (f25), nmibuild26 . . . 282
5.38 x86, 2667MHz, Intel Xeon (f25), nmi0036 . . . 290
5.39 x86, 2791MHz, Intel Xeon (f27), nmi0024 . . . 298
5.40 x86, 2800MHz, Intel Xeon (f41), nmi0057 . . . 306
5.41 x86, 2800MHz, Intel Xeon (f41), nmi0063 . . . 313
5.42 x86, 2801MHz, Intel Xeon (f41), nmi0060 . . . 320
5.43 x86, 2801MHz, Intel Xeon (f41), nmi0061 . . . 328
5.44 x86, 2801MHz, Intel Xeon (f41), nmi0062 . . . 336
5.45 x86, 2802MHz, Intel Xeon (f29), nmibuild40 . . . 345
5.46 x86, 2995MHz, Intel Xeon (f41), nmi0079 . . . 352
5.47 x86, 2996MHz, Intel Xeon (f41), nmi0076 . . . 360
5.48 x86, 3000MHz, Intel Xeon (f4a), nmi0090 . . . 368
5.49 x86, 3000MHz, Intel Xeon (f4a), nmi0102 . . . 374
5.50 x86, 3391MHz, Intel Pentium D (f64), nmi0099 . . . 382
5.51 x86, 3392MHz, Intel Pentium D (f64), nmi0104 . . . 391
5.52 x86, 3392MHz, Intel Pentium D (f64), nmi0241 . . . 399

6 Measurements of hash functions **409**
6.1 Introduction . . . 409
6.2 amd64, 1403MHz, AMD Opteron 240 (f58), nmisles8amd64 . . . 410
6.3 amd64, 2400MHz, Intel Core 2 Duo (6fb), utrecht . . . 412
6.4 amd64, 2800MHz, Intel Xeon (f41), nmi0056 . . . 414
6.5 amd64, 2800MHz, Intel Xeon (f41), nmi0057 . . . 416
6.6 amd64, 2800MHz, Intel Xeon (f41), nmi0063 . . . 418
6.7 amd64, 3000MHz, Intel Pentium D (f64), speed . . . 420

6.8 amd64, 3000MHz, Intel Xeon (f4a), nmi0090 422
6.9 amd64, 3392MHz, Intel Pentium D (f64), nmi0104 424
6.10 amd64, 3392MHz, Intel Pentium D (f64), nmi0161 426
6.11 amd64, 3392MHz, Intel Pentium D (f64), nmi0241 428
6.12 ia64, 900MHz, HP Itanium II, nmi0025 430
6.13 ia64, 997MHz, HP Itanium II, nmi0020 432
6.14 ia64, 997MHz, HP Itanium II, nmi0058 434
6.15 ia64, 1396MHz, HP Itanium II, nmi0065 436
6.16 ppc32, 400MHz, Motorola PowerPC G4 7400, nmi0042 438
6.17 ppc32, 2000MHz, IBM PowerPC G5 970, geespaz 440
6.18 ppc32, 2097MHz, IBM POWER5, nmi0154 442
6.19 ppc32, 3192MHz, IBM Cell PPE, nmips3 444
6.20 ppc64, 2000MHz, IBM PowerPC G5 970, geespaz 446
6.21 ppc64, 2097MHz, IBM POWER5, nmi0154 448
6.22 ppc64, 3192MHz, IBM Cell PPE, nmips3 450
6.23 sparcv9, 300MHz, Sun UltraSPARC IIi, nmi0096 452
6.24 sparcv9, 900MHz, Sun UltraSPARC III, nmi0051 454
6.25 sparcv9, 1200MHz, Sun UltraSPARC III, nmisolaris10 456
6.26 x86, 1196MHz, Intel Celeron (6b1), vieux 458
6.27 x86, 1403MHz, AMD Opteron 240 (f58), nmisles8amd64 460
6.28 x86, 1833MHz, Intel Core Duo, nmi0068 462
6.29 x86, 2400MHz, Intel Pentium 4 (f24), nmitest4 464
6.30 x86, 2400MHz, Intel Core 2 Duo (6fb), utrecht 466
6.31 x86, 2401MHz, Intel Pentium 4 (f24), nmi0086 468
6.32 x86, 2658MHz, Intel Xeon (f25), nmi0013 470
6.33 x86, 2658MHz, Intel Xeon (f25), nmibuild15 472
6.34 x86, 2658MHz, Intel Xeon (f25), nmibuild16 474
6.35 x86, 2658MHz, Intel Xeon (f25), nmibuild22 476
6.36 x86, 2659MHz, Intel Xeon (f25), nmibuild21 478
6.37 x86, 2659MHz, Intel Xeon (f25), nmibuild26 480
6.38 x86, 2667MHz, Intel Xeon (f25), nmi0036 482
6.39 x86, 2791MHz, Intel Xeon (f27), nmi0024 484
6.40 x86, 2800MHz, Intel Xeon (f41), nmi0057 486
6.41 x86, 2800MHz, Intel Xeon (f41), nmi0063 488
6.42 x86, 2801MHz, Intel Xeon (f41), nmi0060 490
6.43 x86, 2801MHz, Intel Xeon (f41), nmi0061 492
6.44 x86, 2801MHz, Intel Xeon (f41), nmi0062 494
6.45 x86, 2802MHz, Intel Xeon (f29), nmibuild40 496
6.46 x86, 2995MHz, Intel Xeon (f41), nmi0079 498
6.47 x86, 2996MHz, Intel Xeon (f41), nmi0076 500
6.48 x86, 3000MHz, Intel Xeon (f4a), nmi0090 502
6.49 x86, 3000MHz, Intel Xeon (f4a), nmi0102 504
6.50 x86, 3391MHz, Intel Pentium D (f64), nmi0099 506
6.51 x86, 3392MHz, Intel Pentium D (f64), nmi0104 508
6.52 x86, 3392MHz, Intel Pentium D (f64), nmi0241 510

7 Measurements of secret-key stream ciphers **513**
7.1 Introduction . . . 513
7.2 amd64, 1403MHz, AMD Opteron 240 (f58), `nmisles8amd64` . . . 514
7.3 amd64, 2400MHz, Intel Core 2 Duo (6fb), `utrecht` . . . 517
7.4 amd64, 2800MHz, Intel Xeon (f41), `nmi0056` . . . 520
7.5 amd64, 2800MHz, Intel Xeon (f41), `nmi0057` . . . 523
7.6 amd64, 2800MHz, Intel Xeon (f41), `nmi0063` . . . 526
7.7 amd64, 3000MHz, Intel Pentium D (f64), `speed` . . . 529
7.8 amd64, 3000MHz, Intel Xeon (f4a), `nmi0090` . . . 532
7.9 amd64, 3392MHz, Intel Pentium D (f64), `nmi0104` . . . 535
7.10 amd64, 3392MHz, Intel Pentium D (f64), `nmi0161` . . . 538
7.11 amd64, 3392MHz, Intel Pentium D (f64), `nmi0241` . . . 541
7.12 ia64, 900MHz, HP Itanium II, `nmi0025` . . . 544
7.13 ia64, 997MHz, HP Itanium II, `nmi0020` . . . 546
7.14 ia64, 997MHz, HP Itanium II, `nmi0058` . . . 548
7.15 ia64, 1396MHz, HP Itanium II, `nmi0065` . . . 550
7.16 ppc32, 400MHz, Motorola PowerPC G4 7400, `nmi0042` . . . 552
7.17 ppc32, 2000MHz, IBM PowerPC G5 970, `geespaz` . . . 555
7.18 ppc32, 2097MHz, IBM POWER5, `nmi0154` . . . 558
7.19 ppc32, 3192MHz, IBM Cell PPE, `nmips3` . . . 561
7.20 ppc64, 2000MHz, IBM PowerPC G5 970, `geespaz` . . . 564
7.21 ppc64, 2097MHz, IBM POWER5, `nmi0154` . . . 566
7.22 ppc64, 3192MHz, IBM Cell PPE, `nmips3` . . . 569
7.23 sparcv9, 300MHz, Sun UltraSPARC IIi, `nmi0096` . . . 572
7.24 sparcv9, 900MHz, Sun UltraSPARC III, `nmi0051` . . . 575
7.25 sparcv9, 1200MHz, Sun UltraSPARC III, `nmisolaris10` . . . 578
7.26 x86, 1196MHz, Intel Celeron (6b1), `vieux` . . . 581
7.27 x86, 1403MHz, AMD Opteron 240 (f58), `nmisles8amd64` . . . 584
7.28 x86, 1833MHz, Intel Core Duo, `nmi0068` . . . 587
7.29 x86, 2400MHz, Intel Pentium 4 (f24), `nmitest4` . . . 590
7.30 x86, 2400MHz, Intel Core 2 Duo (6fb), `utrecht` . . . 593
7.31 x86, 2401MHz, Intel Pentium 4 (f24), `nmi0086` . . . 596
7.32 x86, 2658MHz, Intel Xeon (f25), `nmi0013` . . . 599
7.33 x86, 2658MHz, Intel Xeon (f25), `nmibuild15` . . . 602
7.34 x86, 2658MHz, Intel Xeon (f25), `nmibuild16` . . . 605
7.35 x86, 2658MHz, Intel Xeon (f25), `nmibuild22` . . . 608
7.36 x86, 2659MHz, Intel Xeon (f25), `nmibuild21` . . . 611
7.37 x86, 2659MHz, Intel Xeon (f25), `nmibuild26` . . . 614
7.38 x86, 2667MHz, Intel Xeon (f25), `nmi0036` . . . 617
7.39 x86, 2791MHz, Intel Xeon (f27), `nmi0024` . . . 620
7.40 x86, 2800MHz, Intel Xeon (f41), `nmi0057` . . . 623
7.41 x86, 2800MHz, Intel Xeon (f41), `nmi0063` . . . 626
7.42 x86, 2801MHz, Intel Xeon (f41), `nmi0060` . . . 629
7.43 x86, 2801MHz, Intel Xeon (f41), `nmi0061` . . . 632
7.44 x86, 2801MHz, Intel Xeon (f41), `nmi0062` . . . 635
7.45 x86, 2802MHz, Intel Xeon (f29), `nmibuild40` . . . 638
7.46 x86, 2995MHz, Intel Xeon (f41), `nmi0079` . . . 641

7.47 x86, 2996MHz, Intel Xeon (f41), nmi0076 . . . 644
7.48 x86, 3000MHz, Intel Xeon (f4a), nmi0090 . . . 647
7.49 x86, 3000MHz, Intel Xeon (f4a), nmi0102 . . . 650
7.50 x86, 3391MHz, Intel Pentium D (f64), nmi0099 . . . 653
7.51 x86, 3392MHz, Intel Pentium D (f64), nmi0104 . . . 656
7.52 x86, 3392MHz, Intel Pentium D (f64), nmi0241 . . . 659

8 Measurements of public-key secret-sharing systems 663
8.1 Introduction . . . 663
8.2 amd64, 1403MHz, AMD Opteron 240 (f58), nmisles8amd64 . . . 664
8.3 amd64, 2400MHz, Intel Core 2 Duo (6fb), utrecht . . . 666
8.4 amd64, 2800MHz, Intel Xeon (f41), nmi0056 . . . 668
8.5 amd64, 2800MHz, Intel Xeon (f41), nmi0057 . . . 670
8.6 amd64, 2800MHz, Intel Xeon (f41), nmi0063 . . . 672
8.7 amd64, 3000MHz, Intel Pentium D (f64), speed . . . 674
8.8 amd64, 3000MHz, Intel Xeon (f4a), nmi0090 . . . 676
8.9 amd64, 3392MHz, Intel Pentium D (f64), nmi0104 . . . 678
8.10 amd64, 3392MHz, Intel Pentium D (f64), nmi0161 . . . 680
8.11 amd64, 3392MHz, Intel Pentium D (f64), nmi0241 . . . 682
8.12 ia64, 900MHz, HP Itanium II, nmi0025 . . . 684
8.13 ia64, 997MHz, HP Itanium II, nmi0020 . . . 686
8.14 ia64, 997MHz, HP Itanium II, nmi0058 . . . 688
8.15 ia64, 1396MHz, HP Itanium II, nmi0065 . . . 690
8.16 ppc32, 400MHz, Motorola PowerPC G4 7400, nmi0042 . . . 692
8.17 ppc32, 2000MHz, IBM PowerPC G5 970, geespaz . . . 694
8.18 ppc32, 2097MHz, IBM POWER5, nmi0154 . . . 696
8.19 ppc32, 3192MHz, IBM Cell PPE, nmips3 . . . 698
8.20 ppc64, 2000MHz, IBM PowerPC G5 970, geespaz . . . 700
8.21 ppc64, 2097MHz, IBM POWER5, nmi0154 . . . 702
8.22 ppc64, 3192MHz, IBM Cell PPE, nmips3 . . . 704
8.23 sparcv9, 300MHz, Sun UltraSPARC IIi, nmi0096 . . . 706
8.24 sparcv9, 900MHz, Sun UltraSPARC III, nmi0051 . . . 708
8.25 sparcv9, 1200MHz, Sun UltraSPARC III, nmisolaris10 . . . 710
8.26 x86, 1196MHz, Intel Celeron (6b1), vieux . . . 712
8.27 x86, 1403MHz, AMD Opteron 240 (f58), nmisles8amd64 . . . 714
8.28 x86, 1833MHz, Intel Core Duo, nmi0068 . . . 716
8.29 x86, 2400MHz, Intel Pentium 4 (f24), nmitest4 . . . 718
8.30 x86, 2400MHz, Intel Core 2 Duo (6fb), utrecht . . . 720
8.31 x86, 2401MHz, Intel Pentium 4 (f24), nmi0086 . . . 722
8.32 x86, 2658MHz, Intel Xeon (f25), nmi0013 . . . 724
8.33 x86, 2658MHz, Intel Xeon (f25), nmibuild15 . . . 726
8.34 x86, 2658MHz, Intel Xeon (f25), nmibuild16 . . . 728
8.35 x86, 2658MHz, Intel Xeon (f25), nmibuild22 . . . 730
8.36 x86, 2659MHz, Intel Xeon (f25), nmibuild21 . . . 732
8.37 x86, 2659MHz, Intel Xeon (f25), nmibuild26 . . . 734
8.38 x86, 2667MHz, Intel Xeon (f25), nmi0036 . . . 736
8.39 x86, 2791MHz, Intel Xeon (f27), nmi0024 . . . 738

8.40 x86, 2800MHz, Intel Xeon (f41), nmi0057 . . . 740
8.41 x86, 2800MHz, Intel Xeon (f41), nmi0063 . . . 742
8.42 x86, 2801MHz, Intel Xeon (f41), nmi0060 . . . 744
8.43 x86, 2801MHz, Intel Xeon (f41), nmi0061 . . . 746
8.44 x86, 2801MHz, Intel Xeon (f41), nmi0062 . . . 748
8.45 x86, 2802MHz, Intel Xeon (f29), nmibuild40 . . . 750
8.46 x86, 2995MHz, Intel Xeon (f41), nmi0079 . . . 752
8.47 x86, 2996MHz, Intel Xeon (f41), nmi0076 . . . 754
8.48 x86, 3000MHz, Intel Xeon (f4a), nmi0090 . . . 756
8.49 x86, 3000MHz, Intel Xeon (f4a), nmi0102 . . . 758
8.50 x86, 3391MHz, Intel Pentium D (f64), nmi0099 . . . 760
8.51 x86, 3392MHz, Intel Pentium D (f64), nmi0104 . . . 762
8.52 x86, 3392MHz, Intel Pentium D (f64), nmi0241 . . . 764

9 Measurements of public-key cryptosystems 767
9.1 Introduction . . . 767
9.2 amd64, 1403MHz, AMD Opteron 240 (f58), nmisles8amd64 . . . 768
9.3 amd64, 2400MHz, Intel Core 2 Duo (6fb), utrecht . . . 770
9.4 amd64, 2800MHz, Intel Xeon (f41), nmi0056 . . . 772
9.5 amd64, 2800MHz, Intel Xeon (f41), nmi0057 . . . 774
9.6 amd64, 2800MHz, Intel Xeon (f41), nmi0063 . . . 776
9.7 amd64, 3000MHz, Intel Pentium D (f64), speed . . . 778
9.8 amd64, 3000MHz, Intel Xeon (f4a), nmi0090 . . . 780
9.9 amd64, 3392MHz, Intel Pentium D (f64), nmi0104 . . . 782
9.10 amd64, 3392MHz, Intel Pentium D (f64), nmi0161 . . . 784
9.11 amd64, 3392MHz, Intel Pentium D (f64), nmi0241 . . . 786
9.12 ia64, 900MHz, HP Itanium II, nmi0025 . . . 788
9.13 ia64, 997MHz, HP Itanium II, nmi0020 . . . 790
9.14 ia64, 997MHz, HP Itanium II, nmi0058 . . . 792
9.15 ia64, 1396MHz, HP Itanium II, nmi0065 . . . 794
9.16 ppc32, 400MHz, Motorola PowerPC G4 7400, nmi0042 . . . 796
9.17 ppc32, 3192MHz, IBM Cell PPE, nmips3 . . . 798
9.18 x86, 1196MHz, Intel Celeron (6b1), vieux . . . 800
9.19 x86, 1403MHz, AMD Opteron 240 (f58), nmisles8amd64 . . . 802
9.20 x86, 1833MHz, Intel Core Duo, nmi0068 . . . 804
9.21 x86, 2400MHz, Intel Pentium 4 (f24), nmitest4 . . . 806
9.22 x86, 2400MHz, Intel Core 2 Duo (6fb), utrecht . . . 808
9.23 x86, 2401MHz, Intel Pentium 4 (f24), nmi0086 . . . 810
9.24 x86, 2658MHz, Intel Xeon (f25), nmi0013 . . . 812
9.25 x86, 2658MHz, Intel Xeon (f25), nmibuild15 . . . 814
9.26 x86, 2658MHz, Intel Xeon (f25), nmibuild16 . . . 816
9.27 x86, 2658MHz, Intel Xeon (f25), nmibuild22 . . . 818
9.28 x86, 2659MHz, Intel Xeon (f25), nmibuild21 . . . 820
9.29 x86, 2659MHz, Intel Xeon (f25), nmibuild26 . . . 822
9.30 x86, 2667MHz, Intel Xeon (f25), nmi0036 . . . 824
9.31 x86, 2791MHz, Intel Xeon (f27), nmi0024 . . . 826
9.32 x86, 2800MHz, Intel Xeon (f41), nmi0057 . . . 828

9.33 x86, 2800MHz, Intel Xeon (f41), nmi0063 . . . 830
9.34 x86, 2801MHz, Intel Xeon (f41), nmi0060 . . . 832
9.35 x86, 2801MHz, Intel Xeon (f41), nmi0061 . . . 834
9.36 x86, 2801MHz, Intel Xeon (f41), nmi0062 . . . 836
9.37 x86, 2802MHz, Intel Xeon (f29), nmibuild40 . . . 838
9.38 x86, 2995MHz, Intel Xeon (f41), nmi0079 . . . 840
9.39 x86, 2996MHz, Intel Xeon (f41), nmi0076 . . . 842
9.40 x86, 3000MHz, Intel Xeon (f4a), nmi0090 . . . 844
9.41 x86, 3000MHz, Intel Xeon (f4a), nmi0102 . . . 846
9.42 x86, 3391MHz, Intel Pentium D (f64), nmi0099 . . . 848
9.43 x86, 3392MHz, Intel Pentium D (f64), nmi0104 . . . 850
9.44 x86, 3392MHz, Intel Pentium D (f64), nmi0241 . . . 852

10 Measurements of public-key signature systems 855
10.1 Introduction . . . 855
10.2 amd64, 1403MHz, AMD Opteron 240 (f58), nmisles8amd64 . . . 857
10.3 amd64, 2400MHz, Intel Core 2 Duo (6fb), utrecht . . . 860
10.4 amd64, 2800MHz, Intel Xeon (f41), nmi0056 . . . 865
10.5 amd64, 2800MHz, Intel Xeon (f41), nmi0057 . . . 868
10.6 amd64, 2800MHz, Intel Xeon (f41), nmi0063 . . . 871
10.7 amd64, 3000MHz, Intel Pentium D (f64), speed . . . 874
10.8 amd64, 3000MHz, Intel Xeon (f4a), nmi0090 . . . 879
10.9 amd64, 3392MHz, Intel Pentium D (f64), nmi0104 . . . 882
10.10amd64, 3392MHz, Intel Pentium D (f64), nmi0161 . . . 885
10.11amd64, 3392MHz, Intel Pentium D (f64), nmi0241 . . . 890
10.12ia64, 900MHz, HP Itanium II, nmi0025 . . . 893
10.13ia64, 997MHz, HP Itanium II, nmi0020 . . . 895
10.14ia64, 997MHz, HP Itanium II, nmi0058 . . . 898
10.15ia64, 1396MHz, HP Itanium II, nmi0065 . . . 901
10.16ppc32, 400MHz, Motorola PowerPC G4 7400, nmi0042 . . . 904
10.17ppc32, 2000MHz, IBM PowerPC G5 970, geespaz . . . 907
10.18ppc32, 2097MHz, IBM POWER5, nmi0154 . . . 910
10.19ppc32, 3192MHz, IBM Cell PPE, nmips3 . . . 912
10.20ppc64, 2000MHz, IBM PowerPC G5 970, geespaz . . . 914
10.21ppc64, 2097MHz, IBM POWER5, nmi0154 . . . 916
10.22sparcv9, 300MHz, Sun UltraSPARC IIi, nmi0096 . . . 918
10.23x86, 1196MHz, Intel Celeron (6b1), vieux . . . 920
10.24x86, 1403MHz, AMD Opteron 240 (f58), nmisles8amd64 . . . 925
10.25x86, 1833MHz, Intel Core Duo, nmi0068 . . . 928
10.26x86, 2400MHz, Intel Pentium 4 (f24), nmitest4 . . . 930
10.27x86, 2400MHz, Intel Core 2 Duo (6fb), utrecht . . . 933
10.28x86, 2401MHz, Intel Pentium 4 (f24), nmi0086 . . . 935
10.29x86, 2658MHz, Intel Xeon (f25), nmi0013 . . . 938
10.30x86, 2658MHz, Intel Xeon (f25), nmibuild15 . . . 941
10.31x86, 2658MHz, Intel Xeon (f25), nmibuild16 . . . 944
10.32x86, 2658MHz, Intel Xeon (f25), nmibuild22 . . . 946
10.33x86, 2659MHz, Intel Xeon (f25), nmibuild21 . . . 949

10.34x86, 2659MHz, Intel Xeon (f25), nmibuild26 952
10.35x86, 2667MHz, Intel Xeon (f25), nmi0036 955
10.36x86, 2791MHz, Intel Xeon (f27), nmi0024 958
10.37x86, 2800MHz, Intel Xeon (f41), nmi0057 961
10.38x86, 2800MHz, Intel Xeon (f41), nmi0063 963
10.39x86, 2801MHz, Intel Xeon (f41), nmi0060 965
10.40x86, 2801MHz, Intel Xeon (f41), nmi0061 968
10.41x86, 2801MHz, Intel Xeon (f41), nmi0062 971
10.42x86, 2802MHz, Intel Xeon (f29), nmibuild40 974
10.43x86, 2995MHz, Intel Xeon (f41), nmi0079 976
10.44x86, 2996MHz, Intel Xeon (f41), nmi0076 979
10.45x86, 3000MHz, Intel Xeon (f4a), nmi0090 981
10.46x86, 3000MHz, Intel Xeon (f4a), nmi0102 983
10.47x86, 3391MHz, Intel Pentium D (f64), nmi0099 986
10.48x86, 3392MHz, Intel Pentium D (f64), nmi0104 989
10.49x86, 3392MHz, Intel Pentium D (f64), nmi0241 992

Executive summary

Users of public-key cryptography have a choice of public-key cryptosystems, including RSA, DSA, ECDSA, and many more. Exactly how fast are these systems? How do the speeds vary among Core 2, PowerPC, etc.? How much network bandwidth do the systems consume? The eBATS (ECRYPT Benchmarking of Asymmetric Systems) project aims to answer these questions.

Update: VAMPIRE has expanded the scope of its benchmarking to include (1) eBATS for public-key systems; (2) improved benchmarking of the secret-key stream ciphers submitted to eSTREAM; and (3) a new eBASH (ECRYPT Benchmarking of All Submitted Hashes) project to support the NIST hash-function competition. All of these projects have been combined into a unified cryptographic benchmarking toolkit, SUPERCOP.

This report summarizes the benchmarks collected so far. In particular, it lists the primitives that have been measured; lists the computers used for measurements; lists the compilers tested; lists the compilers that produced the best performance for each primitive; and presents graphical and tabular measurements of hash functions, secret-key stream ciphers, public-key cryptosystems, public-key signature systems, and public-key secret-sharing systems.

Chapter 1

Introduction

SUPERCOP is a toolkit developed by the VAMPIRE lab for measuring the performance of cryptographic software. SUPERCOP stands for System for Unified Performance Evaluation Related to Cryptographic Operations and Primitives; the name was suggested by Paul Bakker.

The latest release of SUPERCOP measures the performance of hash functions, secret-key stream ciphers, public-key encryption systems, public-key signature systems, and public-key secret-sharing systems. SUPERCOP integrates and improves upon

- STVL's benchmarking suite for stream ciphers submitted to eSTREAM, the ECRYPT Stream Cipher Project (which finished in April 2008);
- VAMPIRE's BATMAN (Benchmarking of Asymmetric Tools on Multiple Architectures, Non-interactively) suite for public-key systems submitted to the eBATS (ECRYPT Benchmarking of Asymmetric Systems) project; and
- additional tools developed for VAMPIRE's new eBASH (ECRYPT Benchmarking of All Submitted Hashes) project.

Specifically, SUPERCOP measures cryptographic primitives according to several criteria:

- Time to hash a very short packet of data.
- Time to hash a typical-size Internet packet.
- Time to hash a long message.
- Length of the hash output.
- Time to encrypt a very short packet of data using a secret key and a nonce.
- Time to encrypt a typical-size Internet packet.
- Time to encrypt a long message.
- Length of the secret key.
- Length of the nonce.
- Time to generate a key pair (a private key and a corresponding public key).

- Length of the private key.
- Length of the public key.
- Time to encrypt a message using a public key.
- Length of the encrypted message.
- Time to decrypt a message using a private key.
- Time to sign a message using a private key.
- Length of the signed message.
- Time to verify a signed message using a public key.

"Time" refers to time on real computers: time on an Intel Core 2 Quad, time on an AMD Athlon 64 X2, time on an IBM PowerPC G5 970, etc. The point of these cost measures is that they are directly visible to the cryptographic user.

The previous D.VAM.1 report "Performance Benchmarks" analyzed in detail the number of arithmetic operations carried out by various cryptosystems. SUPERCOP goes further, taking into account the speed at which real computers can carry out those arithmetic operations. For example, the Core 2, PowerPC, etc. do not include fast circuits for multiplication of polynomials modulo 2, but they do include fast circuits for integer multiplication, speeding up cryptosystems that rely on integer multiplication; this effect is clear in the SUPERCOP results. Intel has announced that the "Westmere" CPUs, to be shipped in 2009, *will* include fast circuits for multiplication of polynomials modulo 2; cryptographic software taking advantage of these circuits will have an advantage in future SUPERCOP results.

The previous D.VAM.7 deliverable "Performance Benchmarks—Public Key Cryptography I" (February 2006) announced initial plans for eBATS, and described a preliminary version of the eBATS API. The previous D.VAM.9 deliverable "Report on eBATS Performance Benchmarks" was a comprehensive report on measurements collected in the first stage of eBATS. This document is the D.VAM.14 deliverable "Performing Benchmarks," including not only the latest public-key benchmarks but also benchmarks for hash functions and stream ciphers.

Chapter 2

Which primitives are measured?

2.1 Introduction

This report includes measurements of 210 implementations of 76 cryptographic primitives: specifically,

- 10 different hash functions,
- 21 different secret-key stream ciphers,
- 7 different public-key encryption systems,
- 30 different public-key signature systems, and
- 8 different public-key secret-sharing systems.

The implementations total 122462 lines of C/C++ code and 668054 lines of assembly-language code for various architectures, not counting the lines of code in underlying libraries such as GMP, NTL, and OpenSSL.

Some of these implementations were developed internally as part of the eBATS and eBASH projects, but SUPERCOP also includes submissions from other parts of VAMPIRE, submissions from other parts of ECRYPT, and submissions from outside ECRYPT. The following list of primitives includes acknowledgments to authors of the implementations included in SUPERCOP.

2.2 List of hash primitives measured

SUPERCOP includes implementations of the following hash functions:

- `md2`: The MD2 hash function designed by Ron Rivest. The `md2/openssl` implementation is a wrapper around the OpenSSL library.
- `md4`: The MD4 hash function designed by Ron Rivest. The `md4/openssl` implementation is a wrapper around the OpenSSL library.
- `md5`: The MD5 hash function designed by Ron Rivest. The `md5/openssl` implementation is a wrapper around the OpenSSL library. The `md5/ref` implementation is a new implementation from Rivest's specification.

- `ripemd160`: The RIPEMD-160 hash function designed by Hans Dobbertin, Antoon Bosselaers, and Bart Preneel. The `ripemd160/openssl` implementation is a wrapper around the OpenSSL library.
- `sha1`: The SHA-1 hash function designed by NSA and standardized by NIST. The `sha1/openssl` implementation is a wrapper around the OpenSSL library.
- `sha224`: The SHA-224 hash function designed by NSA and standardized by NIST. The `sha224/openssl` implementation is a wrapper around the OpenSSL library.
- `sha256`: The SHA-256 hash function designed by NSA and standardized by NIST. The `sha256/openssl` implementation is a wrapper around the OpenSSL library. The `sha256/ref` implementation is a new implementation from NIST's specification.
- `sha384`: The SHA-384 hash function designed by NSA and standardized by NIST. The `sha384/openssl` implementation is a wrapper around the OpenSSL library.
- `sha512`: The SHA-512 hash function designed by NSA and standardized by NIST. The `sha512/openssl` implementation is a wrapper around the OpenSSL library. The `sha512/ref` implementation is a new implementation from NIST's specification.
- `whirlpool`: The Whirlpool hash function designed by Vincent Rijmen and Paulo S. L. M. Barreto. The `whirpool/ref` implementation is a wrapper around the reference implementation from the designers.

2.3 List of stream-cipher primitives measured

SUPERCOP includes implementations of the following stream ciphers:

- `aes128estream`: The Advanced Encryption Standard (128-bit key) in a particular counter mode specified by eSTREAM. The `aes128estream/e/gladman` implementation is a wrapper by STVL around Brian Gladman's AES software. Twelve additional implementations, optimized for various CPUs, were contributed to eSTREAM by Daniel J. Bernstein, Hongjun Wu, and Peter Schwabe.
- `aes256estream`: The Advanced Encryption Standard (256-bit key) in a particular counter mode specified by eSTREAM. The `aes256estream/e/gladman` implementation is a wrapper by STVL around Brian Gladman's AES software. Two additional implementations were contributed to eSTREAM by Hongjun Wu.
- `chacha8`: The ChaCha8 stream cipher (256-bit key) designed by Daniel J. Bernstein. Thirteen implementations were contributed to eSTREAM by the designer.
- `chacha12`: The ChaCha12 stream cipher (256-bit key) designed by Daniel J. Bernstein. Thirteen implementations were contributed to eSTREAM by the designer.
- `chacha20`: The ChaCha20 stream cipher (256-bit key) designed by Daniel J. Bernstein. Thirteen implementations were contributed to eSTREAM by the designer.

- `cryptmtv3`: The CryptMT v3 stream cipher (256-bit key) designed by Makoto Matsumoto, Matsuo Saito, Takuji Nishimura, and Mariko Hagita. The `cryptmtv3/e/v3` implementation was contributed to eSTREAM by the designers.
- `dragon`: The Dragon stream cipher (256-bit key) designed by Kevin Chen, Matt Henricksen, William Millan, Joanne Fuller, Leonie Simpson, Ed Dawson, HoonJae Lee, and SangJae Moon. The `dragon/e/submissions/dragon` implementation was contributed to eSTREAM by the designers.
- `hc128`: The HC-128 stream cipher (128-bit key) designed by Hongjun Wu. Three implementations were contributed to eSTREAM by the designer. HC-128 is one of the software ciphers in the final eSTREAM portfolio.
- `hc256`: The HC-256 stream cipher (256-bit key) designed by Hongjun Wu. Two implementations were contributed to eSTREAM by the designer.
- `lexv2`: The LEX v2 stream cipher (128-bit key) designed by Alex Biryukov. The `lexv2/e/v2/ref` implementation was contributed to eSTREAM by the designer. Six additional implementations were contributed to eSTREAM by Peter Schwabe.
- `nlsv2`: The NLS v2 stream cipher (128-bit key) designed by Gregory Rose, Philip Hawkes, Michael Paddon, and Miriam Wiggers de Vries. Two implementations were contributed to eSTREAM by the designers.
- `rabbit`: The Rabbit stream cipher (128-bit key) designed by Martin Boesgaard, Mette Vesterager, Thomas Pedersen, Jesper Christensen, and Ove Scavenius. Ten implementations were contributed to eSTREAM by the designers. Rabbit is one of the software ciphers in the final eSTREAM portfolio.
- `salsa208`: The Salsa20/8 stream cipher (256-bit key) designed by Daniel J. Bernstein. Twenty-two implementations were contributed to eSTREAM by the designer.
- `salsa2012`: The Salsa20/12 stream cipher (256-bit key) designed by Daniel J. Bernstein. Twenty-two implementations were contributed to eSTREAM by the designer. Salsa20/12 is one of the software ciphers in the final eSTREAM portfolio.
- `salsa20`: The Salsa20/20 stream cipher (256-bit key) designed by Daniel J. Bernstein. Twenty-two implementations were contributed to eSTREAM by the designer.
- `snow20`: The SNOW 2.0 stream cipher (256-bit key) designed by Patrik Ekdahl and Thomas Johansson. The `snow20/e/benchmarks/snow-2.0` implementation is a wrapper around the reference implementation from the designers.
- `sosemanuk`: The Sosemanuk stream cipher (256-bit key) designed by Come Berbain, Olivier Billet, Anne Canteaut, Nicolas Courtois, Henri Gilbert, Louis Goubin, Aline Gouget, Louis Granboulan, Cédric Lauradoux, Marine Minier, Thomas Pornin, and Hervé Sibert. The `sosemanuk/e/submissions/sosemanuk` implementation was contributed to eSTREAM by the designers. Sosemanuk is one of the software ciphers in the final eSTREAM portfolio.

- `tpy6`: The TPy6 stream cipher (256-bit key) designed by Eli Biham and Jennifer Seberry. The `tpy6/e/tpy6` implementation was contributed to eSTREAM by the designers.
- `tpy`: The TPy stream cipher (256-bit key) designed by Eli Biham and Jennifer Seberry. The `tpy6/e/tpy6` implementation was contributed to eSTREAM by the designers.
- `tpypy`: The TPypy stream cipher (256-bit key) designed by Eli Biham and Jennifer Seberry. The `tpy6/e/tpy6` implementation was contributed to eSTREAM by the designers.
- `trivium`: The Trivium stream cipher (80-bit key) designed by Christophe De Cannière and Bart Preneel. The `trivium/e/submissions/trivium` implementation was contributed to eSTREAM by the designers. Trivium is one of the hardware ciphers in the final eSTREAM portfolio, and the only one that also has a fast software implementation.

2.4 List of public-key-encryption primitives measured

SUPERCOP includes implementations of the following public-key cryptosystems:

- `mceliece`: A variant of McEliece's code-based cryptosystem. Software written by Bhaskar Biswas and Nicolas Sendrier (INRIA Rocquencourt) as a BAT (Benchmarkable Asymmetric Tool) for eBATS.
- `ntruees787ep1`: NTRU encryption with $N = 787$ and $q = 587$. Software written by Mark Etzel (NTRU Cryptosystems) as a BAT for eBATS.
- `ronald1024`: 1024-bit RSA encryption with malleability defense. Software written internally as a BAT for eBATS. (The inventors of RSA are Ron Rivest, Adi Shamir, and Len Adleman.)
- `ronald1536`: 1536-bit RSA encryption with malleability defense. Software written internally as a BAT for eBATS.
- `ronald2048`: 2048-bit RSA encryption with malleability defense. Software written internally as a BAT for eBATS.
- `ronald3072`: 3072-bit RSA encryption with malleability defense. Software written internally as a BAT for eBATS.
- `ronald4096`: 4096-bit RSA encryption with malleability defense. Software written internally as a BAT for eBATS.

2.5 List of public-key-signature primitives measured

SUPERCOP includes implementations of the following public-key signature systems:

- `bls` (Boneh–Lynn–Shacham), only for x86-architecture computers: Pairing-based short signatures. Software written by Michael Scott (Dublin City University) as a BAT for eBATS.

- `donald512`: DSA signatures using a 512-bit prime. Software written internally on top of OpenSSL as a BAT for eBATS.
- `donald1024`: DSA signatures using a 1024-bit prime. Software written internally on top of OpenSSL as a BAT for eBATS.
- `donald2048`: DSA signatures using a 2048-bit prime. Software written internally on top of OpenSSL as a BAT for eBATS.
- `ecdonaldb163`: ECDSA signatures using the standard NIST B-163 elliptic curve, a curve over a field of size 2^{163}. Software written internally on top of OpenSSL as a BAT for eBATS.
- `ecdonaldb233`: ECDSA signatures using the standard NIST B-233 elliptic curve, a curve over a field of size 2^{233}. Software written internally on top of OpenSSL as a BAT for eBATS.
- `ecdonaldb283`: ECDSA signatures using the standard NIST B-283 elliptic curve, a curve over a field of size 2^{283}. Software written internally on top of OpenSSL as a BAT for eBATS.
- `ecdonaldb409`: ECDSA signatures using the standard NIST B-409 elliptic curve, a curve over a field of size 2^{409}. Software written internally on top of OpenSSL as a BAT for eBATS.
- `ecdonaldb571`: ECDSA signatures using the standard NIST B-571 elliptic curve, a curve over a field of size 2^{571}. Software written internally on top of OpenSSL as a BAT for eBATS.
- `ecdonaldk163`: ECDSA signatures using the standard NIST K-163 elliptic curve, a Koblitz curve over a field of size 2^{163}. Software written internally on top of OpenSSL as a BAT for eBATS.
- `ecdonaldk233`: ECDSA signatures using the standard NIST K-233 elliptic curve, a Koblitz curve over a field of size 2^{233}. Software written internally on top of OpenSSL as a BAT for eBATS.
- `ecdonaldk283`: ECDSA signatures using the standard NIST K-283 elliptic curve, a Koblitz curve over a field of size 2^{283}. Software written internally on top of OpenSSL as a BAT for eBATS.
- `ecdonaldk409`: ECDSA signatures using the standard NIST K-409 elliptic curve, a Koblitz curve over a field of size 2^{409}. Software written internally on top of OpenSSL as a BAT for eBATS.
- `ecdonaldk571`: ECDSA signatures using the standard NIST K-571 elliptic curve, a Koblitz curve over a field of size 2^{571}. Software written internally on top of OpenSSL as a BAT for eBATS.
- `ecdonaldp160`: ECDSA signatures using the standard SECP160R1 elliptic curve, a curve modulo the prime $2^{160} - 2^{31} - 1$. Software written internally on top of OpenSSL as a BAT for eBATS.

- `ecdonaldp192`: ECDSA signatures using the standard NIST P-192 elliptic curve, a curve modulo the prime $2^{192} - 2^{64} - 1$. Software written internally on top of OpenSSL as a BAT for eBATS.
- `ecdonaldp224`: ECDSA signatures using the standard NIST P-224 elliptic curve, a curve modulo the prime $2^{224} - 2^{96} + 1$. Software written internally on top of OpenSSL as a BAT for eBATS.
- `ecdonaldp256`: ECDSA signatures using the standard NIST P-256 elliptic curve, a curve modulo the prime $2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$. Software written internally on top of OpenSSL as a BAT for eBATS.
- `ecdonaldp384`: ECDSA signatures using the standard NIST P-384 elliptic curve, a curve modulo the prime $2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$. Software written internally on top of OpenSSL as a BAT for eBATS.
- `ecdonaldp521`: ECDSA signatures using the standard NIST P-521 elliptic curve, a curve modulo the prime $2^{521} - 1$. Software written internally on top of OpenSSL as a BAT for eBATS.
- `hector` (Hyperelliptic Curve with Two-Rank One): Signatures using a genus-2 hyperelliptic curve of 2-rank 1 over a field of size 2^{113}. Software written by Peter Birkner and Peter Schwabe (Technische Universiteit Eindhoven) as a BAT for eBATS. Finite-field arithmetic software was written by Pierrick Gaudry and Emmanuel Thomé (Laboratoire Lorrain de Recherche en Informatique et ses Applications).
- `rainbow 1`: Rainbow multivariate-quadratic signatures. Software written by Jintai Ding and Dieter Schmidt (University of Cincinnati) as a BAT for eBATS.
- `ronald512`: 512-bit RSA signatures with message recovery. Software written internally as a BAT for eBATS.
- `ronald768`: 768-bit RSA signatures with message recovery. Software written internally as a BAT for eBATS.
- `ronald1024`: 1024-bit RSA signatures with message recovery. Software written internally as a BAT for eBATS.
- `ronald1536`: 1536-bit RSA signatures with message recovery. Software written internally as a BAT for eBATS.
- `ronald2048`: 2048-bit RSA signatures with message recovery. Software written internally as a BAT for eBATS.
- `ronald3072`: 3072-bit RSA signatures with message recovery. Software written internally as a BAT for eBATS.
- `ronald4096`: 4096-bit RSA signatures with message recovery. Software written internally as a BAT for eBATS.
- `sflashv2`: SFLASHv2 multivariate-quadratic signatures. Software written by Louis Goubin (Université de Versailles), Nicolas Courtois (University College London), and Thomas Icart (École Polytechnique) as a BAT for eBATS.

2.6 List of public-key-secret-sharing primitives measured

SUPERCOP includes implementations of the following Diffie–Hellman systems:

- `claus`: Classic Diffie-Hellman secret sharing modulo a 1024-bit prime. The `claus/gmp` implementation was written internally on top of the GMP library. The `claus/ntl` implementation was written internally on top of the NTL library. The `claus/openssl` implementation was written internally on top of the OpenSSL library.
- `curve2251`: Elliptic-curve Diffie–Hellman secret sharing using a curve over a field with 2^{251} elements. Software written by Pierrick Gaudry and Emmanuel Thomé (Laboratoire Lorrain de Recherche en Informatique et ses Applications) as a BAT for eBATS.
- `curve25519`: Elliptic-curve Diffie–Hellman secret sharing using the curve $y^2 = x^3 + 486662x^2 + x$ modulo $2^{255} - 19$. Software written by Pierrick Gaudry and Emmanuel Thomé (Laboratoire Lorrain de Recherche en Informatique et ses Applications) as a BAT for eBATS.
- `gls1271` (Galbraith, Lin, Scott): Elliptic-curve Diffie–Hellman secret sharing using a twist of the curve $y^2 = x^3 - 3x + 44$ over a field with $(2^{127} - 1)^2$ elements. Software written by Michael Scott (Dublin City University) as a BAT for eBATS.
- `hector` (Hyperelliptic Curve with Two-Rank One): Diffie–Hellman secret sharing using a genus-2 hyperelliptic curve of 2-rank 1 over a field of size 2^{113}. Software written by Peter Birkner and Peter Schwabe (Technische Universiteit Eindhoven) as a BAT for eBATS. Finite-field arithmetic software was written by Pierrick Gaudry and Emmanuel Thomé (Laboratoire Lorrain de Recherche en Informatique et ses Applications).
- `nistp256`, sparcv9 architecture: Elliptic-curve Diffie-Hellman secret sharing using the standard NIST P-256 elliptic curve, a curve modulo the prime $2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$. Software written by Yassir Nawaz and Guang Gong (University of Waterloo) as a BAT for eBATS.
- `surf127eps`: Hyperelliptic-curve Diffie-Hellman secret sharing using a genus-2 curve with complex multiplication by $\mathbf{Q}(i\sqrt{5 + \sqrt{53}})$ modulo the prime $2^{127} - 735$. Software written by Pierrick Gaudry (Laboratoire Lorrain de Recherche en Informatique et ses Applications), Thomas Houtmann (École Polytechnique), and Emmanuel Thomé (École Polytechnique) as a BAT for eBATS.
- `surf2113`: Hyperelliptic-curve Diffie-Hellman secret sharing using a genus-2 curve over a field with 2^{113} elements. Software written by Pierrick Gaudry and Emmanuel Thomé (Laboratoire Lorrain de Recherche en Informatique et ses Applications) as a BAT for eBATS.

Chapter 3

Which computers are used for measurements?

3.1 Introduction

Timings depend heavily on the choice of computer. For example, a 2400MHz Core 2 will sign a message much more quickly than a 133MHz Pentium 1.

Reporting CPU cycles (microseconds/2400 on a 2400MHz Core 2, microseconds/1050 on a 1050MHz UltraSPARC III, microseconds/133 on a 133MHz Pentium, etc.) drastically reduces the level of computer dependence but does not eliminate it. For example, a Core 2 can generally do more in one cycle than a Pentium 1.

To ensure direct comparability of all cryptographic primitives on whichever computers are of interest to the users, VAMPIRE uses SUPERCOP to measure each implementation on a wide variety of computers. VAMPIRE currently has access to 81 benchmarking machines with 7 different architectures (amd64, hppa, ia64, ppc32, ppc64, sparcv9, x86) and a broad range of different microarchitectures.

3.2 Notes on multiple-core computers

One computer sometimes has more than one CPU. For example, the computer named `poema` has two CPUs, each CPU being an Intel Pentium III with one 1400MHz processing core.

One CPU sometimes has more than one processing core. For example, the computer named `latour` has one CPU, an Intel Core 2 Quad Q6600 containing four separate 2400MHz cores.

A computation such as public-key encryption can, at least in theory, be spread among two or more parallel cores, reducing the computation time at the expense of some communication between the cores. However, parallel cores are much more commonly used to handle independent computations, running each computation serially on one core and minimizing communication costs.

All of the measured cryptographic implementations are serial, and all of the cycle counts in this report are meant to reflect the number of cycles that a single-core computer would need to carry out the computation. For example, a computation reported to take 300000 cycles on `latour` was observed to take 300000/2400 = 125 microseconds on a single 2400MHz core

of `latour`; this means that a single core can carry out 8 new computations each millisecond, and all four cores together can carry out 32 new computations each millisecond.

3.3 List of computers used for measurements

The following list identifies the architecture, clock frequency, and CPU for each of the computers used by VAMPIRE for benchmarking. The list is sorted first by architecture, second by clock frequency.

- `nmisles8amd64`: amd64 architecture, 1403MHz, 2 cores, AMD Opteron 240 (f58), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `dancer`: amd64 architecture, 2000MHz, 2 cores, AMD Athlon 64 X2 (15,35,2), owned by the Center for Research and Instruction in Technologies for Electronic Security (RITES) at the University of Illinois at Chicago.
- `mace`: amd64 architecture, 2000MHz, 2 cores, AMD Athlon 64 X2 (15,75,2), owned by the Center for Research and Instruction in Technologies for Electronic Security (RITES) at the University of Illinois at Chicago.
- `katana`: amd64 architecture, 2137MHz, 2 cores, Intel Core 2 Duo (6f6), owned by the Center for Research and Instruction in Technologies for Electronic Security (RITES) at the University of Illinois at Chicago.
- `latour`: amd64 architecture, 2394MHz, 4 cores, Intel Core 2 Quad Q6600 (6fb), owned by the Coding and Cryptography Computer Cluster (C4) at Technische Universiteit Eindhoven.
- `utrecht`: amd64 architecture, 2400MHz, 4 cores, Intel Core 2 Quad Q6600 (6fb), owned by D. J. Bernstein and Tanja Lange.
- `nmi0056`: amd64 architecture, 2800MHz, 4 cores, Intel Xeon (f41), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0057`: amd64 architecture, 2800MHz, 4 cores, Intel Xeon (f41), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0063`: amd64 architecture, 2800MHz, 4 cores, Intel Xeon (f41), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `pclin153`: amd64 architecture, 3000MHz, 1 core, Intel Pentium 4 (f43), owned by Technische Universiteit Eindhoven.
- `speed`: amd64 architecture, 3000MHz, 2 cores, Intel Pentium D (f64), owned by Technische Universiteit Eindhoven.
- `svlin001`: amd64 architecture, 3000MHz, 2 cores, Intel Pentium D (f64), owned by Technische Universiteit Eindhoven.
- `nmi0090`: amd64 architecture, 3000MHz, 4 cores, Intel Xeon (f4a), owned by the NMI Build and Test Lab at the University of Wisconsin.

- `nmi0104`: amd64 architecture, 3392MHz, 2 cores, Intel Pentium D (f64), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0161`: amd64 architecture, 3392MHz, 2 cores, Intel Pentium D (f64), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0241`: amd64 architecture, 3392MHz, 2 cores, Intel Pentium D (f64), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `hp400`: hppa architecture, 440MHz, 2 cores, HP 9000/785 J5000, owned by Ruhr-Universität Bochum.
- `nmi0025`: ia64 architecture, 900MHz, 1 core, HP Itanium II, owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0020`: ia64 architecture, 997MHz, 2 cores, HP Itanium II, owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0058`: ia64 architecture, 997MHz, 2 cores, HP Itanium II, owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0065`: ia64 architecture, 1396MHz, 2 cores, HP Itanium II, owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0042`: ppc32 architecture, 400MHz, 1 core, Motorola PowerPC G4 7400, owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0055`: ppc32 architecture, 450MHz, 1 core, IBM POWER3, owned by the NMI Build and Test Lab at the University of Wisconsin.
- `gggg`: ppc32 architecture, 533MHz, 2 cores, Motorola PowerPC G4 7410, owned by the Center for Research and Instruction in Technologies for Electronic Security (RITES) at the University of Illinois at Chicago.
- `daedalus`: ppc32 architecture, 600MHz, 1 core, Motorola PowerPC 750CXe, owned by the Center for Research and Instruction in Technologies for Electronic Security (RITES) at the University of Illinois at Chicago.
- `nmibuild14`: ppc32 architecture, 1200MHz, 2 cores, IBM POWER4, owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmibuild33`: ppc32 architecture, 1200MHz, 2 cores, IBM POWER4, owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0070`: ppc32 architecture, 1333MHz, 1 core, Motorola PowerPC G4 7450, owned by the NMI Build and Test Lab at the University of Wisconsin.
- `tigger`: ppc64 architecture, 1452MHz, 6 cores, IBM POWER4, owned by the University of Illinois at Chicago.
- `geespaz`: ppc64 architecture, 2000MHz, 2 cores, IBM PowerPC G5 970, owned by Phil Carmody.

- `nmi0154`: ppc64 architecture, 2097MHz, 4 cores, IBM POWER5, owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0048`: ppc64 architecture, 2300MHz, 2 cores, IBM PowerPC G5 970, owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmips3`: ppc64 architecture, 3192MHz, 2 cores, IBM Cell PPE, owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0008`: sparcv9 architecture, 300MHz, 1 core, Sun UltraSPARC IIi, owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0096`: sparcv9 architecture, 300MHz, 1 core, Sun UltraSPARC IIi, owned by the NMI Build and Test Lab at the University of Wisconsin.
- `icarus`: sparcv9 architecture, 900MHz, 8 cores, Sun UltraSPARC III, owned by the University of Illinois at Chicago.
- `nmi0051`: sparcv9 architecture, 900MHz, 2 cores, Sun UltraSPARC III, owned by the NMI Build and Test Lab at the University of Wisconsin.
- `t1000`: sparcv9 architecture, 1000MHz, 8 cores, Sun UltraSPARC T1, owned by UNIX Center.
- `hald`: sparcv9 architecture, 1050MHz, 72 cores, Sun UltraSPARC IV, owned by Danmarks Tekniske Universitet.
- `nmisolaris10`: sparcv9 architecture, 1200MHz, 2 cores, Sun UltraSPARC III, owned by the NMI Build and Test Lab at the University of Wisconsin.
- `cruncher`: x86 architecture, 133MHz, 1 core, Intel Pentium (52c), owned by the Center for Research and Instruction in Technologies for Electronic Security (RITES) at the University of Illinois at Chicago.
- `boris`: x86 architecture, 333MHz, 1 core, Intel Pentium 2 (652), owned by the Center for Research and Instruction in Technologies for Electronic Security (RITES) at the University of Illinois at Chicago.
- `orpheus`: x86 architecture, 448MHz, 1 core, Intel Pentium 3 (672), owned by the Center for Research and Instruction in Technologies for Electronic Security (RITES) at the University of Illinois at Chicago.
- `atlas`: x86 architecture, 800MHz, 1 core, Intel Pentium M (6d8), owned by D. J. Bernstein.
- `silverton`: x86 architecture, 853MHz, 1 core, Intel Pentium 3 (686), owned by D. J. Bernstein.
- `thoth`: x86 architecture, 900MHz, 1 core, AMD Athlon (622), owned by the Center for Research and Instruction in Technologies for Electronic Security (RITES) at the University of Illinois at Chicago.

- `neumann`: x86 architecture, 1000MHz, 2 cores, Intel Pentium 3 (68a), owned by the University of Illinois at Chicago.
- `vieux`: x86 architecture, 1196MHz, 1 core, Intel Celeron (6b1), owned by Technische Universiteit Eindhoven.
- `whisper`: x86 architecture, 1300MHz, 1 core, Intel Pentium M (695), owned by D. J. Bernstein.
- `nmiv003`: x86 architecture, 1390MHz, 1 core, Intel Pentium 4 (f18), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0068`: x86 architecture, 1833MHz, 2 cores, Intel Core Duo, owned by the NMI Build and Test Lab at the University of Wisconsin.
- `fireball`: x86 architecture, 1900MHz, 1 core, Intel Pentium 4 (f12), owned by the Center for Research and Instruction in Technologies for Electronic Security (RITES) at the University of Illinois at Chicago.
- `nmitest4`: x86 architecture, 2400MHz, 1 core, Intel Pentium 4 (f24), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0083`: x86 architecture, 2400MHz, 1 core, Intel Pentium 4 (f24), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0086`: x86 architecture, 2401MHz, 1 core, Intel Pentium 4 (f24), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0013`: x86 architecture, 2658MHz, 4 cores, Intel Xeon (f25), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmibuild15`: x86 architecture, 2658MHz, 4 cores, Intel Xeon (f25), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmibuild16`: x86 architecture, 2658MHz, 4 cores, Intel Xeon (f25), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmibuild22`: x86 architecture, 2658MHz, 4 cores, Intel Xeon (f25), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmibuild17`: x86 architecture, 2658MHz, 4 cores, Intel Xeon (f29), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmibuild21`: x86 architecture, 2659MHz, 4 cores, Intel Xeon (f25), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmibuild26`: x86 architecture, 2659MHz, 4 cores, Intel Xeon (f25), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0036`: x86 architecture, 2667MHz, 2 cores, Intel Xeon (f25), owned by the NMI Build and Test Lab at the University of Wisconsin.

- `nmi0024`: x86 architecture, 2791MHz, 2 cores, Intel Xeon (f27), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0059`: x86 architecture, 2800MHz, 4 cores, Intel Xeon (f29), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `poema`: x86 architecture, 2800MHz, 2 cores, Intel Xeon (f29), owned by Technische Universiteit Eindhoven.
- `svlin003`: x86 architecture, 2800MHz, 2 cores, Intel Xeon (f29), owned by Technische Universiteit Eindhoven.
- `nmi0060`: x86 architecture, 2801MHz, 4 cores, Intel Xeon (f41), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0061`: x86 architecture, 2801MHz, 4 cores, Intel Xeon (f41), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0062`: x86 architecture, 2801MHz, 4 cores, Intel Xeon (f41), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmibuild40`: x86 architecture, 2802MHz, 1 core, Intel Xeon (f29), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0079`: x86 architecture, 2995MHz, 2 cores, Intel Xeon (f41), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0084`: x86 architecture, 2996MHz, 2 cores, Intel Pentium 4 (f41), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0076`: x86 architecture, 2996MHz, 1 core, Intel Xeon (f41), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `pclin118`: x86 architecture, 3000MHz, 1 core, Intel Pentium 4 (f41), owned by Technische Universiteit Eindhoven.
- `svlin002`: x86 architecture, 3000MHz, 1 core, Intel Pentium 4 (f41), owned by Technische Universiteit Eindhoven.
- `nmi0100`: x86 architecture, 3000MHz, 4 cores, Intel Xeon (f4a), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `nmi0102`: x86 architecture, 3000MHz, 4 cores, Intel Xeon (f4a), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `shell`: x86 architecture, 3200MHz, 2 cores, Intel Pentium D (f47), owned by the University of Illinois at Chicago.
- `nmi0099`: x86 architecture, 3391MHz, 2 cores, Intel Pentium D (f64), owned by the NMI Build and Test Lab at the University of Wisconsin.
- `shellold`: x86 architecture, 3400MHz, 1 core, Intel Pentium 4 (f29), owned by the University of Illinois at Chicago.

Chapter 4

Which compilers are used for measurements?

4.1 Introduction

New implementations of a primitive can dramatically improve the speed of the primitive—but often it is not clear in advance which implementation will be best. Whenever SUPERCOP includes several implementations of one primitive, it tries compiling each implementation, and automatically selects the implementation that produces the highest speed for the primitive. For example, SUPERCOP tries both `sha256/openssl` and `sha256/ref`, and selects the implementation that hashes 1536 bytes most efficiently. The best implementation can vary from one computer to another, so SUPERCOP tries each implementation of each primitive on each computer.

Even when there is just one implementation, the choice of compiler, including compiler options, can dramatically affect the speed of that implementation. SUPERCOP tries compiling each implementation of a primitive under each of the compilers listed below, and selects the compiler/implementation combination that produces the highest speeds for the primitive. All speed reports for the primitive use the selected combination.

The best compiler can vary from one computer to another. Even on one computer, the best compiler can vary from one cryptographic primitive to another: e.g., the best compiler for SHA-256 is probably not the best compiler for SHA-512. Even for one cryptographic primitive, the best compiler can vary from one implementation to another. Consequently, SUPERCOP tries each compiler again for each combination of computer, primitive, and implementation. For example, on the computer `td186`, SUPERCOP selected `gcc -O -fomit-frame-pointer` for the `ntruees787ep1` public-key system, and selected `gcc -march=nocona -O2 -fomit-frame-pointer` for the `sflashv2` public-key system.

4.2 Notes on multiple operations

A single primitive, such as SHA-256, supports several operations: for example, it can hash 64 bytes, and it can hash 1536 bytes, and it can hash 4096 bytes.

SUPERCOP chooses a compiler and implementation on the basis of one operation, and then uses that combination to measure other operations. For example, SUPERCOP chooses

the SHA-256 implementation that hashes 1536 bytes most efficiently, and that measures the speed of that implementation for hashing 64 bytes and for hashing 4096 bytes.

SUPERCOP does *not* try to mix and match multiple compilers and implementations for different operations supported by a single primitive. The underlying principle is that benchmark results should accurately predict the performance that users will see. It is theoretically possible for applications to link with multiple compiled versions of the same primitive, switching from one version to another when they switch from one operation to another, but in practice applications link with one compiled version of the primitive and expect it to provide good performance for all operations.

Note that different *primitives* do not need to share compilers. The current prototype of NaCl (Networking and Cryptography library), developed by the EU FP7 project CACE (Computer-Aided Cryptography Engineering), demonstrates the practicality of using different compilers for different primitives. VAMPIRE and CACE WP2 are coordinating interface design to minimize the gaps between cryptographic software used for benchmarking, cryptographic software subjected to regression tests, and cryptographic software used for applications.

4.3 Notes on machine-specific compilers

Some compilers (e.g., `gcc -m64 -maltivec -O3 -fomit-frame-pointer`) are specific to particular CPUs. On other CPUs, SUPERCOP sees that those compilers are unable to handle some simple test programs, and does not waste further time trying those compilers.

SUPERCOP also checks whether a compiled implementation passes some simple tests, such as being able to decrypt an encrypted message. If the tests fail, SUPERCOP skips that compiler for that implementation. However, SUPERCOP continues to try that compiler for other implementations and other primitives.

4.4 Notes on multiple ABIs

Some operating systems support multiple ABIs (Application Binary Interfaces). For example, amd64 CPUs (Athlon 64, Core 2, etc.) can run 64-bit amd64 programs *and* 32-bit x86 programs; operating systems for these CPUs often include 64-bit amd64 compilers and 32-bit x86 compilers.

SUPERCOP includes automatic "ABI stratification" on operating systems that support multiple ABIs. SUPERCOP automatically recognizes the amd64 compilers as being compatible with each other but incompatible with the x86 compilers; it runs separate amd64 benchmarks and x86 benchmarks. Usually the amd64 results are better, and users are generally recommended to opt for 64-bit software rather than 32-bit software; but the x86 benchmarks on these CPUs remain of interest for users who are confined to 32-bit operating systems. Occasionally the x86 results are better, because they use highly optimized x86 software that has not yet been ported to the amd64 architecture.

4.5 List of compilers tested

SUPERCOP tries the following compilers:

- `gcc -m64 -O3 -fomit-frame-pointer`
- `gcc -m64 -Os -fomit-frame-pointer`
- `gcc -m64 -O2 -fomit-frame-pointer`
- `gcc -m64 -O -fomit-frame-pointer`
- `gcc -m64`
- `gcc -m64 -maltivec -O3 -fomit-frame-pointer`
- `gcc -m64 -maltivec -Os -fomit-frame-pointer`
- `gcc -m64 -maltivec -O2 -fomit-frame-pointer`
- `gcc -m64 -maltivec -O -fomit-frame-pointer`
- `gcc -m64 -maltivec`
- `gcc -mpowerpc64 -O3 -fomit-frame-pointer`
- `gcc -mpowerpc64 -Os -fomit-frame-pointer`
- `gcc -mpowerpc64 -O2 -fomit-frame-pointer`
- `gcc -mpowerpc64 -fomit-frame-pointer`
- `gcc -mpowerpc64`
- `gcc -mpowerpc64 -maltivec -O3 -fomit-frame-pointer`
- `gcc -mpowerpc64 -maltivec -Os -fomit-frame-pointer`
- `gcc -mpowerpc64 -maltivec -O2 -fomit-frame-pointer`
- `gcc -mpowerpc64 -maltivec -fomit-frame-pointer`
- `gcc -mpowerpc64 -maltivec`
- `gcc -maix64 -mpowerpc64 -O3 -fomit-frame-pointer`
- `gcc -maix64 -mpowerpc64 -Os -fomit-frame-pointer`
- `gcc -maix64 -mpowerpc64 -O2 -fomit-frame-pointer`
- `gcc -maix64 -mpowerpc64 -fomit-frame-pointer`
- `gcc -maix64 -mpowerpc64`
- `gcc -mabi=64 -O3 -fomit-frame-pointer`
- `gcc -mabi=64 -Os -fomit-frame-pointer`
- `gcc -mabi=64 -O2 -fomit-frame-pointer`
- `gcc -mabi=64 -fomit-frame-pointer`

- `gcc -mabi=64`
- `gcc -mpa-risc-2-0 -O3 -fomit-frame-pointer`
- `gcc -mpa-risc-2-0 -Os -fomit-frame-pointer`
- `gcc -mpa-risc-2-0 -O2 -fomit-frame-pointer`
- `gcc -mpa-risc-2-0 -O -fomit-frame-pointer`
- `gcc -mpa-risc-2-0`
- `gcc -m64 -mcpu=ultrasparc3 -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ultrasparc3 -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=ultrasparc3 -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ultrasparc3 -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=ultrasparc3`
- `gcc -m64 -mcpu=ultrasparc -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ultrasparc -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=ultrasparc -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ultrasparc -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=ultrasparc`
- `gcc -m64 -mcpu=hypersparc -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=hypersparc -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=hypersparc -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=hypersparc -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=hypersparc`
- `gcc -m64 -mcpu=supersparc -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=supersparc -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=supersparc -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=supersparc -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=supersparc`
- `gcc -m64 -mcpu=sparclet -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=sparclet -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=sparclet -O2 -fomit-frame-pointer`

- `gcc -m64 -mcpu=sparclet -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=sparclet`
- `gcc -m64 -mcpu=sparclite86x -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=sparclite86x -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=sparclite86x -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=sparclite86x -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=sparclite86x`
- `gcc -m64 -mcpu=sparclite -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=sparclite -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=sparclite -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=sparclite -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=sparclite`
- `gcc -m64 -mcpu=sparc86x -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=sparc86x -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=sparc86x -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=sparc86x -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=sparc86x`
- `gcc -m64 -mcpu=sparc -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=sparc -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=sparc -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=sparc -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=sparc`
- `gcc -m64 -mcpu=v9 -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=v9 -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=v9 -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=v9 -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=v9`
- `gcc -m64 -mcpu=v8 -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=v8 -Os -fomit-frame-pointer`

- `gcc -m64 -mcpu=v8 -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=v8 -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=v8`
- `gcc -m64 -mcpu=pca56 -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=pca56 -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=pca56 -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=pca56 -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=pca56`
- `gcc -m64 -mcpu=ev67 -Wa,-mev67 -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev67 -Wa,-mev67 -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev67 -Wa,-mev67 -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev67 -Wa,-mev67 -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev67 -Wa,-mev67`
- `gcc -m64 -mcpu=ev6 -Wa,-mev6 -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev6 -Wa,-mev6 -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev6 -Wa,-mev6 -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev6 -Wa,-mev6 -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev6 -Wa,-mev6`
- `gcc -m64 -mcpu=ev56 -Wa,-mev56 -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev56 -Wa,-mev56 -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev56 -Wa,-mev56 -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev56 -Wa,-mev56 -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev56 -Wa,-mev56`
- `gcc -m64 -mcpu=ev5 -Wa,-mev5 -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev5 -Wa,-mev5 -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev5 -Wa,-mev5 -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev5 -Wa,-mev5 -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev5 -Wa,-mev5`
- `gcc -m64 -mcpu=ev4 -Wa,-mev4 -O3 -fomit-frame-pointer`

- `gcc -m64 -mcpu=ev4 -Wa,-mev4 -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev4 -Wa,-mev4 -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev4 -Wa,-mev4 -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev4 -Wa,-mev4`
- `gcc -m64 -mcpu=ev67 -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev67 -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev67 -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev67 -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev67`
- `gcc -m64 -mcpu=ev6 -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev6 -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev6 -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev6 -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev6`
- `gcc -m64 -mcpu=ev56 -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev56 -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev56 -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev56 -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev56`
- `gcc -m64 -mcpu=ev5 -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev5 -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev5 -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev5 -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev5`
- `gcc -m64 -mcpu=ev4 -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev4 -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev4 -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev4 -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=ev4`

- `gcc -m64 -mcpu=G5 -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=G5 -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=G5 -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=G5 -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=G5`
- `gcc -m64 -mcpu=G4 -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=G4 -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=G4 -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=G4 -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=G4`
- `gcc -m64 -mcpu=G3 -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=G3 -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=G3 -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=G3 -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=G3`
- `gcc -m64 -mcpu=G5 -maltivec -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=G5 -maltivec -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=G5 -maltivec -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=G5 -maltivec -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=G5 -maltivec`
- `gcc -m64 -mcpu=G4 -maltivec -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=G4 -maltivec -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=G4 -maltivec -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=G4 -maltivec -O -fomit-frame-pointer`
- `gcc -m64 -mcpu=G4 -maltivec`
- `gcc -m64 -mcpu=G3 -maltivec -O3 -fomit-frame-pointer`
- `gcc -m64 -mcpu=G3 -maltivec -Os -fomit-frame-pointer`
- `gcc -m64 -mcpu=G3 -maltivec -O2 -fomit-frame-pointer`
- `gcc -m64 -mcpu=G3 -maltivec -O -fomit-frame-pointer`

- `gcc -m64 -mcpu=G3 -maltivec`
- `gcc -mpowerpc64 -mcpu=G5 -O3 -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G5 -Os -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G5 -O2 -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G5 -O -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G5`
- `gcc -mpowerpc64 -mcpu=G4 -O3 -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G4 -Os -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G4 -O2 -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G4 -O -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G4`
- `gcc -mpowerpc64 -mcpu=G3 -O3 -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G3 -Os -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G3 -O2 -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G3 -O -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G3`
- `gcc -mpowerpc64 -mcpu=G5 -maltivec -O3 -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G5 -maltivec -Os -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G5 -maltivec -O2 -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G5 -maltivec -O -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G5 -maltivec`
- `gcc -mpowerpc64 -mcpu=G4 -maltivec -O3 -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G4 -maltivec -Os -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G4 -maltivec -O2 -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G4 -maltivec -O -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G4 -maltivec`
- `gcc -mpowerpc64 -mcpu=G3 -maltivec -O3 -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G3 -maltivec -Os -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G3 -maltivec -O2 -fomit-frame-pointer`

- `gcc -mpowerpc64 -mcpu=G3 -maltivec -O -fomit-frame-pointer`
- `gcc -mpowerpc64 -mcpu=G3 -maltivec`
- `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`
- `gcc -m64 -march=k8 -Os -fomit-frame-pointer`
- `gcc -m64 -march=k8 -O2 -fomit-frame-pointer`
- `gcc -m64 -march=k8 -O -fomit-frame-pointer`
- `gcc -m64 -march=k8`
- `gcc -m64 -march=athlon-sse -O3 -fomit-frame-pointer`
- `gcc -m64 -march=athlon-sse -Os -fomit-frame-pointer`
- `gcc -m64 -march=athlon-sse -O2 -fomit-frame-pointer`
- `gcc -m64 -march=athlon-sse -O -fomit-frame-pointer`
- `gcc -m64 -march=athlon-sse`
- `gcc -m64 -march=athlon -O3 -fomit-frame-pointer`
- `gcc -m64 -march=athlon -Os -fomit-frame-pointer`
- `gcc -m64 -march=athlon -O2 -fomit-frame-pointer`
- `gcc -m64 -march=athlon -O -fomit-frame-pointer`
- `gcc -m64 -march=athlon`
- `gcc -m64 -march=k6-3 -O3 -fomit-frame-pointer`
- `gcc -m64 -march=k6-3 -Os -fomit-frame-pointer`
- `gcc -m64 -march=k6-3 -O2 -fomit-frame-pointer`
- `gcc -m64 -march=k6-3 -O -fomit-frame-pointer`
- `gcc -m64 -march=k6-3`
- `gcc -m64 -march=k6-2 -O3 -fomit-frame-pointer`
- `gcc -m64 -march=k6-2 -Os -fomit-frame-pointer`
- `gcc -m64 -march=k6-2 -O2 -fomit-frame-pointer`
- `gcc -m64 -march=k6-2 -O -fomit-frame-pointer`
- `gcc -m64 -march=k6-2`
- `gcc -m64 -march=k6 -O3 -fomit-frame-pointer`
- `gcc -m64 -march=k6 -Os -fomit-frame-pointer`

- `gcc -m64 -march=k6 -O2 -fomit-frame-pointer`
- `gcc -m64 -march=k6 -O -fomit-frame-pointer`
- `gcc -m64 -march=k6`
- `gcc -m64 -march=nocona -O3 -fomit-frame-pointer`
- `gcc -m64 -march=nocona -Os -fomit-frame-pointer`
- `gcc -m64 -march=nocona -O2 -fomit-frame-pointer`
- `gcc -m64 -march=nocona -O -fomit-frame-pointer`
- `gcc -m64 -march=nocona`
- `gcc -m64 -march=prescott -O3 -fomit-frame-pointer`
- `gcc -m64 -march=prescott -Os -fomit-frame-pointer`
- `gcc -m64 -march=prescott -O2 -fomit-frame-pointer`
- `gcc -m64 -march=prescott -O -fomit-frame-pointer`
- `gcc -m64 -march=prescott`
- `gcc -m64 -march=pentium-m -O3 -fomit-frame-pointer`
- `gcc -m64 -march=pentium-m -Os -fomit-frame-pointer`
- `gcc -m64 -march=pentium-m -O2 -fomit-frame-pointer`
- `gcc -m64 -march=pentium-m -O -fomit-frame-pointer`
- `gcc -m64 -march=pentium-m`
- `gcc -m64 -march=pentium4 -O3 -fomit-frame-pointer`
- `gcc -m64 -march=pentium4 -Os -fomit-frame-pointer`
- `gcc -m64 -march=pentium4 -O2 -fomit-frame-pointer`
- `gcc -m64 -march=pentium4 -O -fomit-frame-pointer`
- `gcc -m64 -march=pentium4`
- `gcc -m64 -march=pentium3 -O3 -fomit-frame-pointer`
- `gcc -m64 -march=pentium3 -Os -fomit-frame-pointer`
- `gcc -m64 -march=pentium3 -O2 -fomit-frame-pointer`
- `gcc -m64 -march=pentium3 -O -fomit-frame-pointer`
- `gcc -m64 -march=pentium3`
- `gcc -m64 -march=pentium2 -O3 -fomit-frame-pointer`

- `gcc -m64 -march=pentium2 -Os -fomit-frame-pointer`
- `gcc -m64 -march=pentium2 -O2 -fomit-frame-pointer`
- `gcc -m64 -march=pentium2 -O -fomit-frame-pointer`
- `gcc -m64 -march=pentium2`
- `gcc -m64 -march=pentiumpro -O3 -fomit-frame-pointer`
- `gcc -m64 -march=pentiumpro -Os -fomit-frame-pointer`
- `gcc -m64 -march=pentiumpro -O2 -fomit-frame-pointer`
- `gcc -m64 -march=pentiumpro -O -fomit-frame-pointer`
- `gcc -m64 -march=pentiumpro`
- `gcc -m64 -march=pentium-mmx -O3 -fomit-frame-pointer`
- `gcc -m64 -march=pentium-mmx -Os -fomit-frame-pointer`
- `gcc -m64 -march=pentium-mmx -O2 -fomit-frame-pointer`
- `gcc -m64 -march=pentium-mmx -O -fomit-frame-pointer`
- `gcc -m64 -march=pentium-mmx`
- `gcc -m64 -march=pentium -O3 -fomit-frame-pointer`
- `gcc -m64 -march=pentium -Os -fomit-frame-pointer`
- `gcc -m64 -march=pentium -O2 -fomit-frame-pointer`
- `gcc -m64 -march=pentium -O -fomit-frame-pointer`
- `gcc -m64 -march=pentium`
- `gcc -m64 -march=i486 -O3 -fomit-frame-pointer`
- `gcc -m64 -march=i486 -Os -fomit-frame-pointer`
- `gcc -m64 -march=i486 -O2 -fomit-frame-pointer`
- `gcc -m64 -march=i486 -O -fomit-frame-pointer`
- `gcc -m64 -march=i486`
- `gcc -m64 -march=i386 -O3 -fomit-frame-pointer`
- `gcc -m64 -march=i386 -Os -fomit-frame-pointer`
- `gcc -m64 -march=i386 -O2 -fomit-frame-pointer`
- `gcc -m64 -march=i386 -O -fomit-frame-pointer`
- `gcc -m64 -march=i386`

- `xlc xlC -q64 -O2`
- `xlc xlC -q64 -O`
- `xlc xlC -q64`
- `xlc xlC -q64 -qtune=pwr3 -O2`
- `xlc xlC -q64 -qtune=pwr3 -O`
- `xlc xlC -q64 -qtune=pwr3`
- `/opt/SUNWspro/bin/cc /opt/SUNWspro/bin/CC -fast -xarch=v9`
- `/opt/SUNWspro/bin/cc /opt/SUNWspro/bin/CC -xarch=v9`
- `/opt/ansic/bin/cc /opt/aCC/bin/aCC +DD64 -fast`
- `/opt/ansic/bin/cc /opt/aCC/bin/aCC +DD64`
- `/opt/MIPSpro/bin/cc /opt/MIPSpro/bin/CC -64 -Ofast`
- `/opt/MIPSpro/bin/cc /opt/MIPSpro/bin/CC -64`
- `gcc -m32 -O3 -fomit-frame-pointer`
- `gcc -m32 -Os -fomit-frame-pointer`
- `gcc -m32 -O2 -fomit-frame-pointer`
- `gcc -m32 -O -fomit-frame-pointer`
- `gcc -m32`
- `gcc -m32 -maltivec -O3 -fomit-frame-pointer`
- `gcc -m32 -maltivec -Os -fomit-frame-pointer`
- `gcc -m32 -maltivec -O2 -fomit-frame-pointer`
- `gcc -m32 -maltivec -O -fomit-frame-pointer`
- `gcc -m32 -maltivec`
- `gcc -m32 -mcpu=ultrasparc3 -O3 -fomit-frame-pointer`
- `gcc -m32 -mcpu=ultrasparc3 -Os -fomit-frame-pointer`
- `gcc -m32 -mcpu=ultrasparc3 -O2 -fomit-frame-pointer`
- `gcc -m32 -mcpu=ultrasparc3 -O -fomit-frame-pointer`
- `gcc -m32 -mcpu=ultrasparc3`
- `gcc -m32 -mcpu=ultrasparc -O3 -fomit-frame-pointer`
- `gcc -m32 -mcpu=ultrasparc -Os -fomit-frame-pointer`

- gcc -m32 -mcpu=ultrasparc -O2 -fomit-frame-pointer
- gcc -m32 -mcpu=ultrasparc -O -fomit-frame-pointer
- gcc -m32 -mcpu=ultrasparc
- gcc -m32 -mcpu=hypersparc -O3 -fomit-frame-pointer
- gcc -m32 -mcpu=hypersparc -Os -fomit-frame-pointer
- gcc -m32 -mcpu=hypersparc -O2 -fomit-frame-pointer
- gcc -m32 -mcpu=hypersparc -O -fomit-frame-pointer
- gcc -m32 -mcpu=hypersparc
- gcc -m32 -mcpu=supersparc -O3 -fomit-frame-pointer
- gcc -m32 -mcpu=supersparc -Os -fomit-frame-pointer
- gcc -m32 -mcpu=supersparc -O2 -fomit-frame-pointer
- gcc -m32 -mcpu=supersparc -O -fomit-frame-pointer
- gcc -m32 -mcpu=supersparc
- gcc -m32 -mcpu=sparclet -O3 -fomit-frame-pointer
- gcc -m32 -mcpu=sparclet -Os -fomit-frame-pointer
- gcc -m32 -mcpu=sparclet -O2 -fomit-frame-pointer
- gcc -m32 -mcpu=sparclet -O -fomit-frame-pointer
- gcc -m32 -mcpu=sparclet
- gcc -m32 -mcpu=sparclite86x -O3 -fomit-frame-pointer
- gcc -m32 -mcpu=sparclite86x -Os -fomit-frame-pointer
- gcc -m32 -mcpu=sparclite86x -O2 -fomit-frame-pointer
- gcc -m32 -mcpu=sparclite86x -O -fomit-frame-pointer
- gcc -m32 -mcpu=sparclite86x
- gcc -m32 -mcpu=sparclite -O3 -fomit-frame-pointer
- gcc -m32 -mcpu=sparclite -Os -fomit-frame-pointer
- gcc -m32 -mcpu=sparclite -O2 -fomit-frame-pointer
- gcc -m32 -mcpu=sparclite -O -fomit-frame-pointer
- gcc -m32 -mcpu=sparclite
- gcc -m32 -mcpu=sparc86x -O3 -fomit-frame-pointer

- `gcc -m32 -mcpu=sparc86x -Os -fomit-frame-pointer`
- `gcc -m32 -mcpu=sparc86x -O2 -fomit-frame-pointer`
- `gcc -m32 -mcpu=sparc86x -O -fomit-frame-pointer`
- `gcc -m32 -mcpu=sparc86x`
- `gcc -m32 -mcpu=sparc -O3 -fomit-frame-pointer`
- `gcc -m32 -mcpu=sparc -Os -fomit-frame-pointer`
- `gcc -m32 -mcpu=sparc -O2 -fomit-frame-pointer`
- `gcc -m32 -mcpu=sparc -O -fomit-frame-pointer`
- `gcc -m32 -mcpu=sparc`
- `gcc -m32 -mcpu=v9 -O3 -fomit-frame-pointer`
- `gcc -m32 -mcpu=v9 -Os -fomit-frame-pointer`
- `gcc -m32 -mcpu=v9 -O2 -fomit-frame-pointer`
- `gcc -m32 -mcpu=v9 -O -fomit-frame-pointer`
- `gcc -m32 -mcpu=v9`
- `gcc -m32 -mcpu=v8 -O3 -fomit-frame-pointer`
- `gcc -m32 -mcpu=v8 -Os -fomit-frame-pointer`
- `gcc -m32 -mcpu=v8 -O2 -fomit-frame-pointer`
- `gcc -m32 -mcpu=v8 -O -fomit-frame-pointer`
- `gcc -m32 -mcpu=v8`
- `gcc -m32 -mcpu=pca56 -O3 -fomit-frame-pointer`
- `gcc -m32 -mcpu=pca56 -Os -fomit-frame-pointer`
- `gcc -m32 -mcpu=pca56 -O2 -fomit-frame-pointer`
- `gcc -m32 -mcpu=pca56 -O -fomit-frame-pointer`
- `gcc -m32 -mcpu=pca56`
- `gcc -m32 -mcpu=ev67 -Wa,-mev67 -O3 -fomit-frame-pointer`
- `gcc -m32 -mcpu=ev67 -Wa,-mev67 -Os -fomit-frame-pointer`
- `gcc -m32 -mcpu=ev67 -Wa,-mev67 -O2 -fomit-frame-pointer`
- `gcc -m32 -mcpu=ev67 -Wa,-mev67 -O -fomit-frame-pointer`
- `gcc -m32 -mcpu=ev67 -Wa,-mev67`

- gcc -m32 -mcpu=ev6 -Wa,-mev6 -O3 -fomit-frame-pointer
- gcc -m32 -mcpu=ev6 -Wa,-mev6 -Os -fomit-frame-pointer
- gcc -m32 -mcpu=ev6 -Wa,-mev6 -O2 -fomit-frame-pointer
- gcc -m32 -mcpu=ev6 -Wa,-mev6 -O -fomit-frame-pointer
- gcc -m32 -mcpu=ev6 -Wa,-mev6
- gcc -m32 -mcpu=ev56 -Wa,-mev56 -O3 -fomit-frame-pointer
- gcc -m32 -mcpu=ev56 -Wa,-mev56 -Os -fomit-frame-pointer
- gcc -m32 -mcpu=ev56 -Wa,-mev56 -O2 -fomit-frame-pointer
- gcc -m32 -mcpu=ev56 -Wa,-mev56 -O -fomit-frame-pointer
- gcc -m32 -mcpu=ev56 -Wa,-mev56
- gcc -m32 -mcpu=ev5 -Wa,-mev5 -O3 -fomit-frame-pointer
- gcc -m32 -mcpu=ev5 -Wa,-mev5 -Os -fomit-frame-pointer
- gcc -m32 -mcpu=ev5 -Wa,-mev5 -O2 -fomit-frame-pointer
- gcc -m32 -mcpu=ev5 -Wa,-mev5 -O -fomit-frame-pointer
- gcc -m32 -mcpu=ev5 -Wa,-mev5
- gcc -m32 -mcpu=ev4 -Wa,-mev4 -O3 -fomit-frame-pointer
- gcc -m32 -mcpu=ev4 -Wa,-mev4 -Os -fomit-frame-pointer
- gcc -m32 -mcpu=ev4 -Wa,-mev4 -O2 -fomit-frame-pointer
- gcc -m32 -mcpu=ev4 -Wa,-mev4 -O -fomit-frame-pointer
- gcc -m32 -mcpu=ev4 -Wa,-mev4
- gcc -m32 -mcpu=ev67 -O3 -fomit-frame-pointer
- gcc -m32 -mcpu=ev67 -Os -fomit-frame-pointer
- gcc -m32 -mcpu=ev67 -O2 -fomit-frame-pointer
- gcc -m32 -mcpu=ev67 -O -fomit-frame-pointer
- gcc -m32 -mcpu=ev67
- gcc -m32 -mcpu=ev6 -O3 -fomit-frame-pointer
- gcc -m32 -mcpu=ev6 -Os -fomit-frame-pointer
- gcc -m32 -mcpu=ev6 -O2 -fomit-frame-pointer
- gcc -m32 -mcpu=ev6 -O -fomit-frame-pointer

- `gcc -m32 -mcpu=ev6`
- `gcc -m32 -mcpu=ev56 -O3 -fomit-frame-pointer`
- `gcc -m32 -mcpu=ev56 -Os -fomit-frame-pointer`
- `gcc -m32 -mcpu=ev56 -O2 -fomit-frame-pointer`
- `gcc -m32 -mcpu=ev56 -O -fomit-frame-pointer`
- `gcc -m32 -mcpu=ev56`
- `gcc -m32 -mcpu=ev5 -O3 -fomit-frame-pointer`
- `gcc -m32 -mcpu=ev5 -Os -fomit-frame-pointer`
- `gcc -m32 -mcpu=ev5 -O2 -fomit-frame-pointer`
- `gcc -m32 -mcpu=ev5 -O -fomit-frame-pointer`
- `gcc -m32 -mcpu=ev5`
- `gcc -m32 -mcpu=ev4 -O3 -fomit-frame-pointer`
- `gcc -m32 -mcpu=ev4 -Os -fomit-frame-pointer`
- `gcc -m32 -mcpu=ev4 -O2 -fomit-frame-pointer`
- `gcc -m32 -mcpu=ev4 -O -fomit-frame-pointer`
- `gcc -m32 -mcpu=ev4`
- `gcc -m32 -mcpu=G5 -O3 -fomit-frame-pointer`
- `gcc -m32 -mcpu=G5 -Os -fomit-frame-pointer`
- `gcc -m32 -mcpu=G5 -O2 -fomit-frame-pointer`
- `gcc -m32 -mcpu=G5 -O -fomit-frame-pointer`
- `gcc -m32 -mcpu=G5`
- `gcc -m32 -mcpu=G4 -O3 -fomit-frame-pointer`
- `gcc -m32 -mcpu=G4 -Os -fomit-frame-pointer`
- `gcc -m32 -mcpu=G4 -O2 -fomit-frame-pointer`
- `gcc -m32 -mcpu=G4 -O -fomit-frame-pointer`
- `gcc -m32 -mcpu=G4`
- `gcc -m32 -mcpu=G3 -O3 -fomit-frame-pointer`
- `gcc -m32 -mcpu=G3 -Os -fomit-frame-pointer`
- `gcc -m32 -mcpu=G3 -O2 -fomit-frame-pointer`

- `gcc -m32 -mcpu=G3 -O -fomit-frame-pointer`
- `gcc -m32 -mcpu=G3`
- `gcc -m32 -mcpu=G5 -maltivec -O3 -fomit-frame-pointer`
- `gcc -m32 -mcpu=G5 -maltivec -Os -fomit-frame-pointer`
- `gcc -m32 -mcpu=G5 -maltivec -O2 -fomit-frame-pointer`
- `gcc -m32 -mcpu=G5 -maltivec -O -fomit-frame-pointer`
- `gcc -m32 -mcpu=G5 -maltivec`
- `gcc -m32 -mcpu=G4 -maltivec -O3 -fomit-frame-pointer`
- `gcc -m32 -mcpu=G4 -maltivec -Os -fomit-frame-pointer`
- `gcc -m32 -mcpu=G4 -maltivec -O2 -fomit-frame-pointer`
- `gcc -m32 -mcpu=G4 -maltivec -O -fomit-frame-pointer`
- `gcc -m32 -mcpu=G4 -maltivec`
- `gcc -m32 -mcpu=G3 -maltivec -O3 -fomit-frame-pointer`
- `gcc -m32 -mcpu=G3 -maltivec -Os -fomit-frame-pointer`
- `gcc -m32 -mcpu=G3 -maltivec -O2 -fomit-frame-pointer`
- `gcc -m32 -mcpu=G3 -maltivec -O -fomit-frame-pointer`
- `gcc -m32 -mcpu=G3 -maltivec`
- `gcc -m32 -march=k8 -O3 -fomit-frame-pointer`
- `gcc -m32 -march=k8 -Os -fomit-frame-pointer`
- `gcc -m32 -march=k8 -O2 -fomit-frame-pointer`
- `gcc -m32 -march=k8 -O -fomit-frame-pointer`
- `gcc -m32 -march=k8`
- `gcc -m32 -march=athlon-sse -O3 -fomit-frame-pointer`
- `gcc -m32 -march=athlon-sse -Os -fomit-frame-pointer`
- `gcc -m32 -march=athlon-sse -O2 -fomit-frame-pointer`
- `gcc -m32 -march=athlon-sse -O -fomit-frame-pointer`
- `gcc -m32 -march=athlon-sse`
- `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- `gcc -m32 -march=athlon -Os -fomit-frame-pointer`

- `gcc -m32 -march=athlon -O2 -fomit-frame-pointer`
- `gcc -m32 -march=athlon -O -fomit-frame-pointer`
- `gcc -m32 -march=athlon`
- `gcc -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- `gcc -m32 -march=k6-3 -Os -fomit-frame-pointer`
- `gcc -m32 -march=k6-3 -O2 -fomit-frame-pointer`
- `gcc -m32 -march=k6-3 -O -fomit-frame-pointer`
- `gcc -m32 -march=k6-3`
- `gcc -m32 -march=k6-2 -O3 -fomit-frame-pointer`
- `gcc -m32 -march=k6-2 -Os -fomit-frame-pointer`
- `gcc -m32 -march=k6-2 -O2 -fomit-frame-pointer`
- `gcc -m32 -march=k6-2 -O -fomit-frame-pointer`
- `gcc -m32 -march=k6-2`
- `gcc -m32 -march=k6 -O3 -fomit-frame-pointer`
- `gcc -m32 -march=k6 -Os -fomit-frame-pointer`
- `gcc -m32 -march=k6 -O2 -fomit-frame-pointer`
- `gcc -m32 -march=k6 -O -fomit-frame-pointer`
- `gcc -m32 -march=k6`
- `gcc -m32 -march=nocona -O3 -fomit-frame-pointer`
- `gcc -m32 -march=nocona -Os -fomit-frame-pointer`
- `gcc -m32 -march=nocona -O2 -fomit-frame-pointer`
- `gcc -m32 -march=nocona -O -fomit-frame-pointer`
- `gcc -m32 -march=nocona`
- `gcc -m32 -march=prescott -O3 -fomit-frame-pointer`
- `gcc -m32 -march=prescott -Os -fomit-frame-pointer`
- `gcc -m32 -march=prescott -O2 -fomit-frame-pointer`
- `gcc -m32 -march=prescott -O -fomit-frame-pointer`
- `gcc -m32 -march=prescott`
- `gcc -m32 -march=pentium-m -O3 -fomit-frame-pointer`

- gcc -m32 -march=pentium-m -Os -fomit-frame-pointer
- gcc -m32 -march=pentium-m -O2 -fomit-frame-pointer
- gcc -m32 -march=pentium-m -O -fomit-frame-pointer
- gcc -m32 -march=pentium-m
- gcc -m32 -march=pentium4 -O3 -fomit-frame-pointer
- gcc -m32 -march=pentium4 -Os -fomit-frame-pointer
- gcc -m32 -march=pentium4 -O2 -fomit-frame-pointer
- gcc -m32 -march=pentium4 -O -fomit-frame-pointer
- gcc -m32 -march=pentium4
- gcc -m32 -march=pentium3 -O3 -fomit-frame-pointer
- gcc -m32 -march=pentium3 -Os -fomit-frame-pointer
- gcc -m32 -march=pentium3 -O2 -fomit-frame-pointer
- gcc -m32 -march=pentium3 -O -fomit-frame-pointer
- gcc -m32 -march=pentium3
- gcc -m32 -march=pentium2 -O3 -fomit-frame-pointer
- gcc -m32 -march=pentium2 -Os -fomit-frame-pointer
- gcc -m32 -march=pentium2 -O2 -fomit-frame-pointer
- gcc -m32 -march=pentium2 -O -fomit-frame-pointer
- gcc -m32 -march=pentium2
- gcc -m32 -march=pentiumpro -O3 -fomit-frame-pointer
- gcc -m32 -march=pentiumpro -Os -fomit-frame-pointer
- gcc -m32 -march=pentiumpro -O2 -fomit-frame-pointer
- gcc -m32 -march=pentiumpro -O -fomit-frame-pointer
- gcc -m32 -march=pentiumpro
- gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer
- gcc -m32 -march=pentium-mmx -Os -fomit-frame-pointer
- gcc -m32 -march=pentium-mmx -O2 -fomit-frame-pointer
- gcc -m32 -march=pentium-mmx -O -fomit-frame-pointer
- gcc -m32 -march=pentium-mmx

- `gcc -m32 -march=pentium -O3 -fomit-frame-pointer`
- `gcc -m32 -march=pentium -Os -fomit-frame-pointer`
- `gcc -m32 -march=pentium -O2 -fomit-frame-pointer`
- `gcc -m32 -march=pentium -O -fomit-frame-pointer`
- `gcc -m32 -march=pentium`
- `gcc -m32 -march=i486 -O3 -fomit-frame-pointer`
- `gcc -m32 -march=i486 -Os -fomit-frame-pointer`
- `gcc -m32 -march=i486 -O2 -fomit-frame-pointer`
- `gcc -m32 -march=i486 -O -fomit-frame-pointer`
- `gcc -m32 -march=i486`
- `gcc -m32 -march=i386 -O3 -fomit-frame-pointer`
- `gcc -m32 -march=i386 -Os -fomit-frame-pointer`
- `gcc -m32 -march=i386 -O2 -fomit-frame-pointer`
- `gcc -m32 -march=i386 -O -fomit-frame-pointer`
- `gcc -m32 -march=i386`
- `gcc -O3 -fomit-frame-pointer`
- `gcc -Os -fomit-frame-pointer`
- `gcc -O2 -fomit-frame-pointer`
- `gcc -O -fomit-frame-pointer`
- `gcc`
- `gcc -maltivec -O3 -fomit-frame-pointer`
- `gcc -maltivec -Os -fomit-frame-pointer`
- `gcc -maltivec -O2 -fomit-frame-pointer`
- `gcc -maltivec -O -fomit-frame-pointer`
- `gcc -maltivec`
- `gcc -mcpu=ultrasparc3 -O3 -fomit-frame-pointer`
- `gcc -mcpu=ultrasparc3 -Os -fomit-frame-pointer`
- `gcc -mcpu=ultrasparc3 -O2 -fomit-frame-pointer`
- `gcc -mcpu=ultrasparc3 -O -fomit-frame-pointer`

- `gcc -mcpu=ultrasparc3`
- `gcc -mcpu=ultrasparc -O3 -fomit-frame-pointer`
- `gcc -mcpu=ultrasparc -Os -fomit-frame-pointer`
- `gcc -mcpu=ultrasparc -O2 -fomit-frame-pointer`
- `gcc -mcpu=ultrasparc -O -fomit-frame-pointer`
- `gcc -mcpu=ultrasparc`
- `gcc -mcpu=hypersparc -O3 -fomit-frame-pointer`
- `gcc -mcpu=hypersparc -Os -fomit-frame-pointer`
- `gcc -mcpu=hypersparc -O2 -fomit-frame-pointer`
- `gcc -mcpu=hypersparc -O -fomit-frame-pointer`
- `gcc -mcpu=hypersparc`
- `gcc -mcpu=supersparc -O3 -fomit-frame-pointer`
- `gcc -mcpu=supersparc -Os -fomit-frame-pointer`
- `gcc -mcpu=supersparc -O2 -fomit-frame-pointer`
- `gcc -mcpu=supersparc -O -fomit-frame-pointer`
- `gcc -mcpu=supersparc`
- `gcc -mcpu=sparclet -O3 -fomit-frame-pointer`
- `gcc -mcpu=sparclet -Os -fomit-frame-pointer`
- `gcc -mcpu=sparclet -O2 -fomit-frame-pointer`
- `gcc -mcpu=sparclet -O -fomit-frame-pointer`
- `gcc -mcpu=sparclet`
- `gcc -mcpu=sparclite86x -O3 -fomit-frame-pointer`
- `gcc -mcpu=sparclite86x -Os -fomit-frame-pointer`
- `gcc -mcpu=sparclite86x -O2 -fomit-frame-pointer`
- `gcc -mcpu=sparclite86x -O -fomit-frame-pointer`
- `gcc -mcpu=sparclite86x`
- `gcc -mcpu=sparclite -O3 -fomit-frame-pointer`
- `gcc -mcpu=sparclite -Os -fomit-frame-pointer`
- `gcc -mcpu=sparclite -O2 -fomit-frame-pointer`

- `gcc -mcpu=sparclite -O -fomit-frame-pointer`
- `gcc -mcpu=sparclite`
- `gcc -mcpu=sparc86x -O3 -fomit-frame-pointer`
- `gcc -mcpu=sparc86x -Os -fomit-frame-pointer`
- `gcc -mcpu=sparc86x -O2 -fomit-frame-pointer`
- `gcc -mcpu=sparc86x -O -fomit-frame-pointer`
- `gcc -mcpu=sparc86x`
- `gcc -mcpu=sparc -O3 -fomit-frame-pointer`
- `gcc -mcpu=sparc -Os -fomit-frame-pointer`
- `gcc -mcpu=sparc -O2 -fomit-frame-pointer`
- `gcc -mcpu=sparc -O -fomit-frame-pointer`
- `gcc -mcpu=sparc`
- `gcc -mcpu=v9 -O3 -fomit-frame-pointer`
- `gcc -mcpu=v9 -Os -fomit-frame-pointer`
- `gcc -mcpu=v9 -O2 -fomit-frame-pointer`
- `gcc -mcpu=v9 -O -fomit-frame-pointer`
- `gcc -mcpu=v9`
- `gcc -mcpu=v8 -O3 -fomit-frame-pointer`
- `gcc -mcpu=v8 -Os -fomit-frame-pointer`
- `gcc -mcpu=v8 -O2 -fomit-frame-pointer`
- `gcc -mcpu=v8 -O -fomit-frame-pointer`
- `gcc -mcpu=v8`
- `gcc -mcpu=pca56 -O3 -fomit-frame-pointer`
- `gcc -mcpu=pca56 -Os -fomit-frame-pointer`
- `gcc -mcpu=pca56 -O2 -fomit-frame-pointer`
- `gcc -mcpu=pca56 -O -fomit-frame-pointer`
- `gcc -mcpu=pca56`
- `gcc -mcpu=ev67 -Wa,-mev67 -O3 -fomit-frame-pointer`
- `gcc -mcpu=ev67 -Wa,-mev67 -Os -fomit-frame-pointer`

- `gcc -mcpu=ev67 -Wa,-mev67 -O2 -fomit-frame-pointer`
- `gcc -mcpu=ev67 -Wa,-mev67 -O -fomit-frame-pointer`
- `gcc -mcpu=ev67 -Wa,-mev67`
- `gcc -mcpu=ev6 -Wa,-mev6 -O3 -fomit-frame-pointer`
- `gcc -mcpu=ev6 -Wa,-mev6 -Os -fomit-frame-pointer`
- `gcc -mcpu=ev6 -Wa,-mev6 -O2 -fomit-frame-pointer`
- `gcc -mcpu=ev6 -Wa,-mev6 -O -fomit-frame-pointer`
- `gcc -mcpu=ev6 -Wa,-mev6`
- `gcc -mcpu=ev56 -Wa,-mev56 -O3 -fomit-frame-pointer`
- `gcc -mcpu=ev56 -Wa,-mev56 -Os -fomit-frame-pointer`
- `gcc -mcpu=ev56 -Wa,-mev56 -O2 -fomit-frame-pointer`
- `gcc -mcpu=ev56 -Wa,-mev56 -O -fomit-frame-pointer`
- `gcc -mcpu=ev56 -Wa,-mev56`
- `gcc -mcpu=ev5 -Wa,-mev5 -O3 -fomit-frame-pointer`
- `gcc -mcpu=ev5 -Wa,-mev5 -Os -fomit-frame-pointer`
- `gcc -mcpu=ev5 -Wa,-mev5 -O2 -fomit-frame-pointer`
- `gcc -mcpu=ev5 -Wa,-mev5 -O -fomit-frame-pointer`
- `gcc -mcpu=ev5 -Wa,-mev5`
- `gcc -mcpu=ev4 -Wa,-mev4 -O3 -fomit-frame-pointer`
- `gcc -mcpu=ev4 -Wa,-mev4 -Os -fomit-frame-pointer`
- `gcc -mcpu=ev4 -Wa,-mev4 -O2 -fomit-frame-pointer`
- `gcc -mcpu=ev4 -Wa,-mev4 -O -fomit-frame-pointer`
- `gcc -mcpu=ev4 -Wa,-mev4`
- `gcc -mcpu=ev67 -O3 -fomit-frame-pointer`
- `gcc -mcpu=ev67 -Os -fomit-frame-pointer`
- `gcc -mcpu=ev67 -O2 -fomit-frame-pointer`
- `gcc -mcpu=ev67 -O -fomit-frame-pointer`
- `gcc -mcpu=ev67`
- `gcc -mcpu=ev6 -O3 -fomit-frame-pointer`

- `gcc -mcpu=ev6 -Os -fomit-frame-pointer`
- `gcc -mcpu=ev6 -O2 -fomit-frame-pointer`
- `gcc -mcpu=ev6 -O -fomit-frame-pointer`
- `gcc -mcpu=ev6`
- `gcc -mcpu=ev56 -O3 -fomit-frame-pointer`
- `gcc -mcpu=ev56 -Os -fomit-frame-pointer`
- `gcc -mcpu=ev56 -O2 -fomit-frame-pointer`
- `gcc -mcpu=ev56 -O -fomit-frame-pointer`
- `gcc -mcpu=ev56`
- `gcc -mcpu=ev5 -O3 -fomit-frame-pointer`
- `gcc -mcpu=ev5 -Os -fomit-frame-pointer`
- `gcc -mcpu=ev5 -O2 -fomit-frame-pointer`
- `gcc -mcpu=ev5 -O -fomit-frame-pointer`
- `gcc -mcpu=ev5`
- `gcc -mcpu=ev4 -O3 -fomit-frame-pointer`
- `gcc -mcpu=ev4 -Os -fomit-frame-pointer`
- `gcc -mcpu=ev4 -O2 -fomit-frame-pointer`
- `gcc -mcpu=ev4 -O -fomit-frame-pointer`
- `gcc -mcpu=ev4`
- `gcc -mcpu=G5 -O3 -fomit-frame-pointer`
- `gcc -mcpu=G5 -Os -fomit-frame-pointer`
- `gcc -mcpu=G5 -O2 -fomit-frame-pointer`
- `gcc -mcpu=G5 -O -fomit-frame-pointer`
- `gcc -mcpu=G5`
- `gcc -mcpu=G4 -O3 -fomit-frame-pointer`
- `gcc -mcpu=G4 -Os -fomit-frame-pointer`
- `gcc -mcpu=G4 -O2 -fomit-frame-pointer`
- `gcc -mcpu=G4 -O -fomit-frame-pointer`
- `gcc -mcpu=G4`

- `gcc -mcpu=G3 -O3 -fomit-frame-pointer`
- `gcc -mcpu=G3 -Os -fomit-frame-pointer`
- `gcc -mcpu=G3 -O2 -fomit-frame-pointer`
- `gcc -mcpu=G3 -O -fomit-frame-pointer`
- `gcc -mcpu=G3`
- `gcc -mcpu=G5 -maltivec -O3 -fomit-frame-pointer`
- `gcc -mcpu=G5 -maltivec -Os -fomit-frame-pointer`
- `gcc -mcpu=G5 -maltivec -O2 -fomit-frame-pointer`
- `gcc -mcpu=G5 -maltivec -O -fomit-frame-pointer`
- `gcc -mcpu=G5 -maltivec`
- `gcc -mcpu=G4 -maltivec -O3 -fomit-frame-pointer`
- `gcc -mcpu=G4 -maltivec -Os -fomit-frame-pointer`
- `gcc -mcpu=G4 -maltivec -O2 -fomit-frame-pointer`
- `gcc -mcpu=G4 -maltivec -O -fomit-frame-pointer`
- `gcc -mcpu=G4 -maltivec`
- `gcc -mcpu=G3 -maltivec -O3 -fomit-frame-pointer`
- `gcc -mcpu=G3 -maltivec -Os -fomit-frame-pointer`
- `gcc -mcpu=G3 -maltivec -O2 -fomit-frame-pointer`
- `gcc -mcpu=G3 -maltivec -O -fomit-frame-pointer`
- `gcc -mcpu=G3 -maltivec`
- `gcc -march=k8 -O3 -fomit-frame-pointer`
- `gcc -march=k8 -Os -fomit-frame-pointer`
- `gcc -march=k8 -O2 -fomit-frame-pointer`
- `gcc -march=k8 -O -fomit-frame-pointer`
- `gcc -march=k8`
- `gcc -march=athlon-sse -O3 -fomit-frame-pointer`
- `gcc -march=athlon-sse -Os -fomit-frame-pointer`
- `gcc -march=athlon-sse -O2 -fomit-frame-pointer`
- `gcc -march=athlon-sse -O -fomit-frame-pointer`

- `gcc -march=athlon-sse`
- `gcc -march=athlon -O3 -fomit-frame-pointer`
- `gcc -march=athlon -Os -fomit-frame-pointer`
- `gcc -march=athlon -O2 -fomit-frame-pointer`
- `gcc -march=athlon -O -fomit-frame-pointer`
- `gcc -march=athlon`
- `gcc -march=k6-3 -O3 -fomit-frame-pointer`
- `gcc -march=k6-3 -Os -fomit-frame-pointer`
- `gcc -march=k6-3 -O2 -fomit-frame-pointer`
- `gcc -march=k6-3 -O -fomit-frame-pointer`
- `gcc -march=k6-3`
- `gcc -march=k6-2 -O3 -fomit-frame-pointer`
- `gcc -march=k6-2 -Os -fomit-frame-pointer`
- `gcc -march=k6-2 -O2 -fomit-frame-pointer`
- `gcc -march=k6-2 -O -fomit-frame-pointer`
- `gcc -march=k6-2`
- `gcc -march=k6 -O3 -fomit-frame-pointer`
- `gcc -march=k6 -Os -fomit-frame-pointer`
- `gcc -march=k6 -O2 -fomit-frame-pointer`
- `gcc -march=k6 -O -fomit-frame-pointer`
- `gcc -march=k6`
- `gcc -march=nocona -O3 -fomit-frame-pointer`
- `gcc -march=nocona -Os -fomit-frame-pointer`
- `gcc -march=nocona -O2 -fomit-frame-pointer`
- `gcc -march=nocona -O -fomit-frame-pointer`
- `gcc -march=nocona`
- `gcc -march=prescott -O3 -fomit-frame-pointer`
- `gcc -march=prescott -Os -fomit-frame-pointer`
- `gcc -march=prescott -O2 -fomit-frame-pointer`

- `gcc -march=prescott -O -fomit-frame-pointer`
- `gcc -march=prescott`
- `gcc -march=pentium-m -O3 -fomit-frame-pointer`
- `gcc -march=pentium-m -Os -fomit-frame-pointer`
- `gcc -march=pentium-m -O2 -fomit-frame-pointer`
- `gcc -march=pentium-m -O -fomit-frame-pointer`
- `gcc -march=pentium-m`
- `gcc -march=pentium4 -O3 -fomit-frame-pointer`
- `gcc -march=pentium4 -Os -fomit-frame-pointer`
- `gcc -march=pentium4 -O2 -fomit-frame-pointer`
- `gcc -march=pentium4 -O -fomit-frame-pointer`
- `gcc -march=pentium4`
- `gcc -march=pentium3 -O3 -fomit-frame-pointer`
- `gcc -march=pentium3 -Os -fomit-frame-pointer`
- `gcc -march=pentium3 -O2 -fomit-frame-pointer`
- `gcc -march=pentium3 -O -fomit-frame-pointer`
- `gcc -march=pentium3`
- `gcc -march=pentium2 -O3 -fomit-frame-pointer`
- `gcc -march=pentium2 -Os -fomit-frame-pointer`
- `gcc -march=pentium2 -O2 -fomit-frame-pointer`
- `gcc -march=pentium2 -O -fomit-frame-pointer`
- `gcc -march=pentium2`
- `gcc -march=pentiumpro -O3 -fomit-frame-pointer`
- `gcc -march=pentiumpro -Os -fomit-frame-pointer`
- `gcc -march=pentiumpro -O2 -fomit-frame-pointer`
- `gcc -march=pentiumpro -O -fomit-frame-pointer`
- `gcc -march=pentiumpro`
- `gcc -march=pentium-mmx -O3 -fomit-frame-pointer`
- `gcc -march=pentium-mmx -Os -fomit-frame-pointer`

- `gcc -march=pentium-mmx -O2 -fomit-frame-pointer`
- `gcc -march=pentium-mmx -O -fomit-frame-pointer`
- `gcc -march=pentium-mmx`
- `gcc -march=pentium -O3 -fomit-frame-pointer`
- `gcc -march=pentium -Os -fomit-frame-pointer`
- `gcc -march=pentium -O2 -fomit-frame-pointer`
- `gcc -march=pentium -O -fomit-frame-pointer`
- `gcc -march=pentium`
- `gcc -march=i486 -O3 -fomit-frame-pointer`
- `gcc -march=i486 -Os -fomit-frame-pointer`
- `gcc -march=i486 -O2 -fomit-frame-pointer`
- `gcc -march=i486 -O -fomit-frame-pointer`
- `gcc -march=i486`
- `gcc -march=i386 -O3 -fomit-frame-pointer`
- `gcc -march=i386 -Os -fomit-frame-pointer`
- `gcc -march=i386 -O2 -fomit-frame-pointer`
- `gcc -march=i386 -O -fomit-frame-pointer`
- `gcc -march=i386`
- `xlc -O2`
- `xlc -O`
- `xlc`
- `xlc -qarch=ppc -O2`
- `xlc -qarch=ppc -O`
- `xlc -qarch=ppc`
- `xlc -qarch=pwr2 -O2`
- `xlc -qarch=pwr2 -O`
- `xlc -qarch=pwr2`
- `xlc -qarch=pwr -O2`
- `xlc -qarch=pwr -O`

- `xlc -qarch=pwr`
- `xlc -qarch=com -O2`
- `xlc -qarch=com -O`
- `xlc -qarch=com`
- `/opt/SUNWspro/bin/cc -fast`
- `/opt/SUNWspro/bin/cc`
- `/opt/ansic/bin/cc -fast`
- `/opt/ansic/bin/cc`
- `/opt/MIPSpro/bin/cc -n32 -Ofast`
- `/opt/MIPSpro/bin/cc -n32`
- `/opt/MIPSpro/bin/cc -Ofast`
- `/opt/MIPSpro/bin/cc`
- `cc`
- `gcc -funroll-loops -m64 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64`
- `gcc -funroll-loops -m64 -maltivec -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -maltivec -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -maltivec -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -maltivec -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -maltivec`
- `gcc -funroll-loops -mpowerpc64 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64`
- `gcc -funroll-loops -mpowerpc64 -maltivec -O3 -fomit-frame-pointer`

- `gcc -funroll-loops -mpowerpc64 -maltivec -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -maltivec -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -maltivec -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -maltivec`
- `gcc -funroll-loops -maix64 -mpowerpc64 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -maix64 -mpowerpc64 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -maix64 -mpowerpc64 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -maix64 -mpowerpc64 -fomit-frame-pointer`
- `gcc -funroll-loops -maix64 -mpowerpc64`
- `gcc -funroll-loops -mabi=64 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mabi=64 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mabi=64 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mabi=64 -fomit-frame-pointer`
- `gcc -funroll-loops -mabi=64`
- `gcc -funroll-loops -mpa-risc-2-0 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mpa-risc-2-0 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mpa-risc-2-0 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mpa-risc-2-0 -O -fomit-frame-pointer`
- `gcc -funroll-loops -mpa-risc-2-0`
- `gcc -funroll-loops -m64 -mcpu=ultrasparc3 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ultrasparc3 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ultrasparc3 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ultrasparc3 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ultrasparc3`
- `gcc -funroll-loops -m64 -mcpu=ultrasparc -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ultrasparc -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ultrasparc -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ultrasparc -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ultrasparc`

- `gcc -funroll-loops -m64 -mcpu=hypersparc -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=hypersparc -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=hypersparc -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=hypersparc -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=hypersparc`
- `gcc -funroll-loops -m64 -mcpu=supersparc -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=supersparc -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=supersparc -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=supersparc -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=supersparc`
- `gcc -funroll-loops -m64 -mcpu=sparclet -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=sparclet -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=sparclet -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=sparclet -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=sparclet`
- `gcc -funroll-loops -m64 -mcpu=sparclite86x -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=sparclite86x -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=sparclite86x -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=sparclite86x -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=sparclite86x`
- `gcc -funroll-loops -m64 -mcpu=sparclite -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=sparclite -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=sparclite -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=sparclite -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=sparclite`
- `gcc -funroll-loops -m64 -mcpu=sparc86x -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=sparc86x -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=sparc86x -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=sparc86x -O -fomit-frame-pointer`

- `gcc -funroll-loops -m64 -mcpu=sparc86x`
- `gcc -funroll-loops -m64 -mcpu=sparc -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=sparc -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=sparc -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=sparc -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=sparc`
- `gcc -funroll-loops -m64 -mcpu=v9 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=v9 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=v9 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=v9 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=v9`
- `gcc -funroll-loops -m64 -mcpu=v8 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=v8 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=v8 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=v8 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=v8`
- `gcc -funroll-loops -m64 -mcpu=pca56 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=pca56 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=pca56 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=pca56 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=pca56`
- `gcc -funroll-loops -m64 -mcpu=ev67 -Wa,-mev67 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ev67 -Wa,-mev67 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ev67 -Wa,-mev67 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ev67 -Wa,-mev67 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ev67 -Wa,-mev67`
- `gcc -funroll-loops -m64 -mcpu=ev6 -Wa,-mev6 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ev6 -Wa,-mev6 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ev6 -Wa,-mev6 -O2 -fomit-frame-pointer`

- gcc -funroll-loops -m64 -mcpu=ev6 -Wa,-mev6 -O -fomit-frame-pointer
- gcc -funroll-loops -m64 -mcpu=ev6 -Wa,-mev6
- gcc -funroll-loops -m64 -mcpu=ev56 -Wa,-mev56 -O3 -fomit-frame-pointer
- gcc -funroll-loops -m64 -mcpu=ev56 -Wa,-mev56 -Os -fomit-frame-pointer
- gcc -funroll-loops -m64 -mcpu=ev56 -Wa,-mev56 -O2 -fomit-frame-pointer
- gcc -funroll-loops -m64 -mcpu=ev56 -Wa,-mev56 -O -fomit-frame-pointer
- gcc -funroll-loops -m64 -mcpu=ev56 -Wa,-mev56
- gcc -funroll-loops -m64 -mcpu=ev5 -Wa,-mev5 -O3 -fomit-frame-pointer
- gcc -funroll-loops -m64 -mcpu=ev5 -Wa,-mev5 -Os -fomit-frame-pointer
- gcc -funroll-loops -m64 -mcpu=ev5 -Wa,-mev5 -O2 -fomit-frame-pointer
- gcc -funroll-loops -m64 -mcpu=ev5 -Wa,-mev5 -O -fomit-frame-pointer
- gcc -funroll-loops -m64 -mcpu=ev5 -Wa,-mev5
- gcc -funroll-loops -m64 -mcpu=ev4 -Wa,-mev4 -O3 -fomit-frame-pointer
- gcc -funroll-loops -m64 -mcpu=ev4 -Wa,-mev4 -Os -fomit-frame-pointer
- gcc -funroll-loops -m64 -mcpu=ev4 -Wa,-mev4 -O2 -fomit-frame-pointer
- gcc -funroll-loops -m64 -mcpu=ev4 -Wa,-mev4 -O -fomit-frame-pointer
- gcc -funroll-loops -m64 -mcpu=ev4 -Wa,-mev4
- gcc -funroll-loops -m64 -mcpu=ev67 -O3 -fomit-frame-pointer
- gcc -funroll-loops -m64 -mcpu=ev67 -Os -fomit-frame-pointer
- gcc -funroll-loops -m64 -mcpu=ev67 -O2 -fomit-frame-pointer
- gcc -funroll-loops -m64 -mcpu=ev67 -O -fomit-frame-pointer
- gcc -funroll-loops -m64 -mcpu=ev67
- gcc -funroll-loops -m64 -mcpu=ev6 -O3 -fomit-frame-pointer
- gcc -funroll-loops -m64 -mcpu=ev6 -Os -fomit-frame-pointer
- gcc -funroll-loops -m64 -mcpu=ev6 -O2 -fomit-frame-pointer
- gcc -funroll-loops -m64 -mcpu=ev6 -O -fomit-frame-pointer
- gcc -funroll-loops -m64 -mcpu=ev6
- gcc -funroll-loops -m64 -mcpu=ev56 -O3 -fomit-frame-pointer
- gcc -funroll-loops -m64 -mcpu=ev56 -Os -fomit-frame-pointer

- `gcc -funroll-loops -m64 -mcpu=ev56 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ev56 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ev56`
- `gcc -funroll-loops -m64 -mcpu=ev5 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ev5 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ev5 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ev5 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ev5`
- `gcc -funroll-loops -m64 -mcpu=ev4 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ev4 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ev4 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ev4 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=ev4`
- `gcc -funroll-loops -m64 -mcpu=G5 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G5 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G5 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G5 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G5`
- `gcc -funroll-loops -m64 -mcpu=G4 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G4 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G4 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G4 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G4`
- `gcc -funroll-loops -m64 -mcpu=G3 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G3 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G3 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G3 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G3`
- `gcc -funroll-loops -m64 -mcpu=G5 -maltivec -O3 -fomit-frame-pointer`

- `gcc -funroll-loops -m64 -mcpu=G5 -maltivec -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G5 -maltivec -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G5 -maltivec -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G5 -maltivec`
- `gcc -funroll-loops -m64 -mcpu=G4 -maltivec -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G4 -maltivec -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G4 -maltivec -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G4 -maltivec -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G4 -maltivec`
- `gcc -funroll-loops -m64 -mcpu=G3 -maltivec -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G3 -maltivec -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G3 -maltivec -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G3 -maltivec -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -mcpu=G3 -maltivec`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G5 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G5 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G5 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G5 -O -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G5`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G4 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G4 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G4 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G4 -O -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G4`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G3 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G3 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G3 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G3 -O -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G3`

- `gcc -funroll-loops -mpowerpc64 -mcpu=G5 -maltivec -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G5 -maltivec -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G5 -maltivec -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G5 -maltivec -O -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G5 -maltivec`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G4 -maltivec -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G4 -maltivec -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G4 -maltivec -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G4 -maltivec -O -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G4 -maltivec`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G3 -maltivec -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G3 -maltivec -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G3 -maltivec -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G3 -maltivec -O -fomit-frame-pointer`
- `gcc -funroll-loops -mpowerpc64 -mcpu=G3 -maltivec`
- `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=k8 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=k8`
- `gcc -funroll-loops -m64 -march=athlon-sse -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=athlon-sse -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=athlon-sse -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=athlon-sse -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=athlon-sse`
- `gcc -funroll-loops -m64 -march=athlon -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=athlon -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=athlon -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=athlon -O -fomit-frame-pointer`

- gcc -funroll-loops -m64 -march=athlon
- gcc -funroll-loops -m64 -march=k6-3 -O3 -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=k6-3 -Os -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=k6-3 -O2 -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=k6-3 -O -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=k6-3
- gcc -funroll-loops -m64 -march=k6-2 -O3 -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=k6-2 -Os -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=k6-2 -O2 -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=k6-2 -O -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=k6-2
- gcc -funroll-loops -m64 -march=k6 -O3 -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=k6 -Os -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=k6 -O2 -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=k6 -O -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=k6
- gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=nocona -Os -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=nocona -O2 -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=nocona -O -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=nocona
- gcc -funroll-loops -m64 -march=prescott -O3 -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=prescott -Os -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=prescott -O2 -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=prescott -O -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=prescott
- gcc -funroll-loops -m64 -march=pentium-m -O3 -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=pentium-m -Os -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=pentium-m -O2 -fomit-frame-pointer

- `gcc -funroll-loops -m64 -march=pentium-m -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=pentium-m`
- `gcc -funroll-loops -m64 -march=pentium4 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=pentium4 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=pentium4 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=pentium4 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=pentium4`
- `gcc -funroll-loops -m64 -march=pentium3 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=pentium3 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=pentium3 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=pentium3 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=pentium3`
- `gcc -funroll-loops -m64 -march=pentium2 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=pentium2 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=pentium2 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=pentium2 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=pentium2`
- `gcc -funroll-loops -m64 -march=pentiumpro -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=pentiumpro -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=pentiumpro -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=pentiumpro -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=pentiumpro`
- `gcc -funroll-loops -m64 -march=pentium-mmx -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=pentium-mmx -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=pentium-mmx -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=pentium-mmx -O -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=pentium-mmx`
- `gcc -funroll-loops -m64 -march=pentium -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m64 -march=pentium -Os -fomit-frame-pointer`

- gcc -funroll-loops -m64 -march=pentium -O2 -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=pentium -O -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=pentium
- gcc -funroll-loops -m64 -march=i486 -O3 -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=i486 -Os -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=i486 -O2 -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=i486 -O -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=i486
- gcc -funroll-loops -m64 -march=i386 -O3 -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=i386 -Os -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=i386 -O2 -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=i386 -O -fomit-frame-pointer
- gcc -funroll-loops -m64 -march=i386
- gcc -funroll-loops -m32 -O3 -fomit-frame-pointer
- gcc -funroll-loops -m32 -Os -fomit-frame-pointer
- gcc -funroll-loops -m32 -O2 -fomit-frame-pointer
- gcc -funroll-loops -m32 -O -fomit-frame-pointer
- gcc -funroll-loops -m32
- gcc -funroll-loops -m32 -maltivec -O3 -fomit-frame-pointer
- gcc -funroll-loops -m32 -maltivec -Os -fomit-frame-pointer
- gcc -funroll-loops -m32 -maltivec -O2 -fomit-frame-pointer
- gcc -funroll-loops -m32 -maltivec -O -fomit-frame-pointer
- gcc -funroll-loops -m32 -maltivec
- gcc -funroll-loops -m32 -mcpu=ultrasparc3 -O3 -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=ultrasparc3 -Os -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=ultrasparc3 -O2 -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=ultrasparc3 -O -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=ultrasparc3
- gcc -funroll-loops -m32 -mcpu=ultrasparc -O3 -fomit-frame-pointer

- `gcc -funroll-loops -m32 -mcpu=ultrasparc -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ultrasparc -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ultrasparc -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ultrasparc`
- `gcc -funroll-loops -m32 -mcpu=hypersparc -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=hypersparc -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=hypersparc -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=hypersparc -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=hypersparc`
- `gcc -funroll-loops -m32 -mcpu=supersparc -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=supersparc -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=supersparc -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=supersparc -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=supersparc`
- `gcc -funroll-loops -m32 -mcpu=sparclet -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=sparclet -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=sparclet -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=sparclet -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=sparclet`
- `gcc -funroll-loops -m32 -mcpu=sparclite86x -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=sparclite86x -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=sparclite86x -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=sparclite86x -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=sparclite86x`
- `gcc -funroll-loops -m32 -mcpu=sparclite -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=sparclite -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=sparclite -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=sparclite -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=sparclite`

- gcc -funroll-loops -m32 -mcpu=sparc86x -O3 -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=sparc86x -Os -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=sparc86x -O2 -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=sparc86x -O -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=sparc86x
- gcc -funroll-loops -m32 -mcpu=sparc -O3 -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=sparc -Os -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=sparc -O2 -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=sparc -O -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=sparc
- gcc -funroll-loops -m32 -mcpu=v9 -O3 -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=v9 -Os -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=v9 -O2 -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=v9 -O -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=v9
- gcc -funroll-loops -m32 -mcpu=v8 -O3 -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=v8 -Os -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=v8 -O2 -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=v8 -O -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=v8
- gcc -funroll-loops -m32 -mcpu=pca56 -O3 -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=pca56 -Os -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=pca56 -O2 -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=pca56 -O -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=pca56
- gcc -funroll-loops -m32 -mcpu=ev67 -Wa,-mev67 -O3 -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=ev67 -Wa,-mev67 -Os -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=ev67 -Wa,-mev67 -O2 -fomit-frame-pointer
- gcc -funroll-loops -m32 -mcpu=ev67 -Wa,-mev67 -O -fomit-frame-pointer

- `gcc -funroll-loops -m32 -mcpu=ev67 -Wa,-mev67`
- `gcc -funroll-loops -m32 -mcpu=ev6 -Wa,-mev6 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev6 -Wa,-mev6 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev6 -Wa,-mev6 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev6 -Wa,-mev6 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev6 -Wa,-mev6`
- `gcc -funroll-loops -m32 -mcpu=ev56 -Wa,-mev56 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev56 -Wa,-mev56 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev56 -Wa,-mev56 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev56 -Wa,-mev56 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev56 -Wa,-mev56`
- `gcc -funroll-loops -m32 -mcpu=ev5 -Wa,-mev5 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev5 -Wa,-mev5 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev5 -Wa,-mev5 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev5 -Wa,-mev5 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev5 -Wa,-mev5`
- `gcc -funroll-loops -m32 -mcpu=ev4 -Wa,-mev4 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev4 -Wa,-mev4 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev4 -Wa,-mev4 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev4 -Wa,-mev4 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev4 -Wa,-mev4`
- `gcc -funroll-loops -m32 -mcpu=ev67 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev67 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev67 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev67 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev67`
- `gcc -funroll-loops -m32 -mcpu=ev6 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev6 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev6 -O2 -fomit-frame-pointer`

- `gcc -funroll-loops -m32 -mcpu=ev6 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev6`
- `gcc -funroll-loops -m32 -mcpu=ev56 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev56 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev56 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev56 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev56`
- `gcc -funroll-loops -m32 -mcpu=ev5 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev5 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev5 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev5 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev5`
- `gcc -funroll-loops -m32 -mcpu=ev4 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev4 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev4 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev4 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=ev4`
- `gcc -funroll-loops -m32 -mcpu=G5 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G5 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G5 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G5 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G5`
- `gcc -funroll-loops -m32 -mcpu=G4 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G4 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G4 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G4 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G4`
- `gcc -funroll-loops -m32 -mcpu=G3 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G3 -Os -fomit-frame-pointer`

- `gcc -funroll-loops -m32 -mcpu=G3 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G3 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G3`
- `gcc -funroll-loops -m32 -mcpu=G5 -maltivec -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G5 -maltivec -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G5 -maltivec -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G5 -maltivec -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G5 -maltivec`
- `gcc -funroll-loops -m32 -mcpu=G4 -maltivec -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G4 -maltivec -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G4 -maltivec -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G4 -maltivec -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G4 -maltivec`
- `gcc -funroll-loops -m32 -mcpu=G3 -maltivec -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G3 -maltivec -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G3 -maltivec -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G3 -maltivec -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -mcpu=G3 -maltivec`
- `gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=k8 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=k8 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=k8 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=k8`
- `gcc -funroll-loops -m32 -march=athlon-sse -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=athlon-sse -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=athlon-sse -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=athlon-sse -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=athlon-sse`
- `gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer`

- gcc -funroll-loops -m32 -march=athlon -Os -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=athlon -O2 -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=athlon -O -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=athlon
- gcc -funroll-loops -m32 -march=k6-3 -O3 -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=k6-3 -Os -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=k6-3 -O2 -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=k6-3 -O -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=k6-3
- gcc -funroll-loops -m32 -march=k6-2 -O3 -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=k6-2 -Os -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=k6-2 -O2 -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=k6-2 -O -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=k6-2
- gcc -funroll-loops -m32 -march=k6 -O3 -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=k6 -Os -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=k6 -O2 -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=k6 -O -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=k6
- gcc -funroll-loops -m32 -march=nocona -O3 -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=nocona -Os -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=nocona -O2 -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=nocona
- gcc -funroll-loops -m32 -march=prescott -O3 -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=prescott -Os -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=prescott -O2 -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=prescott

- `gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentium-m -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentium-m -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentium-m -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentium-m`
- `gcc -funroll-loops -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentium4 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentium4 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentium4 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentium4`
- `gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentium3 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentium3 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentium3 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentium3`
- `gcc -funroll-loops -m32 -march=pentium2 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentium2 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentium2 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentium2 -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentium2`
- `gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentiumpro -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentiumpro -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentiumpro`
- `gcc -funroll-loops -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentium-mmx -Os -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentium-mmx -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -m32 -march=pentium-mmx -O -fomit-frame-pointer`

- gcc -funroll-loops -m32 -march=pentium-mmx
- gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=pentium -Os -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=pentium -O2 -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=pentium -O -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=pentium
- gcc -funroll-loops -m32 -march=i486 -O3 -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=i486 -Os -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=i486 -O2 -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=i486 -O -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=i486
- gcc -funroll-loops -m32 -march=i386 -O3 -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=i386 -Os -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=i386 -O2 -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=i386 -O -fomit-frame-pointer
- gcc -funroll-loops -m32 -march=i386
- gcc -funroll-loops -O3 -fomit-frame-pointer
- gcc -funroll-loops -Os -fomit-frame-pointer
- gcc -funroll-loops -O2 -fomit-frame-pointer
- gcc -funroll-loops -O -fomit-frame-pointer
- gcc -funroll-loops
- gcc -funroll-loops -maltivec -O3 -fomit-frame-pointer
- gcc -funroll-loops -maltivec -Os -fomit-frame-pointer
- gcc -funroll-loops -maltivec -O2 -fomit-frame-pointer
- gcc -funroll-loops -maltivec -O -fomit-frame-pointer
- gcc -funroll-loops -maltivec
- gcc -funroll-loops -mcpu=ultrasparc3 -O3 -fomit-frame-pointer
- gcc -funroll-loops -mcpu=ultrasparc3 -Os -fomit-frame-pointer
- gcc -funroll-loops -mcpu=ultrasparc3 -O2 -fomit-frame-pointer

- `gcc -funroll-loops -mcpu=ultrasparc3 -O -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ultrasparc3`
- `gcc -funroll-loops -mcpu=ultrasparc -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ultrasparc -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ultrasparc -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ultrasparc -O -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ultrasparc`
- `gcc -funroll-loops -mcpu=hypersparc -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=hypersparc -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=hypersparc -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=hypersparc -O -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=hypersparc`
- `gcc -funroll-loops -mcpu=supersparc -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=supersparc -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=supersparc -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=supersparc -O -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=supersparc`
- `gcc -funroll-loops -mcpu=sparclet -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=sparclet -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=sparclet -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=sparclet -O -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=sparclet`
- `gcc -funroll-loops -mcpu=sparclite86x -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=sparclite86x -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=sparclite86x -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=sparclite86x -O -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=sparclite86x`
- `gcc -funroll-loops -mcpu=sparclite -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=sparclite -Os -fomit-frame-pointer`

- gcc -funroll-loops -mcpu=sparclite -O2 -fomit-frame-pointer
- gcc -funroll-loops -mcpu=sparclite -O -fomit-frame-pointer
- gcc -funroll-loops -mcpu=sparclite
- gcc -funroll-loops -mcpu=sparc86x -O3 -fomit-frame-pointer
- gcc -funroll-loops -mcpu=sparc86x -Os -fomit-frame-pointer
- gcc -funroll-loops -mcpu=sparc86x -O2 -fomit-frame-pointer
- gcc -funroll-loops -mcpu=sparc86x -O -fomit-frame-pointer
- gcc -funroll-loops -mcpu=sparc86x
- gcc -funroll-loops -mcpu=sparc -O3 -fomit-frame-pointer
- gcc -funroll-loops -mcpu=sparc -Os -fomit-frame-pointer
- gcc -funroll-loops -mcpu=sparc -O2 -fomit-frame-pointer
- gcc -funroll-loops -mcpu=sparc -O -fomit-frame-pointer
- gcc -funroll-loops -mcpu=sparc
- gcc -funroll-loops -mcpu=v9 -O3 -fomit-frame-pointer
- gcc -funroll-loops -mcpu=v9 -Os -fomit-frame-pointer
- gcc -funroll-loops -mcpu=v9 -O2 -fomit-frame-pointer
- gcc -funroll-loops -mcpu=v9 -O -fomit-frame-pointer
- gcc -funroll-loops -mcpu=v9
- gcc -funroll-loops -mcpu=v8 -O3 -fomit-frame-pointer
- gcc -funroll-loops -mcpu=v8 -Os -fomit-frame-pointer
- gcc -funroll-loops -mcpu=v8 -O2 -fomit-frame-pointer
- gcc -funroll-loops -mcpu=v8 -O -fomit-frame-pointer
- gcc -funroll-loops -mcpu=v8
- gcc -funroll-loops -mcpu=pca56 -O3 -fomit-frame-pointer
- gcc -funroll-loops -mcpu=pca56 -Os -fomit-frame-pointer
- gcc -funroll-loops -mcpu=pca56 -O2 -fomit-frame-pointer
- gcc -funroll-loops -mcpu=pca56 -O -fomit-frame-pointer
- gcc -funroll-loops -mcpu=pca56
- gcc -funroll-loops -mcpu=ev67 -Wa,-mev67 -O3 -fomit-frame-pointer

- `gcc -funroll-loops -mcpu=ev67 -Wa,-mev67 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev67 -Wa,-mev67 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev67 -Wa,-mev67 -O -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev67 -Wa,-mev67`
- `gcc -funroll-loops -mcpu=ev6 -Wa,-mev6 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev6 -Wa,-mev6 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev6 -Wa,-mev6 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev6 -Wa,-mev6 -O -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev6 -Wa,-mev6`
- `gcc -funroll-loops -mcpu=ev56 -Wa,-mev56 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev56 -Wa,-mev56 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev56 -Wa,-mev56 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev56 -Wa,-mev56 -O -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev56 -Wa,-mev56`
- `gcc -funroll-loops -mcpu=ev5 -Wa,-mev5 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev5 -Wa,-mev5 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev5 -Wa,-mev5 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev5 -Wa,-mev5 -O -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev5 -Wa,-mev5`
- `gcc -funroll-loops -mcpu=ev4 -Wa,-mev4 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev4 -Wa,-mev4 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev4 -Wa,-mev4 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev4 -Wa,-mev4 -O -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev4 -Wa,-mev4`
- `gcc -funroll-loops -mcpu=ev67 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev67 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev67 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev67 -O -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev67`

- `gcc -funroll-loops -mcpu=ev6 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev6 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev6 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev6 -O -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev6`
- `gcc -funroll-loops -mcpu=ev56 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev56 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev56 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev56 -O -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev56`
- `gcc -funroll-loops -mcpu=ev5 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev5 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev5 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev5 -O -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev5`
- `gcc -funroll-loops -mcpu=ev4 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev4 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev4 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev4 -O -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=ev4`
- `gcc -funroll-loops -mcpu=G5 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G5 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G5 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G5 -O -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G5`
- `gcc -funroll-loops -mcpu=G4 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G4 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G4 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G4 -O -fomit-frame-pointer`

- `gcc -funroll-loops -mcpu=G4`
- `gcc -funroll-loops -mcpu=G3 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G3 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G3 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G3 -O -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G3`
- `gcc -funroll-loops -mcpu=G5 -maltivec -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G5 -maltivec -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G5 -maltivec -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G5 -maltivec -O -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G5 -maltivec`
- `gcc -funroll-loops -mcpu=G4 -maltivec -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G4 -maltivec -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G4 -maltivec -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G4 -maltivec -O -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G4 -maltivec`
- `gcc -funroll-loops -mcpu=G3 -maltivec -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G3 -maltivec -Os -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G3 -maltivec -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G3 -maltivec -O -fomit-frame-pointer`
- `gcc -funroll-loops -mcpu=G3 -maltivec`
- `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -march=k8 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -march=k8 -O -fomit-frame-pointer`
- `gcc -funroll-loops -march=k8`
- `gcc -funroll-loops -march=athlon-sse -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -march=athlon-sse -Os -fomit-frame-pointer`
- `gcc -funroll-loops -march=athlon-sse -O2 -fomit-frame-pointer`

- gcc -funroll-loops -march=athlon-sse -O -fomit-frame-pointer
- gcc -funroll-loops -march=athlon-sse
- gcc -funroll-loops -march=athlon -O3 -fomit-frame-pointer
- gcc -funroll-loops -march=athlon -Os -fomit-frame-pointer
- gcc -funroll-loops -march=athlon -O2 -fomit-frame-pointer
- gcc -funroll-loops -march=athlon -O -fomit-frame-pointer
- gcc -funroll-loops -march=athlon
- gcc -funroll-loops -march=k6-3 -O3 -fomit-frame-pointer
- gcc -funroll-loops -march=k6-3 -Os -fomit-frame-pointer
- gcc -funroll-loops -march=k6-3 -O2 -fomit-frame-pointer
- gcc -funroll-loops -march=k6-3 -O -fomit-frame-pointer
- gcc -funroll-loops -march=k6-3
- gcc -funroll-loops -march=k6-2 -O3 -fomit-frame-pointer
- gcc -funroll-loops -march=k6-2 -Os -fomit-frame-pointer
- gcc -funroll-loops -march=k6-2 -O2 -fomit-frame-pointer
- gcc -funroll-loops -march=k6-2 -O -fomit-frame-pointer
- gcc -funroll-loops -march=k6-2
- gcc -funroll-loops -march=k6 -O3 -fomit-frame-pointer
- gcc -funroll-loops -march=k6 -Os -fomit-frame-pointer
- gcc -funroll-loops -march=k6 -O2 -fomit-frame-pointer
- gcc -funroll-loops -march=k6 -O -fomit-frame-pointer
- gcc -funroll-loops -march=k6
- gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer
- gcc -funroll-loops -march=nocona -Os -fomit-frame-pointer
- gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer
- gcc -funroll-loops -march=nocona -O -fomit-frame-pointer
- gcc -funroll-loops -march=nocona
- gcc -funroll-loops -march=prescott -O3 -fomit-frame-pointer
- gcc -funroll-loops -march=prescott -Os -fomit-frame-pointer

- `gcc -funroll-loops -march=prescott -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -march=prescott -O -fomit-frame-pointer`
- `gcc -funroll-loops -march=prescott`
- `gcc -funroll-loops -march=pentium-m -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium-m -Os -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium-m -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium-m -O -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium-m`
- `gcc -funroll-loops -march=pentium4 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium4 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium4 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium4`
- `gcc -funroll-loops -march=pentium3 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium3 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium3 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium3 -O -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium3`
- `gcc -funroll-loops -march=pentium2 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium2 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium2 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium2 -O -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium2`
- `gcc -funroll-loops -march=pentiumpro -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentiumpro -Os -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentiumpro -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentiumpro -O -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentiumpro`
- `gcc -funroll-loops -march=pentium-mmx -O3 -fomit-frame-pointer`

- `gcc -funroll-loops -march=pentium-mmx -Os -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium-mmx -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium-mmx -O -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium-mmx`
- `gcc -funroll-loops -march=pentium -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium -Os -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium -O -fomit-frame-pointer`
- `gcc -funroll-loops -march=pentium`
- `gcc -funroll-loops -march=i486 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -march=i486 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -march=i486 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -march=i486 -O -fomit-frame-pointer`
- `gcc -funroll-loops -march=i486`
- `gcc -funroll-loops -march=i386 -O3 -fomit-frame-pointer`
- `gcc -funroll-loops -march=i386 -Os -fomit-frame-pointer`
- `gcc -funroll-loops -march=i386 -O2 -fomit-frame-pointer`
- `gcc -funroll-loops -march=i386 -O -fomit-frame-pointer`
- `gcc -funroll-loops -march=i386`

The compilers listed above are C compilers. Each C compiler also has an associated C++ compiler; for example, the C compiler `gcc -m64` is associated to the C++ compiler `g++ -m64`.

Chapter 5

Which compilers produced the best results?

5.1 Introduction

This chapter presents a list of primitives and, for each primitive, the compiler that produced the best performance for that primitive. When there are several implementations of one primitive, each implementation appears separately in the list. Each implementation is preceded by a number that indicates the time taken by the implementation, compared to the time taken by the best implementation.

For example, the two list entries

- 1.00: `crypto_hash/sha256/ref`
  using `gcc -m64 -march=nocona -O -fomit-frame-pointer`
- 1.63: `crypto_hash/sha256/openssl`
  using `gcc -march=nocona`

indicate that `gcc -m64 -march=nocona -O -fomit-frame-pointer` was the best compiler for `crypto_hash/sha256/ref` for a standard hashing operation; that `gcc -march=nocona` was the best compiler for `crypto_hash/sha256/openssl`; and that `crypto_hash/sha256/ref` compiled with `gcc -m64 -march=nocona -O -fomit-frame-pointer` was 1.63× faster than `crypto_hash/sha256/openssl` compiled with `gcc -march=nocona`. The standard hashing operation is hashing 1536 bytes.

There is a separate list for each computer. Some computers included in this report used a limited selection of compilers; VAMPIRE will continue to update its benchmark reports online.

5.2 amd64, 1403MHz, AMD Opteron 240 (f58), `nmisles8amd64`

- 1.00: `crypto_dh/claus/openssl`
  using `gcc -march=pentium`
- 1.00: `crypto_dh/gls1271/ref`
  using `gcc -O3 -fomit-frame-pointer`

- 1.00: crypto_encrypt/mceliece/ref
  using gcc -funroll-loops -m64 -march=i386 -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ntruees787ep1/ref
  using gcc -funroll-loops -m64 -march=k6-3 -Os -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald1024/openssl
  using gcc -funroll-loops -march=athlon -Os -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald1536/openssl
  using gcc -march=k6-3 -O -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald2048/openssl
  using gcc -m64 -march=k6 -Os -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald3072/openssl
  using gcc -march=pentium2 -O2 -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald4096/openssl
  using gcc -m64 -march=pentium4 -O2 -fomit-frame-pointer
- 1.00: crypto_hash/md2/openssl
  using gcc -m64 -march=athlon -O2 -fomit-frame-pointer
- 1.00: crypto_hash/md4/openssl
  using gcc -funroll-loops -m64 -march=k6-3 -O2 -fomit-frame-pointer
- 1.00: crypto_hash/md5/ref
  using gcc -funroll-loops -m64 -march=k6-3 -O2 -fomit-frame-pointer
- 2.23: crypto_hash/md5/openssl
  using gcc -m64 -march=athlon -O2 -fomit-frame-pointer
- 1.00: crypto_hash/ripemd160/openssl
  using gcc -funroll-loops -m64 -march=k6-3 -O2 -fomit-frame-pointer
- 1.00: crypto_hash/sha1/openssl
  using gcc -m64 -march=athlon -O -fomit-frame-pointer
- 1.00: crypto_hash/sha256/ref
  using gcc -funroll-loops -march=pentium -O -fomit-frame-pointer
- 1.00: crypto_hash/sha512/ref
  using gcc -funroll-loops -m64 -march=k6-3 -O -fomit-frame-pointer
- 1.00: crypto_hash/whirlpool/ref
  using gcc -funroll-loops -m64 -march=pentium4 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/md5/amd64-1
  using gcc -funroll-loops -m64 -march=k6-3 -O3 -fomit-frame-pointer
- 1.51: crypto_hashblocks/md5/little-1
  using gcc -funroll-loops -m64 -march=k6-3 -Os -fomit-frame-pointer

- 1.71: `crypto_hashblocks/md5/ref`
  using `gcc -funroll-loops -march=pentium4 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha256/ref`
  using `gcc -m64 -march=i486 -Os -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha512/ref`
  using `gcc -funroll-loops -m64 -march=i386 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/donald1024/openssl`
  using `gcc -funroll-loops -m64 -march=k6 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/donald2048/openssl`
  using `gcc -m64 -march=i486 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/donald512/openssl`
  using `gcc -funroll-loops -march=i386 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1024/openssl`
  using `gcc -funroll-loops -m64 -march=k6-3 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1536/openssl`
  using `gcc -funroll-loops -m64 -march=k6-2 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald2048/openssl`
  using `gcc -funroll-loops -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald3072/openssl`
  using `gcc -march=pentium2 -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald4096/openssl`
  using `gcc -m64 -march=athlon -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald512/openssl`
  using `gcc -march=athlon -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald768/openssl`
  using `gcc -funroll-loops -march=k6 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -march=i386 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/bernstein/amd64-1`
  using `gcc -m64 -march=pentium3 -O2 -fomit-frame-pointer`
- 1.02: `crypto_stream/aes128estream/e/bernstein/amd64-2`
  using `gcc -m64 -march=pentium3 -O2 -fomit-frame-pointer`
- 1.06: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -funroll-loops -march=pentium4 -O3 -fomit-frame-pointer`
- 1.13: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -funroll-loops -march=pentium4 -O3 -fomit-frame-pointer`

- 1.39: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -funroll-loops -m64 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.48: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -O2 -fomit-frame-pointer`
- 1.50: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -funroll-loops -m64 -march=i486 -O3 -fomit-frame-pointer`
- 1.52: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -funroll-loops -m64 -march=athlon -O3 -fomit-frame-pointer`
- 1.58: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -funroll-loops -m64 -march=athlon -O2 -fomit-frame-pointer`
- 1.67: `crypto_stream/aes128estream/e/gladman`
  using `gcc -m64 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -funroll-loops -march=pentium4 -O3 -fomit-frame-pointer`
- 1.06: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -funroll-loops -m64 -march=athlon -O3 -fomit-frame-pointer`
- 1.47: `crypto_stream/aes256estream/e/gladman`
  using `gcc -m64 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/amd64-3`
  using `gcc -funroll-loops -m64 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.22: `crypto_stream/chacha12/e/amd64-xmm6`
  using `gcc -funroll-loops -m64 -march=k6-3 -O2 -fomit-frame-pointer`
- 1.25: `crypto_stream/chacha12/e/merged`
  using `gcc -m64 -march=athlon -Os -fomit-frame-pointer`
- 1.73: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -m64 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.91: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -m64 -march=k6-3 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/amd64-3`
  using `gcc -funroll-loops -m64 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.20: `crypto_stream/chacha20/e/amd64-xmm6`
  using `gcc -funroll-loops -m64 -march=k6-3 -O2 -fomit-frame-pointer`
- 1.29: `crypto_stream/chacha20/e/merged`
  using `gcc -m64 -march=athlon -Os -fomit-frame-pointer`
- 1.63: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -m64 -march=k6-3 -O3 -fomit-frame-pointer`

- 1.67: `crypto_stream/chacha20/e/ref`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/amd64-3`
  using `gcc -funroll-loops -m64 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.25: `crypto_stream/chacha8/e/amd64-xmm6`
  using `gcc -funroll-loops -m64 -march=k6-3 -O2 -fomit-frame-pointer`
- 1.25: `crypto_stream/chacha8/e/merged`
  using `gcc -m64 -march=athlon -Os -fomit-frame-pointer`
- 1.89: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -m64 -march=k6-3 -O3 -fomit-frame-pointer`
- 2.18: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -m64 -march=pentium4 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -m64 -march=athlon -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -funroll-loops -m64 -march=pentium4 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -funroll-loops -m64 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -funroll-loops -m64 -march=k6-2 -O2 -fomit-frame-pointer`
- 1.29: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -funroll-loops -march=k6 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -funroll-loops -m64 -march=k6-3 -O -fomit-frame-pointer`
- 1.01: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -m64 -march=pentium4 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/schwabe/amd64-1`
  using `gcc -funroll-loops -m64 -march=k6-3 -Os -fomit-frame-pointer`
- 1.33: `crypto_stream/lexv2/e/v2/schwabe/amd64-2`
  using `gcc -funroll-loops -m64 -march=i486 -O3 -fomit-frame-pointer`
- 1.42: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -funroll-loops -m64 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -m64 -march=k6-3 -O3 -fomit-frame-pointer`
- 2.09: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -march=pentium3 -O3 -fomit-frame-pointer`

- 1.00: crypto_stream/rabbit/e/opt/1/2
  using gcc -funroll-loops -m64 -march=pentium4 -Os -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/1/3
  using gcc -funroll-loops -m64 -march=pentium4 -Os -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/1/4
  using gcc -funroll-loops -m64 -march=pentium4 -Os -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/2/2
  using gcc -funroll-loops -m64 -march=pentium4 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/2/3
  using gcc -funroll-loops -m64 -march=pentium4 -O2 -fomit-frame-pointer
- 1.47: crypto_stream/rabbit/e/opt/1/1
  using gcc -funroll-loops -m64 -march=k6-3 -O3 -fomit-frame-pointer
- 1.47: crypto_stream/rabbit/e/opt/2/1
  using gcc -funroll-loops -m64 -march=k6-3 -O3 -fomit-frame-pointer
- 1.84: crypto_stream/rabbit/e/ref
  using gcc -funroll-loops -m64 -march=i386 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/salsa20/e/amd64-3
  using gcc -funroll-loops -m64 -march=pentium3 -O2 -fomit-frame-pointer
- 1.07: crypto_stream/salsa20/e/merged
  using gcc -m64 -march=i386 -O3 -fomit-frame-pointer
- 1.12: crypto_stream/salsa20/e/amd64-2
  using gcc -m64 -march=pentium-mmx -O3 -fomit-frame-pointer
- 1.21: crypto_stream/salsa20/e/amd64-xmm6
  using gcc -funroll-loops -m64 -march=pentium3 -Os -fomit-frame-pointer
- 1.31: crypto_stream/salsa20/e/amd64-1
  using gcc -funroll-loops -m64 -march=k6-3 -O2 -fomit-frame-pointer
- 1.36: crypto_stream/salsa20/e/regs
  using gcc -funroll-loops -m64 -march=k6 -O3 -fomit-frame-pointer
- 1.37: crypto_stream/salsa20/e/amd64-xmm5
  using gcc -m64 -march=i386 -O3 -fomit-frame-pointer
- 1.47: crypto_stream/salsa20/e/amd64-xmm2
  using gcc -m64 -march=pentium-mmx -O -fomit-frame-pointer
- 1.48: crypto_stream/salsa20/e/ref
  using gcc -funroll-loops -march=k6-3 -O3 -fomit-frame-pointer
- 1.55: crypto_stream/salsa20/ref
  using gcc -m64 -march=pentium-mmx -O3 -fomit-frame-pointer

- 1.62: `crypto_stream/salsa20/e/amd64-xmm`
  using `gcc -funroll-loops -m64 -march=athlon -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/amd64-3`
  using `gcc -funroll-loops -m64 -march=pentium3 -Os -fomit-frame-pointer`
- 1.06: `crypto_stream/salsa2012/e/merged`
  using `gcc -m64 -march=i386 -O2 -fomit-frame-pointer`
- 1.09: `crypto_stream/salsa2012/e/amd64-2`
  using `gcc -m64 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.22: `crypto_stream/salsa2012/e/amd64-xmm6`
  using `gcc -funroll-loops -m64 -march=k6 -O2 -fomit-frame-pointer`
- 1.27: `crypto_stream/salsa2012/e/amd64-1`
  using `gcc -funroll-loops -m64 -march=k6-3 -O2 -fomit-frame-pointer`
- 1.39: `crypto_stream/salsa2012/e/amd64-xmm5`
  using `gcc -m64 -march=i386 -O3 -fomit-frame-pointer`
- 1.47: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -m64 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.48: `crypto_stream/salsa2012/e/amd64-xmm2`
  using `gcc -m64 -march=pentium-mmx -O -fomit-frame-pointer`
- 1.61: `crypto_stream/salsa2012/e/amd64-xmm`
  using `gcc -funroll-loops -m64 -march=athlon -Os -fomit-frame-pointer`
- 1.69: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -m64 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.77: `crypto_stream/salsa2012/ref`
  using `gcc -m64 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/amd64-3`
  using `gcc -funroll-loops -m64 -march=pentium3 -Os -fomit-frame-pointer`
- 1.06: `crypto_stream/salsa208/e/merged`
  using `gcc -funroll-loops -m64 -march=i386 -O3 -fomit-frame-pointer`
- 1.09: `crypto_stream/salsa208/e/amd64-2`
  using `gcc -m64 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.24: `crypto_stream/salsa208/e/amd64-xmm6`
  using `gcc -funroll-loops -m64 -march=k6-3 -O2 -fomit-frame-pointer`
- 1.26: `crypto_stream/salsa208/e/amd64-1`
  using `gcc -funroll-loops -m64 -march=k6-3 -O2 -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa208/e/amd64-xmm5`
  using `gcc -m64 -march=i386 -O3 -fomit-frame-pointer`

- 1.48: crypto_stream/salsa208/e/amd64-xmm2
  using gcc -m64 -march=pentium-mmx -O -fomit-frame-pointer
- 1.60: crypto_stream/salsa208/e/amd64-xmm
  using gcc -funroll-loops -m64 -march=athlon -Os -fomit-frame-pointer
- 1.62: crypto_stream/salsa208/e/regs
  using gcc -funroll-loops -m64 -march=k6-3 -O3 -fomit-frame-pointer
- 1.96: crypto_stream/salsa208/e/ref
  using gcc -funroll-loops -m64 -march=pentium3 -Os -fomit-frame-pointer
- 2.00: crypto_stream/salsa208/ref
  using gcc -m64 -march=i386 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -funroll-loops -m64 -march=k6-3 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -m64 -march=athlon -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpy/e/tpy
  using gcc -funroll-loops -m64 -march=k6-3 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpy6/e/tpy6
  using gcc -funroll-loops -m64 -march=athlon -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpypy/e/tpypy
  using gcc -m64 -march=pentium4 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/trivium/e/submissions/trivium
  using gcc -march=i386 -O2 -fomit-frame-pointer

5.3 amd64, 2400MHz, Intel Core 2 Duo (6fb), utrecht

- 1.00: crypto_dh/claus/gmp
  using g++ -m64 -O3 -fomit-frame-pointer
- 1.21: crypto_dh/claus/openssl
  using gcc -funroll-loops -march=k8 -Os -fomit-frame-pointer
- 1.00: crypto_dh/curve2251/mpfq
  using gcc -funroll-loops -m64 -Os -fomit-frame-pointer
- 1.00: crypto_dh/curve25519/mpfq
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_dh/gls1271/ref
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_dh/hector/ref
  using gcc -funroll-loops -m64 -O3 -fomit-frame-pointer

- 1.00: `crypto_dh/surf127eps/mpfq`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_dh/surf2113/mpfq`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/mceliece/ref`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `gcc -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- 1.03: `crypto_hash/md5/openssl`
  using `gcc -m64 -O -fomit-frame-pointer`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -m64 -march=k8`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha224/openssl`
  using `gcc -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.07: `crypto_hash/sha256/openssl`
  using `gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer`

- 1.00: crypto_hash/sha384/openssl
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/sha512/ref
  using gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer
- 1.04: crypto_hash/sha512/openssl
  using gcc -march=nocona -O2 -fomit-frame-pointer
- 1.00: crypto_hash/whirlpool/ref
  using gcc -march=k8 -O -fomit-frame-pointer
- 1.00: crypto_hashblocks/md5/amd64-1
  using gcc -funroll-loops -m64 -Os -fomit-frame-pointer
- 1.06: crypto_hashblocks/md5/little-1
  using gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer
- 1.17: crypto_hashblocks/md5/ref
  using gcc -march=nocona -O -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha256/ref
  using gcc -march=nocona -Os -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha512/ref
  using gcc -funroll-loops -march=nocona -Os -fomit-frame-pointer
- 1.00: crypto_sign/donald1024/openssl
  using gcc -funroll-loops -O -fomit-frame-pointer
- 1.00: crypto_sign/donald2048/openssl
  using gcc -m64 -O2 -fomit-frame-pointer
- 1.00: crypto_sign/donald512/openssl
  using gcc -m64 -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ecdonaldb163/openssl
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ecdonaldb233/openssl
  using gcc -funroll-loops -m64 -Os -fomit-frame-pointer
- 1.00: crypto_sign/ecdonaldb283/openssl
  using gcc -funroll-loops -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ecdonaldb409/openssl
  using gcc -funroll-loops -Os -fomit-frame-pointer
- 1.00: crypto_sign/ecdonaldb571/openssl
  using gcc -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ecdonaldk163/openssl
  using gcc -m64 -march=nocona -O -fomit-frame-pointer

- 1.00: `crypto_sign/ecdonaldk233/openssl`
  using `gcc -m64 -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldk283/openssl`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldk409/openssl`
  using `gcc -march=nocona -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldk571/openssl`
  using `gcc -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldp160/openssl`
  using `gcc -funroll-loops -m64 -march=nocona -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldp192/openssl`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldp224/openssl`
  using `gcc -funroll-loops`
- 1.00: `crypto_sign/ecdonaldp256/openssl`
  using `gcc -funroll-loops -m64 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldp384/openssl`
  using `gcc -m64 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldp521/openssl`
  using `gcc -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/hector/ref`
  using `gcc -funroll-loops -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/rainbow/ref`
  using `g++ -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1024/openssl`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1536/openssl`
  using `gcc -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald2048/openssl`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald3072/openssl`
  using `gcc -funroll-loops -m64 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald4096/openssl`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald512/openssl`
  using `gcc -m64 -march=nocona -O3 -fomit-frame-pointer`

- 1.00: `crypto_sign/ronald768/openssl`
  using `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -funroll-loops -march=nocona -Os -fomit-frame-pointer`
- 1.02: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.12: `crypto_stream/aes128estream/e/bernstein/amd64-2`
  using `gcc -funroll-loops -m64`
- 1.17: `crypto_stream/aes128estream/e/bernstein/amd64-1`
  using `gcc -m64 -march=nocona -Os -fomit-frame-pointer`
- 1.31: `crypto_stream/aes128estream/e/gladman`
  using `gcc -m64 -march=nocona -Os -fomit-frame-pointer`
- 1.58: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -funroll-loops -m64 -O3 -fomit-frame-pointer`
- 1.67: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.70: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -march=k8 -O3 -fomit-frame-pointer`
- 1.70: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.88: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.02: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- 1.22: `crypto_stream/aes256estream/e/gladman`
  using `gcc -m64 -march=nocona -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/amd64-xmm6`
  using `gcc -m64 -Os -fomit-frame-pointer`
- 1.83: `crypto_stream/chacha12/e/amd64-3`
  using `gcc -O3 -fomit-frame-pointer`
- 2.47: `crypto_stream/chacha12/e/merged`
  using `gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer`

- 3.13: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -march=k8 -Os -fomit-frame-pointer`
- 3.98: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/amd64-xmm6`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.89: `crypto_stream/chacha20/e/amd64-3`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- 2.49: `crypto_stream/chacha20/e/merged`
  using `gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer`
- 2.87: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 3.74: `crypto_stream/chacha20/e/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/amd64-xmm6`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.75: `crypto_stream/chacha8/e/amd64-3`
  using `gcc -march=k8 -O3 -fomit-frame-pointer`
- 2.30: `crypto_stream/chacha8/e/merged`
  using `gcc -funroll-loops -O -fomit-frame-pointer`
- 3.10: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -m64 -O3 -fomit-frame-pointer`
- 4.13: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- 1.04: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`

- 1.01: crypto_stream/hc256/e/hc-256/200701
  using gcc -funroll-loops -m64 -march=k8 -O -fomit-frame-pointer
- 1.00: crypto_stream/lexv2/e/v2/schwabe/amd64-1
  using gcc -m64 -march=nocona
- 1.00: crypto_stream/lexv2/e/v2/schwabe/amd64-2
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.07: crypto_stream/lexv2/e/v2/ref
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/nlsv2/e/v2/sync/2
  using gcc -O3 -fomit-frame-pointer
- 1.90: crypto_stream/nlsv2/e/v2/sync/1
  using gcc -funroll-loops -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/1/2
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/2/3
  using gcc -m64 -march=k8 -Os -fomit-frame-pointer
- 1.01: crypto_stream/rabbit/e/opt/1/3
  using gcc -Os -fomit-frame-pointer
- 1.01: crypto_stream/rabbit/e/opt/1/4
  using gcc -march=nocona -O3 -fomit-frame-pointer
- 1.01: crypto_stream/rabbit/e/opt/2/2
  using gcc -m64 -march=nocona -O3 -fomit-frame-pointer
- 1.29: crypto_stream/rabbit/e/opt/1/1
  using gcc -march=k8 -Os -fomit-frame-pointer
- 1.29: crypto_stream/rabbit/e/opt/2/1
  using gcc -m64 -march=nocona -O -fomit-frame-pointer
- 1.38: crypto_stream/rabbit/e/ref
  using gcc -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_stream/salsa20/e/amd64-xmm6
  using gcc -m64 -march=nocona -Os -fomit-frame-pointer
- 1.12: crypto_stream/salsa20/e/amd64-xmm5
  using gcc -funroll-loops -march=nocona -Os -fomit-frame-pointer
- 1.63: crypto_stream/salsa20/e/amd64-xmm2
  using gcc -march=nocona
- 1.83: crypto_stream/salsa20/e/amd64-3
  using gcc -m64 -march=nocona

- 1.89: `crypto_stream/salsa20/e/amd64-2`
  using `gcc -m64 -march=nocona -O -fomit-frame-pointer`
- 1.92: `crypto_stream/salsa20/e/amd64-xmm`
  using `gcc -march=k8`
- 2.34: `crypto_stream/salsa20/e/merged`
  using `gcc -m64 -march=nocona -O3 -fomit-frame-pointer`
- 2.51: `crypto_stream/salsa20/e/amd64-1`
  using `gcc -march=k8 -O -fomit-frame-pointer`
- 2.56: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 3.02: `crypto_stream/salsa20/ref`
  using `gcc -march=k8 -O3 -fomit-frame-pointer`
- 3.37: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/amd64-xmm6`
  using `gcc -m64 -march=nocona -O2 -fomit-frame-pointer`
- 1.11: `crypto_stream/salsa2012/e/amd64-xmm5`
  using `gcc -funroll-loops -march=nocona -O -fomit-frame-pointer`
- 1.58: `crypto_stream/salsa2012/e/amd64-xmm2`
  using `gcc -march=nocona`
- 1.76: `crypto_stream/salsa2012/e/amd64-3`
  using `gcc -funroll-loops -m64 -march=nocona`
- 1.82: `crypto_stream/salsa2012/e/amd64-2`
  using `gcc -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.85: `crypto_stream/salsa2012/e/amd64-xmm`
  using `gcc -m64 -march=k8`
- 2.25: `crypto_stream/salsa2012/e/merged`
  using `gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer`
- 2.39: `crypto_stream/salsa2012/e/amd64-1`
  using `gcc -m64 -Os -fomit-frame-pointer`
- 2.82: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 3.46: `crypto_stream/salsa2012/ref`
  using `gcc -march=k8 -Os -fomit-frame-pointer`
- 3.62: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -m64 -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/salsa208/e/amd64-xmm6`
  using `gcc -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.11: `crypto_stream/salsa208/e/amd64-xmm5`
  using `gcc -O2 -fomit-frame-pointer`
- 1.53: `crypto_stream/salsa208/e/amd64-xmm2`
  using `gcc -m64`
- 1.70: `crypto_stream/salsa208/e/amd64-3`
  using `gcc -m64 -O -fomit-frame-pointer`
- 1.72: `crypto_stream/salsa208/e/amd64-2`
  using `gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.78: `crypto_stream/salsa208/e/amd64-xmm`
  using `gcc -march=k8`
- 2.02: `crypto_stream/salsa208/e/merged`
  using `gcc -funroll-loops -m64 -march=k8 -O -fomit-frame-pointer`
- 2.32: `crypto_stream/salsa208/e/amd64-1`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`
- 2.90: `crypto_stream/salsa208/e/regs`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 3.02: `crypto_stream/salsa208/ref`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`
- 3.60: `crypto_stream/salsa208/e/ref`
  using `gcc -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -funroll-loops -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -m64 -Os -fomit-frame-pointer`

5.4 amd64, 2800MHz, Intel Xeon (f41), nmi0056

- 1.00: crypto_dh/claus/gmp
  using g++ -m64 -O -fomit-frame-pointer
- 1.08: crypto_dh/claus/openssl
  using gcc -funroll-loops -march=k8 -Os -fomit-frame-pointer
- 1.00: crypto_dh/curve2251/mpfq
  using gcc -funroll-loops -m64 -O2 -fomit-frame-pointer
- 1.00: crypto_dh/curve25519/mpfq
  using gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_dh/gls1271/ref
  using gcc -funroll-loops -march=k8 -O -fomit-frame-pointer
- 1.00: crypto_dh/hector/ref
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_dh/surf127eps/mpfq
  using gcc -funroll-loops -m64 -O -fomit-frame-pointer
- 1.00: crypto_dh/surf2113/mpfq
  using gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_encrypt/mceliece/ref
  using gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ntruees787ep1/ref
  using gcc -funroll-loops -m64 -Os -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald1024/openssl
  using gcc -funroll-loops -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald1536/openssl
  using gcc -funroll-loops -m64 -O2 -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald2048/openssl
  using gcc -funroll-loops -m64 -march=nocona -O2 -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald3072/openssl
  using gcc -m64
- 1.00: crypto_encrypt/ronald4096/openssl
  using gcc -march=k8 -O -fomit-frame-pointer
- 1.00: crypto_hash/md2/openssl
  using gcc -m64 -march=k8
- 1.00: crypto_hash/md4/openssl
  using gcc -O3 -fomit-frame-pointer

- 1.00: crypto_hash/md5/ref
  using gcc -funroll-loops -m64 -O3 -fomit-frame-pointer
- 1.10: crypto_hash/md5/openssl
  using gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer
- 1.00: crypto_hash/ripemd160/openssl
  using gcc -m64 -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_hash/sha1/openssl
  using gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer
- 1.00: crypto_hash/sha224/openssl
  using gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_hash/sha256/ref
  using gcc -funroll-loops -m64 -O -fomit-frame-pointer
- 1.64: crypto_hash/sha256/openssl
  using gcc -m64 -march=nocona -O -fomit-frame-pointer
- 1.00: crypto_hash/sha384/openssl
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_hash/sha512/openssl
  using gcc -funroll-loops -Os -fomit-frame-pointer
- 1.01: crypto_hash/sha512/ref
  using gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_hash/whirlpool/ref
  using gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/md5/amd64-1
  using gcc -m64 -march=k8 -Os -fomit-frame-pointer
- 1.20: crypto_hashblocks/md5/little-1
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.41: crypto_hashblocks/md5/ref
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha256/ref
  using gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha512/ref
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.00: crypto_sign/donald1024/openssl
  using gcc -funroll-loops -march=k8 -O -fomit-frame-pointer
- 1.00: crypto_sign/donald2048/openssl
  using gcc -funroll-loops -march=nocona -Os -fomit-frame-pointer

- 1.00: `crypto_sign/donald512/openssl`
  using `gcc -funroll-loops -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/hector/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/rainbow/ref`
  using `g++ -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1024/openssl`
  using `gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1536/openssl`
  using `gcc -funroll-loops -m64 -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald2048/openssl`
  using `gcc -funroll-loops -m64 -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald3072/openssl`
  using `gcc -m64 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald4096/openssl`
  using `gcc -funroll-loops -m64 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald512/openssl`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald768/openssl`
  using `gcc -funroll-loops -march=nocona -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -funroll-loops -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/bernstein/amd64-2`
  using `gcc -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.06: `crypto_stream/aes128estream/e/bernstein/amd64-1`
  using `gcc -funroll-loops -m64 -march=nocona -Os -fomit-frame-pointer`
- 1.06: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- 1.10: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer`
- 1.39: `crypto_stream/aes128estream/e/gladman`
  using `gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.43: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.66: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -m64 -O3 -fomit-frame-pointer`

- 1.67: crypto_stream/aes128estream/e/bernstein/little-1
  using gcc -march=k8 -Os -fomit-frame-pointer
- 1.77: crypto_stream/aes128estream/e/bernstein/little-2
  using gcc -O2 -fomit-frame-pointer
- 1.91: crypto_stream/aes128estream/e/bernstein/big-1
  using gcc -O -fomit-frame-pointer
- 1.00: crypto_stream/aes256estream/e/hongjun/v1
  using gcc -funroll-loops -march=k8 -Os -fomit-frame-pointer
- 1.01: crypto_stream/aes256estream/e/hongjun/v0
  using gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.23: crypto_stream/aes256estream/e/gladman
  using gcc -funroll-loops -m64 -Os -fomit-frame-pointer
- 1.00: crypto_stream/chacha12/e/amd64-3
  using gcc -m64 -march=k8
- 1.33: crypto_stream/chacha12/e/merged
  using gcc -m64 -march=nocona -O2 -fomit-frame-pointer
- 1.64: crypto_stream/chacha12/e/amd64-xmm6
  using gcc -funroll-loops -march=nocona
- 1.76: crypto_stream/chacha12/e/regs
  using gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer
- 2.16: crypto_stream/chacha12/e/ref
  using gcc -funroll-loops -m64 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/chacha20/e/amd64-3
  using gcc -m64 -march=k8
- 1.31: crypto_stream/chacha20/e/merged
  using gcc -m64 -march=nocona -O2 -fomit-frame-pointer
- 1.56: crypto_stream/chacha20/e/regs
  using gcc -funroll-loops -m64 -O3 -fomit-frame-pointer
- 1.57: crypto_stream/chacha20/e/amd64-xmm6
  using gcc -march=nocona
- 1.74: crypto_stream/chacha20/e/ref
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/chacha8/e/amd64-3
  using gcc -m64 -march=k8
- 1.23: crypto_stream/chacha8/e/merged
  using gcc -march=k8 -O3 -fomit-frame-pointer

- 1.71: `crypto_stream/chacha8/e/amd64-xmm6`
  using `gcc -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.96: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -m64 -O3 -fomit-frame-pointer`
- 2.30: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -m64 -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.04: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/schwabe/amd64-1`
  using `gcc -march=k8 -O2 -fomit-frame-pointer`
- 1.15: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.16: `crypto_stream/lexv2/e/v2/schwabe/amd64-2`
  using `gcc -funroll-loops`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.94: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m64 -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -O3 -fomit-frame-pointer`
- 1.13: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -Os -fomit-frame-pointer`
- 1.14: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.32: `crypto_stream/rabbit/e/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/amd64-xmm6`
  using `gcc`
- 1.09: `crypto_stream/salsa20/e/amd64-xmm5`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- 1.18: `crypto_stream/salsa20/e/merged`
  using `gcc -O3 -fomit-frame-pointer`
- 1.22: `crypto_stream/salsa20/e/amd64-3`
  using `gcc -m64 -Os -fomit-frame-pointer`
- 1.35: `crypto_stream/salsa20/e/amd64-2`
  using `gcc -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.38: `crypto_stream/salsa20/e/amd64-1`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.38: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- 1.53: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- 1.77: `crypto_stream/salsa20/ref`
  using `gcc -funroll-loops -m64 -O3 -fomit-frame-pointer`
- 2.10: `crypto_stream/salsa20/e/amd64-xmm`
  using `gcc -m64 -march=k8 -Os -fomit-frame-pointer`
- 2.85: `crypto_stream/salsa20/e/amd64-xmm2`
  using `gcc -m64 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/amd64-xmm6`
  using `cc`
- 1.10: `crypto_stream/salsa2012/e/amd64-xmm5`
  using `gcc -m64 -march=k8 -O2 -fomit-frame-pointer`

- 1.17: `crypto_stream/salsa2012/e/amd64-3`
  using `gcc -m64 -march=k8`
- 1.17: `crypto_stream/salsa2012/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.29: `crypto_stream/salsa2012/e/amd64-2`
  using `gcc -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.32: `crypto_stream/salsa2012/e/amd64-1`
  using `gcc -O2 -fomit-frame-pointer`
- 1.48: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- 1.68: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- 2.04: `crypto_stream/salsa2012/ref`
  using `gcc -m64 -march=k8 -Os -fomit-frame-pointer`
- 2.30: `crypto_stream/salsa2012/e/amd64-xmm`
  using `gcc -m64 -march=k8 -O2 -fomit-frame-pointer`
- 2.59: `crypto_stream/salsa2012/e/amd64-xmm2`
  using `gcc -funroll-loops -m64 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/amd64-xmm6`
  using `gcc -march=nocona -O -fomit-frame-pointer`
- 1.11: `crypto_stream/salsa208/e/merged`
  using `gcc -funroll-loops -m64 -O -fomit-frame-pointer`
- 1.14: `crypto_stream/salsa208/e/amd64-xmm5`
  using `gcc -m64 -march=nocona -O2 -fomit-frame-pointer`
- 1.15: `crypto_stream/salsa208/e/amd64-3`
  using `gcc -O3 -fomit-frame-pointer`
- 1.26: `crypto_stream/salsa208/e/amd64-2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.31: `crypto_stream/salsa208/e/amd64-1`
  using `gcc -m64 -march=nocona -O -fomit-frame-pointer`
- 1.65: `crypto_stream/salsa208/e/regs`
  using `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.81: `crypto_stream/salsa208/e/ref`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 2.22: `crypto_stream/salsa208/ref`
  using `gcc -m64 -march=k8 -Os -fomit-frame-pointer`

- 2.28: crypto_stream/salsa208/e/amd64-xmm
  using gcc -march=nocona -Os -fomit-frame-pointer
- 2.66: crypto_stream/salsa208/e/amd64-xmm2
  using gcc -funroll-loops -m64 -O -fomit-frame-pointer
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -funroll-loops -m64 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -funroll-loops -m64 -O -fomit-frame-pointer
- 1.00: crypto_stream/tpy/e/tpy
  using gcc -funroll-loops -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpy6/e/tpy6
  using gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/tpypy/e/tpypy
  using gcc -funroll-loops -m64 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/trivium/e/submissions/trivium
  using gcc -funroll-loops -m64 -march=nocona -O -fomit-frame-pointer

5.5 amd64, 2800MHz, Intel Xeon (f41), nmi0057

- 1.00: crypto_dh/claus/gmp
  using g++ -m64 -O -fomit-frame-pointer
- 1.05: crypto_dh/claus/openssl
  using cc
- 1.00: crypto_dh/curve25519/mpfq
  using gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_dh/gls1271/ref
  using gcc -funroll-loops -m64 -march=nocona -O -fomit-frame-pointer
- 1.00: crypto_dh/surf127eps/mpfq
  using gcc -m64 -O2 -fomit-frame-pointer
- 1.00: crypto_encrypt/mceliece/ref
  using gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ntruees787ep1/ref
  using gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald1024/openssl
  using gcc -O -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald1536/openssl
  using gcc -m64 -march=k8 -O -fomit-frame-pointer

- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -funroll-loops -m64 -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `gcc -march=nocona`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O -fomit-frame-pointer`
- 1.63: `crypto_hash/md5/openssl`
  using `gcc -funroll-loops -m64 -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -march=nocona -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -O -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/ref`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/amd64-1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.54: `crypto_hashblocks/md5/little-1`
  using `gcc -m64 -march=k8 -O -fomit-frame-pointer`
- 1.78: `crypto_hashblocks/md5/ref`
  using `gcc -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha256/ref`
  using `gcc -m64 -march=nocona -Os -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha512/ref`
  using `gcc -m64 -march=nocona -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/donald1024/openssl`
  using `gcc -Os -fomit-frame-pointer`

- 1.00: `crypto_sign/donald2048/openssl`
  using `gcc -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/donald512/openssl`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/rainbow/ref`
  using `g++ -m64 -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1024/openssl`
  using `gcc -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1536/openssl`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald2048/openssl`
  using `gcc -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald3072/openssl`
  using `gcc -march=nocona -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald4096/openssl`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald512/openssl`
  using `gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald768/openssl`
  using `gcc -m64 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/bernstein/amd64-2`
  using `gcc -m64 -march=nocona -O2 -fomit-frame-pointer`
- 1.06: `crypto_stream/aes128estream/e/bernstein/amd64-1`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.13: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer`
- 1.16: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.31: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.42: `crypto_stream/aes128estream/e/gladman`
  using `gcc -m64 -march=nocona -O2 -fomit-frame-pointer`
- 1.52: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`

- 1.59: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.61: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -m64 -march=nocona -O2 -fomit-frame-pointer`
- 1.61: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- 1.18: `crypto_stream/aes256estream/e/gladman`
  using `gcc -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/amd64-3`
  using `gcc -funroll-loops -march=k8 -Os -fomit-frame-pointer`
- 1.43: `crypto_stream/chacha12/e/merged`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- 1.90: `crypto_stream/chacha12/e/amd64-xmm6`
  using `gcc -m64 -march=nocona -O2 -fomit-frame-pointer`
- 2.06: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -m64 -march=nocona -Os -fomit-frame-pointer`
- 2.14: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/amd64-3`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.45: `crypto_stream/chacha20/e/merged`
  using `gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer`
- 1.75: `crypto_stream/chacha20/e/amd64-xmm6`
  using `gcc -march=nocona -O3 -fomit-frame-pointer`
- 1.82: `crypto_stream/chacha20/e/ref`
  using `gcc -funroll-loops -march=nocona -Os -fomit-frame-pointer`
- 1.84: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/amd64-3`
  using `gcc -m64 -O2 -fomit-frame-pointer`
- 1.41: `crypto_stream/chacha8/e/merged`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`

- 1.81: `crypto_stream/chacha8/e/amd64-xmm6`
  using `gcc -m64 -march=nocona -O3 -fomit-frame-pointer`
- 2.31: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -m64 -march=nocona -Os -fomit-frame-pointer`
- 2.40: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -m64 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.03: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.06: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -m64 -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/schwabe/amd64-1`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.15: `crypto_stream/lexv2/e/v2/schwabe/amd64-2`
  using `gcc -m64 -O2 -fomit-frame-pointer`
- 1.19: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.83: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -funroll-loops -march=nocona -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -funroll-loops -m64 -march=nocona -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -funroll-loops -m64 -march=nocona -Os -fomit-frame-pointer`

- 1.00: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -funroll-loops -m64 -march=nocona -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- 1.10: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -m64 -march=nocona -Os -fomit-frame-pointer`
- 1.13: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.21: `crypto_stream/rabbit/e/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/amd64-xmm6`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.15: `crypto_stream/salsa20/e/amd64-xmm5`
  using `gcc -O -fomit-frame-pointer`
- 1.21: `crypto_stream/salsa20/e/merged`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.28: `crypto_stream/salsa20/e/amd64-3`
  using `gcc -O2 -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa20/e/amd64-2`
  using `gcc -march=nocona -Os -fomit-frame-pointer`
- 1.44: `crypto_stream/salsa20/e/amd64-1`
  using `gcc -m64 -march=nocona -O2 -fomit-frame-pointer`
- 1.59: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.77: `crypto_stream/salsa20/ref`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.78: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 2.20: `crypto_stream/salsa20/e/amd64-xmm`
  using `gcc -funroll-loops -m64 -march=k8`
- 2.99: `crypto_stream/salsa20/e/amd64-xmm2`
  using `gcc -march=nocona -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/amd64-xmm6`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.17: `crypto_stream/salsa2012/e/amd64-xmm5`
  using `gcc -march=nocona`

- 1.21: crypto_stream/salsa2012/e/merged
  using gcc -O3 -fomit-frame-pointer
- 1.24: crypto_stream/salsa2012/e/amd64-3
  using gcc -funroll-loops -march=k8 -Os -fomit-frame-pointer
- 1.36: crypto_stream/salsa2012/e/amd64-2
  using gcc -funroll-loops -Os -fomit-frame-pointer
- 1.41: crypto_stream/salsa2012/e/amd64-1
  using gcc -march=nocona -O2 -fomit-frame-pointer
- 1.82: crypto_stream/salsa2012/e/regs
  using gcc -funroll-loops -march=nocona -O -fomit-frame-pointer
- 1.97: crypto_stream/salsa2012/e/ref
  using gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer
- 2.27: crypto_stream/salsa2012/ref
  using gcc -march=k8 -O3 -fomit-frame-pointer
- 2.44: crypto_stream/salsa2012/e/amd64-xmm
  using gcc -O2 -fomit-frame-pointer
- 2.84: crypto_stream/salsa2012/e/amd64-xmm2
  using gcc -m64 -march=k8 -Os -fomit-frame-pointer
- 1.00: crypto_stream/salsa208/e/amd64-xmm6
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.05: crypto_stream/salsa208/e/merged
  using gcc -march=nocona -O3 -fomit-frame-pointer
- 1.08: crypto_stream/salsa208/e/amd64-3
  using gcc -m64 -Os -fomit-frame-pointer
- 1.08: crypto_stream/salsa208/e/amd64-xmm5
  using gcc -Os -fomit-frame-pointer
- 1.19: crypto_stream/salsa208/e/amd64-2
  using gcc -m64 -Os -fomit-frame-pointer
- 1.23: crypto_stream/salsa208/e/amd64-1
  using gcc -funroll-loops -m64 -Os -fomit-frame-pointer
- 1.79: crypto_stream/salsa208/e/regs
  using gcc -funroll-loops -march=nocona -O -fomit-frame-pointer
- 1.96: crypto_stream/salsa208/e/ref
  using gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer
- 2.18: crypto_stream/salsa208/ref
  using gcc -march=nocona -O3 -fomit-frame-pointer

- 2.41: `crypto_stream/salsa208/e/amd64-xmm`
  using `gcc -m64 -march=nocona -Os -fomit-frame-pointer`
- 2.52: `crypto_stream/salsa208/e/amd64-xmm2`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -m64 -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -funroll-loops -m64 -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -funroll-loops -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`

5.6 amd64, 2800MHz, Intel Xeon (f41), `nmi0063`

- 1.00: `crypto_dh/claus/gmp`
  using `g++ -m64`
- 1.01: `crypto_dh/claus/openssl`
  using `gcc -funroll-loops -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_dh/curve2251/mpfq`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_dh/curve25519/mpfq`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_dh/gls1271/ref`
  using `gcc -m64 -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_dh/hector/ref`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_dh/surf127eps/mpfq`
  using `gcc -funroll-loops -m64 -O -fomit-frame-pointer`
- 1.00: `crypto_dh/surf2113/mpfq`
  using `gcc -funroll-loops -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/mceliece/ref`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`

- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -m64 -Os -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -funroll-loops -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `gcc -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -funroll-loops -march=nocona -O -fomit-frame-pointer`
- 1.58: `crypto_hash/md5/openssl`
  using `gcc -march=nocona -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -funroll-loops -m64 -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/ref`
  using `gcc -funroll-loops -m64 -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -funroll-loops -m64 -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/amd64-1`
  using `gcc -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.45: `crypto_hashblocks/md5/little-1`
  using `gcc -m64 -march=nocona -O -fomit-frame-pointer`
- 1.64: `crypto_hashblocks/md5/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`

- 1.00: `crypto_hashblocks/sha256/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha512/ref`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/donald1024/openssl`
  using `gcc -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/donald2048/openssl`
  using `gcc -funroll-loops -march=k8 -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/donald512/openssl`
  using `gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/hector/ref`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/rainbow/ref`
  using `g++ -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1024/openssl`
  using `gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1536/openssl`
  using `gcc -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald2048/openssl`
  using `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald3072/openssl`
  using `gcc -funroll-loops -m64 -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald4096/openssl`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald512/openssl`
  using `gcc -m64 -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald768/openssl`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/bernstein/amd64-2`
  using `gcc -march=k8 -O3 -fomit-frame-pointer`
- 1.06: `crypto_stream/aes128estream/e/bernstein/amd64-1`
  using `gcc -O3 -fomit-frame-pointer`
- 1.11: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`

- 1.16: crypto_stream/aes128estream/e/hongjun/v0
  using gcc -O3 -fomit-frame-pointer
- 1.42: crypto_stream/aes128estream/e/bernstein/little-4
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.45: crypto_stream/aes128estream/e/gladman
  using gcc -funroll-loops -m64 -Os -fomit-frame-pointer
- 1.50: crypto_stream/aes128estream/e/bernstein/little-1
  using gcc -funroll-loops -m64 -O3 -fomit-frame-pointer
- 1.58: crypto_stream/aes128estream/e/bernstein/little-3
  using gcc -march=nocona -O -fomit-frame-pointer
- 1.64: crypto_stream/aes128estream/e/bernstein/little-2
  using gcc -O3 -fomit-frame-pointer
- 1.66: crypto_stream/aes128estream/e/bernstein/big-1
  using gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes256estream/e/hongjun/v1
  using gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer
- 1.04: crypto_stream/aes256estream/e/hongjun/v0
  using gcc -funroll-loops -m64 -O2 -fomit-frame-pointer
- 1.23: crypto_stream/aes256estream/e/gladman
  using gcc -funroll-loops -Os -fomit-frame-pointer
- 1.00: crypto_stream/chacha12/e/amd64-3
  using gcc -O2 -fomit-frame-pointer
- 1.47: crypto_stream/chacha12/e/merged
  using gcc -m64 -O -fomit-frame-pointer
- 1.64: crypto_stream/chacha12/e/amd64-xmm6
  using gcc -funroll-loops -m64 -march=nocona
- 1.85: crypto_stream/chacha12/e/ref
  using gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer
- 1.90: crypto_stream/chacha12/e/regs
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.00: crypto_stream/chacha20/e/amd64-3
  using gcc -m64 -march=nocona
- 1.47: crypto_stream/chacha20/e/merged
  using gcc -funroll-loops -march=nocona -O -fomit-frame-pointer
- 1.57: crypto_stream/chacha20/e/amd64-xmm6
  using gcc -funroll-loops -march=nocona

- 1.62: `crypto_stream/chacha20/e/ref`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- 1.66: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/amd64-3`
  using `gcc -O2 -fomit-frame-pointer`
- 1.26: `crypto_stream/chacha8/e/merged`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.72: `crypto_stream/chacha8/e/amd64-xmm6`
  using `gcc -funroll-loops -m64 -march=k8 -O -fomit-frame-pointer`
- 2.08: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- 2.16: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -O -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.05: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -march=nocona -O -fomit-frame-pointer`
- 1.02: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/schwabe/amd64-1`
  using `gcc -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.16: `crypto_stream/lexv2/e/v2/schwabe/amd64-2`
  using `cc`
- 1.18: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -m64 -march=nocona -Os -fomit-frame-pointer`

- 4.25: crypto_stream/nlsv2/e/v2/sync/1
  using gcc -funroll-loops -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/1/2
  using gcc -funroll-loops -m64 -Os -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/1/3
  using gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/1/4
  using gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/2/2
  using gcc -funroll-loops -m64 -Os -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/2/3
  using gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer
- 1.13: crypto_stream/rabbit/e/opt/1/1
  using gcc -m64 -Os -fomit-frame-pointer
- 1.13: crypto_stream/rabbit/e/opt/2/1
  using gcc -march=k8 -Os -fomit-frame-pointer
- 1.23: crypto_stream/rabbit/e/ref
  using gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/salsa20/e/amd64-xmm6
  using gcc -march=k8 -O2 -fomit-frame-pointer
- 1.10: crypto_stream/salsa20/e/amd64-xmm5
  using gcc -march=k8 -O2 -fomit-frame-pointer
- 1.20: crypto_stream/salsa20/e/merged
  using gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer
- 1.23: crypto_stream/salsa20/e/amd64-3
  using gcc -Os -fomit-frame-pointer
- 1.36: crypto_stream/salsa20/e/amd64-2
  using gcc -m64 -march=k8 -Os -fomit-frame-pointer
- 1.39: crypto_stream/salsa20/e/amd64-1
  using gcc -march=nocona -Os -fomit-frame-pointer
- 1.55: crypto_stream/salsa20/e/regs
  using gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer
- 1.66: crypto_stream/salsa20/e/ref
  using gcc -funroll-loops -m64 -march=nocona -O2 -fomit-frame-pointer
- 1.73: crypto_stream/salsa20/ref
  using gcc -funroll-loops -m64 -Os -fomit-frame-pointer

- 2.12: `crypto_stream/salsa20/e/amd64-xmm`
  using `gcc -m64 -march=k8`
- 2.88: `crypto_stream/salsa20/e/amd64-xmm2`
  using `gcc -m64 -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/amd64-xmm6`
  using `gcc -funroll-loops -march=k8`
- 1.09: `crypto_stream/salsa2012/e/amd64-xmm5`
  using `gcc -O2 -fomit-frame-pointer`
- 1.16: `crypto_stream/salsa2012/e/amd64-3`
  using `gcc -m64 -march=nocona -Os -fomit-frame-pointer`
- 1.17: `crypto_stream/salsa2012/e/merged`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.28: `crypto_stream/salsa2012/e/amd64-2`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.32: `crypto_stream/salsa2012/e/amd64-1`
  using `gcc -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.70: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- 1.75: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -m64 -march=nocona -O2 -fomit-frame-pointer`
- 1.92: `crypto_stream/salsa2012/ref`
  using `gcc -funroll-loops -march=k8 -Os -fomit-frame-pointer`
- 2.29: `crypto_stream/salsa2012/e/amd64-xmm`
  using `gcc -funroll-loops -march=k8 -O -fomit-frame-pointer`
- 2.64: `crypto_stream/salsa2012/e/amd64-xmm2`
  using `gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/amd64-xmm6`
  using `gcc -march=nocona -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/merged`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- 1.08: `crypto_stream/salsa208/e/amd64-xmm5`
  using `gcc -march=k8 -O2 -fomit-frame-pointer`
- 1.10: `crypto_stream/salsa208/e/amd64-3`
  using `gcc -Os -fomit-frame-pointer`
- 1.20: `crypto_stream/salsa208/e/amd64-2`
  using `gcc -march=k8 -Os -fomit-frame-pointer`

- 1.25: crypto_stream/salsa208/e/amd64-1
  using gcc -march=nocona -Os -fomit-frame-pointer
- 1.66: crypto_stream/salsa208/e/regs
  using gcc -funroll-loops -m64 -march=nocona -O2 -fomit-frame-pointer
- 1.72: crypto_stream/salsa208/e/ref
  using gcc -funroll-loops -m64 -O2 -fomit-frame-pointer
- 2.11: crypto_stream/salsa208/ref
  using gcc -funroll-loops -Os -fomit-frame-pointer
- 2.40: crypto_stream/salsa208/e/amd64-xmm
  using gcc -m64 -O2 -fomit-frame-pointer
- 2.55: crypto_stream/salsa208/e/amd64-xmm2
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -funroll-loops -O -fomit-frame-pointer
- 1.00: crypto_stream/tpy/e/tpy
  using gcc -funroll-loops -O2 -fomit-frame-pointer
- 1.00: crypto_stream/tpy6/e/tpy6
  using gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/tpypy/e/tpypy
  using gcc -funroll-loops -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/trivium/e/submissions/trivium
  using gcc -funroll-loops -m64 -march=nocona -O -fomit-frame-pointer

5.7 amd64, 3000MHz, Intel Pentium D (f64), speed

- 1.00: crypto_dh/claus/gmp
  using g++ -m64 -march=k8 -O2 -fomit-frame-pointer
- 1.20: crypto_dh/claus/openssl
  using gcc -m64 -march=k8 -Os -fomit-frame-pointer
- 1.00: crypto_dh/curve2251/mpfq
  using gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_dh/curve25519/mpfq
  using gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_dh/gls1271/ref
  using gcc -march=k8 -O -fomit-frame-pointer

- 1.00: `crypto_dh/hector/ref`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_dh/surf127eps/mpfq`
  using `gcc -funroll-loops -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_dh/surf2113/mpfq`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/mceliece/ref`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -funroll-loops -march=nocona`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -m64 -march=nocona`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `gcc -funroll-loops -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.09: `crypto_hash/md5/openssl`
  using `gcc -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -funroll-loops -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_hash/sha224/openssl`
  using `gcc -m64 -O -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -m64 -march=nocona -O -fomit-frame-pointer`

- 1.63: crypto_hash/sha256/openssl
  using gcc -march=nocona
- 1.00: crypto_hash/sha384/openssl
  using gcc -m64 -march=k8
- 1.00: crypto_hash/sha512/ref
  using gcc -funroll-loops -O2 -fomit-frame-pointer
- 1.03: crypto_hash/sha512/openssl
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.00: crypto_hash/whirlpool/ref
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/md5/amd64-1
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.20: crypto_hashblocks/md5/little-1
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.41: crypto_hashblocks/md5/ref
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha256/ref
  using gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha512/ref
  using gcc -funroll-loops -m64 -O2 -fomit-frame-pointer
- 1.00: crypto_sign/donald1024/openssl
  using gcc -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_sign/donald2048/openssl
  using gcc -m64 -march=nocona -Os -fomit-frame-pointer
- 1.00: crypto_sign/donald512/openssl
  using gcc -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ecdonaldb163/openssl
  using gcc -march=nocona -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ecdonaldb233/openssl
  using gcc -m64 -march=nocona -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ecdonaldb283/openssl
  using gcc -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ecdonaldb409/openssl
  using gcc -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ecdonaldb571/openssl
  using gcc -funroll-loops -m64 -march=k8 -O -fomit-frame-pointer

- 1.00: `crypto_sign/ecdonaldk163/openssl`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldk233/openssl`
  using `gcc -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldk283/openssl`
  using `gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldk409/openssl`
  using `gcc -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldk571/openssl`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldp160/openssl`
  using `gcc -funroll-loops -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldp192/openssl`
  using `gcc -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldp224/openssl`
  using `gcc -march=nocona -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldp256/openssl`
  using `gcc -funroll-loops -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldp384/openssl`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldp521/openssl`
  using `gcc -funroll-loops -m64 -march=nocona -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/hector/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/rainbow/ref`
  using `g++ -m64 -march=nocona`
- 1.00: `crypto_sign/ronald1024/openssl`
  using `gcc -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1536/openssl`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald2048/openssl`
  using `gcc -funroll-loops -m64 -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald3072/openssl`
  using `gcc -funroll-loops -m64 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald4096/openssl`
  using `gcc -funroll-loops -m64 -march=nocona -O2 -fomit-frame-pointer`

- 1.00: `crypto_sign/ronald512/openssl`
  using `gcc -m64 -march=nocona -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald768/openssl`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -funroll-loops -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/bernstein/amd64-2`
  using `gcc -m64 -march=k8 -O -fomit-frame-pointer`
- 1.05: `crypto_stream/aes128estream/e/bernstein/amd64-1`
  using `gcc -march=nocona`
- 1.08: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.09: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.41: `crypto_stream/aes128estream/e/gladman`
  using `gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.43: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.59: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.64: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -m64 -O2 -fomit-frame-pointer`
- 1.75: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.84: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -march=k8 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.02: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- 1.24: `crypto_stream/aes256estream/e/gladman`
  using `gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/amd64-3`
  using `gcc -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.33: `crypto_stream/chacha12/e/merged`
  using `gcc -m64 -march=nocona -O3 -fomit-frame-pointer`

- 1.77: `crypto_stream/chacha12/e/amd64-xmm6`
  using `gcc -m64 -O2 -fomit-frame-pointer`
- 1.77: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 2.17: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/amd64-3`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.32: `crypto_stream/chacha20/e/merged`
  using `gcc -funroll-loops -m64 -march=nocona -O2 -fomit-frame-pointer`
- 1.58: `crypto_stream/chacha20/e/amd64-xmm6`
  using `gcc -O -fomit-frame-pointer`
- 1.58: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.76: `crypto_stream/chacha20/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/amd64-3`
  using `gcc -m64 -march=nocona`
- 1.25: `crypto_stream/chacha8/e/merged`
  using `gcc -O3 -fomit-frame-pointer`
- 1.64: `crypto_stream/chacha8/e/amd64-xmm6`
  using `gcc -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.98: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 2.30: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -m64 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.03: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -funroll-loops -march=k8 -Os -fomit-frame-pointer`
- 1.07: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -m64 -march=k8 -Os -fomit-frame-pointer`

- 1.00: crypto_stream/hc256/e/hc-256/200511
  using gcc -funroll-loops -march=nocona -Os -fomit-frame-pointer
- 1.01: crypto_stream/hc256/e/hc-256/200701
  using gcc -funroll-loops -m64 -march=nocona -Os -fomit-frame-pointer
- 1.00: crypto_stream/lexv2/e/v2/schwabe/amd64-1
  using gcc -funroll-loops -m64 -O3 -fomit-frame-pointer
- 1.15: crypto_stream/lexv2/e/v2/ref
  using gcc -funroll-loops -m64 -O3 -fomit-frame-pointer
- 1.16: crypto_stream/lexv2/e/v2/schwabe/amd64-2
  using gcc -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_stream/nlsv2/e/v2/sync/2
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.91: crypto_stream/nlsv2/e/v2/sync/1
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/1/2
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/1/3
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/1/4
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/2/2
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/2/3
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.13: crypto_stream/rabbit/e/opt/1/1
  using gcc -m64 -march=k8 -O2 -fomit-frame-pointer
- 1.13: crypto_stream/rabbit/e/opt/2/1
  using gcc -O3 -fomit-frame-pointer
- 1.32: crypto_stream/rabbit/e/ref
  using gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/salsa20/e/amd64-xmm6
  using gcc -m64 -march=nocona -O2 -fomit-frame-pointer
- 1.11: crypto_stream/salsa20/e/amd64-xmm5
  using gcc -funroll-loops -m64 -O -fomit-frame-pointer
- 1.19: crypto_stream/salsa20/e/merged
  using gcc -O2 -fomit-frame-pointer

- 1.24: `crypto_stream/salsa20/e/amd64-3`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- 1.37: `crypto_stream/salsa20/e/amd64-2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.40: `crypto_stream/salsa20/e/amd64-1`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.43: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.61: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- 1.79: `crypto_stream/salsa20/ref`
  using `gcc -funroll-loops -m64 -O3 -fomit-frame-pointer`
- 2.13: `crypto_stream/salsa20/e/amd64-xmm`
  using `gcc -march=k8 -O2 -fomit-frame-pointer`
- 2.89: `crypto_stream/salsa20/e/amd64-xmm2`
  using `gcc -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/amd64-xmm6`
  using `gcc -m64 -march=nocona -O -fomit-frame-pointer`
- 1.11: `crypto_stream/salsa2012/e/amd64-xmm5`
  using `gcc -march=nocona -O -fomit-frame-pointer`
- 1.18: `crypto_stream/salsa2012/e/merged`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.19: `crypto_stream/salsa2012/e/amd64-3`
  using `gcc -m64 -Os -fomit-frame-pointer`
- 1.31: `crypto_stream/salsa2012/e/amd64-2`
  using `gcc -funroll-loops -march=k8 -O -fomit-frame-pointer`
- 1.35: `crypto_stream/salsa2012/e/amd64-1`
  using `gcc -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.55: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.75: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- 2.04: `crypto_stream/salsa2012/ref`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 2.34: `crypto_stream/salsa2012/e/amd64-xmm`
  using `gcc -funroll-loops -march=nocona -O -fomit-frame-pointer`

- 2.70: `crypto_stream/salsa2012/e/amd64-xmm2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/amd64-xmm6`
  using `gcc -m64 -march=nocona -Os -fomit-frame-pointer`
- 1.08: `crypto_stream/salsa208/e/merged`
  using `gcc -funroll-loops -m64 -march=k8 -O -fomit-frame-pointer`
- 1.10: `crypto_stream/salsa208/e/amd64-xmm5`
  using `gcc -funroll-loops -march=nocona -Os -fomit-frame-pointer`
- 1.12: `crypto_stream/salsa208/e/amd64-3`
  using `gcc`
- 1.22: `crypto_stream/salsa208/e/amd64-2`
  using `gcc -march=nocona -Os -fomit-frame-pointer`
- 1.28: `crypto_stream/salsa208/e/amd64-1`
  using `gcc -march=k8 -O3 -fomit-frame-pointer`
- 1.63: `crypto_stream/salsa208/e/regs`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.77: `crypto_stream/salsa208/e/ref`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 2.22: `crypto_stream/salsa208/e/amd64-xmm`
  using `gcc -O2 -fomit-frame-pointer`
- 2.22: `crypto_stream/salsa208/ref`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- 2.60: `crypto_stream/salsa208/e/amd64-xmm2`
  using `gcc -m64 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -funroll-loops -O -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -funroll-loops -march=nocona -O -fomit-frame-pointer`

5.8 amd64, 3000MHz, Intel Xeon (f4a), `nmi0090`

- 1.00: `crypto_dh/claus/openssl`
  using `cc`
- 1.00: `crypto_dh/gls1271/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -m64`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md2/openssl`
  using `cc`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.53: `crypto_hash/md5/openssl`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -m64`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`

- 1.00: crypto_hashblocks/md5/amd64-1
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.54: crypto_hashblocks/md5/little-1
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.75: crypto_hashblocks/md5/ref
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha256/ref
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha512/ref
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/donald1024/openssl
  using cc
- 1.00: crypto_sign/donald2048/openssl
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/donald512/openssl
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald1024/openssl
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald1536/openssl
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald2048/openssl
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald3072/openssl
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald4096/openssl
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald512/openssl
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald768/openssl
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/sflashv2/ref
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes128estream/e/bernstein/amd64-2
  using cc
- 1.06: crypto_stream/aes128estream/e/bernstein/amd64-1
  using gcc -m64 -O3 -fomit-frame-pointer

- 1.19: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.35: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.57: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.59: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.66: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.66: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.72: `crypto_stream/aes128estream/e/gladman`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.80: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.08: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.53: `crypto_stream/aes256estream/e/gladman`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/amd64-3`
  using `gcc -m64`
- 1.73: `crypto_stream/chacha12/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.92: `crypto_stream/chacha12/e/amd64-xmm6`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.70: `crypto_stream/chacha12/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 3.54: `crypto_stream/chacha12/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/amd64-3`
  using `gcc -m64`
- 1.70: `crypto_stream/chacha20/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`

- 1.71: `crypto_stream/chacha20/e/amd64-xmm6`
  using `cc`
- 2.28: `crypto_stream/chacha20/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.83: `crypto_stream/chacha20/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/amd64-3`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.71: `crypto_stream/chacha8/e/amd64-xmm6`
  using `cc`
- 1.74: `crypto_stream/chacha8/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 3.49: `crypto_stream/chacha8/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 3.78: `crypto_stream/chacha8/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.29: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.08: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/schwabe/amd64-1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.15: `crypto_stream/lexv2/e/v2/schwabe/amd64-2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.46: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 3.96: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.18: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.19: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.78: `crypto_stream/rabbit/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/amd64-xmm6`
  using `gcc -m64`
- 1.12: `crypto_stream/salsa20/e/amd64-xmm5`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.23: `crypto_stream/salsa20/e/amd64-3`
  using `cc`
- 1.24: `crypto_stream/salsa20/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.36: `crypto_stream/salsa20/e/amd64-2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.40: `crypto_stream/salsa20/e/amd64-1`
  using `gcc -m64`
- 1.72: `crypto_stream/salsa20/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.98: `crypto_stream/salsa20/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`

- 2.15: `crypto_stream/salsa20/e/amd64-xmm`
  using `cc`
- 2.36: `crypto_stream/salsa20/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.85: `crypto_stream/salsa20/e/amd64-xmm2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/amd64-xmm6`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.15: `crypto_stream/salsa2012/e/amd64-xmm5`
  using `cc`
- 1.19: `crypto_stream/salsa2012/e/amd64-3`
  using `cc`
- 1.22: `crypto_stream/salsa2012/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.30: `crypto_stream/salsa2012/e/amd64-2`
  using `gcc -m64`
- 1.35: `crypto_stream/salsa2012/e/amd64-1`
  using `cc`
- 1.90: `crypto_stream/salsa2012/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.11: `crypto_stream/salsa2012/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.33: `crypto_stream/salsa2012/e/amd64-xmm`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.76: `crypto_stream/salsa2012/e/amd64-xmm2`
  using `gcc -m64`
- 2.79: `crypto_stream/salsa2012/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/amd64-xmm6`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.11: `crypto_stream/salsa208/e/amd64-3`
  using `cc`
- 1.12: `crypto_stream/salsa208/e/amd64-xmm5`
  using `gcc -m64`
- 1.15: `crypto_stream/salsa208/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`

- 1.21: `crypto_stream/salsa208/e/amd64-2`
  using `cc`
- 1.26: `crypto_stream/salsa208/e/amd64-1`
  using `gcc -m64`
- 2.02: `crypto_stream/salsa208/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.37: `crypto_stream/salsa208/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.44: `crypto_stream/salsa208/e/amd64-xmm`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.56: `crypto_stream/salsa208/e/amd64-xmm2`
  using `cc`
- 3.11: `crypto_stream/salsa208/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -m64 -O3 -fomit-frame-pointer`

5.9 amd64, 3392MHz, Intel Pentium D (f64), `nmi0104`

- 1.00: `crypto_dh/claus/gmp`
  using `g++ -m64 -march=k8 -O -fomit-frame-pointer`
- 1.08: `crypto_dh/claus/openssl`
  using `gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_dh/curve2251/mpfq`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_dh/curve25519/mpfq`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`

- 1.00: crypto_dh/gls1271/ref
  using gcc -m64 -O -fomit-frame-pointer
- 1.00: crypto_dh/hector/ref
  using gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_dh/surf127eps/mpfq
  using gcc -m64 -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_dh/surf2113/mpfq
  using gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_encrypt/mceliece/ref
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ntruees787ep1/ref
  using gcc -funroll-loops -O2 -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald1024/openssl
  using gcc -funroll-loops -m64 -march=nocona -O -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald1536/openssl
  using gcc
- 1.00: crypto_encrypt/ronald2048/openssl
  using gcc -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald3072/openssl
  using gcc -funroll-loops -m64 -march=nocona -Os -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald4096/openssl
  using gcc -m64 -march=nocona -O2 -fomit-frame-pointer
- 1.00: crypto_hash/md2/openssl
  using gcc -funroll-loops -m64 -march=nocona -O -fomit-frame-pointer
- 1.00: crypto_hash/md4/openssl
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/md5/ref
  using gcc -funroll-loops -march=k8 -O -fomit-frame-pointer
- 1.10: crypto_hash/md5/openssl
  using gcc -m64 -march=k8 -O -fomit-frame-pointer
- 1.00: crypto_hash/ripemd160/openssl
  using gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_hash/sha1/openssl
  using gcc
- 1.00: crypto_hash/sha224/openssl
  using gcc -funroll-loops -m64 -march=nocona -Os -fomit-frame-pointer

- 1.00: `crypto_hash/sha256/ref`
  using `gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer`
- 1.67: `crypto_hash/sha256/openssl`
  using `gcc -funroll-loops -march=k8 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/sha384/openssl`
  using `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/openssl`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.11: `crypto_hash/sha512/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -m64 -O -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/amd64-1`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.07: `crypto_hashblocks/md5/little-1`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.38: `crypto_hashblocks/md5/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha256/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha512/ref`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/donald1024/openssl`
  using `gcc -m64 -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/donald2048/openssl`
  using `gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/donald512/openssl`
  using `gcc -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/hector/ref`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/rainbow/ref`
  using `g++ -march=nocona`
- 1.00: `crypto_sign/ronald1024/openssl`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1536/openssl`
  using `gcc -march=nocona -O2 -fomit-frame-pointer`

- 1.00: crypto_sign/ronald2048/openssl
  using gcc -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald3072/openssl
  using gcc -funroll-loops -march=nocona -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald4096/openssl
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald512/openssl
  using gcc -march=nocona -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ronald768/openssl
  using gcc -funroll-loops -m64 -march=nocona -O2 -fomit-frame-pointer
- 1.00: crypto_sign/sflashv2/ref
  using gcc -funroll-loops -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes128estream/e/bernstein/amd64-2
  using gcc -funroll-loops -m64 -O3 -fomit-frame-pointer
- 1.04: crypto_stream/aes128estream/e/hongjun/v1
  using gcc -funroll-loops -O2 -fomit-frame-pointer
- 1.06: crypto_stream/aes128estream/e/bernstein/amd64-1
  using gcc -m64 -march=nocona
- 1.08: crypto_stream/aes128estream/e/hongjun/v0
  using gcc -funroll-loops -O2 -fomit-frame-pointer
- 1.34: crypto_stream/aes128estream/e/gladman
  using gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer
- 1.43: crypto_stream/aes128estream/e/bernstein/little-4
  using gcc -funroll-loops -O2 -fomit-frame-pointer
- 1.53: crypto_stream/aes128estream/e/bernstein/little-1
  using gcc -O3 -fomit-frame-pointer
- 1.61: crypto_stream/aes128estream/e/bernstein/little-2
  using gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer
- 1.72: crypto_stream/aes128estream/e/bernstein/big-1
  using gcc -m64 -O2 -fomit-frame-pointer
- 1.74: crypto_stream/aes128estream/e/bernstein/little-3
  using gcc -Os -fomit-frame-pointer
- 1.00: crypto_stream/aes256estream/e/hongjun/v0
  using gcc -funroll-loops -m64 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/aes256estream/e/hongjun/v1
  using gcc -funroll-loops -m64 -O2 -fomit-frame-pointer

- 1.21: `crypto_stream/aes256estream/e/gladman`
  using `gcc -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/amd64-3`
  using `gcc -m64 -march=nocona -O2 -fomit-frame-pointer`
- 1.47: `crypto_stream/chacha12/e/merged`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.68: `crypto_stream/chacha12/e/amd64-xmm6`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`
- 2.02: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 2.14: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/amd64-3`
  using `gcc -march=k8 -Os -fomit-frame-pointer`
- 1.45: `crypto_stream/chacha20/e/merged`
  using `gcc -funroll-loops -m64 -O3 -fomit-frame-pointer`
- 1.68: `crypto_stream/chacha20/e/amd64-xmm6`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- 1.81: `crypto_stream/chacha20/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.96: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/amd64-3`
  using `gcc -m64 -march=nocona`
- 1.41: `crypto_stream/chacha8/e/merged`
  using `gcc -funroll-loops -m64 -march=k8 -O -fomit-frame-pointer`
- 1.60: `crypto_stream/chacha8/e/amd64-xmm6`
  using `gcc -funroll-loops -m64 -O -fomit-frame-pointer`
- 2.16: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 2.28: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -m64 -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.04: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.04: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -funroll-loops -m64 -march=k8 -O -fomit-frame-pointer`
- 1.03: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -m64 -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/schwabe/amd64-1`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.14: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -funroll-loops -m64 -O3 -fomit-frame-pointer`
- 1.15: `crypto_stream/lexv2/e/v2/schwabe/amd64-2`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.92: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.18: `crypto_stream/rabbit/e/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.19: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.19: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -m64 -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/salsa20/e/amd64-xmm6`
  using `gcc -funroll-loops -m64 -O -fomit-frame-pointer`
- 1.12: `crypto_stream/salsa20/e/amd64-xmm5`
  using `gcc -m64 -O2 -fomit-frame-pointer`
- 1.16: `crypto_stream/salsa20/e/merged`
  using `gcc -m64 -O2 -fomit-frame-pointer`
- 1.24: `crypto_stream/salsa20/e/amd64-3`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- 1.35: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- 1.37: `crypto_stream/salsa20/e/amd64-2`
  using `gcc -march=nocona -Os -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa20/e/amd64-1`
  using `gcc -m64 -Os -fomit-frame-pointer`
- 1.48: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer`
- 1.70: `crypto_stream/salsa20/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 2.13: `crypto_stream/salsa20/e/amd64-xmm`
  using `gcc -march=k8 -O2 -fomit-frame-pointer`
- 2.89: `crypto_stream/salsa20/e/amd64-xmm2`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/amd64-xmm6`
  using `gcc -O -fomit-frame-pointer`
- 1.10: `crypto_stream/salsa2012/e/amd64-xmm5`
  using `gcc -march=k8 -Os -fomit-frame-pointer`
- 1.15: `crypto_stream/salsa2012/e/merged`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.17: `crypto_stream/salsa2012/e/amd64-3`
  using `gcc -O -fomit-frame-pointer`
- 1.29: `crypto_stream/salsa2012/e/amd64-2`
  using `gcc -m64 -O2 -fomit-frame-pointer`
- 1.33: `crypto_stream/salsa2012/e/amd64-1`
  using `gcc -m64 -march=nocona -O2 -fomit-frame-pointer`
- 1.48: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`

- 1.62: crypto_stream/salsa2012/e/ref
  using gcc -funroll-loops -m64 -O2 -fomit-frame-pointer
- 1.95: crypto_stream/salsa2012/ref
  using gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer
- 2.31: crypto_stream/salsa2012/e/amd64-xmm
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 2.68: crypto_stream/salsa2012/e/amd64-xmm2
  using gcc -funroll-loops -m64 -march=nocona
- 1.00: crypto_stream/salsa208/e/amd64-xmm6
  using gcc -m64 -march=k8 -O -fomit-frame-pointer
- 1.09: crypto_stream/salsa208/e/amd64-xmm5
  using gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer
- 1.10: crypto_stream/salsa208/e/amd64-3
  using gcc -funroll-loops -m64 -march=nocona -O -fomit-frame-pointer
- 1.12: crypto_stream/salsa208/e/merged
  using gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer
- 1.20: crypto_stream/salsa208/e/amd64-2
  using gcc -m64 -Os -fomit-frame-pointer
- 1.28: crypto_stream/salsa208/e/amd64-1
  using gcc -m64 -march=nocona -O3 -fomit-frame-pointer
- 1.60: crypto_stream/salsa208/e/regs
  using gcc -funroll-loops -march=k8 -Os -fomit-frame-pointer
- 1.70: crypto_stream/salsa208/e/ref
  using gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer
- 2.06: crypto_stream/salsa208/ref
  using gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer
- 2.19: crypto_stream/salsa208/e/amd64-xmm
  using gcc -funroll-loops -march=nocona -Os -fomit-frame-pointer
- 2.56: crypto_stream/salsa208/e/amd64-xmm2
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -funroll-loops -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpy/e/tpy
  using gcc -funroll-loops -m64 -O2 -fomit-frame-pointer

- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -funroll-loops -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer`

5.10 amd64, 3392MHz, Intel Pentium D (f64), `nmi0161`

- 1.00: `crypto_dh/claus/gmp`
  using `g++ -march=k8 -O -fomit-frame-pointer`
- 1.08: `crypto_dh/claus/openssl`
  using `gcc -funroll-loops`
- 1.00: `crypto_dh/curve2251/mpfq`
  using `gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_dh/curve25519/mpfq`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_dh/gls1271/ref`
  using `gcc -m64 -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_dh/hector/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_dh/surf127eps/mpfq`
  using `gcc -O2 -fomit-frame-pointer`
- 1.00: `crypto_dh/surf2113/mpfq`
  using `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/mceliece/ref`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -funroll-loops -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -funroll-loops -m64 -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -march=k8 -O -fomit-frame-pointer`

- 1.00: crypto_encrypt/ronald4096/openssl
  using gcc -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_hash/md2/openssl
  using gcc -funroll-loops -m64
- 1.00: crypto_hash/md4/openssl
  using gcc -m64 -march=k8 -O -fomit-frame-pointer
- 1.00: crypto_hash/md5/ref
  using gcc -funroll-loops -march=k8 -O -fomit-frame-pointer
- 1.10: crypto_hash/md5/openssl
  using gcc -m64 -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_hash/ripemd160/openssl
  using gcc -funroll-loops -m64 -march=k8 -O -fomit-frame-pointer
- 1.00: crypto_hash/sha1/openssl
  using gcc -m64 -march=nocona -O2 -fomit-frame-pointer
- 1.00: crypto_hash/sha224/openssl
  using gcc -funroll-loops -m64 -Os -fomit-frame-pointer
- 1.00: crypto_hash/sha256/ref
  using gcc -march=k8 -O3 -fomit-frame-pointer
- 1.73: crypto_hash/sha256/openssl
  using gcc -march=k8 -Os -fomit-frame-pointer
- 1.00: crypto_hash/sha384/openssl
  using gcc -m64
- 1.00: crypto_hash/sha512/ref
  using gcc -m64 -march=k8 -O -fomit-frame-pointer
- 1.04: crypto_hash/sha512/openssl
  using gcc -funroll-loops -Os -fomit-frame-pointer
- 1.00: crypto_hash/whirlpool/ref
  using gcc -funroll-loops -m64 -O2 -fomit-frame-pointer
- 1.00: crypto_hashblocks/md5/amd64-1
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.20: crypto_hashblocks/md5/little-1
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.42: crypto_hashblocks/md5/ref
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha256/ref
  using gcc -funroll-loops -m64 -O3 -fomit-frame-pointer

- 1.00: `crypto_hashblocks/sha512/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/donald1024/openssl`
  using `gcc -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/donald2048/openssl`
  using `gcc -march=k8 -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/donald512/openssl`
  using `gcc -m64 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldb163/openssl`
  using `gcc -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldb233/openssl`
  using `gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldb283/openssl`
  using `gcc -m64 -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldb409/openssl`
  using `gcc -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldb571/openssl`
  using `gcc -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldk163/openssl`
  using `gcc -funroll-loops`
- 1.00: `crypto_sign/ecdonaldk233/openssl`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldk283/openssl`
  using `gcc -funroll-loops -march=nocona -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldk409/openssl`
  using `gcc -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldk571/openssl`
  using `gcc -m64 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldp160/openssl`
  using `gcc -m64 -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldp192/openssl`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldp224/openssl`
  using `gcc -funroll-loops -m64 -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldp256/openssl`
  using `gcc -march=k8 -O -fomit-frame-pointer`

- 1.00: crypto_sign/ecdonaldp384/openssl
  using gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ecdonaldp521/openssl
  using gcc -m64 -march=nocona -O -fomit-frame-pointer
- 1.00: crypto_sign/hector/ref
  using gcc -funroll-loops -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/rainbow/ref
  using g++ -march=nocona
- 1.00: crypto_sign/ronald1024/openssl
  using gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ronald1536/openssl
  using gcc -funroll-loops -march=k8 -Os -fomit-frame-pointer
- 1.00: crypto_sign/ronald2048/openssl
  using gcc -funroll-loops -m64 -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald3072/openssl
  using gcc -funroll-loops -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald4096/openssl
  using gcc -funroll-loops -m64 -march=nocona -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald512/openssl
  using gcc -funroll-loops -m64 -march=k8 -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald768/openssl
  using gcc -funroll-loops -march=k8 -O -fomit-frame-pointer
- 1.00: crypto_sign/sflashv2/ref
  using gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes128estream/e/bernstein/amd64-2
  using gcc -m64 -march=k8
- 1.06: crypto_stream/aes128estream/e/bernstein/amd64-1
  using gcc -m64 -march=k8 -O -fomit-frame-pointer
- 1.06: crypto_stream/aes128estream/e/hongjun/v1
  using gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer
- 1.09: crypto_stream/aes128estream/e/hongjun/v0
  using gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.40: crypto_stream/aes128estream/e/gladman
  using gcc -funroll-loops -march=k8 -Os -fomit-frame-pointer
- 1.42: crypto_stream/aes128estream/e/bernstein/little-4
  using gcc -funroll-loops -O2 -fomit-frame-pointer

- 1.66: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -m64 -O2 -fomit-frame-pointer`
- 1.66: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -funroll-loops -O -fomit-frame-pointer`
- 1.76: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.84: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer`
- 1.01: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -funroll-loops -march=k8 -Os -fomit-frame-pointer`
- 1.23: `crypto_stream/aes256estream/e/gladman`
  using `gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/amd64-3`
  using `cc`
- 1.33: `crypto_stream/chacha12/e/merged`
  using `gcc -march=nocona -O3 -fomit-frame-pointer`
- 1.64: `crypto_stream/chacha12/e/amd64-xmm6`
  using `gcc -march=nocona -O2 -fomit-frame-pointer`
- 1.78: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -m64 -O3 -fomit-frame-pointer`
- 2.16: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/amd64-3`
  using `gcc -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.32: `crypto_stream/chacha20/e/merged`
  using `gcc -march=nocona -O2 -fomit-frame-pointer`
- 1.58: `crypto_stream/chacha20/e/amd64-xmm6`
  using `gcc -O -fomit-frame-pointer`
- 1.58: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.90: `crypto_stream/chacha20/e/ref`
  using `gcc -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/amd64-3`
  using `gcc -march=k8 -Os -fomit-frame-pointer`

- 1.24: crypto_stream/chacha8/e/merged
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.61: crypto_stream/chacha8/e/amd64-xmm6
  using gcc -O -fomit-frame-pointer
- 1.97: crypto_stream/chacha8/e/regs
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 2.32: crypto_stream/chacha8/e/ref
  using gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_stream/cryptmtv3/e/v3
  using gcc -funroll-loops -march=nocona -O -fomit-frame-pointer
- 1.00: crypto_stream/dragon/e/submissions/dragon
  using gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_stream/hc128/e/hc-128/200701a
  using gcc -funroll-loops -march=k8 -Os -fomit-frame-pointer
- 1.02: crypto_stream/hc128/e/hc-128/200606
  using gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer
- 1.04: crypto_stream/hc128/e/hc-128/200701b
  using gcc -m64 -Os -fomit-frame-pointer
- 1.00: crypto_stream/hc256/e/hc-256/200511
  using gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer
- 1.01: crypto_stream/hc256/e/hc-256/200701
  using gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer
- 1.00: crypto_stream/lexv2/e/v2/schwabe/amd64-1
  using gcc -O3 -fomit-frame-pointer
- 1.14: crypto_stream/lexv2/e/v2/ref
  using gcc -funroll-loops -m64 -O3 -fomit-frame-pointer
- 1.16: crypto_stream/lexv2/e/v2/schwabe/amd64-2
  using gcc -m64 -march=k8 -Os -fomit-frame-pointer
- 1.00: crypto_stream/nlsv2/e/v2/sync/2
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.91: crypto_stream/nlsv2/e/v2/sync/1
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/1/2
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/1/3
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer

- 1.00: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.13: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.18: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.32: `crypto_stream/rabbit/e/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/amd64-xmm6`
  using `gcc -funroll-loops -march=nocona`
- 1.12: `crypto_stream/salsa20/e/amd64-xmm5`
  using `gcc -march=k8 -O3 -fomit-frame-pointer`
- 1.21: `crypto_stream/salsa20/e/merged`
  using `gcc -march=k8 -O3 -fomit-frame-pointer`
- 1.26: `crypto_stream/salsa20/e/amd64-3`
  using `gcc -funroll-loops -march=nocona -Os -fomit-frame-pointer`
- 1.39: `crypto_stream/salsa20/e/amd64-2`
  using `gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa20/e/amd64-1`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.58: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.82: `crypto_stream/salsa20/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 2.15: `crypto_stream/salsa20/e/amd64-xmm`
  using `gcc -m64 -O2 -fomit-frame-pointer`
- 2.93: `crypto_stream/salsa20/e/amd64-xmm2`
  using `gcc -m64 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/amd64-xmm6`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`

- 1.11: crypto_stream/salsa2012/e/amd64-xmm5
  using gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer
- 1.17: crypto_stream/salsa2012/e/merged
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.18: crypto_stream/salsa2012/e/amd64-3
  using gcc -march=nocona -Os -fomit-frame-pointer
- 1.29: crypto_stream/salsa2012/e/amd64-2
  using gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer
- 1.34: crypto_stream/salsa2012/e/amd64-1
  using gcc -funroll-loops -m64 -march=nocona -Os -fomit-frame-pointer
- 1.49: crypto_stream/salsa2012/e/regs
  using gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer
- 1.70: crypto_stream/salsa2012/e/ref
  using gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer
- 2.06: crypto_stream/salsa2012/ref
  using gcc -m64 -march=k8 -Os -fomit-frame-pointer
- 2.32: crypto_stream/salsa2012/e/amd64-xmm
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 2.68: crypto_stream/salsa2012/e/amd64-xmm2
  using gcc -funroll-loops -march=nocona -Os -fomit-frame-pointer
- 1.00: crypto_stream/salsa208/e/amd64-xmm6
  using gcc -O -fomit-frame-pointer
- 1.10: crypto_stream/salsa208/e/merged
  using gcc -funroll-loops -O -fomit-frame-pointer
- 1.12: crypto_stream/salsa208/e/amd64-xmm5
  using gcc -m64 -O -fomit-frame-pointer
- 1.13: crypto_stream/salsa208/e/amd64-3
  using gcc -m64
- 1.23: crypto_stream/salsa208/e/amd64-2
  using gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer
- 1.29: crypto_stream/salsa208/e/amd64-1
  using gcc -funroll-loops -march=k8 -Os -fomit-frame-pointer
- 1.64: crypto_stream/salsa208/e/regs
  using gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer
- 1.79: crypto_stream/salsa208/e/ref
  using gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer

- 2.24: `crypto_stream/salsa208/e/amd64-xmm`
  using `gcc -m64 -march=nocona -O2 -fomit-frame-pointer`
- 2.34: `crypto_stream/salsa208/ref`
  using `gcc -m64 -march=k8 -Os -fomit-frame-pointer`
- 2.62: `crypto_stream/salsa208/e/amd64-xmm2`
  using `gcc -funroll-loops -m64 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -funroll-loops -m64 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -funroll-loops -march=nocona -O -fomit-frame-pointer`

5.11 amd64, 3392MHz, Intel Pentium D (f64), `nmi0241`

- 1.00: `crypto_dh/claus/gmp`
  using `g++ -march=k8 -O2 -fomit-frame-pointer`
- 1.04: `crypto_dh/claus/openssl`
  using `gcc -m64 -march=nocona`
- 1.00: `crypto_dh/curve25519/mpfq`
  using `gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_dh/gls1271/ref`
  using `gcc -funroll-loops -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_dh/surf127eps/mpfq`
  using `gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/mceliece/ref`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -funroll-loops -m64 -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`

- 1.00: crypto_encrypt/ronald1536/openssl
  using gcc -march=k8
- 1.00: crypto_encrypt/ronald2048/openssl
  using gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald3072/openssl
  using gcc -m64 -march=k8 -O -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald4096/openssl
  using gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/md2/openssl
  using gcc -march=k8
- 1.00: crypto_hash/md4/openssl
  using gcc -m64 -march=k8 -Os -fomit-frame-pointer
- 1.00: crypto_hash/md5/ref
  using gcc -funroll-loops -m64 -march=k8 -O2 -fomit-frame-pointer
- 1.99: crypto_hash/md5/openssl
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/ripemd160/openssl
  using gcc -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_hash/sha1/openssl
  using gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer
- 1.00: crypto_hash/sha256/ref
  using gcc -m64 -march=k8 -Os -fomit-frame-pointer
- 1.00: crypto_hash/sha512/ref
  using gcc -funroll-loops -march=k8 -O -fomit-frame-pointer
- 1.00: crypto_hash/whirlpool/ref
  using gcc -m64 -march=nocona -O -fomit-frame-pointer
- 1.00: crypto_hashblocks/md5/amd64-1
  using gcc -m64 -march=k8 -O3 -fomit-frame-pointer
- 1.51: crypto_hashblocks/md5/little-1
  using gcc -m64 -march=k8 -Os -fomit-frame-pointer
- 1.87: crypto_hashblocks/md5/ref
  using gcc -m64 -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha256/ref
  using gcc -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha512/ref
  using gcc -m64 -march=nocona -Os -fomit-frame-pointer

- 1.00: `crypto_sign/donald1024/openssl`
  using `gcc -funroll-loops -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/donald2048/openssl`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/donald512/openssl`
  using `gcc -funroll-loops -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1024/openssl`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1536/openssl`
  using `gcc -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald2048/openssl`
  using `gcc -funroll-loops -m64 -march=nocona -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald3072/openssl`
  using `gcc -m64 -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald4096/openssl`
  using `gcc -funroll-loops -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald512/openssl`
  using `gcc -march=k8 -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald768/openssl`
  using `gcc -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/bernstein/amd64-2`
  using `gcc -m64 -march=nocona -Os -fomit-frame-pointer`
- 1.06: `crypto_stream/aes128estream/e/bernstein/amd64-1`
  using `gcc -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.14: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -march=nocona -O3 -fomit-frame-pointer`
- 1.17: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.31: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.46: `crypto_stream/aes128estream/e/gladman`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.49: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -march=nocona -O2 -fomit-frame-pointer`

- 1.56: crypto_stream/aes128estream/e/bernstein/little-2
  using gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer
- 1.61: crypto_stream/aes128estream/e/bernstein/big-1
  using gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer
- 1.61: crypto_stream/aes128estream/e/bernstein/little-3
  using gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes256estream/e/hongjun/v1
  using gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer
- 1.02: crypto_stream/aes256estream/e/hongjun/v0
  using gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer
- 1.34: crypto_stream/aes256estream/e/gladman
  using gcc -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/chacha12/e/amd64-3
  using gcc -m64 -march=k8 -O2 -fomit-frame-pointer
- 1.53: crypto_stream/chacha12/e/merged
  using gcc -m64 -march=nocona -O2 -fomit-frame-pointer
- 1.70: crypto_stream/chacha12/e/amd64-xmm6
  using gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer
- 2.09: crypto_stream/chacha12/e/regs
  using gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer
- 2.37: crypto_stream/chacha12/e/ref
  using gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_stream/chacha20/e/amd64-3
  using gcc -m64 -march=nocona -Os -fomit-frame-pointer
- 1.55: crypto_stream/chacha20/e/merged
  using gcc -m64 -march=nocona -O2 -fomit-frame-pointer
- 1.67: crypto_stream/chacha20/e/amd64-xmm6
  using gcc -m64 -march=nocona
- 1.84: crypto_stream/chacha20/e/regs
  using gcc -funroll-loops -march=k8 -Os -fomit-frame-pointer
- 2.08: crypto_stream/chacha20/e/ref
  using gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_stream/chacha8/e/amd64-3
  using gcc -O2 -fomit-frame-pointer
- 1.51: crypto_stream/chacha8/e/merged
  using gcc -march=nocona -Os -fomit-frame-pointer

- 1.72: `crypto_stream/chacha8/e/amd64-xmm6`
  using `gcc`
- 2.35: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -march=k8 -Os -fomit-frame-pointer`
- 2.66: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.22: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -funroll-loops -m64 -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/schwabe/amd64-1`
  using `gcc -m64 -march=nocona -O2 -fomit-frame-pointer`
- 1.15: `crypto_stream/lexv2/e/v2/schwabe/amd64-2`
  using `gcc -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.22: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.68: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -march=nocona -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -march=nocona -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.10: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.10: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer`
- 1.48: `crypto_stream/rabbit/e/ref`
  using `gcc -funroll-loops -m64 -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/amd64-xmm6`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.09: `crypto_stream/salsa20/e/merged`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.11: `crypto_stream/salsa20/e/amd64-xmm5`
  using `gcc -march=nocona -O -fomit-frame-pointer`
- 1.24: `crypto_stream/salsa20/e/amd64-3`
  using `gcc -funroll-loops -m64 -march=nocona -O -fomit-frame-pointer`
- 1.37: `crypto_stream/salsa20/e/amd64-2`
  using `gcc -m64 -march=k8 -O -fomit-frame-pointer`
- 1.40: `crypto_stream/salsa20/e/amd64-1`
  using `gcc -funroll-loops -m64 -march=nocona -O -fomit-frame-pointer`
- 1.57: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.57: `crypto_stream/salsa20/ref`
  using `gcc -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.94: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 2.13: `crypto_stream/salsa20/e/amd64-xmm`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- 2.89: `crypto_stream/salsa20/e/amd64-xmm2`
  using `gcc -m64 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/amd64-xmm6`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.12: `crypto_stream/salsa2012/e/amd64-xmm5`
  using `gcc -march=nocona -O -fomit-frame-pointer`

- 1.20: `crypto_stream/salsa2012/e/amd64-3`
  using `gcc -funroll-loops -march=k8 -O -fomit-frame-pointer`
- 1.22: `crypto_stream/salsa2012/e/merged`
  using `gcc -m64 -march=k8 -O2 -fomit-frame-pointer`
- 1.32: `crypto_stream/salsa2012/e/amd64-2`
  using `gcc -march=nocona -O -fomit-frame-pointer`
- 1.36: `crypto_stream/salsa2012/e/amd64-1`
  using `gcc -funroll-loops -O -fomit-frame-pointer`
- 1.71: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 2.11: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 2.12: `crypto_stream/salsa2012/ref`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 2.36: `crypto_stream/salsa2012/e/amd64-xmm`
  using `gcc -m64 -march=k8 -O2 -fomit-frame-pointer`
- 2.73: `crypto_stream/salsa2012/e/amd64-xmm2`
  using `gcc -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/amd64-xmm6`
  using `gcc -funroll-loops -m64`
- 1.12: `crypto_stream/salsa208/e/amd64-xmm5`
  using `gcc -m64 -march=nocona -O -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa208/e/amd64-3`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`
- 1.18: `crypto_stream/salsa208/e/merged`
  using `gcc -O2 -fomit-frame-pointer`
- 1.24: `crypto_stream/salsa208/e/amd64-2`
  using `gcc -funroll-loops -march=nocona -O -fomit-frame-pointer`
- 1.29: `crypto_stream/salsa208/e/amd64-1`
  using `gcc -funroll-loops -m64 -O -fomit-frame-pointer`
- 1.72: `crypto_stream/salsa208/e/regs`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 2.16: `crypto_stream/salsa208/ref`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 2.28: `crypto_stream/salsa208/e/ref`
  using `gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer`

- 2.50: crypto_stream/salsa208/e/amd64-xmm
  using gcc -march=nocona -O3 -fomit-frame-pointer
- 2.62: crypto_stream/salsa208/e/amd64-xmm2
  using gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -funroll-loops -m64 -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -O2 -fomit-frame-pointer
- 1.00: crypto_stream/tpy/e/tpy
  using gcc -funroll-loops -m64 -march=nocona -O2 -fomit-frame-pointer
- 1.00: crypto_stream/tpy6/e/tpy6
  using gcc -funroll-loops -O2 -fomit-frame-pointer
- 1.00: crypto_stream/tpypy/e/tpypy
  using gcc -funroll-loops -m64 -march=k8 -Os -fomit-frame-pointer
- 1.00: crypto_stream/trivium/e/submissions/trivium
  using gcc -funroll-loops -m64 -march=k8 -O3 -fomit-frame-pointer

5.12 ia64, 900MHz, HP Itanium II, nmi0025

- 1.00: crypto_dh/claus/gmp
  using g++ -O2 -fomit-frame-pointer
- 4.67: crypto_dh/claus/openssl
  using gcc -funroll-loops
- 1.00: crypto_dh/surf127eps/mpfq
  using gcc -funroll-loops -Os -fomit-frame-pointer
- 1.00: crypto_encrypt/mceliece/ref
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ntruees787ep1/ref
  using gcc -Os -fomit-frame-pointer
- 1.00: crypto_hash/md2/openssl
  using gcc -funroll-loops -O2 -fomit-frame-pointer
- 1.00: crypto_hash/md4/openssl
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_hash/md5/openssl
  using gcc -O3 -fomit-frame-pointer
- 1.31: crypto_hash/md5/ref
  using gcc -funroll-loops -O -fomit-frame-pointer

- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/ref`
  using `gcc -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/little-1`
  using `gcc -O3 -fomit-frame-pointer`
- 1.02: `crypto_hashblocks/md5/ref`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha256/ref`
  using `gcc -Os -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha512/ref`
  using `gcc -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.08: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -O2 -fomit-frame-pointer`
- 1.09: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.20: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -O3 -fomit-frame-pointer`
- 1.31: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.43: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.46: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`

- 1.03: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/merged`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.35: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.58: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/merged`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.25: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.43: `crypto_stream/chacha20/e/ref`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/merged`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.45: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.71: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -O -fomit-frame-pointer`
- 1.07: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/merged`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.02: `crypto_stream/salsa20/ref`
  using `gcc -O3 -fomit-frame-pointer`
- 1.24: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.44: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/merged`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`

- 1.04: `crypto_stream/salsa2012/ref`
  using `gcc -O3 -fomit-frame-pointer`
- 1.34: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.58: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/merged`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.03: `crypto_stream/salsa208/ref`
  using `gcc -O3 -fomit-frame-pointer`
- 1.44: `crypto_stream/salsa208/e/regs`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.72: `crypto_stream/salsa208/e/ref`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`

5.13 ia64, 997MHz, HP Itanium II, `nmi0020`

- 1.00: `crypto_dh/claus/gmp`
  using `g++ -O2 -fomit-frame-pointer`
- 4.81: `crypto_dh/claus/openssl`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_dh/surf127eps/mpfq`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/mceliece/ref`
  using `gcc -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -O3 -fomit-frame-pointer`

- 1.00: crypto_encrypt/ronald2048/openssl
  using gcc
- 1.00: crypto_encrypt/ronald3072/openssl
  using gcc -funroll-loops -Os -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald4096/openssl
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_hash/md2/openssl
  using gcc -funroll-loops
- 1.00: crypto_hash/md4/openssl
  using gcc -Os -fomit-frame-pointer
- 1.00: crypto_hash/md5/openssl
  using gcc -O2 -fomit-frame-pointer
- 1.25: crypto_hash/md5/ref
  using gcc -Os -fomit-frame-pointer
- 1.00: crypto_hash/ripemd160/openssl
  using gcc -funroll-loops -O -fomit-frame-pointer
- 1.00: crypto_hash/sha1/openssl
  using gcc -funroll-loops -O -fomit-frame-pointer
- 1.00: crypto_hash/sha256/ref
  using gcc -funroll-loops -Os -fomit-frame-pointer
- 1.00: crypto_hash/sha512/ref
  using gcc -funroll-loops -O -fomit-frame-pointer
- 1.00: crypto_hash/whirlpool/ref
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/md5/little-1
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.01: crypto_hashblocks/md5/ref
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha256/ref
  using gcc -funroll-loops -Os -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha512/ref
  using gcc -Os -fomit-frame-pointer
- 1.00: crypto_sign/donald1024/openssl
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.00: crypto_sign/donald2048/openssl
  using gcc -O2 -fomit-frame-pointer

- 1.00: `crypto_sign/donald512/openssl`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/rainbow/ref`
  using `g++ -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1024/openssl`
  using `gcc -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1536/openssl`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald2048/openssl`
  using `gcc -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald3072/openssl`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald4096/openssl`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald512/openssl`
  using `gcc -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald768/openssl`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -O2 -fomit-frame-pointer`
- 1.33: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -O2 -fomit-frame-pointer`
- 1.41: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 350.06: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -O -fomit-frame-pointer`
- 352.94: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -funroll-loops`
- 361.30: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -O -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -Os -fomit-frame-pointer`

- 1.01: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/merged`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.39: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.60: `crypto_stream/chacha12/e/ref`
  using `gcc -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/merged`
  using `gcc -O2 -fomit-frame-pointer`
- 1.28: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.42: `crypto_stream/chacha20/e/ref`
  using `gcc -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/merged`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.52: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.79: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -O -fomit-frame-pointer`
- 1.39: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/merged`
  using `gcc -O2 -fomit-frame-pointer`
- 1.02: `crypto_stream/salsa20/ref`
  using `gcc -O3 -fomit-frame-pointer`
- 1.28: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.47: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/merged`
  using `gcc -O2 -fomit-frame-pointer`

- 1.02: `crypto_stream/salsa2012/ref`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.67: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/merged`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.04: `crypto_stream/salsa208/ref`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.51: `crypto_stream/salsa208/e/regs`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.81: `crypto_stream/salsa208/e/ref`
  using `gcc -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -O3 -fomit-frame-pointer`

5.14 ia64, 997MHz, HP Itanium II, `nmi0058`

- 1.00: `crypto_dh/claus/gmp`
  using `g++ -O3 -fomit-frame-pointer`
- 4.82: `crypto_dh/claus/openssl`
  using `gcc -O -fomit-frame-pointer`
- 1.00: `crypto_dh/surf127eps/mpfq`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_encrypt/mceliece/ref`
  using `gcc -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`

- 1.00: crypto_encrypt/ronald2048/openssl
  using gcc -funroll-loops -O -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald3072/openssl
  using gcc -funroll-loops -O -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald4096/openssl
  using gcc -Os -fomit-frame-pointer
- 1.00: crypto_hash/md2/openssl
  using gcc -funroll-loops
- 1.00: crypto_hash/md4/openssl
  using gcc -O2 -fomit-frame-pointer
- 1.00: crypto_hash/md5/openssl
  using gcc -O2 -fomit-frame-pointer
- 1.31: crypto_hash/md5/ref
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.00: crypto_hash/ripemd160/openssl
  using gcc -funroll-loops -O2 -fomit-frame-pointer
- 1.00: crypto_hash/sha1/openssl
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.00: crypto_hash/sha256/ref
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.00: crypto_hash/sha512/ref
  using gcc -funroll-loops -Os -fomit-frame-pointer
- 1.00: crypto_hash/whirlpool/ref
  using gcc -funroll-loops -Os -fomit-frame-pointer
- 1.00: crypto_hashblocks/md5/little-1
  using gcc -Os -fomit-frame-pointer
- 1.01: crypto_hashblocks/md5/ref
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha256/ref
  using gcc -O2 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha512/ref
  using gcc -Os -fomit-frame-pointer
- 1.00: crypto_sign/donald1024/openssl
  using gcc -Os -fomit-frame-pointer
- 1.00: crypto_sign/donald2048/openssl
  using gcc -O2 -fomit-frame-pointer

- 1.00: `crypto_sign/donald512/openssl`
  using `gcc -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1024/openssl`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1536/openssl`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald2048/openssl`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald3072/openssl`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald4096/openssl`
  using `gcc -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald512/openssl`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald768/openssl`
  using `gcc -funroll-loops -O -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.08: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -O2 -fomit-frame-pointer`
- 1.11: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.26: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.38: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.51: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.58: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.01: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`

- 1.00: `crypto_stream/chacha12/e/merged`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.43: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.69: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/merged`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.30: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.50: `crypto_stream/chacha20/e/ref`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/merged`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.56: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.87: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -O -fomit-frame-pointer`
- 1.03: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/merged`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.03: `crypto_stream/salsa20/ref`
  using `gcc -O3 -fomit-frame-pointer`
- 1.27: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.48: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/merged`
  using `gcc -O2 -fomit-frame-pointer`
- 1.02: `crypto_stream/salsa2012/ref`
  using `gcc -O3 -fomit-frame-pointer`

- 1.42: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.67: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/merged`
  using `gcc -O2 -fomit-frame-pointer`
- 1.01: `crypto_stream/salsa208/ref`
  using `gcc -O3 -fomit-frame-pointer`
- 1.48: `crypto_stream/salsa208/e/regs`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.81: `crypto_stream/salsa208/e/ref`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`

5.15 ia64, 1396MHz, HP Itanium II, `nmi0065`

- 1.00: `crypto_dh/claus/openssl`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.27: `crypto_dh/claus/gmp`
  using `g++ -Os -fomit-frame-pointer`
- 1.00: `crypto_dh/surf127eps/mpfq`
  using `gcc -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/mceliece/ref`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -Os -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -O3 -fomit-frame-pointer`

- 1.00: crypto_encrypt/ronald3072/openssl
  using gcc -funroll-loops -O -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald4096/openssl
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.00: crypto_hash/md2/openssl
  using gcc -Os -fomit-frame-pointer
- 1.00: crypto_hash/md4/openssl
  using gcc -funroll-loops -Os -fomit-frame-pointer
- 1.00: crypto_hash/md5/openssl
  using gcc -Os -fomit-frame-pointer
- 1.25: crypto_hash/md5/ref
  using gcc -funroll-loops -Os -fomit-frame-pointer
- 1.00: crypto_hash/ripemd160/openssl
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_hash/sha1/openssl
  using gcc -funroll-loops
- 1.00: crypto_hash/sha256/ref
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.00: crypto_hash/sha512/ref
  using gcc -funroll-loops -O2 -fomit-frame-pointer
- 1.00: crypto_hash/whirlpool/ref
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/md5/little-1
  using gcc -O3 -fomit-frame-pointer
- 1.04: crypto_hashblocks/md5/ref
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha256/ref
  using gcc -funroll-loops -Os -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha512/ref
  using gcc -Os -fomit-frame-pointer
- 1.00: crypto_sign/donald1024/openssl
  using gcc -funroll-loops -Os -fomit-frame-pointer
- 1.00: crypto_sign/donald2048/openssl
  using gcc -funroll-loops -O2 -fomit-frame-pointer
- 1.00: crypto_sign/donald512/openssl
  using gcc -O3 -fomit-frame-pointer

- 1.00: `crypto_sign/ronald1024/openssl`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1536/openssl`
  using `gcc -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald2048/openssl`
  using `gcc -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald3072/openssl`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald4096/openssl`
  using `gcc -funroll-loops -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald512/openssl`
  using `gcc -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald768/openssl`
  using `gcc -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -O3 -fomit-frame-pointer`
- 1.03: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -O2 -fomit-frame-pointer`
- 1.40: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.41: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 295.14: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -O -fomit-frame-pointer`
- 298.94: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -funroll-loops`
- 304.09: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -O3 -fomit-frame-pointer`
- 1.10: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/merged`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`

- 1.30: `crypto_stream/chacha12/e/regs`
  using `gcc -O3 -fomit-frame-pointer`
- 1.56: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/merged`
  using `gcc -Os -fomit-frame-pointer`
- 1.22: `crypto_stream/chacha20/e/regs`
  using `gcc -O3 -fomit-frame-pointer`
- 1.41: `crypto_stream/chacha20/e/ref`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/merged`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.38: `crypto_stream/chacha8/e/regs`
  using `gcc -O3 -fomit-frame-pointer`
- 1.69: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -O -fomit-frame-pointer`
- 1.43: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/merged`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.08: `crypto_stream/salsa20/ref`
  using `gcc -O3 -fomit-frame-pointer`
- 1.23: `crypto_stream/salsa20/e/regs`
  using `gcc -Os -fomit-frame-pointer`
- 1.39: `crypto_stream/salsa20/e/ref`
  using `gcc -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/merged`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.09: `crypto_stream/salsa2012/ref`
  using `gcc -O3 -fomit-frame-pointer`
- 1.33: `crypto_stream/salsa2012/e/regs`
  using `gcc -Os -fomit-frame-pointer`

- 1.54: `crypto_stream/salsa2012/e/ref`
  using `gcc -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/merged`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.10: `crypto_stream/salsa208/ref`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa208/e/regs`
  using `gcc -Os -fomit-frame-pointer`
- 1.67: `crypto_stream/salsa208/e/ref`
  using `gcc -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -O2 -fomit-frame-pointer`

5.16 ppc32, 400MHz, Motorola PowerPC G4 7400, `nmi0042`

- 1.00: `crypto_dh/claus/gmp`
  using `g++ -O3 -fomit-frame-pointer`
- 1.44: `crypto_dh/claus/openssl`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_dh/curve25519/mpfq`
  using `gcc -funroll-loops -maltivec -O3 -fomit-frame-pointer`
- 1.00: `crypto_dh/surf127eps/mpfq`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -funroll-loops -maltivec -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -funroll-loops -maltivec -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -Os -fomit-frame-pointer`

- 1.00: crypto_hash/md2/openssl
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_hash/md4/openssl
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_hash/md5/ref
  using gcc -funroll-loops -maltivec -O -fomit-frame-pointer
- 1.13: crypto_hash/md5/openssl
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_hash/ripemd160/openssl
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_hash/sha1/openssl
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_hash/sha256/ref
  using gcc -funroll-loops -maltivec -O -fomit-frame-pointer
- 1.00: crypto_hash/sha512/ref
  using gcc -Os -fomit-frame-pointer
- 1.00: crypto_hash/whirlpool/ref
  using gcc -funroll-loops -maltivec -O -fomit-frame-pointer
- 1.00: crypto_hashblocks/md5/ref
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha256/ref
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha512/ref
  using gcc -funroll-loops -maltivec -O -fomit-frame-pointer
- 1.00: crypto_sign/donald1024/openssl
  using gcc -maltivec -O -fomit-frame-pointer
- 1.00: crypto_sign/donald2048/openssl
  using gcc -funroll-loops -Os -fomit-frame-pointer
- 1.00: crypto_sign/donald512/openssl
  using gcc -maltivec -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald1024/openssl
  using gcc -funroll-loops -maltivec -Os -fomit-frame-pointer
- 1.00: crypto_sign/ronald1536/openssl
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald2048/openssl
  using gcc -funroll-loops -O2 -fomit-frame-pointer

- 1.00: `crypto_sign/ronald3072/openssl`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald4096/openssl`
  using `gcc -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald512/openssl`
  using `gcc -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald768/openssl`
  using `gcc -funroll-loops -maltivec -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -funroll-loops -maltivec -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -funroll-loops -maltivec -O2 -fomit-frame-pointer`
- 1.06: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -O3 -fomit-frame-pointer`
- 1.55: `crypto_stream/aes128estream/e/gladman`
  using `gcc -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/gladman`
  using `gcc -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/merged`
  using `gcc -funroll-loops -maltivec -Os -fomit-frame-pointer`
- 1.01: `crypto_stream/chacha12/e/regs`
  using `gcc -O2 -fomit-frame-pointer`
- 1.20: `crypto_stream/chacha12/e/ref`
  using `gcc -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/merged`
  using `gcc -funroll-loops -maltivec -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/regs`
  using `gcc -O2 -fomit-frame-pointer`
- 1.15: `crypto_stream/chacha20/e/ref`
  using `gcc -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/merged`
  using `gcc -funroll-loops -maltivec -O -fomit-frame-pointer`
- 1.06: `crypto_stream/chacha8/e/regs`
  using `gcc -O2 -fomit-frame-pointer`
- 1.29: `crypto_stream/chacha8/e/ref`
  using `gcc -O2 -fomit-frame-pointer`

- 1.00: crypto_stream/cryptmtv3/e/v3
  using gcc -funroll-loops -Os -fomit-frame-pointer
- 1.00: crypto_stream/dragon/e/submissions/dragon
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_stream/lexv2/e/v2/ref
  using gcc -funroll-loops -maltivec -O2 -fomit-frame-pointer
- 1.00: crypto_stream/nlsv2/e/v2/sync/2
  using gcc -O3 -fomit-frame-pointer
- 3.02: crypto_stream/nlsv2/e/v2/sync/1
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/1/2
  using gcc -O2 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/1/3
  using gcc -O2 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/1/4
  using gcc -O2 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/2/2
  using gcc -O2 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/2/3
  using gcc -O2 -fomit-frame-pointer
- 1.26: crypto_stream/rabbit/e/opt/1/1
  using gcc -O2 -fomit-frame-pointer
- 1.26: crypto_stream/rabbit/e/opt/2/1
  using gcc -O2 -fomit-frame-pointer
- 1.58: crypto_stream/rabbit/e/ref
  using gcc -funroll-loops -maltivec -O3 -fomit-frame-pointer
- 1.00: crypto_stream/salsa20/e/merged
  using gcc -O2 -fomit-frame-pointer
- 1.01: crypto_stream/salsa20/e/regs
  using gcc -O2 -fomit-frame-pointer
- 1.03: crypto_stream/salsa20/ref
  using gcc -O3 -fomit-frame-pointer
- 1.14: crypto_stream/salsa20/e/ref
  using gcc -funroll-loops -maltivec -O3 -fomit-frame-pointer
- 1.00: crypto_stream/salsa2012/e/merged
  using gcc -O2 -fomit-frame-pointer

- 1.02: `crypto_stream/salsa2012/e/regs`
  using `gcc -O2 -fomit-frame-pointer`
- 1.05: `crypto_stream/salsa2012/ref`
  using `gcc -O3 -fomit-frame-pointer`
- 1.20: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -maltivec -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/merged`
  using `gcc -funroll-loops -maltivec -O -fomit-frame-pointer`
- 1.07: `crypto_stream/salsa208/e/regs`
  using `gcc -O2 -fomit-frame-pointer`
- 1.09: `crypto_stream/salsa208/ref`
  using `gcc -O3 -fomit-frame-pointer`
- 1.28: `crypto_stream/salsa208/e/ref`
  using `gcc -funroll-loops -maltivec -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -funroll-loops -maltivec -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -maltivec -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -funroll-loops -maltivec -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -funroll-loops -maltivec -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -funroll-loops -maltivec -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -funroll-loops -maltivec -O -fomit-frame-pointer`

5.17 ppc32, 2000MHz, IBM PowerPC G5 970, geespaz

- 1.00: `crypto_dh/claus/gmp`
  using `g++ -mcpu=G4 -maltivec -O2 -fomit-frame-pointer`
- 2.35: `crypto_dh/claus/openssl`
  using `gcc -mcpu=G5 -O -fomit-frame-pointer`
- 1.00: `crypto_dh/curve25519/mpfq`
  using `gcc -funroll-loops -mcpu=G3 -maltivec -Os -fomit-frame-pointer`
- 1.00: `crypto_dh/surf127eps/mpfq`
  using `gcc -funroll-loops -march=pentium4 -O3 -fomit-frame-pointer`

- 1.00: crypto_hash/md2/openssl
  using gcc -mpowerpc64 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/md4/openssl
  using gcc -mpowerpc64 -maltivec -O3 -fomit-frame-pointer
- 1.00: crypto_hash/md5/ref
  using gcc -funroll-loops -mpowerpc64 -O3 -fomit-frame-pointer
- 1.08: crypto_hash/md5/openssl
  using gcc -mpowerpc64 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/ripemd160/openssl
  using gcc -mpowerpc64 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/sha1/openssl
  using gcc -m32 -maltivec -Os -fomit-frame-pointer
- 1.00: crypto_hash/sha256/ref
  using gcc -funroll-loops -mpowerpc64 -mcpu=G4 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/sha512/ref
  using gcc -funroll-loops -mpowerpc64 -mcpu=G3 -Os -fomit-frame-pointer
- 1.00: crypto_hash/whirlpool/ref using gcc -funroll-loops -mpowerpc64 -mcpu=G4 -maltivec -O -fomit-frame-pointer
- 1.00: crypto_hashblocks/md5/ref
  using gcc -m32 -march=pentium4 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha256/ref
  using gcc -m32 -mcpu=G5 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha512/ref
  using gcc -mcpu=G5 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/donald1024/openssl
  using gcc -funroll-loops -mcpu=G4 -maltivec -O2 -fomit-frame-pointer
- 1.00: crypto_sign/donald2048/openssl
  using gcc -mcpu=G5 -maltivec -O2 -fomit-frame-pointer
- 1.00: crypto_sign/donald512/openssl
  using gcc -funroll-loops -m32 -mcpu=G5 -maltivec -O2 -fomit-frame-pointer
- 1.00: crypto_sign/rainbow/ref
  using g++ -mcpu=G3 -maltivec -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ronald1024/openssl using gcc -funroll-loops -mpowerpc64 -mcpu=G4 -maltivec -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald1536/openssl
  using gcc -funroll-loops -m32 -O2 -fomit-frame-pointer

- 1.00: `crypto_sign/ronald2048/openssl`
  using `gcc -mpowerpc64 -maltivec -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald3072/openssl`
  using `gcc -funroll-loops -mpowerpc64 -mcpu=G5 -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald4096/openssl` using `gcc -funroll-loops -mpowerpc64 -mcpu=G3 -maltivec -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald512/openssl`
  using `gcc -funroll-loops -mpowerpc64 -mcpu=G3 -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald768/openssl`
  using `gcc -funroll-loops -mpowerpc64 -mcpu=G5 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -funroll-loops -mcpu=G5 -maltivec -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -mpowerpc64 -O2 -fomit-frame-pointer`
- 1.04: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -mcpu=G3 -O2 -fomit-frame-pointer`
- 1.23: `crypto_stream/aes128estream/e/gladman`
  using `gcc -m32 -maltivec -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/gladman`
  using `gcc -maltivec -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/ppc-altivec`
  using `gcc -funroll-loops -mpowerpc64 -mcpu=G4 -O3 -fomit-frame-pointer`
- 1.90: `crypto_stream/chacha12/e/merged`
  using `gcc -m32 -mcpu=G5 -maltivec -O3 -fomit-frame-pointer`
- 1.94: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium4 -O2 -fomit-frame-pointer`
- 2.02: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -m32 -maltivec -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/ppc-altivec` using `gcc -funroll-loops -mpowerpc64 -mcpu=G3 -maltivec -O3 -fomit-frame-pointer`
- 1.57: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -m32 -maltivec -O2 -fomit-frame-pointer`
- 1.61: `crypto_stream/chacha20/e/ref`
  using `gcc -funroll-loops -m32 -mcpu=G5 -O2 -fomit-frame-pointer`
- 1.67: `crypto_stream/chacha20/e/merged`
  using `gcc -m32 -mcpu=G5 -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/chacha8/e/ppc-altivec`
  using `gcc -funroll-loops -m32 -mcpu=G4 -O3 -fomit-frame-pointer`
- 2.04: `crypto_stream/chacha8/e/merged`
  using `gcc -funroll-loops -m32 -mcpu=G5 -O3 -fomit-frame-pointer`
- 2.44: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -m32 -mcpu=G5 -Os -fomit-frame-pointer`
- 2.52: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -m32 -mcpu=G5 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -mpowerpc64 -mcpu=G3 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -funroll-loops -m32 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/schwabe/ppc32macos-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.13: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -funroll-loops -m32 -mcpu=G5 -maltivec -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -mcpu=G3 -maltivec -O3 -fomit-frame-pointer`
- 1.47: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -m32 -mcpu=G5 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -funroll-loops -mpowerpc64 -mcpu=G4 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -funroll-loops -mpowerpc64 -mcpu=G4 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -funroll-loops -mpowerpc64 -mcpu=G4 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -funroll-loops -mpowerpc64 -mcpu=G4 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -funroll-loops -mpowerpc64 -mcpu=G4 -Os -fomit-frame-pointer`
- 1.30: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -funroll-loops -mcpu=G4 -O -fomit-frame-pointer`
- 1.30: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -funroll-loops -m32 -mcpu=G3 -O -fomit-frame-pointer`
- 1.53: `crypto_stream/rabbit/e/ref`
  using `gcc -funroll-loops -m32 -mcpu=G5 -maltivec -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/salsa20/e/ppc-altivec`
  using `gcc -funroll-loops -mpowerpc64 -mcpu=G4 -Os -fomit-frame-pointer`
- 1.56: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -m32 -mcpu=G4 -Os -fomit-frame-pointer`
- 1.60: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -m32 -mcpu=G5 -O3 -fomit-frame-pointer`
- 1.65: `crypto_stream/salsa20/e/merged`
  using `gcc -m32 -mcpu=G5 -O3 -fomit-frame-pointer`
- 2.02: `crypto_stream/salsa20/ref`
  using `gcc -m32 -mcpu=G4 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/ppc-altivec`
  using `gcc -funroll-loops -mpowerpc64 -maltivec -O3 -fomit-frame-pointer`
- 1.82: `crypto_stream/salsa2012/e/merged`
  using `gcc -m32 -mcpu=G5 -maltivec -O3 -fomit-frame-pointer`
- 1.91: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -m32 -mcpu=G5 -Os -fomit-frame-pointer`
- 1.99: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -m32 -mcpu=G5 -O3 -fomit-frame-pointer`
- 2.38: `crypto_stream/salsa2012/ref`
  using `gcc -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/ppc-altivec`
  using `gcc -funroll-loops -mpowerpc64 -maltivec -O3 -fomit-frame-pointer`
- 1.89: `crypto_stream/salsa208/e/merged`
  using `gcc -funroll-loops -m32 -mcpu=G5 -Os -fomit-frame-pointer`
- 2.38: `crypto_stream/salsa208/e/regs`
  using `gcc -funroll-loops -mpowerpc64 -Os -fomit-frame-pointer`
- 2.49: `crypto_stream/salsa208/e/ref`
  using `gcc -funroll-loops -m32 -mcpu=G5 -Os -fomit-frame-pointer`
- 2.87: `crypto_stream/salsa208/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -funroll-loops -m32 -mcpu=G4 -maltivec -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -O -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -mpowerpc64 -mcpu=G3 -maltivec -Os -fomit-frame-pointer`

- 1.00: crypto_stream/tpy6/e/tpy6
  using gcc -funroll-loops -mpowerpc64 -mcpu=G3 -Os -fomit-frame-pointer
- 1.00: crypto_stream/tpypy/e/tpypy
  using gcc -mpowerpc64 -mcpu=G3 -maltivec -Os -fomit-frame-pointer
- 1.00: crypto_stream/trivium/e/submissions/trivium
  using gcc -mpowerpc64 -maltivec -Os -fomit-frame-pointer

5.18 ppc32, 2097MHz, IBM POWER5, nmi0154

- 1.00: crypto_dh/claus/gmp
  using g++ -m32
- 1.93: crypto_dh/claus/openssl
  using cc
- 1.00: crypto_dh/curve25519/mpfq
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_dh/surf127eps/mpfq
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/md2/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/md4/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/md5/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/ripemd160/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/sha1/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/whirlpool/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/sflashv2/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes128estream/e/bernstein/big-1
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.07: crypto_stream/aes128estream/e/bernstein/little-1
  using gcc -m32 -O3 -fomit-frame-pointer
- 2.30: crypto_stream/aes128estream/e/gladman
  using gcc -m32 -O3 -fomit-frame-pointer

- 1.00: `crypto_stream/aes256estream/e/gladman`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.32: `crypto_stream/chacha12/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.94: `crypto_stream/chacha12/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.21: `crypto_stream/chacha20/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.73: `crypto_stream/chacha20/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.53: `crypto_stream/chacha8/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.21: `crypto_stream/chacha8/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.96: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.02: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.14: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.14: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.92: `crypto_stream/rabbit/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.16: `crypto_stream/salsa20/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.24: `crypto_stream/salsa20/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.54: `crypto_stream/salsa20/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.28: `crypto_stream/salsa2012/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.31: `crypto_stream/salsa2012/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.72: `crypto_stream/salsa2012/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.38: `crypto_stream/salsa208/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.57: `crypto_stream/salsa208/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.82: `crypto_stream/salsa208/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -m32 -O3 -fomit-frame-pointer`

5.19 ppc32, 3192MHz, IBM Cell PPE, `nmips3`

- 1.00: `crypto_dh/claus/gmp`
  using `g++ -m32`
- 1.17: `crypto_dh/claus/openssl`
  using `gcc -m32`
- 1.00: `crypto_dh/curve25519/mpfq`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_dh/surf127eps/mpfq`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -m32`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `cc`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `cc`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -m32`

- 1.00: `crypto_hash/md5/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -m32`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha224/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha384/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -m32`
- 1.00: `crypto_sign/ronald1024/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1536/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald2048/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald3072/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald4096/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald512/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald768/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.03: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.14: `crypto_stream/aes128estream/e/schwabe/ppc32linux-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.34: `crypto_stream/aes128estream/e/gladman`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/gladman`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/chacha12/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.03: `crypto_stream/chacha12/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/chacha20/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.04: `crypto_stream/chacha20/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.69: `crypto_stream/chacha8/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.02: `crypto_stream/chacha8/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/schwabe/ppc32linux-1`
  using `gcc -m32`
- 1.80: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.07: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.04: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.04: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.04: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.14: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.28: `crypto_stream/rabbit/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.39: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.11: `crypto_stream/salsa20/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.23: `crypto_stream/salsa20/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.53: `crypto_stream/salsa20/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.10: `crypto_stream/salsa2012/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa2012/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.84: `crypto_stream/salsa2012/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/salsa208/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.39: `crypto_stream/salsa208/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.96: `crypto_stream/salsa208/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -m32 -O3 -fomit-frame-pointer`

5.20 ppc64, 2000MHz, IBM PowerPC G5 970, geespaz

- 1.00: `crypto_dh/claus/gmp`
  using `g++ -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_dh/surf127eps/mpfq`
  using `gcc -funroll-loops -m64 -mcpu=G3 -maltivec -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -m64 -maltivec -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -funroll-loops -m64 -mcpu=G5 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/ref`
  using `gcc -funroll-loops -m64 -mcpu=G5 -O -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -funroll-loops -m64 -maltivec -O -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/ref`
  using `gcc -m64 -mcpu=G3 -maltivec -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha256/ref`
  using `gcc -funroll-loops -m64 -maltivec -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha512/ref`
  using `gcc -funroll-loops -m64 -mcpu=G5 -O3 -fomit-frame-pointer`

- 1.00: crypto_sign/rainbow/ref
  using g++ -m64 -mcpu=G3 -maltivec -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes128estream/e/bernstein/little-1
  using gcc -m64 -mcpu=G3 -O2 -fomit-frame-pointer
- 1.01: crypto_stream/aes128estream/e/bernstein/big-1
  using gcc -m64 -mcpu=G3 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/chacha12/e/ppc-altivec
  using gcc -funroll-loops -m64 -mcpu=G3 -maltivec -O3 -fomit-frame-pointer
- 2.80: crypto_stream/chacha12/e/ref
  using gcc -funroll-loops -m64 -mcpu=G4 -Os -fomit-frame-pointer
- 2.81: crypto_stream/chacha12/e/regs
  using gcc -funroll-loops -m64 -mcpu=G3 -Os -fomit-frame-pointer
- 3.13: crypto_stream/chacha12/e/merged
  using gcc -funroll-loops -m64 -mcpu=G4 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/chacha20/e/ppc-altivec
  using gcc -funroll-loops -m64 -mcpu=G3 -maltivec -O3 -fomit-frame-pointer
- 2.34: crypto_stream/chacha20/e/ref
  using gcc -funroll-loops -m64 -march=pentium4 -Os -fomit-frame-pointer
- 2.38: crypto_stream/chacha20/e/regs
  using gcc -funroll-loops -m64 -mcpu=G3 -O3 -fomit-frame-pointer
- 2.64: crypto_stream/chacha20/e/merged
  using gcc -m64 -mcpu=G5 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/chacha8/e/ppc-altivec
  using gcc -funroll-loops -m64 -mcpu=G4 -O3 -fomit-frame-pointer
- 3.26: crypto_stream/chacha8/e/regs
  using gcc -funroll-loops -m64 -mcpu=G5 -maltivec -O3 -fomit-frame-pointer
- 3.36: crypto_stream/chacha8/e/ref
  using gcc -funroll-loops -m64 -mcpu=G5 -maltivec -Os -fomit-frame-pointer
- 3.62: crypto_stream/chacha8/e/merged
  using gcc -m64 -mcpu=G4 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/cryptmtv3/e/v3
  using gcc -funroll-loops -m64 -mcpu=G5 -maltivec -O3 -fomit-frame-pointer
- 1.00: crypto_stream/nlsv2/e/v2/sync/2
  using gcc -funroll-loops -m64 -mcpu=G3 -O3 -fomit-frame-pointer
- 1.38: crypto_stream/nlsv2/e/v2/sync/1
  using gcc -funroll-loops -m64 -mcpu=G4 -maltivec -O3 -fomit-frame-pointer

- 1.00: `crypto_stream/salsa20/e/ppc-altivec`
  using `gcc -m64 -mcpu=G4 -Os -fomit-frame-pointer`
- 1.99: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -m64 -mcpu=G4 -maltivec -O2 -fomit-frame-pointer`
- 2.13: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -m64 -mcpu=G3 -maltivec -O3 -fomit-frame-pointer`
- 2.30: `crypto_stream/salsa20/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.60: `crypto_stream/salsa20/ref`
  using `gcc -m64 -maltivec -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/ppc-altivec`
  using `gcc -funroll-loops -m64 -maltivec -O3 -fomit-frame-pointer`
- 2.41: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -m64 -mcpu=G4 -maltivec -O2 -fomit-frame-pointer`
- 2.59: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -m64 -mcpu=G3 -O3 -fomit-frame-pointer`
- 2.85: `crypto_stream/salsa2012/e/merged`
  using `gcc -m64 -maltivec -Os -fomit-frame-pointer`
- 2.95: `crypto_stream/salsa2012/ref`
  using `gcc -funroll-loops -m64 -mcpu=G5 -maltivec -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/ppc-altivec`
  using `gcc -funroll-loops -m64 -maltivec -O3 -fomit-frame-pointer`
- 2.92: `crypto_stream/salsa208/e/ref`
  using `gcc -funroll-loops -m64 -mcpu=G5 -maltivec -O3 -fomit-frame-pointer`
- 2.95: `crypto_stream/salsa208/e/merged`
  using `gcc -funroll-loops -m64 -maltivec -O -fomit-frame-pointer`
- 2.97: `crypto_stream/salsa208/e/regs`
  using `gcc -funroll-loops -m64 -maltivec -Os -fomit-frame-pointer`
- 3.51: `crypto_stream/salsa208/ref`
  using `gcc -m64 -mcpu=G5 -maltivec -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -funroll-loops -m64 -maltivec -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -funroll-loops -m64 -mcpu=G4 -O3 -fomit-frame-pointer`

5.21 ppc64, 2097MHz, IBM POWER5, nmi0154

- 1.00: crypto_dh/claus/gmp
  using g++ -m64
- 4.03: crypto_dh/claus/openssl
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_dh/surf127eps/mpfq
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/md2/openssl
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/md4/openssl
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/md5/openssl
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/ripemd160/openssl
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/sha1/openssl
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/whirlpool/ref
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/sflashv2/ref
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes128estream/e/bernstein/big-1
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.09: crypto_stream/aes128estream/e/bernstein/little-1
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.63: crypto_stream/aes128estream/e/gladman
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes256estream/e/gladman
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/chacha12/e/merged
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.26: crypto_stream/chacha12/e/regs
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.68: crypto_stream/chacha12/e/ref
  using gcc -m64 -O3 -fomit-frame-pointer

- 1.00: `crypto_stream/chacha20/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.17: `crypto_stream/chacha20/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.39: `crypto_stream/chacha20/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.35: `crypto_stream/chacha8/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.93: `crypto_stream/chacha8/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 4.19: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.13: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.13: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -m64 -O3 -fomit-frame-pointer`

- 1.84: `crypto_stream/rabbit/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.08: `crypto_stream/salsa20/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.16: `crypto_stream/salsa20/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.47: `crypto_stream/salsa20/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.15: `crypto_stream/salsa2012/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.22: `crypto_stream/salsa2012/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.66: `crypto_stream/salsa2012/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.19: `crypto_stream/salsa208/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.27: `crypto_stream/salsa208/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.81: `crypto_stream/salsa208/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -m64 -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -m64 -O3 -fomit-frame-pointer`

5.22 ppc64, 3192MHz, IBM Cell PPE, `nmips3`

- 1.00: `crypto_dh/claus/gmp`
  using `g++ -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_dh/surf127eps/mpfq`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -m64`
- 1.00: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.13: `crypto_stream/aes128estream/e/gladman`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.15: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/gladman`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.05: `crypto_stream/chacha12/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.10: `crypto_stream/chacha12/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/chacha20/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.04: `crypto_stream/chacha20/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.51: `crypto_stream/chacha8/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.55: `crypto_stream/chacha8/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`

- 1.00: crypto_stream/cryptmtv3/e/v3
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/dragon/e/submissions/dragon
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/lexv2/e/v2/ref
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/nlsv2/e/v2/sync/2
  using gcc -m64 -O3 -fomit-frame-pointer
- 2.54: crypto_stream/nlsv2/e/v2/sync/1
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/1/2
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/1/3
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/1/4
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/2/2
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/2/3
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.50: crypto_stream/rabbit/e/opt/1/1
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.50: crypto_stream/rabbit/e/opt/2/1
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.82: crypto_stream/rabbit/e/ref
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/salsa20/e/regs
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.03: crypto_stream/salsa20/e/ref
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.17: crypto_stream/salsa20/e/merged
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.48: crypto_stream/salsa20/ref
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/salsa2012/e/regs
  using gcc -m64 -O3 -fomit-frame-pointer

- 1.01: `crypto_stream/salsa2012/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.19: `crypto_stream/salsa2012/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.44: `crypto_stream/salsa2012/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.47: `crypto_stream/salsa208/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.92: `crypto_stream/salsa208/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.05: `crypto_stream/salsa208/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -m64 -O3 -fomit-frame-pointer`

5.23 sparcv9, 300MHz, Sun UltraSPARC IIi, `nmi0096`

- 1.00: `crypto_dh/claus/openssl`
  using `gcc -m64`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -m64`
- 1.00: `crypto_hash/md5/openssl`
  using `gcc -m64`

- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -m64`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/gladman`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.08: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/gladman`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/sparc`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.32: `crypto_stream/chacha12/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.44: `crypto_stream/chacha12/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.68: `crypto_stream/chacha12/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/sparc`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.98: `crypto_stream/chacha20/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.13: `crypto_stream/chacha20/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.26: `crypto_stream/chacha20/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/sparc`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.66: `crypto_stream/chacha8/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`

- 2.78: `crypto_stream/chacha8/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 3.12: `crypto_stream/chacha8/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/schwabe/sparc-2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.03: `crypto_stream/lexv2/e/v2/schwabe/sparc-1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.74: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.79: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.94: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.94: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.18: `crypto_stream/rabbit/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/sparc`
  using `gcc -m64 -O3 -fomit-frame-pointer`

- 1.89: `crypto_stream/salsa20/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.19: `crypto_stream/salsa20/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.36: `crypto_stream/salsa20/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.40: `crypto_stream/salsa20/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/sparc`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.09: `crypto_stream/salsa2012/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.56: `crypto_stream/salsa2012/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.65: `crypto_stream/salsa2012/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.79: `crypto_stream/salsa2012/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/sparc`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.33: `crypto_stream/salsa208/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.86: `crypto_stream/salsa208/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.99: `crypto_stream/salsa208/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 3.25: `crypto_stream/salsa208/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -m64 -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -m64 -O3 -fomit-frame-pointer`

5.24 sparcv9, 900MHz, Sun UltraSPARC III, `nmi0051`

- 1.00: `crypto_dh/claus/gmp`
  using `g++ -m64 -mcpu=sparclite`
- 1.00: `crypto_dh/nistp256/nawaz`
  using `gcc -funroll-loops -m64 -mcpu=ultrasparc3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_dh/surf127eps/mpfq`
  using `gcc -funroll-loops -m64 -mcpu=ultrasparc -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -funroll-loops -m64 -mcpu=ultrasparc3 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -funroll-loops -m64 -mcpu=ultrasparc -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/ref`
  using `gcc -funroll-loops -m64 -mcpu=ultrasparc -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -funroll-loops -m64 -mcpu=hypersparc -O2 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/ref`
  using `gcc -m64 -mcpu=ultrasparc3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha256/ref`
  using `gcc -funroll-loops -m64 -mcpu=ultrasparc3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha512/ref`
  using `gcc -funroll-loops -m64 -mcpu=ultrasparc3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -funroll-loops -m64 -mcpu=hypersparc -O -fomit-frame-pointer`
- 1.08: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -funroll-loops -m64 -mcpu=hypersparc -O -fomit-frame-pointer`
- 1.40: `crypto_stream/aes128estream/e/gladman`
  using `gcc -m64 -mcpu=hypersparc -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/gladman`
  using `gcc -m64 -mcpu=hypersparc -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/sparc`
  using `gcc -m64 -mcpu=v8 -O3 -fomit-frame-pointer`

- 1.47: `crypto_stream/chacha12/e/merged`
  using `gcc -m64 -mcpu=hypersparc -O2 -fomit-frame-pointer`
- 1.82: `crypto_stream/chacha12/e/regs`
  using `gcc -m64 -mcpu=hypersparc -O2 -fomit-frame-pointer`
- 1.94: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -m64 -mcpu=ultrasparc -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/sparc`
  using `gcc -m64 -mcpu=sparclite -O3 -fomit-frame-pointer`
- 1.36: `crypto_stream/chacha20/e/merged`
  using `gcc -funroll-loops -m64 -mcpu=hypersparc -O3 -fomit-frame-pointer`
- 1.53: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -m64 -mcpu=ultrasparc -O2 -fomit-frame-pointer`
- 1.60: `crypto_stream/chacha20/e/ref`
  using `gcc -funroll-loops -m64 -mcpu=ultrasparc -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/sparc`
  using `gcc -m64 -mcpu=sparclet -O3 -fomit-frame-pointer`
- 1.69: `crypto_stream/chacha8/e/merged`
  using `gcc -m64 -mcpu=hypersparc -O2 -fomit-frame-pointer`
- 2.12: `crypto_stream/chacha8/e/regs`
  using `gcc -m64 -mcpu=hypersparc -O2 -fomit-frame-pointer`
- 2.33: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -m64 -mcpu=ultrasparc -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -m64 -mcpu=ultrasparc -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -funroll-loops -m64 -mcpu=ultrasparc3 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/schwabe/sparc-2`
  using `gcc -m64 -O2 -fomit-frame-pointer`
- 1.05: `crypto_stream/lexv2/e/v2/schwabe/sparc-1`
  using `gcc -funroll-loops -m64 -mcpu=hypersparc -O3 -fomit-frame-pointer`
- 2.02: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -funroll-loops -m64 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -m64 -mcpu=ultrasparc3 -O3 -fomit-frame-pointer`
- 2.84: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -m64 -mcpu=ultrasparc3 -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -m64 -mcpu=ultrasparc3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -m64 -mcpu=ultrasparc3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m64 -mcpu=ultrasparc3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -m64 -mcpu=ultrasparc3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -m64 -mcpu=ultrasparc3 -O3 -fomit-frame-pointer`
- 1.78: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -funroll-loops -m64 -mcpu=ultrasparc3 -Os -fomit-frame-pointer`
- 1.78: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -m64 -mcpu=ultrasparc3 -O2 -fomit-frame-pointer`
- 2.06: `crypto_stream/rabbit/e/ref`
  using `gcc -funroll-loops -m64 -mcpu=ultrasparc3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/sparc`
  using `gcc -m64 -mcpu=sparclet -O3 -fomit-frame-pointer`
- 1.39: `crypto_stream/salsa20/e/merged`
  using `gcc -funroll-loops -m64 -mcpu=hypersparc -O2 -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa20/ref`
  using `gcc -funroll-loops -m64 -mcpu=ultrasparc3 -O3 -fomit-frame-pointer`
- 1.55: `crypto_stream/salsa20/e/regs`
  using `gcc -m64 -mcpu=hypersparc -O2 -fomit-frame-pointer`
- 1.61: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -m64 -mcpu=ultrasparc3 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/sparc`
  using `gcc -m64 -mcpu=sparclite -O3 -fomit-frame-pointer`
- 1.65: `crypto_stream/salsa2012/e/merged`
  using `gcc -m64 -mcpu=hypersparc -O2 -fomit-frame-pointer`
- 1.65: `crypto_stream/salsa2012/ref`
  using `gcc -funroll-loops -m64 -mcpu=ultrasparc3 -O3 -fomit-frame-pointer`
- 1.80: `crypto_stream/salsa2012/e/regs`
  using `gcc -m64 -mcpu=hypersparc -O2 -fomit-frame-pointer`
- 2.00: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -m64 -mcpu=ultrasparc -Os -fomit-frame-pointer`

- 1.00: crypto_stream/salsa208/e/sparc
  using gcc -m64 -mcpu=v9 -O3 -fomit-frame-pointer
- 1.88: crypto_stream/salsa208/e/merged
  using gcc -m64 -mcpu=hypersparc -O2 -fomit-frame-pointer
- 1.95: crypto_stream/salsa208/ref
  using gcc -funroll-loops -m64 -mcpu=ultrasparc3 -O3 -fomit-frame-pointer
- 2.08: crypto_stream/salsa208/e/regs
  using gcc -m64 -mcpu=hypersparc -O2 -fomit-frame-pointer
- 2.37: crypto_stream/salsa208/e/ref
  using gcc -funroll-loops -m64 -mcpu=ultrasparc -Os -fomit-frame-pointer
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -funroll-loops -m64 -mcpu=ultrasparc -O3 -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -m64 -mcpu=ultrasparc -Os -fomit-frame-pointer
- 1.00: crypto_stream/tpy/e/tpy
  using gcc -funroll-loops -m64 -mcpu=ultrasparc3 -Os -fomit-frame-pointer
- 1.00: crypto_stream/tpy6/e/tpy6
  using gcc -funroll-loops -m64 -mcpu=ultrasparc -Os -fomit-frame-pointer
- 1.00: crypto_stream/tpypy/e/tpypy
  using gcc -funroll-loops -m64 -mcpu=ultrasparc3 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/trivium/e/submissions/trivium
  using gcc -funroll-loops -m64 -mcpu=supersparc -Os -fomit-frame-pointer

5.25 sparcv9, 1200MHz, Sun UltraSPARC III, nmisolaris10

- 1.00: crypto_dh/claus/gmp
  using g++ -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_dh/surf127eps/mpfq
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/whirlpool/ref
  using gcc -m64
- 1.00: crypto_stream/aes128estream/e/gladman
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.11: crypto_stream/aes128estream/e/bernstein/big-1
  using gcc -m64 -O3 -fomit-frame-pointer
- 1.12: crypto_stream/aes128estream/e/bernstein/little-1
  using gcc -m64 -O3 -fomit-frame-pointer

- 1.00: `crypto_stream/aes256estream/e/gladman`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/sparc`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.10: `crypto_stream/chacha12/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.39: `crypto_stream/chacha12/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.48: `crypto_stream/chacha12/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/sparc`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.71: `crypto_stream/chacha20/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.02: `crypto_stream/chacha20/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.43: `crypto_stream/chacha20/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/sparc`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.52: `crypto_stream/chacha8/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.88: `crypto_stream/chacha8/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.93: `crypto_stream/chacha8/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/schwabe/sparc-2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.05: `crypto_stream/lexv2/e/v2/schwabe/sparc-1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.44: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 3.11: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.72: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.73: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.43: `crypto_stream/rabbit/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/sparc`
  using `gcc -m64`
- 1.57: `crypto_stream/salsa20/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.73: `crypto_stream/salsa20/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.89: `crypto_stream/salsa20/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.91: `crypto_stream/salsa20/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/sparc`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.81: `crypto_stream/salsa2012/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.10: `crypto_stream/salsa2012/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`

- 2.35: `crypto_stream/salsa2012/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.37: `crypto_stream/salsa2012/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/sparc`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.11: `crypto_stream/salsa208/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.54: `crypto_stream/salsa208/e/regs`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.83: `crypto_stream/salsa208/e/merged`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 2.87: `crypto_stream/salsa208/e/ref`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -m64 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -m64 -O3 -fomit-frame-pointer`

5.26 x86, 1196MHz, Intel Celeron (6b1), `vieux`

- 1.00: `crypto_dh/claus/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/mceliece/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `cc`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -m32`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.09: `crypto_hash/md5/openssl`
  using `gcc -m32`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `cc`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha224/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.40: `crypto_hash/sha256/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha384/openssl`
  using `cc`
- 1.00: `crypto_hash/sha512/openssl`
  using `cc`
- 1.21: `crypto_hash/sha512/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/x86-1`
  using `gcc -m32`

- 1.08: `crypto_hashblocks/md5/little-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.47: `crypto_hashblocks/md5/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha256/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha512/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/donald1024/openssl`
  using `gcc -m32`
- 1.00: `crypto_sign/donald2048/openssl`
  using `gcc -m32`
- 1.00: `crypto_sign/donald512/openssl`
  using `cc`
- 1.00: `crypto_sign/ecdonaldb163/openssl`
  using `cc`
- 1.00: `crypto_sign/ecdonaldb233/openssl`
  using `gcc -m32`
- 1.00: `crypto_sign/ecdonaldb283/openssl`
  using `cc`
- 1.00: `crypto_sign/ecdonaldb409/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldb571/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldk163/openssl`
  using `cc`
- 1.00: `crypto_sign/ecdonaldk233/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ecdonaldk283/openssl`
  using `gcc -m32`
- 1.00: `crypto_sign/ecdonaldk409/openssl`
  using `gcc -m32`
- 1.00: `crypto_sign/ecdonaldk571/openssl`
  using `cc`
- 1.00: `crypto_sign/ecdonaldp160/openssl`
  using `gcc -m32`

- 1.00: crypto_sign/ecdonaldp192/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ecdonaldp224/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ecdonaldp256/openssl
  using gcc -m32
- 1.00: crypto_sign/ecdonaldp384/openssl
  using cc
- 1.00: crypto_sign/ecdonaldp521/openssl
  using cc
- 1.00: crypto_sign/rainbow/ref
  using g++ -m32
- 1.00: crypto_sign/ronald1024/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald1536/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald2048/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald3072/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald4096/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald512/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald768/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/sflashv2/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes128estream/e/bernstein/x86-mmx-1
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.28: crypto_stream/aes128estream/e/hongjun/v1
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.34: crypto_stream/aes128estream/e/hongjun/v0
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.74: crypto_stream/aes128estream/e/bernstein/little-4
  using gcc -m32 -O3 -fomit-frame-pointer

- 1.75: `crypto_stream/aes128estream/e/gladman`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.00: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.24: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.33: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.39: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.03: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.30: `crypto_stream/aes256estream/e/gladman`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.05: `crypto_stream/chacha12/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.06: `crypto_stream/chacha12/e/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.54: `crypto_stream/chacha12/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.03: `crypto_stream/chacha12/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/x86-mmx`
  using `gcc -m32`
- 1.03: `crypto_stream/chacha20/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.06: `crypto_stream/chacha20/e/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.38: `crypto_stream/chacha20/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.88: `crypto_stream/chacha20/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/chacha8/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.06: `crypto_stream/chacha8/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.06: `crypto_stream/chacha8/e/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.66: `crypto_stream/chacha8/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.19: `crypto_stream/chacha8/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.20: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.03: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.38: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.40: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.63: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.63: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.63: `crypto_stream/rabbit/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.80: `crypto_stream/rabbit/e/opt/2/4`
  using `gcc -m32`
- 1.00: `crypto_stream/salsa20/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.14: `crypto_stream/salsa20/e/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.22: `crypto_stream/salsa20/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa20/e/x86-pm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.43: `crypto_stream/salsa20/e/x86-athlon`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.44: `crypto_stream/salsa20/e/x86-2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.44: `crypto_stream/salsa20/e/x86-3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.54: `crypto_stream/salsa20/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.59: `crypto_stream/salsa20/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.74: `crypto_stream/salsa20/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.26: `crypto_stream/salsa2012/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.40: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa2012/e/x86-2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa2012/e/x86-athlon`
  using `cc`
- 1.71: `crypto_stream/salsa2012/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.78: `crypto_stream/salsa2012/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.91: `crypto_stream/salsa2012/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa208/e/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.17: `crypto_stream/salsa208/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.38: `crypto_stream/salsa208/e/x86-pm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.39: `crypto_stream/salsa208/e/x86-2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.39: `crypto_stream/salsa208/e/x86-3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.39: `crypto_stream/salsa208/e/x86-athlon`
  using `gcc -m32`
- 1.84: `crypto_stream/salsa208/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.01: `crypto_stream/salsa208/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.05: `crypto_stream/salsa208/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -m32 -O3 -fomit-frame-pointer`

5.27 x86, 1403MHz, AMD Opteron 240 (f58), `nmisles8amd64`

- 1.00: `crypto_dh/claus/openssl`
  using `gcc -funroll-loops -m32 -march=athlon -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/mceliece/ref`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -funroll-loops -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -funroll-loops -m32 -march=k6 -Os -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -funroll-loops -m32 -march=pentium -Os -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -funroll-loops -m32 -march=athlon -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -funroll-loops -m32 -march=k6-3 -Os -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `gcc -m32 -march=pentium4 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -m32 -march=i486 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -funroll-loops -m32 -march=i486 -O -fomit-frame-pointer`

- 1.03: `crypto_hash/md5/openssl`
  using `gcc -m32 -march=athlon -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -m32 -march=pentium-mmx -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -funroll-loops -m32 -march=pentium3 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -m32 -march=pentium3 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/ref`
  using `gcc -funroll-loops -m32 -march=k6-2 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -funroll-loops -m32 -march=k6-3 -O -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/x86-1`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.50: `crypto_hashblocks/md5/little-1`
  using `gcc -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.90: `crypto_hashblocks/md5/ref`
  using `gcc -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha256/ref`
  using `gcc -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha512/ref`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/bls/ref`
  using `g++ -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/donald1024/openssl`
  using `gcc -m32 -march=pentium2 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/donald2048/openssl`
  using `gcc -funroll-loops -m32 -march=pentium -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/donald512/openssl`
  using `gcc -m32 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1024/openssl`
  using `gcc -funroll-loops -m32 -march=athlon -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1536/openssl`
  using `gcc -funroll-loops -m32 -march=pentium -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald2048/openssl`
  using `gcc -funroll-loops -m32 -march=pentiumpro -Os -fomit-frame-pointer`

- 1.00: `crypto_sign/ronald3072/openssl`
  using `gcc -funroll-loops -m32 -march=pentium3 -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald4096/openssl`
  using `gcc -funroll-loops -m32 -march=k6-2 -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald512/openssl`
  using `gcc -funroll-loops -m32 -march=athlon -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald768/openssl`
  using `gcc -funroll-loops -m32 -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -funroll-loops -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/bernstein/x86-mmx-1`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.19: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -funroll-loops -m32 -march=pentium-mmx -O -fomit-frame-pointer`
- 1.45: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -funroll-loops -m32 -march=pentium4 -O2 -fomit-frame-pointer`
- 1.46: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -funroll-loops -m32 -march=k6-3 -Os -fomit-frame-pointer`
- 1.46: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -m32 -march=k6-3 -Os -fomit-frame-pointer`
- 1.47: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -funroll-loops -m32 -march=i486 -Os -fomit-frame-pointer`
- 1.55: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.56: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -m32 -march=i486 -O3 -fomit-frame-pointer`
- 2.10: `crypto_stream/aes128estream/e/gladman`
  using `gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -funroll-loops -m32 -march=pentium4 -Os -fomit-frame-pointer`
- 1.23: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.53: `crypto_stream/aes256estream/e/gladman`
  using `gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/x86-xmm6`
  using `gcc -funroll-loops -m32 -march=pentium4 -O -fomit-frame-pointer`

- 1.01: `crypto_stream/chacha12/e/x86-1`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.18: `crypto_stream/chacha12/e/x86-xmm5`
  using `gcc -m32 -march=athlon -O2 -fomit-frame-pointer`
- 1.21: `crypto_stream/chacha12/e/x86-xmm`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.21: `crypto_stream/chacha12/e/x86-xmm2`
  using `gcc -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.48: `crypto_stream/chacha12/e/x86-mmx`
  using `gcc -m32 -march=pentium3 -Os -fomit-frame-pointer`
- 1.78: `crypto_stream/chacha12/e/merged`
  using `gcc -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 2.41: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -m32 -march=pentium4 -O -fomit-frame-pointer`
- 2.42: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/x86-xmm6`
  using `gcc -funroll-loops -m32 -march=athlon -O -fomit-frame-pointer`
- 1.04: `crypto_stream/chacha20/e/x86-1`
  using `gcc -m32 -march=pentium3 -Os -fomit-frame-pointer`
- 1.20: `crypto_stream/chacha20/e/x86-xmm5`
  using `gcc -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.30: `crypto_stream/chacha20/e/x86-xmm`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.30: `crypto_stream/chacha20/e/x86-xmm2`
  using `gcc -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.51: `crypto_stream/chacha20/e/x86-mmx`
  using `gcc -m32 -march=pentium3 -Os -fomit-frame-pointer`
- 1.83: `crypto_stream/chacha20/e/merged`
  using `gcc -m32 -march=k6 -O2 -fomit-frame-pointer`
- 2.30: `crypto_stream/chacha20/e/ref`
  using `gcc -funroll-loops -m32 -march=pentium4 -O -fomit-frame-pointer`
- 2.38: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -m32 -march=i486 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/x86-1`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`

- 1.01: `crypto_stream/chacha8/e/x86-xmm6`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 1.14: `crypto_stream/chacha8/e/x86-xmm`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.15: `crypto_stream/chacha8/e/x86-xmm2`
  using `gcc -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.18: `crypto_stream/chacha8/e/x86-xmm5`
  using `gcc -m32 -march=athlon -O2 -fomit-frame-pointer`
- 1.47: `crypto_stream/chacha8/e/x86-mmx`
  using `gcc -m32 -march=pentium3 -Os -fomit-frame-pointer`
- 1.75: `crypto_stream/chacha8/e/merged`
  using `gcc -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 2.52: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -m32 -march=k6-3 -O -fomit-frame-pointer`
- 2.53: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -m32 -march=pentium4 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -funroll-loops -m32 -march=pentium-mmx -Os -fomit-frame-pointer`
- 1.01: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -funroll-loops -m32 -march=pentiumpro -Os -fomit-frame-pointer`
- 1.03: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -funroll-loops -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -funroll-loops -m32 -march=pentium3 -Os -fomit-frame-pointer`
- 1.03: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -funroll-loops -m32 -march=pentium-mmx -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -funroll-loops -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.93: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -m32 -march=k6-3 -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/rabbit/e/opt/2/5`
  using `gcc -m32 -march=k6-3`
- 1.58: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer`
- 1.62: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.63: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.68: `crypto_stream/rabbit/e/opt/2/4`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.99: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -m32 -march=athlon -O2 -fomit-frame-pointer`
- 2.01: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 2.82: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 2.83: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m32 -march=i486 -O2 -fomit-frame-pointer`
- 3.17: `crypto_stream/rabbit/e/ref`
  using `gcc -funroll-loops -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/x86-1`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/x86-athlon`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/salsa20/e/x86-pm`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.04: `crypto_stream/salsa20/e/x86-2`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.04: `crypto_stream/salsa20/e/x86-3`
  using `gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer`
- 1.14: `crypto_stream/salsa20/e/x86-xmm5`
  using `gcc -m32 -march=athlon`
- 1.22: `crypto_stream/salsa20/e/x86-xmm2`
  using `gcc -m32 -march=athlon`
- 1.22: `crypto_stream/salsa20/e/x86-xmm4`
  using `gcc -m32 -march=k6-2 -O -fomit-frame-pointer`

- 1.33: `crypto_stream/salsa20/e/x86-xmm`
  using `gcc -m32 -march=athlon`
- 1.35: `crypto_stream/salsa20/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.55: `crypto_stream/salsa20/e/x86-mmx`
  using `gcc -funroll-loops -m32 -march=pentium3 -Os -fomit-frame-pointer`
- 1.59: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer`
- 1.64: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -m32 -march=k6-2 -Os -fomit-frame-pointer`
- 1.86: `crypto_stream/salsa20/ref`
  using `gcc -m32 -march=i386 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/salsa2012/e/x86-athlon`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.04: `crypto_stream/salsa2012/e/x86-2`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.04: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer`
- 1.14: `crypto_stream/salsa2012/e/x86-xmm5`
  using `gcc -m32 -march=athlon`
- 1.21: `crypto_stream/salsa2012/e/x86-xmm2`
  using `gcc -m32 -march=athlon`
- 1.21: `crypto_stream/salsa2012/e/x86-xmm4`
  using `gcc -m32 -march=pentium4`
- 1.31: `crypto_stream/salsa2012/e/x86-xmm`
  using `gcc -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.35: `crypto_stream/salsa2012/e/merged`
  using `gcc -funroll-loops -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.55: `crypto_stream/salsa2012/e/x86-mmx`
  using `gcc -m32 -march=pentium3 -Os -fomit-frame-pointer`
- 1.68: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer`

- 1.80: crypto_stream/salsa2012/e/ref
  using gcc -funroll-loops -m32 -march=athlon -O2 -fomit-frame-pointer
- 2.09: crypto_stream/salsa2012/ref
  using gcc -m32 -march=i386 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/salsa208/e/x86-1
  using gcc -m32 -march=athlon -O3 -fomit-frame-pointer
- 1.02: crypto_stream/salsa208/e/x86-athlon
  using gcc -m32 -march=athlon -O3 -fomit-frame-pointer
- 1.03: crypto_stream/salsa208/e/x86-pm
  using gcc -m32 -march=athlon -O3 -fomit-frame-pointer
- 1.04: crypto_stream/salsa208/e/x86-2
  using gcc -m32 -march=athlon -O3 -fomit-frame-pointer
- 1.04: crypto_stream/salsa208/e/x86-3
  using gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer
- 1.15: crypto_stream/salsa208/e/x86-xmm5
  using gcc -m32
- 1.20: crypto_stream/salsa208/e/x86-xmm2
  using gcc -m32 -march=athlon
- 1.22: crypto_stream/salsa208/e/x86-xmm4
  using gcc -m32 -march=pentium4
- 1.29: crypto_stream/salsa208/e/x86-xmm
  using gcc -m32 -march=k6-3 -O3 -fomit-frame-pointer
- 1.38: crypto_stream/salsa208/e/merged
  using gcc -m32 -O2 -fomit-frame-pointer
- 1.52: crypto_stream/salsa208/e/x86-mmx
  using gcc -m32 -march=pentium3 -Os -fomit-frame-pointer
- 1.81: crypto_stream/salsa208/e/regs
  using gcc -funroll-loops -m32 -march=pentium3 -O2 -fomit-frame-pointer
- 1.94: crypto_stream/salsa208/e/ref
  using gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer
- 2.37: crypto_stream/salsa208/ref
  using gcc -m32 -march=i486 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -funroll-loops -m32 -march=athlon -O -fomit-frame-pointer

- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -funroll-loops -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -funroll-loops -m32 -march=i386 -O3 -fomit-frame-pointer`

5.28 x86, 1833MHz, Intel Core Duo, `nmi0068`

- 1.00: `crypto_dh/claus/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `cc`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `cc`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -m32`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.40: `crypto_hash/md5/openssl`
  using `gcc -m32`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -m32`

- 1.00: crypto_hash/sha256/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/sha512/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/whirlpool/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/md5/x86-1
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.26: crypto_hashblocks/md5/little-1
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.53: crypto_hashblocks/md5/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha256/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha512/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/rainbow/ref
  using g++ -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald1024/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald1536/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald2048/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald3072/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald4096/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald512/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald768/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/sflashv2/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes128estream/e/hongjun/v1
  using gcc -m32 -O3 -fomit-frame-pointer

- 1.03: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.26: `crypto_stream/aes128estream/e/gladman`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.28: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.29: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.70: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.71: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.76: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.13: `crypto_stream/aes256estream/e/gladman`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.30: `crypto_stream/chacha12/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.29: `crypto_stream/chacha12/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.18: `crypto_stream/chacha20/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.15: `crypto_stream/chacha20/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.44: `crypto_stream/chacha8/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 2.41: `crypto_stream/chacha8/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.17: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.90: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.09: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.51: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.51: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.84: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.84: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.21: `crypto_stream/rabbit/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/salsa20/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.09: `crypto_stream/salsa20/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa20/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.38: `crypto_stream/salsa20/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.21: `crypto_stream/salsa2012/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.25: `crypto_stream/salsa2012/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.53: `crypto_stream/salsa2012/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.45: `crypto_stream/salsa208/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.48: `crypto_stream/salsa208/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.88: `crypto_stream/salsa208/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -m32 -O3 -fomit-frame-pointer`

5.29 x86, 2400MHz, Intel Pentium 4 (f24), nmitest4

- 1.00: crypto_dh/claus/gmp
  using g++ -m32 -march=pentium4 -O -fomit-frame-pointer
- 2.66: crypto_dh/claus/openssl
  using gcc -m32 -march=k6-2 -Os -fomit-frame-pointer
- 1.00: crypto_dh/curve25519/mpfq
  using gcc -funroll-loops -m32 -march=i486 -O3 -fomit-frame-pointer
- 1.00: crypto_dh/surf127eps/mpfq
  using gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer
- 1.00: crypto_encrypt/mceliece/ref
  using gcc -funroll-loops -march=pentium3 -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ntruees787ep1/ref
  using gcc -funroll-loops -m32 -march=athlon -O2 -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald1024/openssl
  using gcc -funroll-loops -march=k6 -O2 -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald1536/openssl
  using gcc -funroll-loops -march=athlon -O -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald2048/openssl
  using gcc -funroll-loops -m32 -march=pentium4 -O -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald3072/openssl
  using gcc -funroll-loops -march=athlon -O -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald4096/openssl
  using gcc -funroll-loops -march=pentium3 -O -fomit-frame-pointer
- 1.00: crypto_hash/md2/openssl
  using gcc -funroll-loops -m32 -march=pentium
- 1.00: crypto_hash/md4/openssl
  using gcc -march=i486 -Os -fomit-frame-pointer
- 1.00: crypto_hash/md5/ref
  using gcc -funroll-loops -march=k6 -O -fomit-frame-pointer
- 1.03: crypto_hash/md5/openssl
  using gcc -funroll-loops -march=pentiumpro -O2 -fomit-frame-pointer
- 1.00: crypto_hash/ripemd160/openssl
  using gcc -funroll-loops -m32 -march=pentiumpro -O2 -fomit-frame-pointer
- 1.00: crypto_hash/sha1/openssl
  using gcc -march=pentium4 -O3 -fomit-frame-pointer

- 1.00: `crypto_hash/sha256/ref`
  using `gcc -funroll-loops -march=pentium-mmx -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/ref`
  using `gcc -funroll-loops -m32 -march=i486 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -funroll-loops -m32 -march=pentium4 -O -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/x86-1`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.19: `crypto_hashblocks/md5/little-1`
  using `gcc -march=i386 -O -fomit-frame-pointer`
- 1.65: `crypto_hashblocks/md5/ref`
  using `gcc -march=i386 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha256/ref`
  using `gcc -funroll-loops -march=pentium -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha512/ref`
  using `gcc -m32 -march=pentium3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/bls/ref`
  using `g++ -m32 -march=pentium -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/donald1024/openssl`
  using `gcc -march=k6 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/donald2048/openssl`
  using `gcc -funroll-loops -march=pentium -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/donald512/openssl`
  using `gcc -march=athlon -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1024/openssl`
  using `gcc -funroll-loops -march=k6-3 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1536/openssl`
  using `gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald2048/openssl`
  using `gcc -march=pentium3 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald3072/openssl`
  using `gcc -march=pentiumpro -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald4096/openssl`
  using `gcc -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald512/openssl`
  using `gcc -m32 -march=k6-2 -O2 -fomit-frame-pointer`

- 1.00: crypto_sign/ronald768/openssl
  using gcc -march=i486 -O -fomit-frame-pointer
- 1.00: crypto_sign/sflashv2/ref
  using gcc -funroll-loops -m32 -march=k6-3 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes128estream/e/bernstein/x86-mmx-1
  using gcc -m32 -march=i386 -O3 -fomit-frame-pointer
- 1.11: crypto_stream/aes128estream/e/hongjun/v1
  using gcc -funroll-loops -march=i386 -O -fomit-frame-pointer
- 1.25: crypto_stream/aes128estream/e/hongjun/v0
  using gcc -m32 -march=pentium3 -O -fomit-frame-pointer
- 1.50: crypto_stream/aes128estream/e/bernstein/little-3
  using gcc -m32 -march=k6-2 -Os -fomit-frame-pointer
- 1.66: crypto_stream/aes128estream/e/bernstein/little-4
  using gcc -m32 -O2 -fomit-frame-pointer
- 1.75: crypto_stream/aes128estream/e/bernstein/little-1
  using gcc -funroll-loops -m32 -march=pentium4 -O2 -fomit-frame-pointer
- 1.76: crypto_stream/aes128estream/e/bernstein/little-2
  using gcc -march=pentium4 -O3 -fomit-frame-pointer
- 1.87: crypto_stream/aes128estream/e/gladman
  using gcc -m32 -march=k6 -O -fomit-frame-pointer
- 2.07: crypto_stream/aes128estream/e/bernstein/big-1
  using gcc -m32 -march=k6 -Os -fomit-frame-pointer
- 1.00: crypto_stream/aes256estream/e/hongjun/v1
  using gcc -m32 -march=pentium2 -O -fomit-frame-pointer
- 1.08: crypto_stream/aes256estream/e/hongjun/v0
  using gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer
- 1.59: crypto_stream/aes256estream/e/gladman
  using gcc -funroll-loops -m32 -march=athlon -O -fomit-frame-pointer
- 1.00: crypto_stream/chacha12/e/x86-xmm6
  using gcc -m32 -march=pentium4 -O2 -fomit-frame-pointer
- 1.19: crypto_stream/chacha12/e/x86-xmm5
  using gcc -funroll-loops -m32 -march=k6-2 -O -fomit-frame-pointer
- 1.52: crypto_stream/chacha12/e/x86-1
  using gcc -m32 -march=athlon
- 1.90: crypto_stream/chacha12/e/x86-mmx
  using gcc -march=i386 -O -fomit-frame-pointer

- 1.95: `crypto_stream/chacha12/e/x86-xmm2`
  using `gcc -march=k6-3 -O -fomit-frame-pointer`
- 1.99: `crypto_stream/chacha12/e/x86-xmm`
  using `gcc -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 3.63: `crypto_stream/chacha12/e/merged`
  using `gcc -march=i386 -O -fomit-frame-pointer`
- 3.98: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -m32 -march=i386 -O -fomit-frame-pointer`
- 4.17: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -m32 -march=k6 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/x86-xmm6`
  using `gcc -m32 -march=k6-2 -O -fomit-frame-pointer`
- 1.21: `crypto_stream/chacha20/e/x86-xmm5`
  using `gcc -march=pentium -O -fomit-frame-pointer`
- 1.57: `crypto_stream/chacha20/e/x86-1`
  using `gcc -funroll-loops -m32 -march=k6-2 -O2 -fomit-frame-pointer`
- 2.01: `crypto_stream/chacha20/e/x86-mmx`
  using `gcc -funroll-loops -m32 -march=pentium3 -O -fomit-frame-pointer`
- 2.04: `crypto_stream/chacha20/e/x86-xmm2`
  using `gcc -m32 -march=i486 -O -fomit-frame-pointer`
- 2.06: `crypto_stream/chacha20/e/x86-xmm`
  using `gcc -m32 -march=k6-2 -O -fomit-frame-pointer`
- 3.68: `crypto_stream/chacha20/e/merged`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 4.15: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -m32 -march=i386 -O -fomit-frame-pointer`
- 4.17: `crypto_stream/chacha20/e/ref`
  using `gcc -funroll-loops -m32 -march=k6 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/x86-xmm6`
  using `gcc -m32 -march=pentium2 -O3 -fomit-frame-pointer`
- 1.20: `crypto_stream/chacha8/e/x86-xmm5`
  using `gcc -funroll-loops -march=pentium-mmx -O -fomit-frame-pointer`
- 1.51: `crypto_stream/chacha8/e/x86-1`
  using `gcc -m32 -march=pentium3 -Os -fomit-frame-pointer`
- 1.79: `crypto_stream/chacha8/e/x86-mmx`
  using `gcc -funroll-loops -m32 -march=pentium3 -O -fomit-frame-pointer`

- 1.87: crypto_stream/chacha8/e/x86-xmm2
  using gcc -m32 -march=pentium-mmx -O -fomit-frame-pointer
- 1.90: crypto_stream/chacha8/e/x86-xmm
  using gcc -m32 -march=pentium4 -O -fomit-frame-pointer
- 3.47: crypto_stream/chacha8/e/merged
  using gcc -O -fomit-frame-pointer
- 4.06: crypto_stream/chacha8/e/regs
  using gcc -funroll-loops -m32 -march=i386 -O -fomit-frame-pointer
- 4.18: crypto_stream/chacha8/e/ref
  using gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer
- 1.00: crypto_stream/cryptmtv3/e/v3
  using gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer
- 1.00: crypto_stream/dragon/e/submissions/dragon
  using gcc -funroll-loops -m32 -march=pentium4 -O -fomit-frame-pointer
- 1.00: crypto_stream/hc128/e/hc-128/200701b
  using gcc -march=pentium-mmx -O2 -fomit-frame-pointer
- 1.04: crypto_stream/hc128/e/hc-128/200606
  using gcc -march=i486 -O2 -fomit-frame-pointer
- 1.06: crypto_stream/hc128/e/hc-128/200701a
  using gcc -march=i486 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/hc256/e/hc-256/200511
  using gcc -m32 -march=athlon -O2 -fomit-frame-pointer
- 1.00: crypto_stream/hc256/e/hc-256/200701
  using gcc -march=athlon -O2 -fomit-frame-pointer
- 1.00: crypto_stream/lexv2/e/v2/ref
  using gcc -funroll-loops -march=pentium4 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/nlsv2/e/v2/sync/2
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.63: crypto_stream/nlsv2/e/v2/sync/1
  using gcc -funroll-loops -m32 -march=k6-2 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/2/5
  using gcc -funroll-loops -march=k6
- 1.28: crypto_stream/rabbit/e/opt/1/3
  using gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer
- 1.30: crypto_stream/rabbit/e/opt/1/4
  using gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer

- 1.30: `crypto_stream/rabbit/e/opt/2/4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.31: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.75: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -funroll-loops -march=pentium -O -fomit-frame-pointer`
- 1.78: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -funroll-loops -march=i486 -O -fomit-frame-pointer`
- 2.01: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -march=pentium-mmx -O2 -fomit-frame-pointer`
- 2.01: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -march=pentium -O2 -fomit-frame-pointer`
- 2.90: `crypto_stream/rabbit/e/ref`
  using `gcc -funroll-loops -m32 -march=pentium -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/x86-xmm5`
  using `gcc -m32 -march=pentium-mmx -O2 -fomit-frame-pointer`
- 1.20: `crypto_stream/salsa20/e/x86-xmm4`
  using `gcc -m32 -march=i386`
- 1.40: `crypto_stream/salsa20/e/x86-3`
  using `gcc -m32 -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.40: `crypto_stream/salsa20/e/x86-athlon`
  using `gcc -funroll-loops -m32 -march=k6 -O2 -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa20/e/x86-2`
  using `gcc -march=k6-2 -Os -fomit-frame-pointer`
- 1.43: `crypto_stream/salsa20/e/x86-pm`
  using `gcc -march=pentium4 -O3 -fomit-frame-pointer`
- 1.83: `crypto_stream/salsa20/e/x86-xmm`
  using `gcc -m32 -O2 -fomit-frame-pointer`
- 1.89: `crypto_stream/salsa20/e/x86-xmm2`
  using `gcc -funroll-loops -m32 -march=pentium3 -O -fomit-frame-pointer`
- 2.68: `crypto_stream/salsa20/e/x86-mmx`
  using `gcc -m32 -march=k6 -O -fomit-frame-pointer`
- 2.78: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -march=athlon -O3 -fomit-frame-pointer`
- 2.86: `crypto_stream/salsa20/e/merged`
  using `gcc -funroll-loops -m32 -march=pentium2 -Os -fomit-frame-pointer`

- 2.86: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -march=pentium4 -O3 -fomit-frame-pointer`
- 2.88: `crypto_stream/salsa20/e/x86-1`
  using `gcc -march=pentium-mmx -O2 -fomit-frame-pointer`
- 3.49: `crypto_stream/salsa20/ref`
  using `gcc -funroll-loops -march=pentium2 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/x86-xmm5`
  using `gcc -m32 -march=k6-3 -O2 -fomit-frame-pointer`
- 1.23: `crypto_stream/salsa2012/e/x86-xmm4`
  using `gcc -funroll-loops -m32 -march=pentium2 -O2 -fomit-frame-pointer`
- 1.40: `crypto_stream/salsa2012/e/x86-2`
  using `gcc -march=i486 -O3 -fomit-frame-pointer`
- 1.40: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.40: `crypto_stream/salsa2012/e/x86-athlon`
  using `gcc -funroll-loops -march=pentium2 -O3 -fomit-frame-pointer`
- 1.40: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -funroll-loops -m32 -march=athlon -O2 -fomit-frame-pointer`
- 1.85: `crypto_stream/salsa2012/e/x86-xmm2`
  using `gcc -m32 -march=pentiumpro -O2 -fomit-frame-pointer`
- 2.07: `crypto_stream/salsa2012/e/x86-xmm`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O2 -fomit-frame-pointer`
- 2.57: `crypto_stream/salsa2012/e/x86-mmx`
  using `gcc -march=k6-2 -O3 -fomit-frame-pointer`
- 2.74: `crypto_stream/salsa2012/e/merged`
  using `gcc -funroll-loops -m32 -march=pentium2 -Os -fomit-frame-pointer`
- 2.76: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -march=athlon -O -fomit-frame-pointer`
- 2.87: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer`
- 3.16: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -m32 -march=pentium4 -O2 -fomit-frame-pointer`
- 3.72: `crypto_stream/salsa2012/ref`
  using `gcc -m32 -march=pentium3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/x86-xmm5`
  using `gcc -m32 -march=k6-2 -O2 -fomit-frame-pointer`

- 1.26: `crypto_stream/salsa208/e/x86-xmm4`
  using `gcc -march=pentium4 -O -fomit-frame-pointer`
- 1.38: `crypto_stream/salsa208/e/x86-athlon`
  using `gcc -funroll-loops -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.38: `crypto_stream/salsa208/e/x86-pm`
  using `gcc -m32 -march=pentium3 -O3 -fomit-frame-pointer`
- 1.39: `crypto_stream/salsa208/e/x86-2`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.39: `crypto_stream/salsa208/e/x86-3`
  using `gcc -m32 -march=pentiumpro -O2 -fomit-frame-pointer`
- 1.76: `crypto_stream/salsa208/e/x86-xmm2`
  using `gcc -m32 -march=k6-2 -O -fomit-frame-pointer`
- 1.79: `crypto_stream/salsa208/e/x86-xmm`
  using `gcc -m32 -march=pentium-mmx -O2 -fomit-frame-pointer`
- 2.45: `crypto_stream/salsa208/e/x86-mmx`
  using `gcc -funroll-loops -m32 -march=i486 -Os -fomit-frame-pointer`
- 2.58: `crypto_stream/salsa208/e/x86-1`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 2.67: `crypto_stream/salsa208/e/merged`
  using `gcc -funroll-loops -march=k6 -Os -fomit-frame-pointer`
- 2.81: `crypto_stream/salsa208/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer`
- 3.40: `crypto_stream/salsa208/e/ref`
  using `gcc -funroll-loops -march=pentium4 -O3 -fomit-frame-pointer`
- 3.88: `crypto_stream/salsa208/ref`
  using `gcc -march=pentium2 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -funroll-loops -m32 -march=i386 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -funroll-loops -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -funroll-loops -m32 -march=pentium4 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -funroll-loops -m32 -march=pentium3 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -funroll-loops -march=pentium4 -O2 -fomit-frame-pointer`

- 1.00: crypto_stream/trivium/e/submissions/trivium
  using gcc -march=pentiumpro -O3 -fomit-frame-pointer

5.30 x86, 2400MHz, Intel Core 2 Duo (6fb), utrecht

- 1.00: crypto_dh/claus/gmp
  using g++ -m32 -march=athlon -Os -fomit-frame-pointer
- 1.00: crypto_dh/curve2251/mpfq
  using gcc -funroll-loops -m32 -march=k8 -O -fomit-frame-pointer
- 1.00: crypto_dh/curve25519/mpfq
  using gcc -funroll-loops -m32 -march=pentium2 -O3 -fomit-frame-pointer
- 1.00: crypto_dh/hector/ref
  using gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer
- 1.00: crypto_dh/surf127eps/mpfq
  using gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer
- 1.00: crypto_dh/surf2113/mpfq
  using gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer
- 1.00: crypto_encrypt/mceliece/ref
  using gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ntruees787ep1/ref
  using gcc -m32 -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_hash/md5/ref
  using gcc -funroll-loops -m32 -march=k6-2 -O -fomit-frame-pointer
- 1.00: crypto_hash/sha256/ref
  using gcc -m32 -march=k6-3 -Os -fomit-frame-pointer
- 1.00: crypto_hash/sha512/ref
  using gcc -funroll-loops -m32 -O2 -fomit-frame-pointer
- 1.00: crypto_hash/whirlpool/ref
  using gcc -m32 -march=k8 -O -fomit-frame-pointer
- 1.00: crypto_hashblocks/md5/x86-1
  using gcc -m32 -march=k8 -O3 -fomit-frame-pointer
- 1.04: crypto_hashblocks/md5/little-1
  using gcc -m32 -march=prescott -O -fomit-frame-pointer
- 1.22: crypto_hashblocks/md5/ref
  using gcc -funroll-loops -m32 -march=k6-2 -Os -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha256/ref
  using gcc -m32 -march=pentium4 -O2 -fomit-frame-pointer

- 1.00: `crypto_hashblocks/sha512/ref`
  using `gcc -m32 -march=pentium2`
- 1.00: `crypto_sign/bls/ref`
  using `g++ -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/hector/ref`
  using `gcc -funroll-loops -m32 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/rainbow/ref`
  using `g++ -m32 -march=pentium-m`
- 1.00: `crypto_stream/aes128estream/e/bernstein/x86-mmx-1`
  using `gcc -m32 -march=prescott -Os -fomit-frame-pointer`
- 1.07: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -funroll-loops -m32 -march=athlon -O -fomit-frame-pointer`
- 1.10: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -m32 -march=k8 -O -fomit-frame-pointer`
- 1.43: `crypto_stream/aes128estream/e/gladman`
  using `gcc -m32 -march=nocona -O -fomit-frame-pointer`
- 1.61: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -m32 -march=k6-2 -O3 -fomit-frame-pointer`
- 1.62: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.81: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -m32 -march=k6 -O3 -fomit-frame-pointer`
- 1.90: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -m32 -march=k6-3 -O2 -fomit-frame-pointer`
- 1.92: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -m32 -march=k6 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -m32 -O -fomit-frame-pointer`
- 1.02: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -m32 -march=pentium-m -O -fomit-frame-pointer`
- 1.24: `crypto_stream/aes256estream/e/gladman`
  using `gcc -m32 -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/x86-xmm6`
  using `gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.10: `crypto_stream/chacha12/e/x86-xmm5`
  using `gcc -m32 -march=pentiumpro -Os -fomit-frame-pointer`

- 1.47: crypto_stream/chacha12/e/x86-xmm2
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.53: crypto_stream/chacha12/e/x86-xmm
  using gcc -funroll-loops -m32 -march=k6-2 -O2 -fomit-frame-pointer
- 2.16: crypto_stream/chacha12/e/x86-1
  using gcc -funroll-loops -m32 -march=k6 -Os -fomit-frame-pointer
- 2.17: crypto_stream/chacha12/e/x86-mmx
  using gcc -m32 -march=k8 -O3 -fomit-frame-pointer
- 2.24: crypto_stream/chacha12/e/merged
  using gcc -m32 -march=pentium -O2 -fomit-frame-pointer
- 2.85: crypto_stream/chacha12/e/regs
  using gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer
- 3.50: crypto_stream/chacha12/e/ref
  using gcc -funroll-loops -m32 -march=athlon -Os -fomit-frame-pointer
- 1.00: crypto_stream/chacha20/e/x86-xmm6
  using gcc -m32 -march=pentium2 -O3 -fomit-frame-pointer
- 1.12: crypto_stream/chacha20/e/x86-xmm5
  using gcc -funroll-loops -m32 -march=k6 -O3 -fomit-frame-pointer
- 1.54: crypto_stream/chacha20/e/x86-xmm2
  using gcc -m32 -march=k6-2 -O -fomit-frame-pointer
- 1.60: crypto_stream/chacha20/e/x86-xmm
  using gcc -m32 -march=pentium4 -O2 -fomit-frame-pointer
- 2.15: crypto_stream/chacha20/e/x86-1
  using gcc -funroll-loops -m32 -march=pentium -O2 -fomit-frame-pointer
- 2.21: crypto_stream/chacha20/e/merged
  using gcc -m32 -march=pentium -O2 -fomit-frame-pointer
- 2.21: crypto_stream/chacha20/e/x86-mmx
  using gcc -funroll-loops -m32 -march=i486
- 2.64: crypto_stream/chacha20/e/regs
  using gcc -m32 -march=pentium -O3 -fomit-frame-pointer
- 3.35: crypto_stream/chacha20/e/ref
  using gcc -funroll-loops -m32 -march=k8 -Os -fomit-frame-pointer
- 1.00: crypto_stream/chacha8/e/x86-xmm6
  using gcc -m32 -march=athlon -O -fomit-frame-pointer
- 1.09: crypto_stream/chacha8/e/x86-xmm5
  using gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer

- 1.38: `crypto_stream/chacha8/e/x86-xmm2`
  using `gcc -m32 -march=pentium-m -O3 -fomit-frame-pointer`
- 1.46: `crypto_stream/chacha8/e/x86-xmm`
  using `gcc -m32 -march=k8 -O2 -fomit-frame-pointer`
- 2.05: `crypto_stream/chacha8/e/x86-mmx`
  using `gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer`
- 2.12: `crypto_stream/chacha8/e/x86-1`
  using `gcc -m32 -march=athlon -O2 -fomit-frame-pointer`
- 2.20: `crypto_stream/chacha8/e/merged`
  using `gcc -funroll-loops -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 2.89: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -m32 -march=k6 -O3 -fomit-frame-pointer`
- 3.67: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -m32 -march=athlon -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -m32 -march=pentium4 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -m32 -march=pentium-m -O -fomit-frame-pointer`
- 1.01: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -m32 -march=prescott -O -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -m32 -march=pentium2 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -m32 -march=pentium3 -O -fomit-frame-pointer`
- 2.17: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -m32 -march=i486 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/5`
  using `gcc -m32 -march=pentium-m`

- 1.86: crypto_stream/rabbit/e/opt/1/3
  using gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer
- 1.90: crypto_stream/rabbit/e/opt/2/3
  using gcc -m32 -march=pentium3 -O3 -fomit-frame-pointer
- 1.93: crypto_stream/rabbit/e/opt/1/4
  using gcc -m32 -march=k6-3 -O3 -fomit-frame-pointer
- 2.24: crypto_stream/rabbit/e/opt/1/2
  using gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer
- 2.24: crypto_stream/rabbit/e/opt/2/2
  using gcc -m32 -march=nocona -O -fomit-frame-pointer
- 2.68: crypto_stream/rabbit/e/opt/2/1
  using gcc -funroll-loops -m32 -march=pentium3 -O -fomit-frame-pointer
- 2.70: crypto_stream/rabbit/e/opt/1/1
  using gcc -funroll-loops -m32 -march=k8 -O -fomit-frame-pointer
- 2.95: crypto_stream/rabbit/e/ref
  using gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer
- 3.64: crypto_stream/rabbit/e/opt/2/4
  using gcc -m32 -march=i386
- 1.00: crypto_stream/salsa20/e/x86-xmm5
  using gcc -funroll-loops -m32 -march=pentium3 -Os -fomit-frame-pointer
- 1.12: crypto_stream/salsa20/e/x86-xmm4
  using gcc -m32 -O2 -fomit-frame-pointer
- 1.45: crypto_stream/salsa20/e/x86-xmm2
  using gcc -m32 -march=pentium4 -O -fomit-frame-pointer
- 1.70: crypto_stream/salsa20/e/x86-xmm
  using gcc -funroll-loops -m32 -march=pentium-mmx -O2 -fomit-frame-pointer
- 2.22: crypto_stream/salsa20/e/x86-athlon
  using gcc -m32 -march=i386 -O2 -fomit-frame-pointer
- 2.23: crypto_stream/salsa20/e/x86-2
  using gcc -m32 -march=prescott -O -fomit-frame-pointer
- 2.23: crypto_stream/salsa20/e/x86-3
  using gcc -m32 -march=k6-3 -O3 -fomit-frame-pointer
- 2.23: crypto_stream/salsa20/e/x86-pm
  using gcc -m32 -march=pentium4 -Os -fomit-frame-pointer
- 2.26: crypto_stream/salsa20/e/x86-mmx
  using gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer

- 2.30: `crypto_stream/salsa20/e/x86-1`
  using `gcc -m32 -march=pentium-m -O3 -fomit-frame-pointer`
- 2.49: `crypto_stream/salsa20/e/merged`
  using `gcc -m32 -march=k6-3 -O -fomit-frame-pointer`
- 3.00: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium -O -fomit-frame-pointer`
- 3.36: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer`
- 3.43: `crypto_stream/salsa20/ref`
  using `gcc -m32 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/x86-xmm5`
  using `gcc -m32 -march=nocona -O3 -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa2012/e/x86-xmm4`
  using `gcc -m32 -march=k6-3 -Os -fomit-frame-pointer`
- 1.39: `crypto_stream/salsa2012/e/x86-xmm2`
  using `gcc -funroll-loops -m32 -march=pentium2 -O2 -fomit-frame-pointer`
- 1.67: `crypto_stream/salsa2012/e/x86-xmm`
  using `gcc -m32 -march=athlon -O -fomit-frame-pointer`
- 2.18: `crypto_stream/salsa2012/e/x86-athlon`
  using `gcc -funroll-loops -m32 -march=pentium-m -Os -fomit-frame-pointer`
- 2.19: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -m32 -march=nocona -Os -fomit-frame-pointer`
- 2.20: `crypto_stream/salsa2012/e/x86-2`
  using `gcc -m32 -march=prescott -O3 -fomit-frame-pointer`
- 2.20: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 2.20: `crypto_stream/salsa2012/e/x86-mmx`
  using `gcc -funroll-loops -m32 -march=pentium-m -O -fomit-frame-pointer`
- 2.25: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 2.53: `crypto_stream/salsa2012/e/merged`
  using `gcc -funroll-loops -m32 -march=k6-2 -O -fomit-frame-pointer`
- 3.15: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -m32 -O -fomit-frame-pointer`
- 3.57: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -m32 -march=k6-3 -O3 -fomit-frame-pointer`

- 3.68: crypto_stream/salsa2012/ref
  using gcc -m32 -Os -fomit-frame-pointer
- 1.00: crypto_stream/salsa208/e/x86-xmm5
  using gcc -m32 -march=i386 -Os -fomit-frame-pointer
- 1.13: crypto_stream/salsa208/e/x86-xmm4
  using gcc -m32 -march=k6-2 -O -fomit-frame-pointer
- 1.38: crypto_stream/salsa208/e/x86-xmm2
  using gcc -m32 -march=k6-2 -O2 -fomit-frame-pointer
- 1.61: crypto_stream/salsa208/e/x86-xmm
  using gcc -m32 -march=pentium2 -O2 -fomit-frame-pointer
- 2.13: crypto_stream/salsa208/e/x86-mmx
  using gcc -m32 -march=athlon -O -fomit-frame-pointer
- 2.14: crypto_stream/salsa208/e/x86-athlon
  using gcc -m32 -march=athlon -O -fomit-frame-pointer
- 2.15: crypto_stream/salsa208/e/x86-2
  using gcc -m32 -march=pentium2 -O2 -fomit-frame-pointer
- 2.15: crypto_stream/salsa208/e/x86-3
  using gcc -m32 -march=k8 -O3 -fomit-frame-pointer
- 2.17: crypto_stream/salsa208/e/x86-pm
  using gcc -m32 -march=k8 -O -fomit-frame-pointer
- 2.19: crypto_stream/salsa208/e/x86-1
  using gcc -funroll-loops -m32 -march=pentium3 -O -fomit-frame-pointer
- 2.32: crypto_stream/salsa208/e/merged
  using gcc -funroll-loops -m32 -march=pentium-m -O -fomit-frame-pointer
- 3.32: crypto_stream/salsa208/e/regs
  using gcc -funroll-loops -m32 -O -fomit-frame-pointer
- 3.77: crypto_stream/salsa208/e/ref
  using gcc -funroll-loops -m32 -march=pentium-mmx -O -fomit-frame-pointer
- 3.80: crypto_stream/salsa208/ref
  using gcc -m32 -march=pentium -Os -fomit-frame-pointer
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -funroll-loops -m32 -march=k6-3 -O -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -funroll-loops -m32 -march=athlon -O -fomit-frame-pointer
- 1.00: crypto_stream/tpy/e/tpy
  using gcc -funroll-loops -m32 -march=nocona -Os -fomit-frame-pointer

- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -funroll-loops -m32 -march=prescott -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -m32 -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer`

5.31 x86, 2401MHz, Intel Pentium 4 (f24), `nmi0086`

- 1.00: `crypto_dh/claus/gmp`
  using `g++ -m32 -O3 -fomit-frame-pointer`
- 2.86: `crypto_dh/claus/openssl`
  using `gcc -m32`
- 1.00: `crypto_dh/curve25519/mpfq`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_dh/surf127eps/mpfq`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `cc`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `gcc -m32`
- 1.00: `crypto_hash/md2/openssl`
  using `cc`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.08: `crypto_hash/md5/openssl`
  using `cc`

- 1.00: crypto_hash/ripemd160/openssl
  using cc
- 1.00: crypto_hash/sha1/openssl
  using gcc -m32
- 1.00: crypto_hash/sha256/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/sha512/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/whirlpool/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/md5/x86-1
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.16: crypto_hashblocks/md5/little-1
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.65: crypto_hashblocks/md5/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha256/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha512/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/bls/ref
  using g++ -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/rainbow/ref
  using g++ -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald1024/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald1536/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald2048/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald3072/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald4096/openssl
  using gcc -m32
- 1.00: crypto_sign/ronald512/openssl
  using gcc -m32 -O3 -fomit-frame-pointer

- 1.00: `crypto_sign/ronald768/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/bernstein/x86-mmx-1`
  using `gcc -m32`
- 1.46: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.64: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.66: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.08: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.29: `crypto_stream/aes128estream/e/gladman`
  using `cc`
- 2.87: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.88: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.62: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.20: `crypto_stream/aes256estream/e/gladman`
  using `cc`
- 1.32: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/x86-xmm6`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.26: `crypto_stream/chacha12/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.66: `crypto_stream/chacha12/e/x86-1`
  using `cc`
- 1.73: `crypto_stream/chacha12/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.91: `crypto_stream/chacha12/e/x86-mmx`
  using `gcc -m32`
- 1.97: `crypto_stream/chacha12/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.06: `crypto_stream/chacha12/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.24: `crypto_stream/chacha12/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 6.42: `crypto_stream/chacha12/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/x86-xmm6`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.25: `crypto_stream/chacha20/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.67: `crypto_stream/chacha20/e/x86-1`
  using `cc`
- 1.71: `crypto_stream/chacha20/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.06: `crypto_stream/chacha20/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.06: `crypto_stream/chacha20/e/x86-mmx`
  using `gcc -m32`
- 2.10: `crypto_stream/chacha20/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.12: `crypto_stream/chacha20/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 6.40: `crypto_stream/chacha20/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/x86-xmm6`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.27: `crypto_stream/chacha8/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.59: `crypto_stream/chacha8/e/x86-1`
  using `gcc -m32`
- 1.66: `crypto_stream/chacha8/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.79: `crypto_stream/chacha8/e/x86-mmx`
  using `cc`
- 1.93: `crypto_stream/chacha8/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.94: `crypto_stream/chacha8/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.42: `crypto_stream/chacha8/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 6.57: `crypto_stream/chacha8/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.04: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.31: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/5`
  using `gcc -m32`
- 1.44: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.44: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.47: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.86: `crypto_stream/rabbit/e/opt/2/4`
  using `cc`
- 2.09: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.09: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.53: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.55: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.46: `crypto_stream/rabbit/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.31: `crypto_stream/salsa20/e/x86-xmm4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.39: `crypto_stream/salsa20/e/x86-2`
  using `cc`
- 1.39: `crypto_stream/salsa20/e/x86-3`
  using `cc`
- 1.39: `crypto_stream/salsa20/e/x86-athlon`
  using `cc`
- 1.42: `crypto_stream/salsa20/e/x86-pm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.91: `crypto_stream/salsa20/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.17: `crypto_stream/salsa20/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.65: `crypto_stream/salsa20/e/x86-mmx`
  using `gcc -m32`
- 2.75: `crypto_stream/salsa20/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.86: `crypto_stream/salsa20/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 2.88: `crypto_stream/salsa20/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.98: `crypto_stream/salsa20/e/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.19: `crypto_stream/salsa20/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.23: `crypto_stream/salsa2012/e/x86-xmm4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa2012/e/x86-2`
  using `cc`
- 1.41: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -m32`
- 1.41: `crypto_stream/salsa2012/e/x86-athlon`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.45: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -m32`
- 1.86: `crypto_stream/salsa2012/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.10: `crypto_stream/salsa2012/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.57: `crypto_stream/salsa2012/e/x86-mmx`
  using `gcc -m32`
- 2.78: `crypto_stream/salsa2012/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.79: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.83: `crypto_stream/salsa2012/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.25: `crypto_stream/salsa2012/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.55: `crypto_stream/salsa2012/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.22: `crypto_stream/salsa208/e/x86-xmm4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.35: `crypto_stream/salsa208/e/x86-pm`
  using `cc`
- 1.36: `crypto_stream/salsa208/e/x86-2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.36: `crypto_stream/salsa208/e/x86-3`
  using `cc`
- 1.38: `crypto_stream/salsa208/e/x86-athlon`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.74: `crypto_stream/salsa208/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.77: `crypto_stream/salsa208/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.38: `crypto_stream/salsa208/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.46: `crypto_stream/salsa208/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.65: `crypto_stream/salsa208/e/x86-1`
  using `cc`
- 2.86: `crypto_stream/salsa208/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.43: `crypto_stream/salsa208/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.80: `crypto_stream/salsa208/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -m32 -O3 -fomit-frame-pointer`

5.32 x86, 2658MHz, Intel Xeon (f25), `nmi0013`

- 1.00: `crypto_dh/claus/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -m32`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `gcc -m32`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -m32`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.09: `crypto_hash/md5/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -m32`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -m32`
- 1.00: `crypto_hash/sha224/openssl`
  using `gcc -m32`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.30: `crypto_hash/sha256/openssl`
  using `gcc -m32`

- 1.00: `crypto_hash/sha384/openssl`
  using `gcc -m32`
- 1.00: `crypto_hash/sha512/openssl`
  using `cc`
- 3.45: `crypto_hash/sha512/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.05: `crypto_hashblocks/md5/little-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.43: `crypto_hashblocks/md5/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha256/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha512/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/bls/ref`
  using `g++ -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/rainbow/ref`
  using `g++ -m32`
- 1.00: `crypto_sign/ronald1024/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1536/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald2048/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald3072/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald4096/openssl`
  using `cc`
- 1.00: `crypto_sign/ronald512/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald768/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/bernstein/x86-mmx-1`
  using `gcc -m32`
- 1.26: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.74: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.08: `crypto_stream/aes128estream/e/gladman`
  using `gcc -m32`
- 2.10: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.20: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.95: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.10: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.80: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.43: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.50: `crypto_stream/aes256estream/e/gladman`
  using `cc`
- 1.00: `crypto_stream/chacha12/e/x86-xmm6`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.04: `crypto_stream/chacha12/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.25: `crypto_stream/chacha12/e/x86-1`
  using `gcc -m32`
- 1.35: `crypto_stream/chacha12/e/x86-mmx`
  using `gcc -m32`
- 1.38: `crypto_stream/chacha12/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.76: `crypto_stream/chacha12/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.78: `crypto_stream/chacha12/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.88: `crypto_stream/chacha12/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 6.51: `crypto_stream/chacha12/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/x86-xmm6`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.11: `crypto_stream/chacha20/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.35: `crypto_stream/chacha20/e/x86-1`
  using `cc`
- 1.46: `crypto_stream/chacha20/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.49: `crypto_stream/chacha20/e/x86-mmx`
  using `gcc -m32`
- 1.91: `crypto_stream/chacha20/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.94: `crypto_stream/chacha20/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.96: `crypto_stream/chacha20/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 6.38: `crypto_stream/chacha20/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/x86-xmm6`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/chacha8/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.21: `crypto_stream/chacha8/e/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.28: `crypto_stream/chacha8/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.70: `crypto_stream/chacha8/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.70: `crypto_stream/chacha8/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.79: `crypto_stream/chacha8/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 4.96: `crypto_stream/chacha8/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 6.37: `crypto_stream/chacha8/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.03: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.23: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.06: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.60: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/5`
  using `gcc -m32`
- 1.32: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.33: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.61: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.74: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.79: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.85: `crypto_stream/rabbit/e/opt/2/4`
  using `cc`
- 2.24: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.25: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.65: `crypto_stream/rabbit/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.34: `crypto_stream/salsa20/e/x86-xmm4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa20/e/x86-3`
  using `gcc -m32`
- 1.42: `crypto_stream/salsa20/e/x86-athlon`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa20/e/x86-pm`
  using `gcc -m32`
- 1.43: `crypto_stream/salsa20/e/x86-2`
  using `gcc -m32`
- 1.67: `crypto_stream/salsa20/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.84: `crypto_stream/salsa20/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.96: `crypto_stream/salsa20/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.18: `crypto_stream/salsa20/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.54: `crypto_stream/salsa20/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.71: `crypto_stream/salsa20/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 2.99: `crypto_stream/salsa20/e/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.56: `crypto_stream/salsa20/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.35: `crypto_stream/salsa2012/e/x86-xmm4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa2012/e/x86-2`
  using `gcc -m32`
- 1.42: `crypto_stream/salsa2012/e/x86-athlon`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.43: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -m32`
- 1.50: `crypto_stream/salsa2012/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.90: `crypto_stream/salsa2012/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.14: `crypto_stream/salsa2012/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.27: `crypto_stream/salsa2012/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.60: `crypto_stream/salsa2012/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.66: `crypto_stream/salsa2012/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.81: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -m32`
- 3.79: `crypto_stream/salsa2012/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.35: `crypto_stream/salsa208/e/x86-xmm4`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.41: `crypto_stream/salsa208/e/x86-2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa208/e/x86-athlon`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa208/e/x86-3`
  using `gcc -m32`
- 1.42: `crypto_stream/salsa208/e/x86-pm`
  using `gcc -m32`
- 1.78: `crypto_stream/salsa208/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.81: `crypto_stream/salsa208/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.91: `crypto_stream/salsa208/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.49: `crypto_stream/salsa208/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.76: `crypto_stream/salsa208/e/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.90: `crypto_stream/salsa208/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.41: `crypto_stream/salsa208/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.46: `crypto_stream/salsa208/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -m32 -O3 -fomit-frame-pointer`

5.33 x86, 2658MHz, Intel Xeon (f25), `nmibuild15`

- 1.00: `crypto_dh/claus/openssl`
  using `gcc -funroll-loops -march=k6 -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/mceliece/ref`
  using `gcc -funroll-loops -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -funroll-loops -march=pentium -Os -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -march=i486`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -funroll-loops -march=i386 -Os -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -funroll-loops -march=athlon -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -march=i486`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `gcc -march=pentiumpro`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -march=k6 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -march=athlon -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/openssl`
  using `gcc -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -funroll-loops -O -fomit-frame-pointer`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -march=athlon -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -march=k6 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/ref`
  using `gcc -funroll-loops -O -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -funroll-loops -march=pentiumpro -O -fomit-frame-pointer`

- 1.00: `crypto_hashblocks/md5/x86-1`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 1.15: `crypto_hashblocks/md5/little-1`
  using `gcc -march=k6 -O -fomit-frame-pointer`
- 1.59: `crypto_hashblocks/md5/ref`
  using `gcc -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha256/ref`
  using `gcc -march=pentium -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha512/ref`
  using `gcc -march=athlon -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/bls/ref`
  using `g++ -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/donald1024/openssl`
  using `gcc -funroll-loops -march=pentiumpro -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/donald2048/openssl`
  using `gcc`
- 1.00: `crypto_sign/donald512/openssl`
  using `gcc -funroll-loops -march=athlon -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/rainbow/ref`
  using `g++ -march=athlon -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1024/openssl`
  using `gcc -march=pentiumpro -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1536/openssl`
  using `gcc -march=pentiumpro -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald2048/openssl`
  using `gcc -march=pentiumpro -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald3072/openssl`
  using `gcc -funroll-loops -march=k6 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald4096/openssl`
  using `gcc -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald512/openssl`
  using `gcc -march=athlon -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald768/openssl`
  using `gcc -march=athlon -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -funroll-loops -march=k6 -O -fomit-frame-pointer`

- 1.00: `crypto_stream/aes128estream/e/bernstein/x86-mmx-1`
  using `gcc -march=pentium -Os -fomit-frame-pointer`
- 1.08: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -march=athlon -O -fomit-frame-pointer`
- 1.18: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -march=athlon -O -fomit-frame-pointer`
- 1.62: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -O -fomit-frame-pointer`
- 1.65: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -funroll-loops -march=athlon -O2 -fomit-frame-pointer`
- 1.66: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -funroll-loops -march=i386 -O -fomit-frame-pointer`
- 1.70: `crypto_stream/aes128estream/e/gladman`
  using `gcc -march=athlon -O -fomit-frame-pointer`
- 1.71: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -funroll-loops -march=athlon -O3 -fomit-frame-pointer`
- 1.98: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -funroll-loops -march=athlon -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -march=athlon -O -fomit-frame-pointer`
- 1.11: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -march=pentiumpro -O -fomit-frame-pointer`
- 1.47: `crypto_stream/aes256estream/e/gladman`
  using `gcc -funroll-loops -march=pentiumpro -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/x86-xmm6`
  using `gcc -march=i386`
- 1.09: `crypto_stream/chacha12/e/x86-xmm5`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.32: `crypto_stream/chacha12/e/x86-1`
  using `gcc -march=athlon`
- 1.43: `crypto_stream/chacha12/e/x86-mmx`
  using `gcc -funroll-loops -march=i386 -O3 -fomit-frame-pointer`
- 1.69: `crypto_stream/chacha12/e/x86-xmm`
  using `gcc -funroll-loops -march=athlon`
- 1.81: `crypto_stream/chacha12/e/x86-xmm2`
  using `gcc -funroll-loops -march=i386 -O -fomit-frame-pointer`

- 2.77: `crypto_stream/chacha12/e/ref`
  using `gcc -march=k6 -O -fomit-frame-pointer`
- 3.98: `crypto_stream/chacha12/e/merged`
  using `gcc -funroll-loops -march=i386 -O -fomit-frame-pointer`
- 4.32: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -march=i486 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/x86-xmm6`
  using `gcc -march=i386`
- 1.14: `crypto_stream/chacha20/e/x86-xmm5`
  using `gcc -march=athlon -O3 -fomit-frame-pointer`
- 1.38: `crypto_stream/chacha20/e/x86-1`
  using `gcc -march=athlon -O2 -fomit-frame-pointer`
- 1.53: `crypto_stream/chacha20/e/x86-mmx`
  using `gcc -funroll-loops -march=pentium -O2 -fomit-frame-pointer`
- 1.71: `crypto_stream/chacha20/e/x86-xmm`
  using `gcc -O -fomit-frame-pointer`
- 1.94: `crypto_stream/chacha20/e/x86-xmm2`
  using `gcc -march=pentiumpro -O -fomit-frame-pointer`
- 2.45: `crypto_stream/chacha20/e/ref`
  using `gcc -march=i486 -O -fomit-frame-pointer`
- 4.13: `crypto_stream/chacha20/e/merged`
  using `gcc -funroll-loops -march=pentium -O -fomit-frame-pointer`
- 4.46: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -march=pentiumpro -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/x86-xmm6`
  using `gcc -funroll-loops -march=athlon -Os -fomit-frame-pointer`
- 1.05: `crypto_stream/chacha8/e/x86-xmm5`
  using `gcc -funroll-loops -march=pentium -O3 -fomit-frame-pointer`
- 1.26: `crypto_stream/chacha8/e/x86-1`
  using `gcc -march=pentium -O2 -fomit-frame-pointer`
- 1.34: `crypto_stream/chacha8/e/x86-mmx`
  using `gcc -march=pentium -O2 -fomit-frame-pointer`
- 1.69: `crypto_stream/chacha8/e/x86-xmm2`
  using `gcc -O -fomit-frame-pointer`
- 1.71: `crypto_stream/chacha8/e/x86-xmm`
  using `gcc -march=pentiumpro -O -fomit-frame-pointer`

- 3.02: `crypto_stream/chacha8/e/ref`
  using `gcc -march=i386 -O -fomit-frame-pointer`
- 3.62: `crypto_stream/chacha8/e/merged`
  using `gcc -funroll-loops -march=i386 -O -fomit-frame-pointer`
- 4.00: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -march=pentiumpro -O -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -march=athlon -O -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -funroll-loops -march=pentiumpro -O -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -march=pentium -O -fomit-frame-pointer`
- 1.01: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -march=pentium -O -fomit-frame-pointer`
- 1.18: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -march=pentiumpro -O -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -march=pentium -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -funroll-loops -O -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.48: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -march=k6 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -funroll-loops -march=pentium -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -march=pentium -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -funroll-loops -march=pentium -O2 -fomit-frame-pointer`
- 1.13: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -march=pentium -O -fomit-frame-pointer`
- 1.14: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -march=pentium -O -fomit-frame-pointer`

- 1.55: `crypto_stream/rabbit/e/opt/2/4`
  using `gcc -funroll-loops -march=i486`
- 1.68: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -march=athlon -O -fomit-frame-pointer`
- 1.68: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -march=pentium -O2 -fomit-frame-pointer`
- 2.54: `crypto_stream/rabbit/e/ref`
  using `gcc -funroll-loops -march=pentium -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/x86-xmm5`
  using `gcc -march=athlon -O3 -fomit-frame-pointer`
- 1.21: `crypto_stream/salsa20/e/x86-xmm4`
  using `gcc -funroll-loops -march=athlon -Os -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa20/e/x86-2`
  using `gcc -Os -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa20/e/x86-3`
  using `gcc -O3 -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa20/e/x86-athlon`
  using `gcc -march=pentium -O2 -fomit-frame-pointer`
- 1.45: `crypto_stream/salsa20/e/x86-pm`
  using `gcc -march=i486 -O2 -fomit-frame-pointer`
- 1.61: `crypto_stream/salsa20/e/x86-xmm`
  using `gcc -funroll-loops -march=i386 -Os -fomit-frame-pointer`
- 1.72: `crypto_stream/salsa20/e/x86-xmm2`
  using `gcc -Os -fomit-frame-pointer`
- 2.68: `crypto_stream/salsa20/e/ref`
  using `gcc -march=athlon -O -fomit-frame-pointer`
- 2.71: `crypto_stream/salsa20/e/x86-mmx`
  using `gcc -funroll-loops -march=pentiumpro -O2 -fomit-frame-pointer`
- 2.91: `crypto_stream/salsa20/e/x86-1`
  using `gcc -march=k6 -O -fomit-frame-pointer`
- 2.93: `crypto_stream/salsa20/e/merged`
  using `gcc -funroll-loops -march=pentium -Os -fomit-frame-pointer`
- 3.03: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -march=pentiumpro -O3 -fomit-frame-pointer`
- 3.46: `crypto_stream/salsa20/ref`
  using `gcc -march=pentiumpro -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/salsa2012/e/x86-xmm5`
  using `gcc -funroll-loops -march=pentium -O3 -fomit-frame-pointer`
- 1.24: `crypto_stream/salsa2012/e/x86-xmm4`
  using `gcc -funroll-loops -march=pentiumpro -O -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa2012/e/x86-2`
  using `gcc -march=pentium -O2 -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -march=pentiumpro -O2 -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa2012/e/x86-athlon`
  using `gcc -march=i486 -O -fomit-frame-pointer`
- 1.46: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -funroll-loops -march=athlon -O2 -fomit-frame-pointer`
- 1.72: `crypto_stream/salsa2012/e/x86-xmm`
  using `gcc -funroll-loops -march=i386 -Os -fomit-frame-pointer`
- 1.86: `crypto_stream/salsa2012/e/x86-xmm2`
  using `gcc -march=pentium -Os -fomit-frame-pointer`
- 2.61: `crypto_stream/salsa2012/e/x86-mmx`
  using `gcc -O3 -fomit-frame-pointer`
- 2.81: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -funroll-loops -march=i486 -O2 -fomit-frame-pointer`
- 2.82: `crypto_stream/salsa2012/e/merged`
  using `gcc -march=pentium -Os -fomit-frame-pointer`
- 3.03: `crypto_stream/salsa2012/e/ref`
  using `gcc -march=athlon -O -fomit-frame-pointer`
- 3.05: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -march=pentiumpro -O2 -fomit-frame-pointer`
- 3.79: `crypto_stream/salsa2012/ref`
  using `gcc -funroll-loops -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/x86-xmm5`
  using `gcc -funroll-loops -march=pentium -O3 -fomit-frame-pointer`
- 1.27: `crypto_stream/salsa208/e/x86-xmm4`
  using `gcc -march=k6 -O -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa208/e/x86-2`
  using `gcc -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa208/e/x86-3`
  using `gcc -funroll-loops -march=athlon -O -fomit-frame-pointer`

- 1.41: crypto_stream/salsa208/e/x86-pm
  using gcc -march=pentiumpro -O2 -fomit-frame-pointer
- 1.42: crypto_stream/salsa208/e/x86-athlon
  using gcc -funroll-loops
- 1.56: crypto_stream/salsa208/e/x86-xmm
  using gcc -funroll-loops -march=i486 -Os -fomit-frame-pointer
- 1.79: crypto_stream/salsa208/e/x86-xmm2
  using gcc -march=k6 -O2 -fomit-frame-pointer
- 2.50: crypto_stream/salsa208/e/x86-mmx
  using gcc -march=athlon -O2 -fomit-frame-pointer
- 2.51: crypto_stream/salsa208/e/x86-1
  using gcc -O3 -fomit-frame-pointer
- 2.79: crypto_stream/salsa208/e/merged
  using gcc -funroll-loops -march=k6 -Os -fomit-frame-pointer
- 3.23: crypto_stream/salsa208/e/regs
  using gcc -funroll-loops -march=k6 -O -fomit-frame-pointer
- 3.30: crypto_stream/salsa208/e/ref
  using gcc -march=athlon -O -fomit-frame-pointer
- 4.06: crypto_stream/salsa208/ref
  using gcc -march=pentiumpro -O3 -fomit-frame-pointer
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -funroll-loops -march=i486 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -funroll-loops -march=pentiumpro -O -fomit-frame-pointer
- 1.00: crypto_stream/trivium/e/submissions/trivium
  using gcc -funroll-loops -march=pentiumpro -O2 -fomit-frame-pointer

5.34 x86, 2658MHz, Intel Xeon (f25), nmibuild16

- 1.00: crypto_dh/claus/gmp
  using g++ -m32 -O3 -fomit-frame-pointer
- 2.66: crypto_dh/claus/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_dh/curve25519/mpfq
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_dh/surf127eps/mpfq
  using gcc -m32 -O3 -fomit-frame-pointer

- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `cc`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `cc`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.01: `crypto_hash/md5/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -m32`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -m32`
- 1.00: `crypto_hash/sha512/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.17: `crypto_hashblocks/md5/little-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.72: `crypto_hashblocks/md5/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.00: `crypto_hashblocks/sha256/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha512/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/bls/ref`
  using `g++ -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1024/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1536/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald2048/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald3072/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald4096/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald512/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald768/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/bernstein/x86-mmx-1`
  using `gcc -m32`
- 1.69: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.81: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.84: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.06: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.07: `crypto_stream/aes128estream/e/gladman`
  using `gcc -m32`
- 2.50: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 2.76: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.20: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/gladman`
  using `cc`
- 1.39: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.71: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/x86-xmm6`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.11: `crypto_stream/chacha12/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.34: `crypto_stream/chacha12/e/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.44: `crypto_stream/chacha12/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.83: `crypto_stream/chacha12/e/x86-xmm2`
  using `gcc -m32`
- 1.91: `crypto_stream/chacha12/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 4.38: `crypto_stream/chacha12/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 5.47: `crypto_stream/chacha12/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 7.31: `crypto_stream/chacha12/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/x86-xmm6`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/chacha20/e/x86-xmm5`
  using `cc`
- 1.24: `crypto_stream/chacha20/e/x86-1`
  using `gcc -m32`
- 1.36: `crypto_stream/chacha20/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.73: `crypto_stream/chacha20/e/x86-xmm2`
  using `gcc -m32`
- 1.76: `crypto_stream/chacha20/e/x86-xmm`
  using `gcc -m32`
- 4.05: `crypto_stream/chacha20/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 5.28: `crypto_stream/chacha20/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 5.47: `crypto_stream/chacha20/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/x86-xmm5`
  using `cc`
- 1.00: `crypto_stream/chacha8/e/x86-xmm6`
  using `cc`
- 1.21: `crypto_stream/chacha8/e/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.26: `crypto_stream/chacha8/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.59: `crypto_stream/chacha8/e/x86-xmm2`
  using `gcc -m32`
- 1.62: `crypto_stream/chacha8/e/x86-xmm`
  using `cc`
- 3.81: `crypto_stream/chacha8/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 5.06: `crypto_stream/chacha8/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 6.32: `crypto_stream/chacha8/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.20: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.41: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.33: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.76: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/5`
  using `gcc -m32`
- 1.38: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.39: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.97: `crypto_stream/rabbit/e/opt/2/4`
  using `gcc -m32`
- 2.03: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.44: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.45: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.46: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.47: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 4.01: `crypto_stream/rabbit/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/x86-xmm5`
  using `cc`
- 1.21: `crypto_stream/salsa20/e/x86-xmm4`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.42: `crypto_stream/salsa20/e/x86-2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa20/e/x86-3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa20/e/x86-athlon`
  using `cc`
- 1.47: `crypto_stream/salsa20/e/x86-pm`
  using `gcc -m32`
- 1.55: `crypto_stream/salsa20/e/x86-xmm`
  using `cc`
- 1.92: `crypto_stream/salsa20/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.70: `crypto_stream/salsa20/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.88: `crypto_stream/salsa20/e/x86-1`
  using `gcc -m32`
- 3.50: `crypto_stream/salsa20/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.52: `crypto_stream/salsa20/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.55: `crypto_stream/salsa20/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 4.00: `crypto_stream/salsa20/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/x86-xmm5`
  using `cc`
- 1.24: `crypto_stream/salsa2012/e/x86-xmm4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.44: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -m32`
- 1.45: `crypto_stream/salsa2012/e/x86-2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.46: `crypto_stream/salsa2012/e/x86-athlon`
  using `cc`
- 1.49: `crypto_stream/salsa2012/e/x86-pm`
  using `cc`

- 1.63: `crypto_stream/salsa2012/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.87: `crypto_stream/salsa2012/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.60: `crypto_stream/salsa2012/e/x86-mmx`
  using `gcc -m32`
- 2.84: `crypto_stream/salsa2012/e/x86-1`
  using `cc`
- 3.22: `crypto_stream/salsa2012/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.78: `crypto_stream/salsa2012/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 4.08: `crypto_stream/salsa2012/e/merged`
  using `gcc -m32`
- 4.42: `crypto_stream/salsa2012/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/x86-xmm5`
  using `cc`
- 1.27: `crypto_stream/salsa208/e/x86-xmm4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.44: `crypto_stream/salsa208/e/x86-athlon`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.44: `crypto_stream/salsa208/e/x86-pm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.45: `crypto_stream/salsa208/e/x86-2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.45: `crypto_stream/salsa208/e/x86-3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.78: `crypto_stream/salsa208/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.81: `crypto_stream/salsa208/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.49: `crypto_stream/salsa208/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.70: `crypto_stream/salsa208/e/x86-1`
  using `gcc -m32`

- 3.32: crypto_stream/salsa208/e/merged
  using gcc -m32 -O3 -fomit-frame-pointer
- 4.10: crypto_stream/salsa208/e/regs
  using gcc -m32 -O3 -fomit-frame-pointer
- 4.57: crypto_stream/salsa208/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 5.11: crypto_stream/salsa208/e/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpy/e/tpy
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpy6/e/tpy6
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpypy/e/tpypy
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/trivium/e/submissions/trivium
  using gcc -m32 -O3 -fomit-frame-pointer

5.35 x86, 2658MHz, Intel Xeon (f25), nmibuild22

- 1.00: crypto_dh/claus/openssl
  using gcc -m32 -march=k6 -Os -fomit-frame-pointer
- 1.00: crypto_encrypt/mceliece/ref
  using gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ntruees787ep1/ref
  using gcc -funroll-loops -march=athlon -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald1024/openssl
  using gcc -m32 -march=athlon -O2 -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald1536/openssl
  using gcc -m32 -march=pentium-mmx -O -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald2048/openssl
  using gcc -m32 -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald3072/openssl
  using gcc -m32 -march=pentiumpro

- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `gcc -O -fomit-frame-pointer`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -m32 -march=k6-3 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -m32 -march=prescott -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/openssl`
  using `gcc -m32 -march=pentium -O -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -funroll-loops -march=pentium3 -O -fomit-frame-pointer`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -funroll-loops -m32 -march=pentium2 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -m32 -O -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -funroll-loops -march=i386 -O -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/ref`
  using `gcc -funroll-loops -march=pentium2 -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -funroll-loops -march=prescott -O -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/x86-1`
  using `gcc -m32 -march=k8 -Os -fomit-frame-pointer`
- 1.15: `crypto_hashblocks/md5/little-1`
  using `gcc -m32 -march=k8 -O -fomit-frame-pointer`
- 1.59: `crypto_hashblocks/md5/ref`
  using `gcc -m32 -march=i386 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha256/ref`
  using `gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha512/ref`
  using `gcc -funroll-loops -march=i386 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/bls/ref`
  using `g++ -m32 -march=prescott -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/donald1024/openssl`
  using `gcc -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_sign/donald2048/openssl`
  using `gcc -funroll-loops -m32 -march=nocona -Os -fomit-frame-pointer`

- 1.00: crypto_sign/donald512/openssl
  using gcc -funroll-loops -m32 -march=prescott -Os -fomit-frame-pointer
- 1.00: crypto_sign/ronald1024/openssl
  using gcc -funroll-loops -m32 -march=k8 -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald1536/openssl
  using gcc -funroll-loops -march=pentium3 -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald2048/openssl
  using gcc -funroll-loops -m32 -march=pentium3 -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald3072/openssl
  using gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald4096/openssl
  using gcc -march=k6-3 -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald512/openssl
  using gcc -m32 -march=k6 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald768/openssl
  using gcc -funroll-loops -march=pentium-mmx -O -fomit-frame-pointer
- 1.00: crypto_sign/sflashv2/ref
  using gcc -m32 -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes128estream/e/bernstein/x86-mmx-1
  using gcc -funroll-loops -march=pentium3 -O3 -fomit-frame-pointer
- 1.05: crypto_stream/aes128estream/e/hongjun/v1
  using gcc -funroll-loops -m32 -march=k6 -O -fomit-frame-pointer
- 1.18: crypto_stream/aes128estream/e/hongjun/v0
  using gcc -march=pentium4 -O -fomit-frame-pointer
- 1.44: crypto_stream/aes128estream/e/bernstein/little-3
  using gcc -funroll-loops -march=k6 -Os -fomit-frame-pointer
- 1.54: crypto_stream/aes128estream/e/bernstein/little-4
  using gcc -m32 -march=pentium4 -O -fomit-frame-pointer
- 1.60: crypto_stream/aes128estream/e/gladman
  using gcc -m32 -march=pentiumpro -O -fomit-frame-pointer
- 1.65: crypto_stream/aes128estream/e/bernstein/little-1
  using gcc -funroll-loops -m32 -march=pentium4 -O2 -fomit-frame-pointer
- 1.70: crypto_stream/aes128estream/e/bernstein/little-2
  using gcc -m32 -march=k8 -O3 -fomit-frame-pointer
- 1.92: crypto_stream/aes128estream/e/bernstein/big-1
  using gcc -m32 -march=pentium2 -Os -fomit-frame-pointer

- 1.00: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -funroll-loops -m32 -O -fomit-frame-pointer`
- 1.06: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -march=pentium4 -O -fomit-frame-pointer`
- 1.39: `crypto_stream/aes256estream/e/gladman`
  using `gcc -m32 -march=pentium3 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/x86-xmm6`
  using `gcc -m32 -march=athlon`
- 1.12: `crypto_stream/chacha12/e/x86-xmm5`
  using `gcc -march=k8 -O -fomit-frame-pointer`
- 1.36: `crypto_stream/chacha12/e/x86-1`
  using `gcc -m32 -march=k8 -O3 -fomit-frame-pointer`
- 1.47: `crypto_stream/chacha12/e/x86-mmx`
  using `gcc -m32 -march=nocona -O3 -fomit-frame-pointer`
- 1.86: `crypto_stream/chacha12/e/x86-xmm2`
  using `gcc -funroll-loops -m32 -march=pentium -O -fomit-frame-pointer`
- 1.90: `crypto_stream/chacha12/e/x86-xmm`
  using `gcc -funroll-loops -march=pentium-mmx -O -fomit-frame-pointer`
- 3.43: `crypto_stream/chacha12/e/merged`
  using `gcc -funroll-loops -m32 -march=k6-2 -O -fomit-frame-pointer`
- 3.88: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -m32 -march=i386 -O -fomit-frame-pointer`
- 3.96: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -march=athlon -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/x86-xmm6`
  using `gcc -funroll-loops -m32 -march=pentium4`
- 1.16: `crypto_stream/chacha20/e/x86-xmm5`
  using `gcc -m32 -march=athlon -O2 -fomit-frame-pointer`
- 1.41: `crypto_stream/chacha20/e/x86-1`
  using `gcc -march=pentium2 -O3 -fomit-frame-pointer`
- 1.56: `crypto_stream/chacha20/e/x86-mmx`
  using `gcc -march=pentium4 -O3 -fomit-frame-pointer`
- 1.98: `crypto_stream/chacha20/e/x86-xmm2`
  using `gcc -m32 -march=pentium3`
- 2.00: `crypto_stream/chacha20/e/x86-xmm`
  using `gcc -m32 -march=k8`

- 3.67: crypto_stream/chacha20/e/merged
  using gcc -funroll-loops -m32 -march=pentium -O -fomit-frame-pointer
- 4.11: crypto_stream/chacha20/e/ref
  using gcc -funroll-loops -march=nocona -O -fomit-frame-pointer
- 4.24: crypto_stream/chacha20/e/regs
  using gcc -funroll-loops -march=k6-3 -O -fomit-frame-pointer
- 1.00: crypto_stream/chacha8/e/x86-xmm6
  using gcc -march=pentium-mmx -O -fomit-frame-pointer
- 1.07: crypto_stream/chacha8/e/x86-xmm5
  using gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer
- 1.30: crypto_stream/chacha8/e/x86-1
  using gcc -funroll-loops -march=pentium2 -O3 -fomit-frame-pointer
- 1.38: crypto_stream/chacha8/e/x86-mmx
  using gcc -funroll-loops -march=pentium2 -O -fomit-frame-pointer
- 1.74: crypto_stream/chacha8/e/x86-xmm2
  using gcc -funroll-loops -m32 -march=pentium3 -O -fomit-frame-pointer
- 1.76: crypto_stream/chacha8/e/x86-xmm
  using gcc -m32 -march=k8
- 3.27: crypto_stream/chacha8/e/merged
  using gcc -funroll-loops -m32 -O -fomit-frame-pointer
- 3.77: crypto_stream/chacha8/e/regs
  using gcc -funroll-loops -m32 -march=athlon -O -fomit-frame-pointer
- 3.78: crypto_stream/chacha8/e/ref
  using gcc -funroll-loops -march=pentium2 -O -fomit-frame-pointer
- 1.00: crypto_stream/cryptmtv3/e/v3
  using gcc -funroll-loops -m32 -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/dragon/e/submissions/dragon
  using gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer
- 1.00: crypto_stream/hc128/e/hc-128/200606
  using gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer
- 1.00: crypto_stream/hc128/e/hc-128/200701b
  using gcc -march=pentium-mmx -O3 -fomit-frame-pointer
- 1.03: crypto_stream/hc128/e/hc-128/200701a
  using gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer
- 1.00: crypto_stream/hc256/e/hc-256/200511
  using gcc -funroll-loops -march=athlon -O2 -fomit-frame-pointer

- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -funroll-loops -m32 -march=athlon -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -funroll-loops -m32 -march=pentium2 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -march=i386 -O3 -fomit-frame-pointer`
- 1.50: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -march=k6-3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/5`
  using `gcc -m32 -march=nocona`
- 1.22: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.29: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer`
- 1.30: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -funroll-loops -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.56: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -m32 -march=pentium-mmx -O2 -fomit-frame-pointer`
- 1.62: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -march=pentium -Os -fomit-frame-pointer`
- 1.93: `crypto_stream/rabbit/e/opt/2/4`
  using `gcc -m32 -march=k6-3`
- 2.00: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -march=pentium -O2 -fomit-frame-pointer`
- 2.00: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -march=pentium -O2 -fomit-frame-pointer`
- 2.87: `crypto_stream/rabbit/e/ref`
  using `gcc -funroll-loops -march=pentium-mmx -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/x86-xmm5`
  using `gcc -m32 -march=athlon -O2 -fomit-frame-pointer`
- 1.20: `crypto_stream/salsa20/e/x86-xmm4`
  using `gcc -funroll-loops -m32 -O2 -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa20/e/x86-2`
  using `gcc -march=pentium4 -Os -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa20/e/x86-3`
  using `gcc -m32 -march=prescott -O2 -fomit-frame-pointer`

- 1.42: crypto_stream/salsa20/e/x86-athlon
  using gcc -m32 -march=i486 -O3 -fomit-frame-pointer
- 1.45: crypto_stream/salsa20/e/x86-pm
  using gcc -funroll-loops -m32 -march=pentium -O2 -fomit-frame-pointer
- 1.52: crypto_stream/salsa20/e/x86-xmm
  using gcc -funroll-loops -march=i486
- 1.72: crypto_stream/salsa20/e/x86-xmm2
  using gcc -funroll-loops -march=k6-3 -O3 -fomit-frame-pointer
- 2.65: crypto_stream/salsa20/e/regs
  using gcc -funroll-loops -march=pentiumpro -O3 -fomit-frame-pointer
- 2.71: crypto_stream/salsa20/e/x86-mmx
  using gcc -m32 -march=k6-3 -O -fomit-frame-pointer
- 2.84: crypto_stream/salsa20/e/merged
  using gcc -funroll-loops -march=k6-3 -Os -fomit-frame-pointer
- 2.91: crypto_stream/salsa20/e/x86-1
  using gcc -funroll-loops -march=pentium4 -O3 -fomit-frame-pointer
- 3.14: crypto_stream/salsa20/e/ref
  using gcc -funroll-loops -march=pentium4 -O2 -fomit-frame-pointer
- 3.38: crypto_stream/salsa20/ref
  using gcc -march=pentiumpro -O3 -fomit-frame-pointer
- 1.00: crypto_stream/salsa2012/e/x86-xmm5
  using gcc -m32 -march=pentium3 -O3 -fomit-frame-pointer
- 1.23: crypto_stream/salsa2012/e/x86-xmm4
  using gcc -march=prescott -O -fomit-frame-pointer
- 1.42: crypto_stream/salsa2012/e/x86-2
  using gcc -m32 -march=pentium -Os -fomit-frame-pointer
- 1.42: crypto_stream/salsa2012/e/x86-3
  using gcc -m32 -O2 -fomit-frame-pointer
- 1.42: crypto_stream/salsa2012/e/x86-athlon
  using gcc -funroll-loops -m32 -march=i386 -O3 -fomit-frame-pointer
- 1.42: crypto_stream/salsa2012/e/x86-pm
  using gcc -funroll-loops -m32 -march=nocona -Os -fomit-frame-pointer
- 1.52: crypto_stream/salsa2012/e/x86-xmm
  using gcc -funroll-loops -march=pentium3 -O -fomit-frame-pointer
- 1.76: crypto_stream/salsa2012/e/x86-xmm2
  using gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer

- 2.61: `crypto_stream/salsa2012/e/x86-mmx`
  using `gcc -m32 -march=nocona -O3 -fomit-frame-pointer`
- 2.70: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium2 -O3 -fomit-frame-pointer`
- 2.80: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -funroll-loops -m32 -march=pentium3 -O2 -fomit-frame-pointer`
- 2.81: `crypto_stream/salsa2012/e/merged`
  using `gcc -funroll-loops -march=pentium4 -Os -fomit-frame-pointer`
- 3.15: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -march=pentium4 -O3 -fomit-frame-pointer`
- 3.69: `crypto_stream/salsa2012/ref`
  using `gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/x86-xmm5`
  using `gcc -m32 -march=athlon -O2 -fomit-frame-pointer`
- 1.26: `crypto_stream/salsa208/e/x86-xmm4`
  using `gcc -march=prescott -O2 -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa208/e/x86-2`
  using `gcc -march=pentium -O3 -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa208/e/x86-3`
  using `gcc -m32 -march=k6-3 -Os -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa208/e/x86-athlon`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa208/e/x86-pm`
  using `gcc -funroll-loops -march=nocona -Os -fomit-frame-pointer`
- 1.57: `crypto_stream/salsa208/e/x86-xmm`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.79: `crypto_stream/salsa208/e/x86-xmm2`
  using `gcc -m32 -march=k8 -O -fomit-frame-pointer`
- 2.50: `crypto_stream/salsa208/e/x86-mmx`
  using `gcc -funroll-loops -O -fomit-frame-pointer`
- 2.60: `crypto_stream/salsa208/e/x86-1`
  using `gcc -funroll-loops -m32 -march=pentium2 -O -fomit-frame-pointer`
- 2.73: `crypto_stream/salsa208/e/merged`
  using `gcc -funroll-loops -march=k6-2 -Os -fomit-frame-pointer`
- 2.85: `crypto_stream/salsa208/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer`

- 3.40: crypto_stream/salsa208/e/ref
  using gcc -funroll-loops -m32 -march=pentium4 -O2 -fomit-frame-pointer
- 3.92: crypto_stream/salsa208/ref
  using gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -funroll-loops -m32 -march=nocona -O2 -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -funroll-loops -march=pentium2 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/tpy/e/tpy
  using gcc -funroll-loops -march=pentium2 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/tpy6/e/tpy6
  using gcc -funroll-loops -m32 -march=pentiumpro -O2 -fomit-frame-pointer
- 1.00: crypto_stream/tpypy/e/tpypy
  using gcc -funroll-loops -m32 -march=athlon -O2 -fomit-frame-pointer
- 1.00: crypto_stream/trivium/e/submissions/trivium
  using gcc -funroll-loops -march=pentiumpro -O3 -fomit-frame-pointer

5.36 x86, 2659MHz, Intel Xeon (f25), nmibuild21

- 1.00: crypto_dh/claus/gmp
  using g++ -m32 -march=pentiumpro -O -fomit-frame-pointer
- 2.63: crypto_dh/claus/openssl
  using gcc -funroll-loops -march=pentiumpro -O2 -fomit-frame-pointer
- 1.00: crypto_dh/curve25519/mpfq
  using gcc -funroll-loops -m32 -march=nocona -O2 -fomit-frame-pointer
- 1.00: crypto_dh/surf127eps/mpfq
  using gcc -funroll-loops -march=athlon -O2 -fomit-frame-pointer
- 1.00: crypto_encrypt/mceliece/ref
  using gcc -funroll-loops -march=pentium2 -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ntruees787ep1/ref
  using gcc -funroll-loops -march=prescott -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald1024/openssl
  using gcc -funroll-loops -m32 -march=pentium-mmx -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald1536/openssl
  using gcc -funroll-loops -O2 -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald2048/openssl
  using gcc -funroll-loops -march=pentiumpro -O2 -fomit-frame-pointer

- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -funroll-loops -march=prescott -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `gcc -m32 -march=pentium3 -O -fomit-frame-pointer`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -march=k6 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -funroll-loops -march=pentium -O -fomit-frame-pointer`
- 1.04: `crypto_hash/md5/openssl`
  using `gcc -m32 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -march=i486 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -funroll-loops -march=pentium2 -O -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -march=i486 -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/ref`
  using `gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -funroll-loops -march=k6-2 -O -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/x86-1`
  using `gcc -m32 -march=k8 -Os -fomit-frame-pointer`
- 1.15: `crypto_hashblocks/md5/little-1`
  using `gcc -m32 -march=k8 -O -fomit-frame-pointer`
- 1.58: `crypto_hashblocks/md5/ref`
  using `gcc -funroll-loops -march=i386 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha256/ref`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha512/ref`
  using `gcc -march=i386 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/bls/ref`
  using `g++ -march=pentium4 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/donald1024/openssl`
  using `gcc -march=k8 -O3 -fomit-frame-pointer`

- 1.00: crypto_sign/donald2048/openssl
  using gcc -funroll-loops -m32 -O -fomit-frame-pointer
- 1.00: crypto_sign/donald512/openssl
  using gcc -march=pentium-mmx -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald1024/openssl
  using gcc -funroll-loops -m32 -march=k6-2 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald1536/openssl
  using gcc -funroll-loops -m32 -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ronald2048/openssl
  using gcc -funroll-loops -march=k6-3 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald3072/openssl
  using gcc -m32 -march=prescott -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald4096/openssl
  using gcc -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ronald512/openssl
  using gcc -funroll-loops -march=pentium -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ronald768/openssl
  using gcc -funroll-loops -m32 -march=k6-2 -Os -fomit-frame-pointer
- 1.00: crypto_sign/sflashv2/ref
  using gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes128estream/e/bernstein/x86-mmx-1
  using gcc -m32 -march=pentium -Os -fomit-frame-pointer
- 1.04: crypto_stream/aes128estream/e/hongjun/v1
  using gcc -funroll-loops -m32 -march=athlon -O -fomit-frame-pointer
- 1.17: crypto_stream/aes128estream/e/hongjun/v0
  using gcc -m32 -march=pentium4 -O -fomit-frame-pointer
- 1.39: crypto_stream/aes128estream/e/bernstein/little-3
  using gcc -funroll-loops -m32 -march=pentiumpro -Os -fomit-frame-pointer
- 1.53: crypto_stream/aes128estream/e/bernstein/little-4
  using gcc -funroll-loops -march=pentium-mmx -O -fomit-frame-pointer
- 1.61: crypto_stream/aes128estream/e/gladman
  using gcc -m32 -march=pentiumpro -O -fomit-frame-pointer
- 1.65: crypto_stream/aes128estream/e/bernstein/little-1
  using gcc -funroll-loops -march=pentium4 -O3 -fomit-frame-pointer
- 1.66: crypto_stream/aes128estream/e/bernstein/little-2
  using gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer

- 1.97: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -march=pentium2 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer`
- 1.08: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -march=prescott -O -fomit-frame-pointer`
- 1.41: `crypto_stream/aes256estream/e/gladman`
  using `gcc -m32 -march=i386 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/x86-xmm6`
  using `cc`
- 1.10: `crypto_stream/chacha12/e/x86-xmm5`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.32: `crypto_stream/chacha12/e/x86-1`
  using `gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer`
- 1.43: `crypto_stream/chacha12/e/x86-mmx`
  using `gcc -funroll-loops -m32 -march=pentium4 -Os -fomit-frame-pointer`
- 1.81: `crypto_stream/chacha12/e/x86-xmm2`
  using `gcc -funroll-loops -march=i486 -O3 -fomit-frame-pointer`
- 1.84: `crypto_stream/chacha12/e/x86-xmm`
  using `gcc -funroll-loops -m32 -march=i486 -O3 -fomit-frame-pointer`
- 3.50: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer`
- 3.60: `crypto_stream/chacha12/e/merged`
  using `gcc -m32 -march=pentium3 -O -fomit-frame-pointer`
- 3.85: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/x86-xmm6`
  using `gcc -m32 -march=k6-2`
- 1.15: `crypto_stream/chacha20/e/x86-xmm5`
  using `gcc -funroll-loops -march=pentium -O3 -fomit-frame-pointer`
- 1.38: `crypto_stream/chacha20/e/x86-1`
  using `gcc -funroll-loops -m32 -march=k6 -O -fomit-frame-pointer`
- 1.53: `crypto_stream/chacha20/e/x86-mmx`
  using `gcc -funroll-loops -march=pentium -O2 -fomit-frame-pointer`
- 1.94: `crypto_stream/chacha20/e/x86-xmm2`
  using `gcc -march=pentium3 -O3 -fomit-frame-pointer`

- 1.96: `crypto_stream/chacha20/e/x86-xmm`
  using `gcc -m32 -march=athlon`
- 3.81: `crypto_stream/chacha20/e/regs`
  using `gcc -march=k8 -O -fomit-frame-pointer`
- 4.01: `crypto_stream/chacha20/e/ref`
  using `gcc -funroll-loops -march=k8 -O -fomit-frame-pointer`
- 4.04: `crypto_stream/chacha20/e/merged`
  using `gcc -funroll-loops -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/x86-xmm6`
  using `gcc -m32 -march=k6-2`
- 1.05: `crypto_stream/chacha8/e/x86-xmm5`
  using `gcc -funroll-loops -march=pentium -O3 -fomit-frame-pointer`
- 1.25: `crypto_stream/chacha8/e/x86-1`
  using `gcc -march=pentium2 -O2 -fomit-frame-pointer`
- 1.34: `crypto_stream/chacha8/e/x86-mmx`
  using `gcc -march=pentium -O -fomit-frame-pointer`
- 1.69: `crypto_stream/chacha8/e/x86-xmm2`
  using `gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer`
- 1.70: `crypto_stream/chacha8/e/x86-xmm`
  using `gcc -m32 -march=prescott`
- 3.29: `crypto_stream/chacha8/e/merged`
  using `gcc -m32 -march=nocona -O -fomit-frame-pointer`
- 3.39: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -march=nocona -O -fomit-frame-pointer`
- 3.73: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -m32 -march=pentium4 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -march=pentium2 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer`
- 1.06: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -funroll-loops -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.10: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer`
- 1.02: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -funroll-loops -march=athlon -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -funroll-loops -m32 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.57: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/5`
  using `gcc -march=k6-2`
- 1.25: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -m32 -march=pentium -O3 -fomit-frame-pointer`
- 1.30: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -march=i486 -O2 -fomit-frame-pointer`
- 1.30: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -funroll-loops -march=i486 -O2 -fomit-frame-pointer`
- 1.45: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O2 -fomit-frame-pointer`
- 1.46: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -funroll-loops -march=pentium2 -O2 -fomit-frame-pointer`
- 1.93: `crypto_stream/rabbit/e/opt/2/4`
  using `gcc -march=k6-3`
- 2.01: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -march=pentiumpro -O3 -fomit-frame-pointer`
- 2.02: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -march=pentium3 -O3 -fomit-frame-pointer`
- 2.97: `crypto_stream/rabbit/e/ref`
  using `gcc -funroll-loops -m32 -march=k6 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/x86-xmm5`
  using `gcc -funroll-loops -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.20: `crypto_stream/salsa20/e/x86-xmm4`
  using `gcc -funroll-loops -march=i386 -O3 -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa20/e/x86-2`
  using `gcc -funroll-loops -march=pentium2 -Os -fomit-frame-pointer`

- 1.42: `crypto_stream/salsa20/e/x86-3`
  using `gcc -funroll-loops -m32 -march=i486 -Os -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa20/e/x86-athlon`
  using `gcc -funroll-loops -m32 -march=k6 -O3 -fomit-frame-pointer`
- 1.44: `crypto_stream/salsa20/e/x86-pm`
  using `gcc -m32 -march=k8 -O3 -fomit-frame-pointer`
- 1.52: `crypto_stream/salsa20/e/x86-xmm`
  using `gcc -funroll-loops -march=k6-3`
- 1.92: `crypto_stream/salsa20/e/x86-xmm2`
  using `gcc -m32 -march=k8 -O2 -fomit-frame-pointer`
- 2.63: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -march=pentium3 -O3 -fomit-frame-pointer`
- 2.70: `crypto_stream/salsa20/e/x86-mmx`
  using `gcc -m32 -march=i486 -Os -fomit-frame-pointer`
- 2.90: `crypto_stream/salsa20/e/x86-1`
  using `gcc -march=athlon -Os -fomit-frame-pointer`
- 2.92: `crypto_stream/salsa20/e/merged`
  using `gcc -funroll-loops -march=k6 -Os -fomit-frame-pointer`
- 3.19: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -m32 -march=k8 -Os -fomit-frame-pointer`
- 3.39: `crypto_stream/salsa20/ref`
  using `gcc -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/x86-xmm5`
  using `gcc -m32 -march=pentium2 -O3 -fomit-frame-pointer`
- 1.23: `crypto_stream/salsa2012/e/x86-xmm4`
  using `gcc -m32 -march=k6-2 -O3 -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -funroll-loops -m32 -march=nocona -Os -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -m32 -march=i486 -O -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa2012/e/x86-2`
  using `gcc -m32 -march=pentium3 -Os -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa2012/e/x86-athlon`
  using `gcc -funroll-loops -m32 -march=k6-2 -O3 -fomit-frame-pointer`
- 1.52: `crypto_stream/salsa2012/e/x86-xmm`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`

- 1.74: `crypto_stream/salsa2012/e/x86-xmm2`
  using `gcc -funroll-loops -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 2.60: `crypto_stream/salsa2012/e/x86-mmx`
  using `gcc -march=i486 -Os -fomit-frame-pointer`
- 2.74: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -march=pentium3 -O3 -fomit-frame-pointer`
- 2.74: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer`
- 2.81: `crypto_stream/salsa2012/e/merged`
  using `gcc -funroll-loops -Os -fomit-frame-pointer`
- 3.16: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -march=prescott -O3 -fomit-frame-pointer`
- 3.69: `crypto_stream/salsa2012/ref`
  using `gcc -funroll-loops -march=pentium3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/x86-xmm5`
  using `gcc -march=pentium3 -O3 -fomit-frame-pointer`
- 1.26: `crypto_stream/salsa208/e/x86-xmm4`
  using `gcc -m32 -march=pentium3 -O3 -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa208/e/x86-2`
  using `gcc -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa208/e/x86-3`
  using `gcc -funroll-loops -m32 -march=athlon -Os -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa208/e/x86-pm`
  using `gcc -m32 -march=k6-3 -Os -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa208/e/x86-athlon`
  using `gcc -m32 -march=i386 -O3 -fomit-frame-pointer`
- 1.66: `crypto_stream/salsa208/e/x86-xmm2`
  using `gcc -funroll-loops -m32 -march=i386 -O3 -fomit-frame-pointer`
- 1.81: `crypto_stream/salsa208/e/x86-xmm`
  using `gcc -m32 -march=athlon -O -fomit-frame-pointer`
- 2.49: `crypto_stream/salsa208/e/x86-mmx`
  using `gcc -march=athlon -O2 -fomit-frame-pointer`
- 2.50: `crypto_stream/salsa208/e/x86-1`
  using `gcc -march=pentium3 -O -fomit-frame-pointer`
- 2.71: `crypto_stream/salsa208/e/merged`
  using `gcc -m32 -Os -fomit-frame-pointer`

- 2.80: crypto_stream/salsa208/e/regs
  using gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer
- 3.32: crypto_stream/salsa208/e/ref
  using gcc -funroll-loops -m32 -march=nocona -O2 -fomit-frame-pointer
- 3.92: crypto_stream/salsa208/ref
  using gcc -m32 -march=pentium3 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -funroll-loops -m32 -march=prescott -O3 -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpy/e/tpy
  using gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/tpy6/e/tpy6
  using gcc -funroll-loops -m32 -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpypy/e/tpypy
  using gcc -funroll-loops -m32 -march=prescott -O2 -fomit-frame-pointer
- 1.00: crypto_stream/trivium/e/submissions/trivium
  using gcc -funroll-loops -m32 -march=k6-2 -O -fomit-frame-pointer

5.37 x86, 2659MHz, Intel Xeon (f25), nmibuild26

- 1.00: crypto_dh/claus/gmp
  using g++ -march=k6 -O3 -fomit-frame-pointer
- 2.64: crypto_dh/claus/openssl
  using gcc -funroll-loops -march=pentium-m -Os -fomit-frame-pointer
- 1.00: crypto_dh/curve25519/mpfq
  using gcc -funroll-loops -march=pentium -O3 -fomit-frame-pointer
- 1.00: crypto_dh/surf127eps/mpfq
  using gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_encrypt/mceliece/ref
  using gcc -funroll-loops -march=pentiumpro -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ntruees787ep1/ref
  using gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald1024/openssl
  using gcc -march=k6 -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald1536/openssl
  using gcc -funroll-loops -m32 -march=pentium-mmx

- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -march=pentium-m`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `gcc -m32 -march=k6 -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -funroll-loops -m32 -march=pentium-m -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -m32 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -funroll-loops -m32 -O -fomit-frame-pointer`
- 1.07: `crypto_hash/md5/openssl`
  using `gcc -funroll-loops -m32 -march=pentium-m -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -funroll-loops -march=k6-2 -O -fomit-frame-pointer`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -funroll-loops -march=pentium2 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/ref`
  using `gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/x86-1`
  using `gcc -march=k6-2 -O3 -fomit-frame-pointer`
- 1.15: `crypto_hashblocks/md5/little-1`
  using `gcc -m32 -march=k8 -O -fomit-frame-pointer`
- 1.60: `crypto_hashblocks/md5/ref`
  using `gcc -funroll-loops -m32 -march=pentium3 -O2 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha256/ref`
  using `gcc -funroll-loops -m32 -march=prescott -Os -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha512/ref`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/bls/ref`
  using `g++ -march=pentium4 -O3 -fomit-frame-pointer`

- 1.00: crypto_sign/donald1024/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/donald2048/openssl
  using gcc -funroll-loops -march=k6 -O -fomit-frame-pointer
- 1.00: crypto_sign/donald512/openssl
  using gcc -m32 -march=pentium -O3 -fomit-frame-pointer
- 1.00: crypto_sign/rainbow/ref
  using g++ -m32 -march=pentium-m -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald1024/openssl
  using gcc -m32 -march=pentium-m -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ronald1536/openssl
  using gcc -funroll-loops -march=prescott -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald2048/openssl
  using gcc -funroll-loops -m32 -march=pentium3 -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ronald3072/openssl
  using gcc -m32 -march=athlon -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald4096/openssl
  using gcc -m32 -march=athlon -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald512/openssl
  using gcc -funroll-loops -m32 -march=k6-3 -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ronald768/openssl
  using gcc -march=k6 -Os -fomit-frame-pointer
- 1.00: crypto_sign/sflashv2/ref
  using gcc -funroll-loops -m32 -march=prescott -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes128estream/e/bernstein/x86-mmx-1
  using gcc -march=k8 -O3 -fomit-frame-pointer
- 1.04: crypto_stream/aes128estream/e/hongjun/v1
  using gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer
- 1.18: crypto_stream/aes128estream/e/hongjun/v0
  using gcc -funroll-loops -march=pentium3 -O -fomit-frame-pointer
- 1.45: crypto_stream/aes128estream/e/gladman
  using gcc -march=pentium4 -O -fomit-frame-pointer
- 1.47: crypto_stream/aes128estream/e/bernstein/little-4
  using gcc -funroll-loops -m32 -march=pentium-mmx -O -fomit-frame-pointer
- 1.59: crypto_stream/aes128estream/e/bernstein/little-3
  using gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer

- 1.64: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -funroll-loops -march=k6-3 -Os -fomit-frame-pointer`
- 1.69: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -funroll-loops -march=prescott -O2 -fomit-frame-pointer`
- 1.96: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -march=athlon -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer`
- 1.08: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer`
- 1.31: `crypto_stream/aes256estream/e/gladman`
  using `gcc -funroll-loops -march=k6 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/x86-xmm6`
  using `gcc -funroll-loops -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.12: `crypto_stream/chacha12/e/x86-xmm5`
  using `gcc -march=pentium3 -O -fomit-frame-pointer`
- 1.36: `crypto_stream/chacha12/e/x86-1`
  using `gcc -m32 -march=pentium -O3 -fomit-frame-pointer`
- 1.47: `crypto_stream/chacha12/e/x86-mmx`
  using `gcc -m32 -march=k8`
- 1.65: `crypto_stream/chacha12/e/merged`
  using `gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.86: `crypto_stream/chacha12/e/x86-xmm2`
  using `gcc -march=pentium-m -O -fomit-frame-pointer`
- 1.89: `crypto_stream/chacha12/e/x86-xmm`
  using `gcc -march=pentium-m -O -fomit-frame-pointer`
- 2.02: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer`
- 2.49: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/x86-xmm6`
  using `gcc -march=pentiumpro -O -fomit-frame-pointer`
- 1.19: `crypto_stream/chacha20/e/x86-xmm5`
  using `gcc -m32 -march=pentium2 -O -fomit-frame-pointer`
- 1.44: `crypto_stream/chacha20/e/x86-1`
  using `gcc -march=pentium-mmx -O3 -fomit-frame-pointer`

- 1.59: crypto_stream/chacha20/e/x86-mmx
  using gcc -funroll-loops -march=k6-3 -Os -fomit-frame-pointer
- 1.72: crypto_stream/chacha20/e/merged
  using gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer
- 1.89: crypto_stream/chacha20/e/x86-xmm
  using gcc -m32 -march=pentium-m -O2 -fomit-frame-pointer
- 2.02: crypto_stream/chacha20/e/x86-xmm2
  using gcc -funroll-loops -m32 -march=pentium2 -O -fomit-frame-pointer
- 2.03: crypto_stream/chacha20/e/regs
  using gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer
- 2.47: crypto_stream/chacha20/e/ref
  using gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/chacha8/e/x86-xmm6
  using gcc -m32 -march=athlon -O3 -fomit-frame-pointer
- 1.07: crypto_stream/chacha8/e/x86-xmm5
  using gcc -m32 -march=k8
- 1.29: crypto_stream/chacha8/e/x86-1
  using gcc -m32 -march=prescott -Os -fomit-frame-pointer
- 1.38: crypto_stream/chacha8/e/x86-mmx
  using gcc -funroll-loops -m32 -march=pentium4 -O -fomit-frame-pointer
- 1.58: crypto_stream/chacha8/e/merged
  using gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer
- 1.73: crypto_stream/chacha8/e/x86-xmm2
  using gcc -funroll-loops -m32 -march=athlon -O -fomit-frame-pointer
- 1.75: crypto_stream/chacha8/e/x86-xmm
  using gcc -m32 -march=pentium4 -O -fomit-frame-pointer
- 2.14: crypto_stream/chacha8/e/regs
  using gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer
- 2.53: crypto_stream/chacha8/e/ref
  using gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/cryptmtv3/e/v3
  using gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/dragon/e/submissions/dragon
  using gcc -m32 -march=prescott -O -fomit-frame-pointer
- 1.00: crypto_stream/hc128/e/hc-128/200606
  using gcc -funroll-loops -march=pentium4 -O2 -fomit-frame-pointer

- 1.01: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer`
- 1.14: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -m32 -march=i486 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -funroll-loops -march=athlon -O2 -fomit-frame-pointer`
- 1.03: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -funroll-loops -march=pentium -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -m32 -march=i386 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -march=i386 -O2 -fomit-frame-pointer`
- 1.50: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -m32 -march=k6 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/5`
  using `gcc -m32 -march=nocona`
- 1.19: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m32 -march=i486 -O3 -fomit-frame-pointer`
- 1.19: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -m32 -march=i486 -O3 -fomit-frame-pointer`
- 1.31: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -funroll-loops -m32 -march=i486 -O3 -fomit-frame-pointer`
- 1.39: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -funroll-loops -m32 -march=i486 -O -fomit-frame-pointer`
- 1.39: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -funroll-loops -m32 -march=pentium -O -fomit-frame-pointer`
- 1.93: `crypto_stream/rabbit/e/opt/2/4`
  using `gcc -march=i486`
- 2.05: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m32 -march=athlon -O2 -fomit-frame-pointer`
- 2.07: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -march=athlon -O2 -fomit-frame-pointer`
- 2.53: `crypto_stream/rabbit/e/ref`
  using `gcc -funroll-loops -m32 -march=pentium-mmx -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/x86-xmm5`
  using `gcc -march=athlon -O -fomit-frame-pointer`

- 1.21: crypto_stream/salsa20/e/x86-xmm4
  using gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer
- 1.42: crypto_stream/salsa20/e/x86-2
  using gcc -funroll-loops -m32 -march=k6 -O2 -fomit-frame-pointer
- 1.42: crypto_stream/salsa20/e/x86-3
  using gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer
- 1.42: crypto_stream/salsa20/e/x86-athlon
  using gcc -funroll-loops -march=pentium -Os -fomit-frame-pointer
- 1.45: crypto_stream/salsa20/e/x86-pm
  using gcc -march=prescott -O -fomit-frame-pointer
- 1.84: crypto_stream/salsa20/e/x86-xmm
  using gcc -m32 -march=k6-2 -O2 -fomit-frame-pointer
- 1.92: crypto_stream/salsa20/e/x86-xmm2
  using gcc -O3 -fomit-frame-pointer
- 2.25: crypto_stream/salsa20/e/regs
  using gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer
- 2.61: crypto_stream/salsa20/e/merged
  using gcc -funroll-loops -m32 -march=k6-2 -O3 -fomit-frame-pointer
- 2.71: crypto_stream/salsa20/e/x86-mmx
  using gcc -m32 -march=k6 -O -fomit-frame-pointer
- 2.79: crypto_stream/salsa20/ref
  using gcc -m32 -march=pentiumpro -O3 -fomit-frame-pointer
- 2.87: crypto_stream/salsa20/e/ref
  using gcc -funroll-loops -march=pentiumpro -O2 -fomit-frame-pointer
- 2.91: crypto_stream/salsa20/e/x86-1
  using gcc -funroll-loops -march=pentium-mmx -O -fomit-frame-pointer
- 1.00: crypto_stream/salsa2012/e/x86-xmm5
  using gcc -funroll-loops -m32 -march=k6-2
- 1.23: crypto_stream/salsa2012/e/x86-xmm4
  using gcc -funroll-loops -m32 -march=k8 -O -fomit-frame-pointer
- 1.42: crypto_stream/salsa2012/e/x86-2
  using gcc -funroll-loops -m32 -march=k8 -O -fomit-frame-pointer
- 1.42: crypto_stream/salsa2012/e/x86-3
  using gcc -m32 -march=k6 -O2 -fomit-frame-pointer
- 1.42: crypto_stream/salsa2012/e/x86-athlon
  using gcc -funroll-loops -Os -fomit-frame-pointer

- 1.42: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -m32 -march=pentium-mmx -O -fomit-frame-pointer`
- 1.88: `crypto_stream/salsa2012/e/x86-xmm2`
  using `gcc -funroll-loops -march=pentium-mmx -O -fomit-frame-pointer`
- 2.12: `crypto_stream/salsa2012/e/x86-xmm`
  using `gcc -O2 -fomit-frame-pointer`
- 2.46: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer`
- 2.52: `crypto_stream/salsa2012/e/merged`
  using `gcc -funroll-loops -march=k6 -O3 -fomit-frame-pointer`
- 2.61: `crypto_stream/salsa2012/e/x86-mmx`
  using `gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer`
- 2.81: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -m32 -march=pentium-m`
- 2.96: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O2 -fomit-frame-pointer`
- 3.12: `crypto_stream/salsa2012/ref`
  using `gcc -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/x86-xmm5`
  using `gcc -m32 -march=prescott -O -fomit-frame-pointer`
- 1.26: `crypto_stream/salsa208/e/x86-xmm4`
  using `gcc -march=pentium3 -O3 -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa208/e/x86-2`
  using `gcc -march=pentium3 -Os -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa208/e/x86-3`
  using `gcc -march=nocona -O -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa208/e/x86-pm`
  using `gcc -march=prescott -O -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa208/e/x86-athlon`
  using `gcc -funroll-loops -m32 -march=pentium2 -Os -fomit-frame-pointer`
- 1.59: `crypto_stream/salsa208/e/x86-xmm`
  using `gcc -funroll-loops -O2 -fomit-frame-pointer`
- 1.79: `crypto_stream/salsa208/e/x86-xmm2`
  using `gcc -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 2.05: `crypto_stream/salsa208/e/merged`
  using `gcc -funroll-loops -march=pentium3 -O3 -fomit-frame-pointer`

- 2.50: crypto_stream/salsa208/e/x86-mmx
  using gcc -march=pentium2 -O2 -fomit-frame-pointer
- 2.59: crypto_stream/salsa208/e/x86-1
  using gcc -march=k6-2 -Os -fomit-frame-pointer
- 2.61: crypto_stream/salsa208/e/regs
  using gcc -funroll-loops -march=pentium2 -O3 -fomit-frame-pointer
- 3.02: crypto_stream/salsa208/e/ref
  using gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer
- 3.41: crypto_stream/salsa208/ref
  using gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -funroll-loops -m32 -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -funroll-loops -m32 -march=k6 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpy/e/tpy
  using gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpy6/e/tpy6
  using gcc -funroll-loops -march=pentium4 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpypy/e/tpypy
  using gcc -funroll-loops -march=athlon -O2 -fomit-frame-pointer
- 1.00: crypto_stream/trivium/e/submissions/trivium
  using gcc -m32 -march=k8 -O3 -fomit-frame-pointer

5.38 x86, 2667MHz, Intel Xeon (f25), nmi0036

- 1.00: crypto_dh/claus/gmp
  using g++ -march=pentium-mmx -Os -fomit-frame-pointer
- 2.47: crypto_dh/claus/openssl
  using gcc -march=pentium3 -O -fomit-frame-pointer
- 1.00: crypto_dh/curve25519/mpfq
  using gcc -funroll-loops -march=i386 -O3 -fomit-frame-pointer
- 1.00: crypto_dh/surf127eps/mpfq
  using gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_encrypt/mceliece/ref
  using gcc -funroll-loops -march=pentiumpro -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ntruees787ep1/ref
  using gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer

- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -march=pentium-m -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -funroll-loops -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -funroll-loops -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -funroll-loops -march=athlon -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -funroll-loops -m32 -march=pentium2 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -march=athlon`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer`
- 1.07: `crypto_hash/md5/openssl`
  using `gcc -funroll-loops -m32 -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -funroll-loops -march=pentium4 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -march=pentium-m -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/ref`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -funroll-loops -march=prescott -O -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.15: `crypto_hashblocks/md5/little-1`
  using `gcc -m32 -march=k6-2 -O -fomit-frame-pointer`
- 1.61: `crypto_hashblocks/md5/ref`
  using `gcc -march=k6 -O2 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha256/ref`
  using `gcc -march=prescott -Os -fomit-frame-pointer`

- 1.00: crypto_hashblocks/sha512/ref
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.00: crypto_sign/bls/ref
  using g++ -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_sign/donald1024/openssl
  using gcc -funroll-loops -march=k6-2 -O2 -fomit-frame-pointer
- 1.00: crypto_sign/donald2048/openssl
  using gcc -march=pentium2 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/donald512/openssl
  using gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer
- 1.00: crypto_sign/rainbow/ref
  using g++ -march=athlon -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald1024/openssl
  using gcc -march=k6 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald1536/openssl
  using gcc -funroll-loops -m32 -march=athlon -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ronald2048/openssl
  using gcc -funroll-loops -m32 -march=pentium3 -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ronald3072/openssl
  using gcc -funroll-loops -march=pentium -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald4096/openssl
  using gcc -funroll-loops -march=prescott -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ronald512/openssl
  using gcc -m32 -march=nocona -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald768/openssl
  using gcc -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_sign/sflashv2/ref
  using gcc -funroll-loops -march=pentium4 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes128estream/e/bernstein/x86-mmx-1
  using gcc -m32 -march=nocona -O -fomit-frame-pointer
- 1.04: crypto_stream/aes128estream/e/hongjun/v1
  using gcc -funroll-loops -march=k8 -O -fomit-frame-pointer
- 1.18: crypto_stream/aes128estream/e/hongjun/v0
  using gcc -funroll-loops -m32 -march=athlon -O -fomit-frame-pointer
- 1.46: crypto_stream/aes128estream/e/gladman
  using gcc -m32 -march=k6 -O -fomit-frame-pointer

- 1.47: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -funroll-loops -m32 -march=i386 -O -fomit-frame-pointer`
- 1.61: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -m32 -march=nocona -Os -fomit-frame-pointer`
- 1.65: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -march=k6-3 -Os -fomit-frame-pointer`
- 1.65: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -m32 -march=pentiumpro -O2 -fomit-frame-pointer`
- 1.94: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -m32 -march=pentium-m -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer`
- 1.08: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -m32 -march=k8 -O -fomit-frame-pointer`
- 1.32: `crypto_stream/aes256estream/e/gladman`
  using `gcc -funroll-loops -m32 -march=athlon -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/x86-xmm6`
  using `gcc -m32 -march=pentium`
- 1.10: `crypto_stream/chacha12/e/x86-xmm5`
  using `gcc -march=k6-2`
- 1.32: `crypto_stream/chacha12/e/x86-1`
  using `gcc -m32 -march=k6-2 -Os -fomit-frame-pointer`
- 1.43: `crypto_stream/chacha12/e/x86-mmx`
  using `gcc -march=pentium2 -O3 -fomit-frame-pointer`
- 1.56: `crypto_stream/chacha12/e/merged`
  using `gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer`
- 1.81: `crypto_stream/chacha12/e/x86-xmm2`
  using `gcc -funroll-loops -march=k8`
- 1.84: `crypto_stream/chacha12/e/x86-xmm`
  using `gcc -funroll-loops -m32 -march=athlon`
- 1.92: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer`
- 2.32: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/x86-xmm6`
  using `cc`

- 1.15: `crypto_stream/chacha20/e/x86-xmm5`
  using `gcc -m32 -march=pentium`
- 1.39: `crypto_stream/chacha20/e/x86-1`
  using `gcc -m32 -march=pentium -Os -fomit-frame-pointer`
- 1.53: `crypto_stream/chacha20/e/x86-mmx`
  using `gcc -funroll-loops -march=k6-3 -O3 -fomit-frame-pointer`
- 1.64: `crypto_stream/chacha20/e/merged`
  using `gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.91: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -march=athlon -O3 -fomit-frame-pointer`
- 1.94: `crypto_stream/chacha20/e/x86-xmm2`
  using `gcc -march=pentium-m -O2 -fomit-frame-pointer`
- 1.96: `crypto_stream/chacha20/e/x86-xmm`
  using `gcc -funroll-loops -march=nocona -O -fomit-frame-pointer`
- 2.39: `crypto_stream/chacha20/e/ref`
  using `gcc -m32 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/x86-xmm6`
  using `gcc -m32 -march=pentium-mmx`
- 1.06: `crypto_stream/chacha8/e/x86-xmm5`
  using `gcc -m32 -march=i386`
- 1.25: `crypto_stream/chacha8/e/x86-1`
  using `gcc -march=pentium4 -Os -fomit-frame-pointer`
- 1.34: `crypto_stream/chacha8/e/x86-mmx`
  using `gcc -funroll-loops -march=k6 -Os -fomit-frame-pointer`
- 1.55: `crypto_stream/chacha8/e/merged`
  using `gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.68: `crypto_stream/chacha8/e/x86-xmm2`
  using `gcc -funroll-loops -m32 -march=athlon`
- 1.70: `crypto_stream/chacha8/e/x86-xmm`
  using `gcc -funroll-loops -m32 -march=pentium2`
- 2.04: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 2.34: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -march=prescott -O -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -funroll-loops -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.13: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -m32 -march=i486 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -funroll-loops -m32 -march=athlon -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -funroll-loops -m32 -march=pentium3 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -m32 -march=i386 -O2 -fomit-frame-pointer`
- 1.53: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -march=k6-3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/5`
  using `gcc -m32 -march=nocona`
- 1.19: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m32 -march=i486 -O3 -fomit-frame-pointer`
- 1.20: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -march=i486 -O3 -fomit-frame-pointer`
- 1.30: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -m32 -march=pentium -O -fomit-frame-pointer`
- 1.40: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -funroll-loops -march=pentium -O -fomit-frame-pointer`
- 1.40: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -funroll-loops -m32 -march=i486 -O -fomit-frame-pointer`
- 1.95: `crypto_stream/rabbit/e/opt/2/4`
  using `gcc -m32 -march=pentium`
- 2.06: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -funroll-loops -m32 -march=athlon -O2 -fomit-frame-pointer`
- 2.07: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -funroll-loops -march=athlon -O2 -fomit-frame-pointer`

- 2.53: crypto_stream/rabbit/e/ref
  using gcc -funroll-loops -march=pentium -O2 -fomit-frame-pointer
- 1.00: crypto_stream/salsa20/e/x86-xmm5
  using gcc -funroll-loops -m32 -march=athlon
- 1.21: crypto_stream/salsa20/e/x86-xmm4
  using gcc -march=pentium
- 1.42: crypto_stream/salsa20/e/x86-2
  using gcc -funroll-loops -march=k6 -Os -fomit-frame-pointer
- 1.43: crypto_stream/salsa20/e/x86-3
  using gcc -funroll-loops -march=pentium-mmx -O2 -fomit-frame-pointer
- 1.43: crypto_stream/salsa20/e/x86-athlon
  using gcc -march=k6
- 1.45: crypto_stream/salsa20/e/x86-pm
  using gcc -funroll-loops -m32 -march=pentium -Os -fomit-frame-pointer
- 1.49: crypto_stream/salsa20/e/x86-xmm
  using gcc -march=pentium4 -O2 -fomit-frame-pointer
- 1.72: crypto_stream/salsa20/e/x86-xmm2
  using gcc -funroll-loops -march=pentium2 -O -fomit-frame-pointer
- 2.02: crypto_stream/salsa20/e/regs
  using gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer
- 2.63: crypto_stream/salsa20/e/merged
  using gcc -funroll-loops -m32 -march=k6 -O3 -fomit-frame-pointer
- 2.70: crypto_stream/salsa20/e/x86-mmx
  using gcc -m32 -march=nocona -Os -fomit-frame-pointer
- 2.79: crypto_stream/salsa20/ref
  using gcc -funroll-loops -march=pentiumpro -O3 -fomit-frame-pointer
- 2.86: crypto_stream/salsa20/e/ref
  using gcc -funroll-loops -m32 -march=pentiumpro -O2 -fomit-frame-pointer
- 2.91: crypto_stream/salsa20/e/x86-1
  using gcc -m32 -march=nocona -Os -fomit-frame-pointer
- 1.00: crypto_stream/salsa2012/e/x86-xmm5
  using gcc -funroll-loops -march=athlon
- 1.24: crypto_stream/salsa2012/e/x86-xmm4
  using gcc -march=pentium
- 1.42: crypto_stream/salsa2012/e/x86-2
  using gcc -m32 -march=k6-2 -Os -fomit-frame-pointer

- 1.42: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -funroll-loops -march=pentium2 -Os -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -m32 -march=i386 -Os -fomit-frame-pointer`
- 1.43: `crypto_stream/salsa2012/e/x86-athlon`
  using `gcc -march=k6-2`
- 1.52: `crypto_stream/salsa2012/e/x86-xmm`
  using `gcc -march=k6 -O3 -fomit-frame-pointer`
- 1.78: `crypto_stream/salsa2012/e/x86-xmm2`
  using `gcc -march=pentiumpro -O -fomit-frame-pointer`
- 2.06: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer`
- 2.51: `crypto_stream/salsa2012/e/merged`
  using `gcc -funroll-loops -march=k6-2 -O3 -fomit-frame-pointer`
- 2.60: `crypto_stream/salsa2012/e/x86-mmx`
  using `gcc -m32 -march=prescott -Os -fomit-frame-pointer`
- 2.81: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -march=i386 -Os -fomit-frame-pointer`
- 2.95: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -march=pentium2 -O2 -fomit-frame-pointer`
- 3.12: `crypto_stream/salsa2012/ref`
  using `gcc -march=pentium-m -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/x86-xmm5`
  using `gcc -funroll-loops -m32 -march=pentium4`
- 1.27: `crypto_stream/salsa208/e/x86-xmm4`
  using `gcc`
- 1.41: `crypto_stream/salsa208/e/x86-2`
  using `gcc -m32 -march=athlon -Os -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa208/e/x86-3`
  using `gcc -m32 -march=k6 -Os -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa208/e/x86-pm`
  using `gcc -march=k8 -Os -fomit-frame-pointer`
- 1.42: `crypto_stream/salsa208/e/x86-athlon`
  using `gcc -funroll-loops -march=i386 -Os -fomit-frame-pointer`
- 1.56: `crypto_stream/salsa208/e/x86-xmm`
  using `gcc -funroll-loops -m32 -march=pentium4`

- 1.78: crypto_stream/salsa208/e/x86-xmm2
  using gcc -march=prescott -O2 -fomit-frame-pointer
- 2.08: crypto_stream/salsa208/e/merged
  using gcc -march=i486 -O3 -fomit-frame-pointer
- 2.19: crypto_stream/salsa208/e/regs
  using gcc -funroll-loops -march=pentium-m -O3 -fomit-frame-pointer
- 2.49: crypto_stream/salsa208/e/x86-mmx
  using gcc -march=k8 -Os -fomit-frame-pointer
- 2.61: crypto_stream/salsa208/e/x86-1
  using gcc -funroll-loops -march=k6-3 -O2 -fomit-frame-pointer
- 2.96: crypto_stream/salsa208/e/ref
  using gcc -funroll-loops -m32 -march=pentium4 -O -fomit-frame-pointer
- 3.33: crypto_stream/salsa208/ref
  using gcc -march=pentiumpro -O3 -fomit-frame-pointer
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -funroll-loops -march=prescott -O3 -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -funroll-loops -m32 -march=k6-2 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpy/e/tpy
  using gcc -m32 -march=pentium4 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpy6/e/tpy6
  using gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpypy/e/tpypy
  using gcc -funroll-loops -m32 -march=pentium4 -O -fomit-frame-pointer
- 1.00: crypto_stream/trivium/e/submissions/trivium
  using gcc -m32 -march=athlon -O3 -fomit-frame-pointer

5.39 x86, 2791MHz, Intel Xeon (f27), nmi0024

- 1.00: crypto_dh/claus/openssl
  using cc
- 1.00: crypto_encrypt/ntruees787ep1/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald1024/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald1536/openssl
  using cc

- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `cc`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `cc`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `gcc -m32`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.04: `crypto_hash/md5/openssl`
  using `gcc -m32`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha1/openssl`
  using `cc`
- 1.00: `crypto_hash/sha224/openssl`
  using `cc`
- 1.00: `crypto_hash/sha256/ref`
  using `cc`
- 1.15: `crypto_hash/sha256/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha384/openssl`
  using `cc`
- 1.00: `crypto_hash/sha512/openssl`
  using `gcc -m32`
- 3.49: `crypto_hash/sha512/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.06: `crypto_hashblocks/md5/little-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.43: crypto_hashblocks/md5/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha256/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha512/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/bls/ref
  using g++ -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/rainbow/ref
  using g++ -m32
- 1.00: crypto_sign/ronald1024/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald1536/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald2048/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald3072/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald4096/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald512/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald768/openssl
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/sflashv2/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes128estream/e/bernstein/x86-mmx-1
  using gcc -m32
- 1.26: crypto_stream/aes128estream/e/hongjun/v0
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.58: crypto_stream/aes128estream/e/hongjun/v1
  using gcc -m32 -O3 -fomit-frame-pointer
- 2.04: crypto_stream/aes128estream/e/bernstein/little-3
  using gcc -m32 -O3 -fomit-frame-pointer
- 2.11: crypto_stream/aes128estream/e/bernstein/little-4
  using gcc -m32 -O3 -fomit-frame-pointer

- 2.16: `crypto_stream/aes128estream/e/gladman`
  using `cc`
- 2.75: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.84: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.14: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.44: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.55: `crypto_stream/aes256estream/e/gladman`
  using `cc`
- 1.00: `crypto_stream/chacha12/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/x86-xmm6`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.19: `crypto_stream/chacha12/e/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.30: `crypto_stream/chacha12/e/x86-mmx`
  using `cc`
- 1.34: `crypto_stream/chacha12/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.69: `crypto_stream/chacha12/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.71: `crypto_stream/chacha12/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.73: `crypto_stream/chacha12/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 6.46: `crypto_stream/chacha12/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/x86-xmm6`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.09: `crypto_stream/chacha20/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.32: `crypto_stream/chacha20/e/x86-1`
  using `cc`
- 1.44: `crypto_stream/chacha20/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.46: `crypto_stream/chacha20/e/x86-mmx`
  using `gcc -m32`
- 1.69: `crypto_stream/chacha20/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.90: `crypto_stream/chacha20/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.93: `crypto_stream/chacha20/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 7.15: `crypto_stream/chacha20/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.04: `crypto_stream/chacha8/e/x86-xmm6`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.19: `crypto_stream/chacha8/e/x86-1`
  using `cc`
- 1.27: `crypto_stream/chacha8/e/x86-mmx`
  using `cc`
- 1.66: `crypto_stream/chacha8/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.68: `crypto_stream/chacha8/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.97: `crypto_stream/chacha8/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 4.80: `crypto_stream/chacha8/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 5.87: `crypto_stream/chacha8/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.21: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.07: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.94: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/5`
  using `cc`
- 1.49: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.50: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.63: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.83: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.84: `crypto_stream/rabbit/e/opt/2/4`
  using `gcc -m32`
- 1.87: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.19: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.20: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.94: `crypto_stream/rabbit/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/salsa20/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.21: `crypto_stream/salsa20/e/x86-xmm4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa20/e/x86-2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa20/e/x86-3`
  using `gcc -m32`
- 1.41: `crypto_stream/salsa20/e/x86-pm`
  using `gcc -m32`
- 1.44: `crypto_stream/salsa20/e/x86-athlon`
  using `gcc -m32`
- 1.83: `crypto_stream/salsa20/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.93: `crypto_stream/salsa20/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.69: `crypto_stream/salsa20/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.76: `crypto_stream/salsa20/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.79: `crypto_stream/salsa20/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.80: `crypto_stream/salsa20/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.93: `crypto_stream/salsa20/e/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.57: `crypto_stream/salsa20/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.23: `crypto_stream/salsa2012/e/x86-xmm4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.40: `crypto_stream/salsa2012/e/x86-2`
  using `cc`
- 1.40: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -m32`

- 1.40: `crypto_stream/salsa2012/e/x86-athlon`
  using `cc`
- 1.40: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.74: `crypto_stream/salsa2012/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.87: `crypto_stream/salsa2012/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.12: `crypto_stream/salsa2012/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.57: `crypto_stream/salsa2012/e/x86-mmx`
  using `cc`
- 2.73: `crypto_stream/salsa2012/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.78: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -m32`
- 3.14: `crypto_stream/salsa2012/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.53: `crypto_stream/salsa2012/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.24: `crypto_stream/salsa208/e/x86-xmm4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.38: `crypto_stream/salsa208/e/x86-3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.38: `crypto_stream/salsa208/e/x86-pm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.39: `crypto_stream/salsa208/e/x86-2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.39: `crypto_stream/salsa208/e/x86-athlon`
  using `gcc -m32`
- 1.75: `crypto_stream/salsa208/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.09: `crypto_stream/salsa208/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 2.26: crypto_stream/salsa208/e/merged
  using gcc -m32 -O3 -fomit-frame-pointer
- 2.44: crypto_stream/salsa208/e/x86-mmx
  using gcc -m32 -O3 -fomit-frame-pointer
- 2.72: crypto_stream/salsa208/e/x86-1
  using gcc -m32 -O3 -fomit-frame-pointer
- 2.86: crypto_stream/salsa208/e/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 3.51: crypto_stream/salsa208/e/regs
  using gcc -m32 -O3 -fomit-frame-pointer
- 3.80: crypto_stream/salsa208/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpy/e/tpy
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpy6/e/tpy6
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpypy/e/tpypy
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/trivium/e/submissions/trivium
  using gcc -m32 -O3 -fomit-frame-pointer

5.40 x86, 2800MHz, Intel Xeon (f41), nmi0057

- 1.00: crypto_dh/claus/gmp
  using g++ -m32 -march=i386 -O -fomit-frame-pointer
- 1.00: crypto_dh/curve25519/mpfq
  using gcc -funroll-loops -m32 -march=k6 -O3 -fomit-frame-pointer
- 1.00: crypto_dh/surf127eps/mpfq
  using gcc -funroll-loops -m32 -march=pentium2 -O2 -fomit-frame-pointer
- 1.00: crypto_encrypt/mceliece/ref
  using gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ntruees787ep1/ref
  using gcc -funroll-loops -m32 -march=i386 -O3 -fomit-frame-pointer

- 1.00: `crypto_hash/md5/ref`
  using `gcc -funroll-loops -m32 -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -funroll-loops -m32 -march=pentium4 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/ref`
  using `gcc -funroll-loops -m32 -march=i486 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -funroll-loops -m32 -march=pentium4 -O -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/x86-1`
  using `gcc -m32 -march=prescott -O3 -fomit-frame-pointer`
- 1.55: `crypto_hashblocks/md5/little-1`
  using `gcc -m32 -march=athlon -O -fomit-frame-pointer`
- 2.00: `crypto_hashblocks/md5/ref`
  using `gcc -m32 -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha256/ref`
  using `gcc -m32 -march=prescott -O -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha512/ref`
  using `gcc -funroll-loops -m32 -march=k6 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/bls/ref`
  using `g++ -m32 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/rainbow/ref`
  using `g++ -m32 -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/bernstein/x86-mmx-1`
  using `gcc -m32 -march=athlon -O -fomit-frame-pointer`
- 1.08: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer`
- 1.21: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -funroll-loops -m32 -O -fomit-frame-pointer`
- 1.39: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -m32 -march=k6-2 -O2 -fomit-frame-pointer`
- 1.51: `crypto_stream/aes128estream/e/gladman`
  using `gcc -m32 -march=nocona -O -fomit-frame-pointer`
- 1.60: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer`
- 1.61: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -m32 -march=athlon -Os -fomit-frame-pointer`

- 1.62: crypto_stream/aes128estream/e/bernstein/little-1
  using gcc -m32 -Os -fomit-frame-pointer
- 1.77: crypto_stream/aes128estream/e/bernstein/big-1
  using gcc -m32 -march=k8 -Os -fomit-frame-pointer
- 1.00: crypto_stream/aes256estream/e/hongjun/v1
  using gcc -funroll-loops -m32 -march=pentium3 -O -fomit-frame-pointer
- 1.07: crypto_stream/aes256estream/e/hongjun/v0
  using gcc -m32 -march=prescott -O -fomit-frame-pointer
- 1.41: crypto_stream/aes256estream/e/gladman
  using gcc -m32 -march=pentium4 -O -fomit-frame-pointer
- 1.00: crypto_stream/chacha12/e/x86-1
  using gcc -m32 -march=k8 -Os -fomit-frame-pointer
- 1.00: crypto_stream/chacha12/e/x86-xmm6
  using gcc -funroll-loops -m32 -march=prescott
- 1.12: crypto_stream/chacha12/e/x86-xmm5
  using gcc -funroll-loops -m32 -O -fomit-frame-pointer
- 1.19: crypto_stream/chacha12/e/merged
  using gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer
- 1.23: crypto_stream/chacha12/e/x86-mmx
  using gcc -funroll-loops -m32 -march=pentium -O -fomit-frame-pointer
- 1.66: crypto_stream/chacha12/e/ref
  using gcc -funroll-loops -m32 -march=pentium4 -O3 -fomit-frame-pointer
- 1.67: crypto_stream/chacha12/e/regs
  using gcc -funroll-loops -m32 -march=pentium-mmx -O3 -fomit-frame-pointer
- 2.22: crypto_stream/chacha12/e/x86-xmm
  using gcc -m32 -march=pentium2 -O3 -fomit-frame-pointer
- 2.62: crypto_stream/chacha12/e/x86-xmm2
  using gcc -m32 -march=pentium2 -O -fomit-frame-pointer
- 1.00: crypto_stream/chacha20/e/x86-xmm6
  using gcc -funroll-loops -m32 -march=nocona
- 1.01: crypto_stream/chacha20/e/x86-1
  using gcc -m32 -march=athlon -Os -fomit-frame-pointer
- 1.17: crypto_stream/chacha20/e/merged
  using gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer
- 1.18: crypto_stream/chacha20/e/x86-xmm5
  using gcc -funroll-loops -m32 -march=pentiumpro

- 1.28: `crypto_stream/chacha20/e/x86-mmx`
  using `gcc -m32 -march=k8`
- 1.44: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.50: `crypto_stream/chacha20/e/ref`
  using `gcc -funroll-loops -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 2.22: `crypto_stream/chacha20/e/x86-xmm`
  using `gcc -funroll-loops -m32 -march=prescott -O3 -fomit-frame-pointer`
- 2.55: `crypto_stream/chacha20/e/x86-xmm2`
  using `gcc -funroll-loops -m32 -march=pentium3 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/x86-1`
  using `gcc -funroll-loops -m32 -march=prescott -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/chacha8/e/x86-xmm6`
  using `gcc -funroll-loops -m32 -march=athlon`
- 1.17: `crypto_stream/chacha8/e/x86-xmm5`
  using `gcc -m32 -march=pentium-m -O2 -fomit-frame-pointer`
- 1.19: `crypto_stream/chacha8/e/x86-mmx`
  using `gcc -m32 -march=pentium3 -O2 -fomit-frame-pointer`
- 1.22: `crypto_stream/chacha8/e/merged`
  using `gcc -funroll-loops -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.71: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer`
- 1.90: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -m32 -march=i486 -O3 -fomit-frame-pointer`
- 2.06: `crypto_stream/chacha8/e/x86-xmm`
  using `gcc -m32 -march=k6-2 -O -fomit-frame-pointer`
- 2.34: `crypto_stream/chacha8/e/x86-xmm2`
  using `gcc -m32 -march=k6-3 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -funroll-loops -m32 -march=prescott -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -m32 -march=pentium4 -O -fomit-frame-pointer`
- 1.01: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -m32 -march=k8 -O -fomit-frame-pointer`

- 1.03: crypto_stream/hc128/e/hc-128/200701b
  using gcc -m32 -march=pentium4 -O -fomit-frame-pointer
- 1.00: crypto_stream/hc256/e/hc-256/200511
  using gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer
- 1.00: crypto_stream/hc256/e/hc-256/200701
  using gcc -funroll-loops -m32 -march=prescott -O2 -fomit-frame-pointer
- 1.00: crypto_stream/lexv2/e/v2/ref
  using gcc -funroll-loops -m32 -march=k6 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/nlsv2/e/v2/sync/2
  using gcc -funroll-loops -m32 -march=k6-3 -O -fomit-frame-pointer
- 1.74: crypto_stream/nlsv2/e/v2/sync/1
  using gcc -funroll-loops -m32 -march=k6 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/1/4
  using gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/2/3
  using gcc -m32 -march=pentium -O3 -fomit-frame-pointer
- 1.08: crypto_stream/rabbit/e/opt/1/3
  using gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer
- 1.30: crypto_stream/rabbit/e/opt/2/5
  using gcc -m32 -march=pentium4
- 1.40: crypto_stream/rabbit/e/opt/1/2
  using gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer
- 1.40: crypto_stream/rabbit/e/opt/2/2
  using gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer
- 1.60: crypto_stream/rabbit/e/ref
  using gcc -funroll-loops -m32 -march=pentium-mmx -O2 -fomit-frame-pointer
- 1.64: crypto_stream/rabbit/e/opt/1/1
  using gcc -m32 -march=pentium4 -O3 -fomit-frame-pointer
- 1.64: crypto_stream/rabbit/e/opt/2/1
  using gcc -funroll-loops -m32 -march=nocona -O3 -fomit-frame-pointer
- 1.95: crypto_stream/rabbit/e/opt/2/4
  using gcc -m32 -march=i386
- 1.00: crypto_stream/salsa20/e/x86-xmm5
  using gcc -m32 -march=nocona -O3 -fomit-frame-pointer
- 1.17: crypto_stream/salsa20/e/x86-2
  using gcc -m32 -march=pentium4 -Os -fomit-frame-pointer

- 1.17: `crypto_stream/salsa20/e/x86-3`
  using `gcc -m32 -march=pentiumpro -Os -fomit-frame-pointer`
- 1.17: `crypto_stream/salsa20/e/x86-athlon`
  using `gcc -funroll-loops -m32 -march=pentium-mmx -Os -fomit-frame-pointer`
- 1.21: `crypto_stream/salsa20/e/x86-pm`
  using `gcc -funroll-loops -m32 -march=pentium-m -Os -fomit-frame-pointer`
- 1.27: `crypto_stream/salsa20/e/x86-1`
  using `gcc -m32 -march=nocona -O2 -fomit-frame-pointer`
- 1.30: `crypto_stream/salsa20/e/x86-xmm4`
  using `gcc -funroll-loops -m32 -march=pentium2`
- 1.41: `crypto_stream/salsa20/e/x86-mmx`
  using `gcc -m32 -march=pentium4 -O -fomit-frame-pointer`
- 1.50: `crypto_stream/salsa20/e/merged`
  using `gcc -funroll-loops -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.62: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -m32 -march=i486 -O3 -fomit-frame-pointer`
- 1.72: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer`
- 1.92: `crypto_stream/salsa20/e/x86-xmm`
  using `gcc -m32 -march=pentium-m -O2 -fomit-frame-pointer`
- 1.99: `crypto_stream/salsa20/ref`
  using `gcc -m32 -march=pentium -O3 -fomit-frame-pointer`
- 2.62: `crypto_stream/salsa20/e/x86-xmm2`
  using `gcc -m32 -march=i386`
- 1.00: `crypto_stream/salsa2012/e/x86-xmm5`
  using `gcc -m32 -march=pentium3`
- 1.14: `crypto_stream/salsa2012/e/x86-2`
  using `gcc -m32 -march=pentium2 -Os -fomit-frame-pointer`
- 1.14: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -funroll-loops -m32 -march=nocona -Os -fomit-frame-pointer`
- 1.14: `crypto_stream/salsa2012/e/x86-athlon`
  using `gcc -m32 -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.16: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -m32 -march=pentium`
- 1.23: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -m32 -march=athlon -O2 -fomit-frame-pointer`

- 1.33: crypto_stream/salsa2012/e/x86-xmm4
  using gcc -funroll-loops -m32 -march=prescott
- 1.34: crypto_stream/salsa2012/e/x86-mmx
  using gcc -m32 -march=k8 -Os -fomit-frame-pointer
- 1.61: crypto_stream/salsa2012/e/merged
  using gcc -m32 -march=athlon -O2 -fomit-frame-pointer
- 1.78: crypto_stream/salsa2012/e/regs
  using gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer
- 1.85: crypto_stream/salsa2012/e/ref
  using gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer
- 2.11: crypto_stream/salsa2012/e/x86-xmm
  using gcc -m32 -march=pentium3 -O2 -fomit-frame-pointer
- 2.15: crypto_stream/salsa2012/ref
  using gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer
- 2.48: crypto_stream/salsa2012/e/x86-xmm2
  using gcc -m32 -march=prescott -O2 -fomit-frame-pointer
- 1.00: crypto_stream/salsa208/e/x86-xmm5
  using gcc -m32 -march=athlon -O2 -fomit-frame-pointer
- 1.15: crypto_stream/salsa208/e/x86-2
  using gcc -funroll-loops -m32 -O2 -fomit-frame-pointer
- 1.15: crypto_stream/salsa208/e/x86-3
  using gcc -funroll-loops -m32 -march=pentium3 -Os -fomit-frame-pointer
- 1.15: crypto_stream/salsa208/e/x86-athlon
  using gcc -funroll-loops -m32 -march=k6-2 -O3 -fomit-frame-pointer
- 1.15: crypto_stream/salsa208/e/x86-pm
  using gcc -m32 -march=athlon -O -fomit-frame-pointer
- 1.22: crypto_stream/salsa208/e/x86-1
  using gcc -funroll-loops -m32 -march=k8 -O2 -fomit-frame-pointer
- 1.29: crypto_stream/salsa208/e/x86-mmx
  using gcc -m32 -march=pentium-m -Os -fomit-frame-pointer
- 1.34: crypto_stream/salsa208/e/x86-xmm4
  using gcc -funroll-loops -m32 -march=pentium-m
- 1.40: crypto_stream/salsa208/e/merged
  using gcc -m32 -march=pentium2 -O3 -fomit-frame-pointer
- 1.88: crypto_stream/salsa208/e/regs
  using gcc -funroll-loops -m32 -march=pentium4 -O3 -fomit-frame-pointer

- 2.04: `crypto_stream/salsa208/e/ref`
  using `gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer`
- 2.31: `crypto_stream/salsa208/e/x86-xmm`
  using `gcc -funroll-loops -m32 -march=k8 -O2 -fomit-frame-pointer`
- 2.39: `crypto_stream/salsa208/ref`
  using `gcc -funroll-loops -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 2.41: `crypto_stream/salsa208/e/x86-xmm2`
  using `gcc -m32 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -funroll-loops -m32 -march=pentium -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -funroll-loops -m32 -march=i386 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -funroll-loops -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -funroll-loops -m32 -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -m32 -march=k8 -O3 -fomit-frame-pointer`

5.41 x86, 2800MHz, Intel Xeon (f41), `nmi0063`

- 1.00: `crypto_dh/claus/gmp`
  using `g++ -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 1.00: `crypto_dh/curve2251/mpfq`
  using `gcc -funroll-loops -m32 -march=pentium-m -O -fomit-frame-pointer`
- 1.00: `crypto_dh/curve25519/mpfq`
  using `gcc -funroll-loops -m32 -march=pentium-m -Os -fomit-frame-pointer`
- 1.00: `crypto_dh/hector/ref`
  using `gcc -funroll-loops -m32 -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_dh/surf127eps/mpfq`
  using `gcc -funroll-loops -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_dh/surf2113/mpfq`
  using `gcc -funroll-loops -m32 -march=pentium-m -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/mceliece/ref`
  using `gcc -funroll-loops -m32 -march=nocona -O3 -fomit-frame-pointer`

- 1.00: crypto_encrypt/ntruees787ep1/ref
  using gcc -funroll-loops -m32 -march=pentium2 -O -fomit-frame-pointer
- 1.00: crypto_hash/md5/ref
  using gcc -funroll-loops -m32 -march=athlon -O -fomit-frame-pointer
- 1.00: crypto_hash/sha256/ref
  using gcc -funroll-loops -m32 -march=k6-2 -O2 -fomit-frame-pointer
- 1.00: crypto_hash/sha512/ref
  using gcc -funroll-loops -m32 -march=prescott -O2 -fomit-frame-pointer
- 1.00: crypto_hash/whirlpool/ref
  using gcc -funroll-loops -m32 -march=pentium-mmx -Os -fomit-frame-pointer
- 1.00: crypto_hashblocks/md5/x86-1
  using gcc -m32 -march=k6 -O3 -fomit-frame-pointer
- 1.45: crypto_hashblocks/md5/little-1
  using gcc -m32 -march=k8 -O -fomit-frame-pointer
- 1.77: crypto_hashblocks/md5/ref
  using gcc -funroll-loops -m32 -march=k6-2 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha256/ref
  using gcc -m32 -march=pentiumpro
- 1.00: crypto_hashblocks/sha512/ref
  using gcc -m32 -march=i386 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/bls/ref
  using g++ -m32 -march=pentium-m -Os -fomit-frame-pointer
- 1.00: crypto_sign/hector/ref
  using gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer
- 1.00: crypto_sign/rainbow/ref
  using g++ -m32 -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes128estream/e/bernstein/x86-mmx-1
  using gcc -m32 -march=athlon -O3 -fomit-frame-pointer
- 1.10: crypto_stream/aes128estream/e/hongjun/v1
  using gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer
- 1.12: crypto_stream/aes128estream/e/hongjun/v0
  using gcc -funroll-loops -m32 -march=pentium2 -O -fomit-frame-pointer
- 1.19: crypto_stream/aes128estream/e/bernstein/little-4
  using gcc -m32 -march=i486 -O -fomit-frame-pointer
- 1.31: crypto_stream/aes128estream/e/bernstein/little-3
  using gcc -m32 -march=k6 -O -fomit-frame-pointer

- 1.43: `crypto_stream/aes128estream/e/gladman`
  using `gcc -m32 -march=prescott -O -fomit-frame-pointer`
- 1.69: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -m32 -march=pentium -O -fomit-frame-pointer`
- 1.71: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -m32 -march=k6 -O -fomit-frame-pointer`
- 1.90: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -m32 -march=athlon -O -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -funroll-loops -m32 -march=pentium2 -O -fomit-frame-pointer`
- 1.01: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -funroll-loops -m32 -march=athlon -O -fomit-frame-pointer`
- 1.23: `crypto_stream/aes256estream/e/gladman`
  using `gcc -m32 -march=athlon -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/x86-xmm6`
  using `gcc -m32 -march=k6-3 -O2 -fomit-frame-pointer`
- 1.01: `crypto_stream/chacha12/e/x86-1`
  using `gcc -funroll-loops -m32 -march=pentium3 -O -fomit-frame-pointer`
- 1.12: `crypto_stream/chacha12/e/merged`
  using `gcc -funroll-loops -m32 -O2 -fomit-frame-pointer`
- 1.12: `crypto_stream/chacha12/e/x86-xmm5`
  using `gcc -m32 -march=i386 -O -fomit-frame-pointer`
- 1.24: `crypto_stream/chacha12/e/x86-mmx`
  using `gcc -funroll-loops -m32 -march=athlon -Os -fomit-frame-pointer`
- 1.35: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer`
- 2.08: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -m32 -march=pentium-m -O -fomit-frame-pointer`
- 2.24: `crypto_stream/chacha12/e/x86-xmm`
  using `gcc -m32 -march=pentium2 -O3 -fomit-frame-pointer`
- 2.64: `crypto_stream/chacha12/e/x86-xmm2`
  using `gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/x86-xmm6`
  using `gcc -m32 -march=k6 -O2 -fomit-frame-pointer`
- 1.02: `crypto_stream/chacha20/e/x86-1`
  using `gcc -m32 -march=k8 -Os -fomit-frame-pointer`

- 1.09: `crypto_stream/chacha20/e/merged`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.18: `crypto_stream/chacha20/e/x86-xmm5`
  using `gcc -funroll-loops -m32 -march=k6 -O2 -fomit-frame-pointer`
- 1.25: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.29: `crypto_stream/chacha20/e/x86-mmx`
  using `gcc -m32 -march=pentium3 -O -fomit-frame-pointer`
- 2.01: `crypto_stream/chacha20/e/ref`
  using `gcc -funroll-loops -m32 -march=pentium2 -O -fomit-frame-pointer`
- 2.23: `crypto_stream/chacha20/e/x86-xmm`
  using `gcc -m32 -march=pentium2 -O3 -fomit-frame-pointer`
- 2.58: `crypto_stream/chacha20/e/x86-xmm2`
  using `gcc -m32 -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/x86-1`
  using `gcc -m32 -march=pentium2 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/x86-xmm6`
  using `gcc -funroll-loops -m32 -march=k6 -O2 -fomit-frame-pointer`
- 1.13: `crypto_stream/chacha8/e/merged`
  using `gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.17: `crypto_stream/chacha8/e/x86-xmm5`
  using `gcc -m32 -march=pentium3 -O -fomit-frame-pointer`
- 1.19: `crypto_stream/chacha8/e/x86-mmx`
  using `gcc -funroll-loops -m32 -march=k6-2 -Os -fomit-frame-pointer`
- 1.75: `crypto_stream/chacha8/e/regs`
  using `gcc -m32 -march=prescott -O3 -fomit-frame-pointer`
- 2.06: `crypto_stream/chacha8/e/x86-xmm`
  using `gcc -funroll-loops -m32 -march=pentium3 -O -fomit-frame-pointer`
- 2.20: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -m32 -march=pentium4 -O -fomit-frame-pointer`
- 2.34: `crypto_stream/chacha8/e/x86-xmm2`
  using `gcc -funroll-loops -m32 -march=pentium4 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -m32 -march=pentium4 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -funroll-loops -m32 -march=nocona -O2 -fomit-frame-pointer`

- 1.00: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -m32 -march=pentium -O2 -fomit-frame-pointer`
- 1.02: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -funroll-loops -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.04: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -funroll-loops -m32 -march=pentium-mmx -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -m32 -march=pentium4 -O -fomit-frame-pointer`
- 1.03: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -m32 -march=pentium4 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -funroll-loops -m32 -march=pentium-m -O -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -m32 -march=pentium2 -O -fomit-frame-pointer`
- 1.79: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -funroll-loops -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -funroll-loops -m32 -march=k6 -O3 -fomit-frame-pointer`
- 1.03: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer`
- 1.29: `crypto_stream/rabbit/e/opt/2/5`
  using `gcc -funroll-loops -m32 -march=athlon`
- 1.52: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -funroll-loops -m32 -march=pentium3 -O -fomit-frame-pointer`
- 1.52: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -funroll-loops -m32 -march=athlon -O -fomit-frame-pointer`
- 1.68: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m32 -march=pentium-mmx -O2 -fomit-frame-pointer`
- 1.68: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -m32 -march=pentium -O3 -fomit-frame-pointer`
- 1.84: `crypto_stream/rabbit/e/opt/2/4`
  using `gcc -m32 -march=k8`
- 1.97: `crypto_stream/rabbit/e/ref`
  using `gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/salsa20/e/x86-xmm5`
  using `gcc -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.16: `crypto_stream/salsa20/e/x86-2`
  using `gcc -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.16: `crypto_stream/salsa20/e/x86-3`
  using `gcc -m32 -march=k6-3 -O2 -fomit-frame-pointer`
- 1.16: `crypto_stream/salsa20/e/x86-athlon`
  using `gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer`
- 1.21: `crypto_stream/salsa20/e/x86-pm`
  using `gcc -m32 -march=pentium3 -Os -fomit-frame-pointer`
- 1.27: `crypto_stream/salsa20/e/x86-1`
  using `gcc -m32 -march=k8 -O3 -fomit-frame-pointer`
- 1.29: `crypto_stream/salsa20/e/x86-xmm4`
  using `gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer`
- 1.34: `crypto_stream/salsa20/e/merged`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 1.40: `crypto_stream/salsa20/e/x86-mmx`
  using `gcc -m32 -march=k8 -Os -fomit-frame-pointer`
- 1.46: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer`
- 1.67: `crypto_stream/salsa20/ref`
  using `gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer`
- 1.70: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 1.92: `crypto_stream/salsa20/e/x86-xmm`
  using `gcc -m32 -march=k8 -O2 -fomit-frame-pointer`
- 2.61: `crypto_stream/salsa20/e/x86-xmm2`
  using `gcc -m32 -march=pentium2 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/x86-xmm5`
  using `gcc -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.14: `crypto_stream/salsa2012/e/x86-2`
  using `gcc -funroll-loops -m32 -march=k6 -O3 -fomit-frame-pointer`
- 1.14: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -m32 -march=pentium2 -O2 -fomit-frame-pointer`
- 1.14: `crypto_stream/salsa2012/e/x86-athlon`
  using `gcc -m32 -march=k6 -O -fomit-frame-pointer`

- 1.15: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -m32 -march=pentium4 -O2 -fomit-frame-pointer`
- 1.24: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -m32 -march=nocona`
- 1.29: `crypto_stream/salsa2012/e/x86-xmm4`
  using `gcc -m32 -O2 -fomit-frame-pointer`
- 1.34: `crypto_stream/salsa2012/e/merged`
  using `gcc -funroll-loops -m32 -march=k8 -O -fomit-frame-pointer`
- 1.34: `crypto_stream/salsa2012/e/x86-mmx`
  using `gcc -m32 -march=pentium3 -Os -fomit-frame-pointer`
- 1.71: `crypto_stream/salsa2012/e/regs`
  using `gcc -m32 -march=nocona -O -fomit-frame-pointer`
- 1.81: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer`
- 1.91: `crypto_stream/salsa2012/ref`
  using `gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 2.11: `crypto_stream/salsa2012/e/x86-xmm`
  using `gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer`
- 2.48: `crypto_stream/salsa2012/e/x86-xmm2`
  using `gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/x86-xmm5`
  using `gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa208/e/x86-2`
  using `gcc -funroll-loops -m32 -march=k8 -Os -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa208/e/x86-3`
  using `gcc -funroll-loops -m32 -march=pentium4 -Os -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa208/e/x86-athlon`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa208/e/x86-pm`
  using `gcc -m32 -march=k6-3 -O -fomit-frame-pointer`
- 1.20: `crypto_stream/salsa208/e/x86-1`
  using `gcc -m32 -O -fomit-frame-pointer`
- 1.28: `crypto_stream/salsa208/e/x86-mmx`
  using `gcc -m32 -march=k8 -Os -fomit-frame-pointer`
- 1.32: `crypto_stream/salsa208/e/merged`
  using `gcc -m32 -march=pentium-mmx -O -fomit-frame-pointer`

- 1.32: crypto_stream/salsa208/e/x86-xmm4
  using gcc -m32 -march=pentium-m -O2 -fomit-frame-pointer
- 1.84: crypto_stream/salsa208/e/ref
  using gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer
- 1.84: crypto_stream/salsa208/e/regs
  using gcc -funroll-loops -m32 -march=prescott -O3 -fomit-frame-pointer
- 2.27: crypto_stream/salsa208/ref
  using gcc -m32 -march=pentium -O3 -fomit-frame-pointer
- 2.28: crypto_stream/salsa208/e/x86-xmm
  using gcc -m32 -march=prescott -O -fomit-frame-pointer
- 2.38: crypto_stream/salsa208/e/x86-xmm2
  using gcc -m32 -march=k8 -O -fomit-frame-pointer
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -funroll-loops -m32 -march=pentium-m -O2 -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -funroll-loops -m32 -march=k8 -O -fomit-frame-pointer
- 1.00: crypto_stream/tpy/e/tpy
  using gcc -funroll-loops -m32 -march=k6-2 -Os -fomit-frame-pointer
- 1.00: crypto_stream/tpy6/e/tpy6
  using gcc -m32 -march=k8 -Os -fomit-frame-pointer
- 1.00: crypto_stream/tpypy/e/tpypy
  using gcc -m32 -march=prescott -O -fomit-frame-pointer
- 1.00: crypto_stream/trivium/e/submissions/trivium
  using gcc -m32 -march=pentiumpro -Os -fomit-frame-pointer

5.42 x86, 2801MHz, Intel Xeon (f41), nmi0060

- 1.00: crypto_dh/claus/gmp
  using g++ -march=k6-3
- 2.69: crypto_dh/claus/openssl
  using gcc -funroll-loops -march=i386 -O2 -fomit-frame-pointer
- 1.00: crypto_dh/curve25519/mpfq
  using gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer
- 1.00: crypto_dh/surf127eps/mpfq
  using gcc -funroll-loops -m32 -march=pentium3 -O2 -fomit-frame-pointer
- 1.00: crypto_encrypt/mceliece/ref
  using gcc -funroll-loops -march=pentium-m -O3 -fomit-frame-pointer

- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -funroll-loops -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -funroll-loops -march=pentium -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -march=k8`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -funroll-loops -m32 -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `gcc -funroll-loops -march=pentium2 -O -fomit-frame-pointer`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -funroll-loops -march=k8 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -funroll-loops -march=prescott -O -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -funroll-loops -march=prescott -O3 -fomit-frame-pointer`
- 1.11: `crypto_hash/md5/openssl`
  using `gcc -march=athlon -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -funroll-loops -m32 -march=k6-2`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -funroll-loops -march=k6-3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -funroll-loops -march=pentium-mmx -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/ref`
  using `gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -funroll-loops -m32 -march=pentium-m -O -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/x86-1`
  using `gcc -m32 -march=k8 -O -fomit-frame-pointer`
- 1.55: `crypto_hashblocks/md5/little-1`
  using `gcc -m32 -march=k6-3 -O -fomit-frame-pointer`
- 2.00: `crypto_hashblocks/md5/ref`
  using `gcc -m32 -march=pentium4 -O2 -fomit-frame-pointer`

- 1.00: crypto_hashblocks/sha256/ref
  using gcc -funroll-loops -m32 -march=pentium2 -O -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha512/ref
  using gcc -funroll-loops -march=k6 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/bls/ref
  using g++ -m32 -march=prescott -O3 -fomit-frame-pointer
- 1.00: crypto_sign/donald1024/openssl
  using gcc -funroll-loops -m32 -march=prescott -O2 -fomit-frame-pointer
- 1.00: crypto_sign/donald2048/openssl
  using gcc -funroll-loops -m32 -march=pentium4 -O2 -fomit-frame-pointer
- 1.00: crypto_sign/donald512/openssl
  using gcc -funroll-loops -march=pentium3 -Os -fomit-frame-pointer
- 1.00: crypto_sign/rainbow/ref
  using g++ -march=prescott -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ronald1024/openssl
  using gcc -m32 -march=athlon -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald1536/openssl
  using gcc -funroll-loops -m32 -march=i386 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald2048/openssl
  using gcc -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ronald3072/openssl
  using gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald4096/openssl
  using gcc -funroll-loops -march=prescott -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald512/openssl
  using gcc -march=athlon -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald768/openssl
  using gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_sign/sflashv2/ref
  using gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes128estream/e/bernstein/x86-mmx-1
  using gcc -m32 -march=pentium2 -O -fomit-frame-pointer
- 1.07: crypto_stream/aes128estream/e/hongjun/v1
  using gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer
- 1.21: crypto_stream/aes128estream/e/hongjun/v0
  using gcc -funroll-loops -m32 -march=athlon -O -fomit-frame-pointer

- 1.40: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -m32 -march=k6-2 -O2 -fomit-frame-pointer`
- 1.50: `crypto_stream/aes128estream/e/gladman`
  using `gcc -funroll-loops -O -fomit-frame-pointer`
- 1.60: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -funroll-loops -m32 -march=pentium2 -O3 -fomit-frame-pointer`
- 1.63: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -funroll-loops -m32 -march=athlon -O2 -fomit-frame-pointer`
- 1.63: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -funroll-loops -march=athlon -O2 -fomit-frame-pointer`
- 1.76: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -m32 -march=pentiumpro -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer`
- 1.07: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -funroll-loops -march=nocona -O -fomit-frame-pointer`
- 1.39: `crypto_stream/aes256estream/e/gladman`
  using `gcc -funroll-loops -m32 -march=pentium4 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/x86-1`
  using `gcc -m32 -march=prescott -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/x86-xmm6`
  using `gcc -m32 -march=i386 -O -fomit-frame-pointer`
- 1.19: `crypto_stream/chacha12/e/merged`
  using `gcc -funroll-loops -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.19: `crypto_stream/chacha12/e/x86-xmm5`
  using `gcc -march=pentium-m -O2 -fomit-frame-pointer`
- 1.24: `crypto_stream/chacha12/e/x86-mmx`
  using `gcc -m32 -march=nocona -O2 -fomit-frame-pointer`
- 1.57: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer`
- 1.65: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -march=athlon -O3 -fomit-frame-pointer`
- 2.24: `crypto_stream/chacha12/e/x86-xmm`
  using `gcc -funroll-loops -march=k6-2 -O3 -fomit-frame-pointer`
- 2.63: `crypto_stream/chacha12/e/x86-xmm2`
  using `gcc -funroll-loops -m32 -march=pentium -O2 -fomit-frame-pointer`

- 1.00: `crypto_stream/chacha20/e/x86-xmm6`
  using `gcc`
- 1.01: `crypto_stream/chacha20/e/x86-1`
  using `gcc -m32 -march=k6-2 -O2 -fomit-frame-pointer`
- 1.13: `crypto_stream/chacha20/e/x86-xmm5`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.17: `crypto_stream/chacha20/e/merged`
  using `gcc -funroll-loops -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.28: `crypto_stream/chacha20/e/x86-mmx`
  using `gcc -m32 -march=k6-2 -O3 -fomit-frame-pointer`
- 1.45: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer`
- 1.47: `crypto_stream/chacha20/e/ref`
  using `gcc -funroll-loops -march=athlon -O3 -fomit-frame-pointer`
- 2.22: `crypto_stream/chacha20/e/x86-xmm`
  using `gcc -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 2.54: `crypto_stream/chacha20/e/x86-xmm2`
  using `gcc -march=k6-3 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/x86-1`
  using `gcc -m32 -march=nocona -O2 -fomit-frame-pointer`
- 1.01: `crypto_stream/chacha8/e/x86-xmm6`
  using `gcc -funroll-loops -m32 -march=pentium3 -O -fomit-frame-pointer`
- 1.19: `crypto_stream/chacha8/e/x86-mmx`
  using `gcc -march=pentium-m -O3 -fomit-frame-pointer`
- 1.19: `crypto_stream/chacha8/e/x86-xmm5`
  using `gcc -march=pentium-m -O2 -fomit-frame-pointer`
- 1.21: `crypto_stream/chacha8/e/merged`
  using `gcc -funroll-loops -march=pentium -O3 -fomit-frame-pointer`
- 1.72: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -march=pentium -O3 -fomit-frame-pointer`
- 1.78: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer`
- 2.06: `crypto_stream/chacha8/e/x86-xmm`
  using `gcc -funroll-loops -march=pentium -O3 -fomit-frame-pointer`
- 2.34: `crypto_stream/chacha8/e/x86-xmm2`
  using `gcc -m32 -march=k6-2 -O2 -fomit-frame-pointer`

- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -m32 -march=k6 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -m32 -march=prescott -O -fomit-frame-pointer`
- 1.02: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -funroll-loops -march=i386 -O -fomit-frame-pointer`
- 1.02: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -funroll-loops -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -funroll-loops -march=k6-2 -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -funroll-loops -m32 -march=k6-2 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -funroll-loops -m32 -march=k6 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -m32 -march=pentium2 -O -fomit-frame-pointer`
- 1.74: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m32 -march=pentium -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.08: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -funroll-loops -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.29: `crypto_stream/rabbit/e/opt/2/5`
  using `gcc -march=k6-3`
- 1.39: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -funroll-loops -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.40: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -march=pentium -O3 -fomit-frame-pointer`
- 1.59: `crypto_stream/rabbit/e/ref`
  using `gcc -funroll-loops -march=pentium -O2 -fomit-frame-pointer`
- 1.63: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`

- 1.64: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -march=prescott -O3 -fomit-frame-pointer`
- 1.95: `crypto_stream/rabbit/e/opt/2/4`
  using `gcc -m32 -march=k6-3`
- 1.00: `crypto_stream/salsa20/e/x86-xmm5`
  using `gcc -m32 -march=nocona -O3 -fomit-frame-pointer`
- 1.16: `crypto_stream/salsa20/e/x86-2`
  using `gcc -funroll-loops -march=prescott -Os -fomit-frame-pointer`
- 1.16: `crypto_stream/salsa20/e/x86-3`
  using `gcc -m32 -march=k8 -O2 -fomit-frame-pointer`
- 1.16: `crypto_stream/salsa20/e/x86-athlon`
  using `gcc -m32 -march=nocona -O3 -fomit-frame-pointer`
- 1.20: `crypto_stream/salsa20/e/x86-pm`
  using `gcc -funroll-loops -m32 -march=pentium -O -fomit-frame-pointer`
- 1.26: `crypto_stream/salsa20/e/x86-1`
  using `gcc -m32 -march=pentium2 -O -fomit-frame-pointer`
- 1.29: `crypto_stream/salsa20/e/x86-xmm4`
  using `gcc -m32 -march=athlon`
- 1.39: `crypto_stream/salsa20/e/x86-mmx`
  using `gcc -funroll-loops -m32 -O -fomit-frame-pointer`
- 1.49: `crypto_stream/salsa20/e/merged`
  using `gcc -funroll-loops -m32 -march=k6-2 -O3 -fomit-frame-pointer`
- 1.61: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer`
- 1.70: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer`
- 1.90: `crypto_stream/salsa20/ref`
  using `gcc -funroll-loops -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.91: `crypto_stream/salsa20/e/x86-xmm`
  using `gcc -m32 -march=nocona -O3 -fomit-frame-pointer`
- 2.61: `crypto_stream/salsa20/e/x86-xmm2`
  using `gcc -funroll-loops -m32 -march=k6 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/x86-xmm5`
  using `gcc -funroll-loops -m32 -march=i486 -O -fomit-frame-pointer`
- 1.09: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -m32 -march=pentium2 -O2 -fomit-frame-pointer`

- 1.10: `crypto_stream/salsa2012/e/x86-2`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.10: `crypto_stream/salsa2012/e/x86-athlon`
  using `gcc -m32 -march=prescott -O2 -fomit-frame-pointer`
- 1.10: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -march=nocona -O -fomit-frame-pointer`
- 1.18: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.26: `crypto_stream/salsa2012/e/x86-xmm4`
  using `gcc -O -fomit-frame-pointer`
- 1.28: `crypto_stream/salsa2012/e/x86-mmx`
  using `gcc -march=pentium -O -fomit-frame-pointer`
- 1.43: `crypto_stream/salsa2012/e/merged`
  using `gcc -funroll-loops -m32 -march=k6 -O3 -fomit-frame-pointer`
- 1.62: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.78: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer`
- 2.03: `crypto_stream/salsa2012/e/x86-xmm`
  using `gcc -march=pentium -O3 -fomit-frame-pointer`
- 2.10: `crypto_stream/salsa2012/ref`
  using `gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer`
- 2.39: `crypto_stream/salsa2012/e/x86-xmm2`
  using `gcc -m32 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/x86-xmm5`
  using `gcc -m32 -march=pentium4 -O2 -fomit-frame-pointer`
- 1.12: `crypto_stream/salsa208/e/x86-athlon`
  using `gcc -funroll-loops -m32 -march=k6 -O2 -fomit-frame-pointer`
- 1.12: `crypto_stream/salsa208/e/x86-pm`
  using `gcc -funroll-loops -m32 -march=i386 -O3 -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa208/e/x86-2`
  using `gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa208/e/x86-3`
  using `gcc -funroll-loops -march=pentium2 -O3 -fomit-frame-pointer`
- 1.20: `crypto_stream/salsa208/e/x86-1`
  using `gcc -m32 -march=nocona -O -fomit-frame-pointer`

- 1.27: crypto_stream/salsa208/e/x86-mmx
  using gcc -m32 -march=pentium3 -O -fomit-frame-pointer
- 1.32: crypto_stream/salsa208/e/x86-xmm4
  using gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer
- 1.38: crypto_stream/salsa208/e/merged
  using gcc -funroll-loops -march=k6-3 -Os -fomit-frame-pointer
- 1.83: crypto_stream/salsa208/e/regs
  using gcc -funroll-loops -march=i486 -O3 -fomit-frame-pointer
- 2.00: crypto_stream/salsa208/e/ref
  using gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer
- 2.28: crypto_stream/salsa208/e/x86-xmm
  using gcc -march=pentium2 -O2 -fomit-frame-pointer
- 2.32: crypto_stream/salsa208/ref
  using gcc -funroll-loops -m32 -march=pentium-mmx -O3 -fomit-frame-pointer
- 2.37: crypto_stream/salsa208/e/x86-xmm2
  using gcc -march=pentium4
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -funroll-loops -march=pentium4 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -funroll-loops -m32 -march=pentium-m -O -fomit-frame-pointer
- 1.00: crypto_stream/tpy/e/tpy
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpy6/e/tpy6
  using gcc -funroll-loops -march=athlon -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpypy/e/tpypy
  using gcc -funroll-loops -m32 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/trivium/e/submissions/trivium
  using gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer

5.43 x86, 2801MHz, Intel Xeon (f41), nmi0061

- 1.00: crypto_dh/claus/openssl
  using gcc -funroll-loops
- 1.00: crypto_encrypt/mceliece/ref
  using gcc -funroll-loops -m32 -march=pentium4 -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ntruees787ep1/ref
  using gcc -funroll-loops -m32 -march=i386 -O3 -fomit-frame-pointer

- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -m32 -march=k6`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -funroll-loops -march=i486 -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -funroll-loops -m32 -march=prescott -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -march=i386 -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `gcc -funroll-loops -m32 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -march=prescott -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -march=pentium4 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -funroll-loops -march=nocona -O -fomit-frame-pointer`
- 1.13: `crypto_hash/md5/openssl`
  using `gcc -m32 -O -fomit-frame-pointer`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -funroll-loops -m32 -march=i386 -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/ref`
  using `gcc -funroll-loops -m32 -march=prescott -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -funroll-loops -march=k6-2 -O -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/x86-1`
  using `gcc -m32 -march=k6-3 -O -fomit-frame-pointer`
- 1.52: `crypto_hashblocks/md5/little-1`
  using `gcc -m32 -march=k8 -Os -fomit-frame-pointer`
- 1.92: `crypto_hashblocks/md5/ref`
  using `gcc -m32 -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha256/ref`
  using `gcc -funroll-loops -march=k6-3 -O -fomit-frame-pointer`

- 1.00: crypto_hashblocks/sha512/ref
  using gcc -m32 -march=pentium-m -O3 -fomit-frame-pointer
- 1.00: crypto_sign/bls/ref
  using g++ -m32 -march=nocona -O2 -fomit-frame-pointer
- 1.00: crypto_sign/donald1024/openssl
  using gcc -march=pentium-mmx -Os -fomit-frame-pointer
- 1.00: crypto_sign/donald2048/openssl
  using gcc -funroll-loops -m32 -march=k6-2 -O2 -fomit-frame-pointer
- 1.00: crypto_sign/donald512/openssl
  using gcc -m32 -Os -fomit-frame-pointer
- 1.00: crypto_sign/ronald1024/openssl
  using gcc -funroll-loops -march=pentium4 -Os -fomit-frame-pointer
- 1.00: crypto_sign/ronald1536/openssl
  using gcc -m32 -march=pentium-m -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald2048/openssl
  using gcc -funroll-loops -march=prescott -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald3072/openssl
  using gcc -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald4096/openssl
  using gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald512/openssl
  using gcc -m32 -march=nocona -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald768/openssl
  using gcc -funroll-loops -march=pentium2 -O -fomit-frame-pointer
- 1.00: crypto_sign/sflashv2/ref
  using gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes128estream/e/bernstein/x86-mmx-1
  using gcc -funroll-loops -march=pentium-mmx -O -fomit-frame-pointer
- 1.08: crypto_stream/aes128estream/e/hongjun/v1
  using gcc -funroll-loops -m32 -march=pentium4 -O -fomit-frame-pointer
- 1.22: crypto_stream/aes128estream/e/hongjun/v0
  using gcc -funroll-loops -m32 -march=k8 -O -fomit-frame-pointer
- 1.33: crypto_stream/aes128estream/e/bernstein/little-4
  using gcc -march=pentium4 -O2 -fomit-frame-pointer
- 1.50: crypto_stream/aes128estream/e/bernstein/little-3
  using gcc -funroll-loops -m32 -march=k6-2 -O3 -fomit-frame-pointer

- 1.62: `crypto_stream/aes128estream/e/gladman`
  using `gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer`
- 1.64: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -funroll-loops -march=pentium -Os -fomit-frame-pointer`
- 1.65: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -funroll-loops -m32 -march=athlon -O2 -fomit-frame-pointer`
- 1.76: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -funroll-loops -m32 -march=athlon -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer`
- 1.07: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -funroll-loops -march=k8 -O -fomit-frame-pointer`
- 1.38: `crypto_stream/aes256estream/e/gladman`
  using `gcc -funroll-loops -march=pentium3 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/x86-1`
  using `gcc -funroll-loops -m32 -march=prescott -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/x86-xmm6`
  using `gcc -funroll-loops -march=pentium3`
- 1.10: `crypto_stream/chacha12/e/x86-xmm5`
  using `gcc -funroll-loops -march=pentiumpro -O -fomit-frame-pointer`
- 1.11: `crypto_stream/chacha12/e/merged`
  using `gcc -funroll-loops -m32 -march=i486 -O3 -fomit-frame-pointer`
- 1.23: `crypto_stream/chacha12/e/x86-mmx`
  using `gcc -funroll-loops -m32 -march=k8 -Os -fomit-frame-pointer`
- 1.65: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.74: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 2.24: `crypto_stream/chacha12/e/x86-xmm`
  using `gcc -march=i486`
- 2.63: `crypto_stream/chacha12/e/x86-xmm2`
  using `gcc -m32 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/x86-xmm6`
  using `gcc -funroll-loops -march=pentium3`
- 1.01: `crypto_stream/chacha20/e/x86-1`
  using `gcc -funroll-loops -m32 -march=prescott -O2 -fomit-frame-pointer`

- 1.15: crypto_stream/chacha20/e/merged
  using gcc -m32 -march=i486 -O3 -fomit-frame-pointer
- 1.15: crypto_stream/chacha20/e/x86-xmm5
  using gcc -march=pentium -O3 -fomit-frame-pointer
- 1.28: crypto_stream/chacha20/e/x86-mmx
  using gcc -funroll-loops -m32 -O3 -fomit-frame-pointer
- 1.55: crypto_stream/chacha20/e/regs
  using gcc -funroll-loops -march=pentium-mmx -O3 -fomit-frame-pointer
- 1.57: crypto_stream/chacha20/e/ref
  using gcc -funroll-loops -m32 -march=nocona -O3 -fomit-frame-pointer
- 2.22: crypto_stream/chacha20/e/x86-xmm
  using gcc -funroll-loops -march=pentium2 -O2 -fomit-frame-pointer
- 2.54: crypto_stream/chacha20/e/x86-xmm2
  using gcc -march=pentium2 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/chacha8/e/x86-1
  using gcc -m32 -march=nocona -O2 -fomit-frame-pointer
- 1.00: crypto_stream/chacha8/e/x86-xmm6
  using gcc -funroll-loops -m32 -march=athlon
- 1.13: crypto_stream/chacha8/e/merged
  using gcc -funroll-loops -march=i486 -O3 -fomit-frame-pointer
- 1.13: crypto_stream/chacha8/e/x86-xmm5
  using gcc -funroll-loops -m32 -march=pentium-mmx
- 1.19: crypto_stream/chacha8/e/x86-mmx
  using gcc -march=pentium2 -Os -fomit-frame-pointer
- 1.81: crypto_stream/chacha8/e/ref
  using gcc -funroll-loops -march=pentium3 -O3 -fomit-frame-pointer
- 1.95: crypto_stream/chacha8/e/regs
  using gcc -funroll-loops -march=pentium -O3 -fomit-frame-pointer
- 2.06: crypto_stream/chacha8/e/x86-xmm
  using gcc -m32 -march=k6
- 2.33: crypto_stream/chacha8/e/x86-xmm2
  using gcc -funroll-loops -m32 -march=athlon -O2 -fomit-frame-pointer
- 1.00: crypto_stream/cryptmtv3/e/v3
  using gcc -funroll-loops -march=pentiumpro -O3 -fomit-frame-pointer
- 1.00: crypto_stream/dragon/e/submissions/dragon
  using gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer

- 1.00: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -m32 -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.04: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -m32 -march=pentium4 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -march=k6-2 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -march=pentium -O -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -funroll-loops -march=k6 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -march=athlon -O3 -fomit-frame-pointer`
- 1.80: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -m32 -march=k6-2 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -funroll-loops -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -funroll-loops -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer`
- 1.14: `crypto_stream/rabbit/e/opt/2/4`
  using `gcc -m32 -march=pentium-m -O3 -fomit-frame-pointer`
- 1.28: `crypto_stream/rabbit/e/opt/2/5`
  using `gcc -march=k6`
- 1.38: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -march=pentium -O3 -fomit-frame-pointer`
- 1.39: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.61: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -funroll-loops -m32 -march=pentium2 -O3 -fomit-frame-pointer`
- 1.62: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -funroll-loops -march=pentium3 -O3 -fomit-frame-pointer`
- 1.84: `crypto_stream/rabbit/e/ref`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`

- 1.00: crypto_stream/salsa20/e/x86-xmm5
  using gcc -funroll-loops -m32 -march=prescott -O2 -fomit-frame-pointer
- 1.16: crypto_stream/salsa20/e/x86-2
  using gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer
- 1.16: crypto_stream/salsa20/e/x86-3
  using gcc -m32 -march=pentium4 -O -fomit-frame-pointer
- 1.17: crypto_stream/salsa20/e/x86-athlon
  using gcc -m32 -march=prescott -Os -fomit-frame-pointer
- 1.21: crypto_stream/salsa20/e/x86-pm
  using gcc -m32 -march=athlon -O3 -fomit-frame-pointer
- 1.23: crypto_stream/salsa20/e/merged
  using gcc -m32 -march=i486 -O3 -fomit-frame-pointer
- 1.26: crypto_stream/salsa20/e/x86-1
  using gcc -march=pentium2 -O3 -fomit-frame-pointer
- 1.29: crypto_stream/salsa20/e/x86-xmm4
  using gcc -m32 -march=athlon -O2 -fomit-frame-pointer
- 1.40: crypto_stream/salsa20/e/x86-mmx
  using gcc -m32 -march=prescott -O -fomit-frame-pointer
- 1.61: crypto_stream/salsa20/e/regs
  using gcc -funroll-loops -march=pentium3 -O3 -fomit-frame-pointer
- 1.83: crypto_stream/salsa20/e/ref
  using gcc -funroll-loops -march=pentium4 -Os -fomit-frame-pointer
- 1.90: crypto_stream/salsa20/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.92: crypto_stream/salsa20/e/x86-xmm
  using gcc -m32
- 2.61: crypto_stream/salsa20/e/x86-xmm2
  using gcc -funroll-loops
- 1.00: crypto_stream/salsa2012/e/x86-xmm5
  using gcc -march=nocona -O3 -fomit-frame-pointer
- 1.14: crypto_stream/salsa2012/e/x86-pm
  using gcc -march=pentium-mmx -O2 -fomit-frame-pointer
- 1.15: crypto_stream/salsa2012/e/x86-2
  using gcc -march=athlon -Os -fomit-frame-pointer
- 1.15: crypto_stream/salsa2012/e/x86-3
  using gcc -m32 -march=k8 -Os -fomit-frame-pointer

- 1.15: `crypto_stream/salsa2012/e/x86-athlon`
  using `gcc -funroll-loops -march=k6 -O -fomit-frame-pointer`
- 1.24: `crypto_stream/salsa2012/e/merged`
  using `gcc -march=i486 -O3 -fomit-frame-pointer`
- 1.24: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -m32 -march=pentium3 -O2 -fomit-frame-pointer`
- 1.30: `crypto_stream/salsa2012/e/x86-xmm4`
  using `gcc -march=k6-3 -O2 -fomit-frame-pointer`
- 1.34: `crypto_stream/salsa2012/e/x86-mmx`
  using `gcc -m32 -march=nocona -O -fomit-frame-pointer`
- 1.73: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium2 -O3 -fomit-frame-pointer`
- 1.91: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer`
- 2.10: `crypto_stream/salsa2012/e/x86-xmm`
  using `gcc -march=prescott -O2 -fomit-frame-pointer`
- 2.17: `crypto_stream/salsa2012/ref`
  using `gcc -march=pentium -O3 -fomit-frame-pointer`
- 2.49: `crypto_stream/salsa2012/e/x86-xmm2`
  using `gcc -m32 -march=pentium2 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/x86-xmm5`
  using `gcc -m32 -O2 -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa208/e/x86-2`
  using `gcc -funroll-loops -march=k6-2 -Os -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa208/e/x86-3`
  using `gcc -funroll-loops -march=k6-3 -O3 -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa208/e/x86-pm`
  using `gcc -march=pentium-m -O3 -fomit-frame-pointer`
- 1.14: `crypto_stream/salsa208/e/x86-athlon`
  using `gcc -march=k8 -Os -fomit-frame-pointer`
- 1.21: `crypto_stream/salsa208/e/x86-1`
  using `gcc -m32 -Os -fomit-frame-pointer`
- 1.26: `crypto_stream/salsa208/e/merged`
  using `gcc -funroll-loops -m32 -march=i386 -O3 -fomit-frame-pointer`
- 1.28: `crypto_stream/salsa208/e/x86-mmx`
  using `gcc -march=pentium-m -O -fomit-frame-pointer`

- 1.33: crypto_stream/salsa208/e/x86-xmm4
  using gcc -funroll-loops -m32 -march=k8
- 1.84: crypto_stream/salsa208/e/regs
  using gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer
- 2.10: crypto_stream/salsa208/e/ref
  using gcc -funroll-loops -march=prescott -O -fomit-frame-pointer
- 2.26: crypto_stream/salsa208/e/x86-xmm
  using gcc -funroll-loops -march=pentium2
- 2.40: crypto_stream/salsa208/e/x86-xmm2
  using gcc -funroll-loops -march=k8
- 2.40: crypto_stream/salsa208/ref
  using gcc -m32 -march=pentium -O3 -fomit-frame-pointer
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -funroll-loops -march=prescott -O2 -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer
- 1.00: crypto_stream/tpy/e/tpy
  using gcc -funroll-loops -m32 -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpy6/e/tpy6
  using gcc -funroll-loops -march=athlon -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpypy/e/tpypy
  using gcc -funroll-loops -march=pentium4 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/trivium/e/submissions/trivium
  using gcc -funroll-loops -m32 -march=k6-3 -O -fomit-frame-pointer

5.44 x86, 2801MHz, Intel Xeon (f41), nmi0062

- 1.00: crypto_dh/claus/gmp
  using g++ -m32 -march=pentium2 -O2 -fomit-frame-pointer
- 2.59: crypto_dh/claus/openssl
  using gcc -m32 -march=pentium3 -O2 -fomit-frame-pointer
- 1.00: crypto_dh/curve2251/mpfq
  using gcc -funroll-loops -march=k8 -O -fomit-frame-pointer
- 1.00: crypto_dh/curve25519/mpfq
  using gcc -funroll-loops -march=pentium3 -O3 -fomit-frame-pointer
- 1.00: crypto_dh/hector/ref
  using gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer

- 1.00: `crypto_dh/surf127eps/mpfq`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_dh/surf2113/mpfq`
  using `gcc -funroll-loops -m32 -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/mceliece/ref`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -funroll-loops -march=pentium-m -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -m32 -march=pentium-m -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -march=pentiumpro -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -m32 -march=k6-3 -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `gcc -m32 -march=i386`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -m32 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -funroll-loops -m32 -march=pentium4`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -funroll-loops -m32 -march=k6 -O -fomit-frame-pointer`
- 1.15: `crypto_hash/md5/openssl`
  using `gcc -m32 -march=prescott -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -m32 -march=pentium-mmx -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -march=i386 -O -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/ref`
  using `gcc -funroll-loops -m32 -march=pentium2 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -funroll-loops -march=pentium -Os -fomit-frame-pointer`

- 1.00: crypto_hashblocks/md5/x86-1
  using gcc -march=pentium-m -Os -fomit-frame-pointer
- 1.45: crypto_hashblocks/md5/little-1
  using gcc -m32 -march=k6-3 -O -fomit-frame-pointer
- 1.76: crypto_hashblocks/md5/ref
  using gcc -funroll-loops -march=k6 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha256/ref
  using gcc -march=nocona -O -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha512/ref
  using gcc -funroll-loops -m32 -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_sign/bls/ref
  using g++ -m32 -march=k8 -Os -fomit-frame-pointer
- 1.00: crypto_sign/donald1024/openssl
  using gcc -m32 -march=athlon -O2 -fomit-frame-pointer
- 1.00: crypto_sign/donald2048/openssl
  using gcc -m32 -march=pentium4 -O -fomit-frame-pointer
- 1.00: crypto_sign/donald512/openssl
  using gcc -march=k6-3 -Os -fomit-frame-pointer
- 1.00: crypto_sign/hector/ref
  using gcc -funroll-loops -march=pentium-m -O3 -fomit-frame-pointer
- 1.00: crypto_sign/rainbow/ref
  using g++ -m32 -march=prescott -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald1024/openssl
  using gcc -march=athlon -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ronald1536/openssl
  using gcc -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald2048/openssl
  using gcc -funroll-loops -m32 -march=prescott -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ronald3072/openssl
  using gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ronald4096/openssl
  using gcc -funroll-loops -march=nocona -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald512/openssl
  using gcc -march=pentium-m -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald768/openssl
  using gcc -march=pentium2 -O2 -fomit-frame-pointer

- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -funroll-loops -m32 -march=prescott -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/bernstein/x86-mmx-1`
  using `gcc -m32 -march=k6-2 -O2 -fomit-frame-pointer`
- 1.09: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer`
- 1.12: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -m32 -march=nocona -O -fomit-frame-pointer`
- 1.19: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -m32 -march=pentium-mmx -O -fomit-frame-pointer`
- 1.30: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -m32 -march=k6-2 -O -fomit-frame-pointer`
- 1.41: `crypto_stream/aes128estream/e/gladman`
  using `gcc -march=pentium-m -O -fomit-frame-pointer`
- 1.70: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -march=athlon -O -fomit-frame-pointer`
- 1.72: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -m32 -march=athlon -O -fomit-frame-pointer`
- 1.90: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer`
- 1.02: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -funroll-loops -march=prescott -O -fomit-frame-pointer`
- 1.22: `crypto_stream/aes256estream/e/gladman`
  using `gcc -march=pentium2 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/x86-xmm6`
  using `gcc -funroll-loops -m32 -march=k6-3 -O -fomit-frame-pointer`
- 1.01: `crypto_stream/chacha12/e/x86-1`
  using `gcc -funroll-loops -m32 -march=pentium4 -Os -fomit-frame-pointer`
- 1.12: `crypto_stream/chacha12/e/merged`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.12: `crypto_stream/chacha12/e/x86-xmm5`
  using `gcc -m32 -march=i386 -O2 -fomit-frame-pointer`
- 1.24: `crypto_stream/chacha12/e/x86-mmx`
  using `gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer`

- 1.35: crypto_stream/chacha12/e/regs
  using gcc -funroll-loops -march=pentium3 -O3 -fomit-frame-pointer
- 2.11: crypto_stream/chacha12/e/ref
  using gcc -funroll-loops -march=pentiumpro -O -fomit-frame-pointer
- 2.23: crypto_stream/chacha12/e/x86-xmm
  using gcc -m32 -march=k6-2 -O -fomit-frame-pointer
- 2.59: crypto_stream/chacha12/e/x86-xmm2
  using gcc -funroll-loops -march=pentium2 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/chacha20/e/x86-xmm6
  using gcc -m32 -march=k6-3 -O2 -fomit-frame-pointer
- 1.02: crypto_stream/chacha20/e/x86-1
  using gcc -O -fomit-frame-pointer
- 1.09: crypto_stream/chacha20/e/merged
  using gcc -m32 -march=athlon -O3 -fomit-frame-pointer
- 1.15: crypto_stream/chacha20/e/x86-xmm5
  using gcc -march=k6-2 -O2 -fomit-frame-pointer
- 1.24: crypto_stream/chacha20/e/regs
  using gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer
- 1.29: crypto_stream/chacha20/e/x86-mmx
  using gcc -funroll-loops -m32 -march=nocona -O2 -fomit-frame-pointer
- 1.99: crypto_stream/chacha20/e/ref
  using gcc -funroll-loops -march=athlon -O -fomit-frame-pointer
- 2.23: crypto_stream/chacha20/e/x86-xmm
  using gcc -march=pentium -O -fomit-frame-pointer
- 2.56: crypto_stream/chacha20/e/x86-xmm2
  using gcc -march=i486 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/chacha8/e/x86-1
  using gcc -m32 -march=athlon -Os -fomit-frame-pointer
- 1.00: crypto_stream/chacha8/e/x86-xmm6
  using gcc -funroll-loops -march=pentium -O -fomit-frame-pointer
- 1.14: crypto_stream/chacha8/e/merged
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.17: crypto_stream/chacha8/e/x86-xmm5
  using gcc -m32 -march=athlon -O2 -fomit-frame-pointer
- 1.19: crypto_stream/chacha8/e/x86-mmx
  using gcc -m32 -march=i386 -Os -fomit-frame-pointer

- 1.75: `crypto_stream/chacha8/e/regs`
  using `gcc -march=prescott -O3 -fomit-frame-pointer`
- 2.06: `crypto_stream/chacha8/e/x86-xmm`
  using `gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer`
- 2.23: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -march=pentiumpro -O -fomit-frame-pointer`
- 2.34: `crypto_stream/chacha8/e/x86-xmm2`
  using `gcc -march=i386 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -march=pentium4 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -funroll-loops -march=prescott -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -march=pentium-mmx -O2 -fomit-frame-pointer`
- 1.02: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -funroll-loops -march=pentium -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -m32 -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -funroll-loops -march=i386 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -m32 -march=nocona -O3 -fomit-frame-pointer`
- 1.78: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -funroll-loops -march=i486 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -funroll-loops -march=i486 -O3 -fomit-frame-pointer`
- 1.04: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer`
- 1.20: `crypto_stream/rabbit/e/opt/2/5`
  using `gcc -funroll-loops -m32 -march=k6`

- 1.41: crypto_stream/rabbit/e/opt/1/2
  using gcc -funroll-loops -march=pentium3 -O -fomit-frame-pointer
- 1.41: crypto_stream/rabbit/e/opt/2/2
  using gcc -funroll-loops -march=pentium3 -O -fomit-frame-pointer
- 1.56: crypto_stream/rabbit/e/opt/1/1
  using gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer
- 1.56: crypto_stream/rabbit/e/opt/2/1
  using gcc -march=pentium-mmx -O2 -fomit-frame-pointer
- 1.70: crypto_stream/rabbit/e/opt/2/4
  using gcc -funroll-loops -march=i386
- 1.82: crypto_stream/rabbit/e/ref
  using gcc -funroll-loops -march=pentium-m -O2 -fomit-frame-pointer
- 1.00: crypto_stream/salsa20/e/x86-xmm5
  using gcc -funroll-loops -march=k6-2 -O2 -fomit-frame-pointer
- 1.16: crypto_stream/salsa20/e/x86-2
  using gcc -march=pentium2 -O3 -fomit-frame-pointer
- 1.16: crypto_stream/salsa20/e/x86-3
  using gcc -m32 -march=pentiumpro -Os -fomit-frame-pointer
- 1.16: crypto_stream/salsa20/e/x86-athlon
  using gcc -m32 -march=prescott -Os -fomit-frame-pointer
- 1.16: crypto_stream/salsa20/e/x86-pm
  using gcc -m32 -march=pentium -Os -fomit-frame-pointer
- 1.26: crypto_stream/salsa20/e/x86-1
  using gcc -m32 -march=k6-2 -Os -fomit-frame-pointer
- 1.29: crypto_stream/salsa20/e/x86-xmm4
  using gcc -m32 -O2 -fomit-frame-pointer
- 1.34: crypto_stream/salsa20/e/merged
  using gcc -march=k6-2 -O -fomit-frame-pointer
- 1.39: crypto_stream/salsa20/e/x86-mmx
  using gcc -funroll-loops -march=pentium-mmx -Os -fomit-frame-pointer
- 1.45: crypto_stream/salsa20/e/regs
  using gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer
- 1.70: crypto_stream/salsa20/e/ref
  using gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer
- 1.70: crypto_stream/salsa20/ref
  using gcc -funroll-loops -m32 -march=nocona -Os -fomit-frame-pointer

- 1.91: `crypto_stream/salsa20/e/x86-xmm`
  using `gcc -march=k8 -O2 -fomit-frame-pointer`
- 2.60: `crypto_stream/salsa20/e/x86-xmm2`
  using `gcc -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/x86-xmm5`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O2 -fomit-frame-pointer`
- 1.14: `crypto_stream/salsa2012/e/x86-2`
  using `gcc -funroll-loops -march=i486 -O2 -fomit-frame-pointer`
- 1.14: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -m32 -march=i486 -Os -fomit-frame-pointer`
- 1.14: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -m32 -march=pentium4 -Os -fomit-frame-pointer`
- 1.15: `crypto_stream/salsa2012/e/x86-athlon`
  using `gcc -m32 -march=k6 -Os -fomit-frame-pointer`
- 1.24: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -funroll-loops -m32 -march=k6-2 -Os -fomit-frame-pointer`
- 1.30: `crypto_stream/salsa2012/e/x86-xmm4`
  using `gcc -funroll-loops -m32 -march=i386 -O -fomit-frame-pointer`
- 1.34: `crypto_stream/salsa2012/e/merged`
  using `gcc -m32 -march=k6-3 -O -fomit-frame-pointer`
- 1.34: `crypto_stream/salsa2012/e/x86-mmx`
  using `gcc -funroll-loops -m32 -march=k6 -O2 -fomit-frame-pointer`
- 1.56: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer`
- 1.81: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer`
- 1.93: `crypto_stream/salsa2012/ref`
  using `gcc -m32 -march=i386 -Os -fomit-frame-pointer`
- 2.10: `crypto_stream/salsa2012/e/x86-xmm`
  using `gcc -m32 -march=pentium3 -O -fomit-frame-pointer`
- 2.48: `crypto_stream/salsa2012/e/x86-xmm2`
  using `gcc -funroll-loops -m32 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/x86-xmm5`
  using `gcc -m32 -march=nocona -O2 -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa208/e/x86-2`
  using `gcc -m32 -march=k6 -O3 -fomit-frame-pointer`

- 1.13: crypto_stream/salsa208/e/x86-3
  using gcc -march=k8 -Os -fomit-frame-pointer
- 1.13: crypto_stream/salsa208/e/x86-athlon
  using gcc -march=i486 -Os -fomit-frame-pointer
- 1.14: crypto_stream/salsa208/e/x86-pm
  using gcc -m32 -march=pentium-m -O2 -fomit-frame-pointer
- 1.21: crypto_stream/salsa208/e/x86-1
  using gcc -m32 -march=pentium3 -Os -fomit-frame-pointer
- 1.28: crypto_stream/salsa208/e/x86-mmx
  using gcc -m32 -march=prescott -Os -fomit-frame-pointer
- 1.32: crypto_stream/salsa208/e/x86-xmm4
  using gcc -funroll-loops -m32 -march=pentium -O2 -fomit-frame-pointer
- 1.33: crypto_stream/salsa208/e/merged
  using gcc -march=pentium -O -fomit-frame-pointer
- 1.84: crypto_stream/salsa208/e/ref
  using gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer
- 1.87: crypto_stream/salsa208/e/regs
  using gcc -march=pentium4 -O -fomit-frame-pointer
- 2.13: crypto_stream/salsa208/e/x86-xmm
  using gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer
- 2.17: crypto_stream/salsa208/ref
  using gcc -march=pentium4 -Os -fomit-frame-pointer
- 2.40: crypto_stream/salsa208/e/x86-xmm2
  using gcc -funroll-loops -march=pentium-m -O3 -fomit-frame-pointer
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -march=pentium2 -O -fomit-frame-pointer
- 1.00: crypto_stream/tpy/e/tpy
  using gcc -funroll-loops -march=k6-3 -Os -fomit-frame-pointer
- 1.00: crypto_stream/tpy6/e/tpy6
  using gcc -funroll-loops -m32 -march=k6-3 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpypy/e/tpypy
  using gcc -m32 -march=nocona -O -fomit-frame-pointer
- 1.00: crypto_stream/trivium/e/submissions/trivium
  using gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer

5.45 x86, 2802MHz, Intel Xeon (f29), `nmibuild40`

- 1.00: `crypto_dh/claus/openssl`
  using `gcc -m32`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `cc`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -m32`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `cc`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -m32`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.03: `crypto_hash/md5/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -m32`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -m32`
- 1.00: `crypto_hash/sha512/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `cc`
- 1.00: `crypto_hashblocks/md5/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.15: `crypto_hashblocks/md5/little-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.73: `crypto_hashblocks/md5/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha256/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha512/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/bls/ref`
  using `g++ -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1024/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1536/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald2048/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald3072/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald4096/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald512/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald768/openssl`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/bernstein/x86-mmx-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.77: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.78: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.79: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.90: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.94: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.08: `crypto_stream/aes128estream/e/gladman`
  using `cc`
- 2.30: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.66: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/gladman`
  using `cc`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.05: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/x86-xmm6`
  using `cc`
- 1.04: `crypto_stream/chacha12/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.26: `crypto_stream/chacha12/e/x86-1`
  using `gcc -m32`
- 1.41: `crypto_stream/chacha12/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.71: `crypto_stream/chacha12/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.76: `crypto_stream/chacha12/e/x86-xmm`
  using `gcc -m32`
- 4.06: `crypto_stream/chacha12/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 4.68: `crypto_stream/chacha12/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 5.77: `crypto_stream/chacha12/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/x86-xmm6`
  using `cc`
- 1.08: `crypto_stream/chacha20/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.32: `crypto_stream/chacha20/e/x86-1`
  using `cc`
- 1.44: `crypto_stream/chacha20/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.84: `crypto_stream/chacha20/e/x86-xmm2`
  using `gcc -m32`
- 1.87: `crypto_stream/chacha20/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 4.38: `crypto_stream/chacha20/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 4.90: `crypto_stream/chacha20/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 5.23: `crypto_stream/chacha20/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.08: `crypto_stream/chacha8/e/x86-xmm6`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.22: `crypto_stream/chacha8/e/x86-1`
  using `cc`
- 1.32: `crypto_stream/chacha8/e/x86-mmx`
  using `cc`
- 1.62: `crypto_stream/chacha8/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.65: `crypto_stream/chacha8/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.69: `crypto_stream/chacha8/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 4.33: `crypto_stream/chacha8/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 5.34: `crypto_stream/chacha8/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.07: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.06: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.05: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/5`
  using `gcc -m32`
- 1.33: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.33: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.35: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.53: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.71: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.95: `crypto_stream/rabbit/e/opt/2/4`
  using `gcc -m32`
- 2.00: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.01: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.20: `crypto_stream/rabbit/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/salsa20/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.26: `crypto_stream/salsa20/e/x86-xmm4`
  using `gcc -m32`
- 1.44: `crypto_stream/salsa20/e/x86-2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.44: `crypto_stream/salsa20/e/x86-3`
  using `gcc -m32`
- 1.44: `crypto_stream/salsa20/e/x86-athlon`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.45: `crypto_stream/salsa20/e/x86-pm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.84: `crypto_stream/salsa20/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.92: `crypto_stream/salsa20/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.71: `crypto_stream/salsa20/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.95: `crypto_stream/salsa20/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.06: `crypto_stream/salsa20/e/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.43: `crypto_stream/salsa20/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.48: `crypto_stream/salsa20/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.55: `crypto_stream/salsa20/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.24: `crypto_stream/salsa2012/e/x86-xmm4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.43: `crypto_stream/salsa2012/e/x86-athlon`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.44: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.45: `crypto_stream/salsa2012/e/x86-2`
  using `cc`
- 1.47: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.89: `crypto_stream/salsa2012/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.14: `crypto_stream/salsa2012/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.61: `crypto_stream/salsa2012/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.83: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -m32`
- 3.13: `crypto_stream/salsa2012/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.42: `crypto_stream/salsa2012/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.74: `crypto_stream/salsa2012/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.90: `crypto_stream/salsa2012/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/x86-xmm5`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.36: `crypto_stream/salsa208/e/x86-xmm4`
  using `gcc -m32`
- 1.44: `crypto_stream/salsa208/e/x86-pm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.45: `crypto_stream/salsa208/e/x86-2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.45: `crypto_stream/salsa208/e/x86-3`
  using `cc`
- 1.48: `crypto_stream/salsa208/e/x86-athlon`
  using `cc`
- 1.79: `crypto_stream/salsa208/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.82: `crypto_stream/salsa208/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 2.54: crypto_stream/salsa208/e/x86-mmx
  using gcc -m32
- 2.80: crypto_stream/salsa208/e/x86-1
  using gcc -m32 -O3 -fomit-frame-pointer
- 3.27: crypto_stream/salsa208/e/merged
  using gcc -m32 -O3 -fomit-frame-pointer
- 3.29: crypto_stream/salsa208/e/regs
  using gcc -m32 -O3 -fomit-frame-pointer
- 3.95: crypto_stream/salsa208/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 4.00: crypto_stream/salsa208/e/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpy/e/tpy
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpy6/e/tpy6
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpypy/e/tpypy
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/trivium/e/submissions/trivium
  using gcc -m32 -O3 -fomit-frame-pointer

5.46 x86, 2995MHz, Intel Xeon (f41), nmi0079

- 1.00: crypto_dh/claus/openssl
  using gcc -funroll-loops -m32 -march=pentium -O -fomit-frame-pointer
- 1.00: crypto_encrypt/mceliece/ref
  using gcc -funroll-loops -march=prescott -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ntruees787ep1/ref
  using gcc -funroll-loops -march=nocona -O -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald1024/openssl
  using gcc -funroll-loops -march=pentium-mmx -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ronald1536/openssl
  using gcc -march=pentium2 -O2 -fomit-frame-pointer

- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -funroll-loops -march=pentium-m -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -funroll-loops -march=k6-3 -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `gcc -march=pentium-m -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -m32 -march=pentium-m -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -march=i386 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -funroll-loops -m32 -march=k8 -O -fomit-frame-pointer`
- 1.12: `crypto_hash/md5/openssl`
  using `gcc -march=pentium-m -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -funroll-loops -march=pentium -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -march=nocona -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/sha224/openssl`
  using `gcc -funroll-loops -m32 -march=pentium2 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -funroll-loops -m32 -march=i386 -O3 -fomit-frame-pointer`
- 1.29: `crypto_hash/sha256/openssl`
  using `gcc -m32 -march=i486 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/sha384/openssl`
  using `gcc -march=prescott -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/openssl`
  using `gcc -march=pentium2 -Os -fomit-frame-pointer`
- 4.41: `crypto_hash/sha512/ref`
  using `gcc -funroll-loops -m32 -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/x86-1`
  using `gcc -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.24: `crypto_hashblocks/md5/little-1`
  using `gcc -march=pentium-m -O3 -fomit-frame-pointer`

- 1.51: crypto_hashblocks/md5/ref
  using gcc -march=pentium4 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha256/ref
  using gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha512/ref
  using gcc -march=pentiumpro -O -fomit-frame-pointer
- 1.00: crypto_sign/bls/ref
  using g++ -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/donald1024/openssl
  using gcc -funroll-loops -march=nocona -Os -fomit-frame-pointer
- 1.00: crypto_sign/donald2048/openssl
  using gcc -march=pentium4
- 1.00: crypto_sign/donald512/openssl
  using gcc -m32 -march=nocona -Os -fomit-frame-pointer
- 1.00: crypto_sign/rainbow/ref
  using g++ -m32 -march=prescott
- 1.00: crypto_sign/ronald1024/openssl
  using gcc -m32 -march=pentium-m -Os -fomit-frame-pointer
- 1.00: crypto_sign/ronald1536/openssl
  using gcc -funroll-loops -m32 -march=pentium4 -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ronald2048/openssl
  using gcc -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald3072/openssl
  using gcc -m32 -march=pentium3 -Os -fomit-frame-pointer
- 1.00: crypto_sign/ronald4096/openssl
  using gcc -march=i386 -Os -fomit-frame-pointer
- 1.00: crypto_sign/ronald512/openssl
  using gcc -march=pentiumpro -Os -fomit-frame-pointer
- 1.00: crypto_sign/ronald768/openssl
  using gcc -m32 -march=prescott -O3 -fomit-frame-pointer
- 1.00: crypto_sign/sflashv2/ref
  using gcc -funroll-loops -m32 -march=nocona -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes128estream/e/bernstein/x86-mmx-1
  using gcc -m32 -march=k6 -Os -fomit-frame-pointer
- 1.11: crypto_stream/aes128estream/e/hongjun/v0
  using gcc -m32 -march=pentiumpro -O -fomit-frame-pointer

- 1.18: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -march=pentium2 -O -fomit-frame-pointer`
- 1.24: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -m32 -march=prescott -O -fomit-frame-pointer`
- 1.46: `crypto_stream/aes128estream/e/gladman`
  using `gcc -funroll-loops -m32 -march=i386 -O -fomit-frame-pointer`
- 1.55: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer`
- 2.01: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -march=athlon -O -fomit-frame-pointer`
- 2.07: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -m32 -march=athlon -O -fomit-frame-pointer`
- 2.11: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -march=i386 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -m32 -march=nocona -O -fomit-frame-pointer`
- 1.07: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -funroll-loops -march=athlon -O -fomit-frame-pointer`
- 1.21: `crypto_stream/aes256estream/e/gladman`
  using `gcc -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/x86-xmm6`
  using `gcc -funroll-loops -march=k6-3 -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/chacha12/e/x86-1`
  using `gcc -m32 -march=k6-2 -Os -fomit-frame-pointer`
- 1.02: `crypto_stream/chacha12/e/merged`
  using `gcc -funroll-loops -march=k6-2 -Os -fomit-frame-pointer`
- 1.12: `crypto_stream/chacha12/e/x86-xmm5`
  using `gcc -march=nocona -O3 -fomit-frame-pointer`
- 1.24: `crypto_stream/chacha12/e/x86-mmx`
  using `gcc -m32 -march=i386 -O -fomit-frame-pointer`
- 1.31: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer`
- 1.50: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 2.25: `crypto_stream/chacha12/e/x86-xmm`
  using `gcc -march=pentium3 -O2 -fomit-frame-pointer`

- 2.63: `crypto_stream/chacha12/e/x86-xmm2`
  using `gcc -march=pentium2 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/x86-xmm6`
  using `gcc -m32 -march=k6-2 -O -fomit-frame-pointer`
- 1.01: `crypto_stream/chacha20/e/merged`
  using `gcc -march=k6-3 -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/chacha20/e/x86-1`
  using `gcc -m32 -march=pentiumpro -Os -fomit-frame-pointer`
- 1.17: `crypto_stream/chacha20/e/x86-xmm5`
  using `gcc -funroll-loops -march=pentium-m -O2 -fomit-frame-pointer`
- 1.21: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.28: `crypto_stream/chacha20/e/x86-mmx`
  using `gcc -funroll-loops -march=k6-2`
- 1.37: `crypto_stream/chacha20/e/ref`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 2.23: `crypto_stream/chacha20/e/x86-xmm`
  using `gcc -m32 -march=k8 -O3 -fomit-frame-pointer`
- 2.55: `crypto_stream/chacha20/e/x86-xmm2`
  using `gcc -m32 -march=k6-3 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/x86-1`
  using `gcc -m32 -march=i386 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/x86-xmm6`
  using `gcc -m32 -march=pentium -O -fomit-frame-pointer`
- 1.02: `crypto_stream/chacha8/e/merged`
  using `gcc -funroll-loops -m32 -march=k6-3 -Os -fomit-frame-pointer`
- 1.17: `crypto_stream/chacha8/e/x86-xmm5`
  using `gcc -m32 -march=k8 -O3 -fomit-frame-pointer`
- 1.20: `crypto_stream/chacha8/e/x86-mmx`
  using `gcc -m32 -march=pentium -Os -fomit-frame-pointer`
- 1.65: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -march=k6-2 -Os -fomit-frame-pointer`
- 1.76: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 2.09: `crypto_stream/chacha8/e/x86-xmm`
  using `gcc -funroll-loops -march=pentiumpro -O3 -fomit-frame-pointer`

- 2.34: `crypto_stream/chacha8/e/x86-xmm2`
  using `gcc -m32 -march=k6 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -march=prescott -O -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -funroll-loops -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -O -fomit-frame-pointer`
- 1.03: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -m32 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -funroll-loops -march=pentium3 -Os -fomit-frame-pointer`
- 1.02: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -funroll-loops -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -funroll-loops -march=pentium-mmx -O -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.94: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.09: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -funroll-loops -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.30: `crypto_stream/rabbit/e/opt/2/5`
  using `gcc -march=pentium4`
- 1.49: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -march=prescott -O -fomit-frame-pointer`
- 1.49: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -m32 -march=i386 -O -fomit-frame-pointer`
- 1.66: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -funroll-loops -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`

- 1.66: crypto_stream/rabbit/e/opt/2/1
  using gcc -funroll-loops -march=pentium -O3 -fomit-frame-pointer
- 1.84: crypto_stream/rabbit/e/opt/2/4
  using gcc -march=k8
- 1.87: crypto_stream/rabbit/e/ref
  using gcc -march=pentium2 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/salsa20/e/x86-xmm5
  using gcc -march=k8 -O3 -fomit-frame-pointer
- 1.15: crypto_stream/salsa20/e/x86-2
  using gcc -funroll-loops -m32 -march=pentium4 -O2 -fomit-frame-pointer
- 1.16: crypto_stream/salsa20/e/x86-3
  using gcc -march=pentiumpro -Os -fomit-frame-pointer
- 1.16: crypto_stream/salsa20/e/x86-athlon
  using gcc -march=k6
- 1.16: crypto_stream/salsa20/e/x86-pm
  using gcc -march=pentium4
- 1.20: crypto_stream/salsa20/e/merged
  using gcc -march=i386 -O -fomit-frame-pointer
- 1.26: crypto_stream/salsa20/e/x86-1
  using gcc -funroll-loops -m32 -march=pentiumpro -Os -fomit-frame-pointer
- 1.29: crypto_stream/salsa20/e/x86-xmm4
  using gcc -m32 -march=pentium-m -O3 -fomit-frame-pointer
- 1.40: crypto_stream/salsa20/e/x86-mmx
  using gcc -m32 -march=prescott -Os -fomit-frame-pointer
- 1.46: crypto_stream/salsa20/e/ref
  using gcc -funroll-loops -march=pentium2 -O3 -fomit-frame-pointer
- 1.49: crypto_stream/salsa20/e/regs
  using gcc -funroll-loops -march=pentium2 -O2 -fomit-frame-pointer
- 1.63: crypto_stream/salsa20/ref
  using gcc -funroll-loops -m32 -Os -fomit-frame-pointer
- 1.91: crypto_stream/salsa20/e/x86-xmm
  using gcc -funroll-loops -m32 -march=pentium-m -O -fomit-frame-pointer
- 2.61: crypto_stream/salsa20/e/x86-xmm2
  using gcc -m32 -march=pentium3 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/salsa2012/e/x86-xmm5
  using gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer

- 1.14: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -march=pentium -Os -fomit-frame-pointer`
- 1.15: `crypto_stream/salsa2012/e/x86-2`
  using `gcc -m32 -march=k8 -Os -fomit-frame-pointer`
- 1.15: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -funroll-loops -m32 -Os -fomit-frame-pointer`
- 1.15: `crypto_stream/salsa2012/e/x86-athlon`
  using `gcc -m32 -march=pentium3 -O2 -fomit-frame-pointer`
- 1.17: `crypto_stream/salsa2012/e/merged`
  using `gcc -march=k6 -O3 -fomit-frame-pointer`
- 1.24: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -m32 -march=k8 -Os -fomit-frame-pointer`
- 1.31: `crypto_stream/salsa2012/e/x86-xmm4`
  using `gcc -funroll-loops -m32 -march=i486 -O3 -fomit-frame-pointer`
- 1.34: `crypto_stream/salsa2012/e/x86-mmx`
  using `gcc -m32 -march=pentiumpro -Os -fomit-frame-pointer`
- 1.55: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.63: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -march=pentium-m -O3 -fomit-frame-pointer`
- 1.83: `crypto_stream/salsa2012/ref`
  using `gcc -funroll-loops -m32 -Os -fomit-frame-pointer`
- 2.12: `crypto_stream/salsa2012/e/x86-xmm`
  using `gcc -m32 -march=pentium2 -O3 -fomit-frame-pointer`
- 2.49: `crypto_stream/salsa2012/e/x86-xmm2`
  using `gcc -m32 -march=k6-3 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/x86-xmm5`
  using `gcc -funroll-loops -m32 -march=pentium3 -O -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa208/e/x86-2`
  using `gcc -funroll-loops -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa208/e/x86-3`
  using `gcc -funroll-loops -march=k6 -Os -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa208/e/x86-athlon`
  using `gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa208/e/x86-pm`
  using `gcc -m32 -march=pentium2 -Os -fomit-frame-pointer`

- 1.18: crypto_stream/salsa208/e/merged
  using gcc -march=k6-3 -O2 -fomit-frame-pointer
- 1.21: crypto_stream/salsa208/e/x86-1
  using gcc -m32 -Os -fomit-frame-pointer
- 1.28: crypto_stream/salsa208/e/x86-mmx
  using gcc -m32 -march=pentium3 -Os -fomit-frame-pointer
- 1.33: crypto_stream/salsa208/e/x86-xmm4
  using gcc -march=k6-2 -O2 -fomit-frame-pointer
- 1.78: crypto_stream/salsa208/e/regs
  using gcc -funroll-loops -m32 -march=pentium2 -O2 -fomit-frame-pointer
- 1.89: crypto_stream/salsa208/e/ref
  using gcc -funroll-loops -march=pentium3 -O3 -fomit-frame-pointer
- 2.02: crypto_stream/salsa208/ref
  using gcc -funroll-loops -Os -fomit-frame-pointer
- 2.12: crypto_stream/salsa208/e/x86-xmm
  using gcc -march=pentium-mmx -O3 -fomit-frame-pointer
- 2.40: crypto_stream/salsa208/e/x86-xmm2
  using gcc -funroll-loops -m32 -march=k6-3 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -funroll-loops -m32 -march=pentium-m -O -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -march=athlon -O -fomit-frame-pointer
- 1.00: crypto_stream/tpy/e/tpy
  using gcc -funroll-loops -march=k6-2 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/tpy6/e/tpy6
  using gcc -funroll-loops -m32 -march=k6-2 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpypy/e/tpypy
  using gcc -m32 -march=k6-3 -O -fomit-frame-pointer
- 1.00: crypto_stream/trivium/e/submissions/trivium
  using gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer

5.47 x86, 2996MHz, Intel Xeon (f41), nmi0076

- 1.00: crypto_dh/claus/gmp
  using g++ -m32 -march=pentium-m -O2 -fomit-frame-pointer
- 1.00: crypto_dh/curve2251/mpfq
  using gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer

- 1.00: `crypto_dh/curve25519/mpfq`
  using `gcc -funroll-loops -m32 -march=pentium2 -O3 -fomit-frame-pointer`
- 1.00: `crypto_dh/hector/ref`
  using `gcc -funroll-loops -march=pentium-m -O3 -fomit-frame-pointer`
- 1.00: `crypto_dh/surf127eps/mpfq`
  using `gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_dh/surf2113/mpfq`
  using `gcc -funroll-loops -march=pentium-m -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/mceliece/ref`
  using `gcc -funroll-loops -m32 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -funroll-loops -march=pentiumpro -O -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -funroll-loops -m32 -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -funroll-loops -m32 -march=k6-2 -O -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/ref`
  using `gcc -funroll-loops -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -m32 -march=athlon -O -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/x86-1`
  using `gcc -m32 -march=prescott -O3 -fomit-frame-pointer`
- 1.45: `crypto_hashblocks/md5/little-1`
  using `gcc -m32 -march=prescott -O -fomit-frame-pointer`
- 1.75: `crypto_hashblocks/md5/ref`
  using `gcc -m32 -march=k6 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha256/ref`
  using `gcc -m32 -march=prescott`
- 1.00: `crypto_hashblocks/sha512/ref`
  using `gcc -funroll-loops -march=i386 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/bls/ref`
  using `g++ -march=k6 -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/hector/ref`
  using `gcc -funroll-loops -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/rainbow/ref`
  using `g++ -m32 -march=prescott -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/aes128estream/e/bernstein/x86-mmx-1`
  using `gcc -funroll-loops -march=pentium2 -O -fomit-frame-pointer`
- 1.09: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 1.11: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -march=prescott -O -fomit-frame-pointer`
- 1.19: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -march=pentium -O -fomit-frame-pointer`
- 1.30: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -m32 -march=k6 -O -fomit-frame-pointer`
- 1.41: `crypto_stream/aes128estream/e/gladman`
  using `gcc -m32 -march=pentium4 -O -fomit-frame-pointer`
- 1.69: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -m32 -march=pentium3 -O -fomit-frame-pointer`
- 1.72: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -march=k8 -O -fomit-frame-pointer`
- 1.90: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -m32 -march=pentium-mmx -O -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -funroll-loops -m32 -march=pentium-m -O -fomit-frame-pointer`
- 1.01: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 1.21: `crypto_stream/aes256estream/e/gladman`
  using `gcc -m32 -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/x86-xmm6`
  using `gcc -m32 -march=k6-2 -O2 -fomit-frame-pointer`
- 1.01: `crypto_stream/chacha12/e/x86-1`
  using `gcc -m32 -march=k6 -Os -fomit-frame-pointer`
- 1.12: `crypto_stream/chacha12/e/merged`
  using `gcc -funroll-loops -m32 -march=k8 -O2 -fomit-frame-pointer`
- 1.12: `crypto_stream/chacha12/e/x86-xmm5`
  using `gcc -m32 -march=k8 -O2 -fomit-frame-pointer`
- 1.24: `crypto_stream/chacha12/e/x86-mmx`
  using `gcc -march=prescott -O -fomit-frame-pointer`
- 1.35: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -march=pentiumpro -O3 -fomit-frame-pointer`

- 2.09: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -march=pentium3 -O -fomit-frame-pointer`
- 2.24: `crypto_stream/chacha12/e/x86-xmm`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 2.63: `crypto_stream/chacha12/e/x86-xmm2`
  using `gcc -m32 -march=k6-3 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/x86-xmm6`
  using `gcc -m32 -march=k6-2 -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/chacha20/e/x86-1`
  using `gcc -m32 -march=pentium4 -Os -fomit-frame-pointer`
- 1.09: `crypto_stream/chacha20/e/merged`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.18: `crypto_stream/chacha20/e/x86-xmm5`
  using `gcc -march=nocona -O -fomit-frame-pointer`
- 1.25: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -march=pentium-m -O3 -fomit-frame-pointer`
- 1.29: `crypto_stream/chacha20/e/x86-mmx`
  using `gcc -m32 -march=prescott -Os -fomit-frame-pointer`
- 1.98: `crypto_stream/chacha20/e/ref`
  using `gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer`
- 2.23: `crypto_stream/chacha20/e/x86-xmm`
  using `gcc -funroll-loops -m32 -march=pentium-m -O2 -fomit-frame-pointer`
- 2.57: `crypto_stream/chacha20/e/x86-xmm2`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/x86-1`
  using `gcc -march=pentium -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/x86-xmm6`
  using `gcc -m32 -march=pentium -O -fomit-frame-pointer`
- 1.13: `crypto_stream/chacha8/e/merged`
  using `gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.17: `crypto_stream/chacha8/e/x86-xmm5`
  using `gcc -funroll-loops -march=nocona -O2 -fomit-frame-pointer`
- 1.19: `crypto_stream/chacha8/e/x86-mmx`
  using `gcc -funroll-loops -m32 -march=k6-2 -Os -fomit-frame-pointer`
- 1.76: `crypto_stream/chacha8/e/regs`
  using `gcc -m32 -march=nocona -O3 -fomit-frame-pointer`

- 2.09: crypto_stream/chacha8/e/x86-xmm
  using gcc -funroll-loops -m32 -march=pentium4 -O3 -fomit-frame-pointer
- 2.21: crypto_stream/chacha8/e/ref
  using gcc -funroll-loops -march=pentium-m -O -fomit-frame-pointer
- 2.34: crypto_stream/chacha8/e/x86-xmm2
  using gcc -funroll-loops -m32 -march=k6 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/cryptmtv3/e/v3
  using gcc -march=pentium4 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/dragon/e/submissions/dragon
  using gcc -funroll-loops -march=prescott -O3 -fomit-frame-pointer
- 1.00: crypto_stream/hc128/e/hc-128/200701a
  using gcc -funroll-loops -m32 -march=pentium -O2 -fomit-frame-pointer
- 1.01: crypto_stream/hc128/e/hc-128/200701b
  using gcc -m32 -march=pentium -O3 -fomit-frame-pointer
- 1.02: crypto_stream/hc128/e/hc-128/200606
  using gcc -funroll-loops -march=pentium -O3 -fomit-frame-pointer
- 1.00: crypto_stream/hc256/e/hc-256/200701
  using gcc -march=i486 -O -fomit-frame-pointer
- 1.01: crypto_stream/hc256/e/hc-256/200511
  using gcc -march=pentium -O -fomit-frame-pointer
- 1.00: crypto_stream/lexv2/e/v2/ref
  using gcc -funroll-loops -m32 -march=k8 -O -fomit-frame-pointer
- 1.00: crypto_stream/nlsv2/e/v2/sync/2
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.78: crypto_stream/nlsv2/e/v2/sync/1
  using gcc -funroll-loops -march=athlon -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/1/4
  using gcc -funroll-loops -m32 -march=i486 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/2/3
  using gcc -funroll-loops -m32 -march=i486 -O3 -fomit-frame-pointer
- 1.04: crypto_stream/rabbit/e/opt/1/3
  using gcc -funroll-loops -m32 -march=pentium-mmx -O3 -fomit-frame-pointer
- 1.20: crypto_stream/rabbit/e/opt/2/5
  using gcc -funroll-loops -march=i386
- 1.41: crypto_stream/rabbit/e/opt/1/2
  using gcc -funroll-loops -m32 -march=athlon -O -fomit-frame-pointer

- 1.41: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -funroll-loops -m32 -march=k8 -O -fomit-frame-pointer`
- 1.57: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.57: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -march=pentium -O2 -fomit-frame-pointer`
- 1.70: `crypto_stream/rabbit/e/opt/2/4`
  using `gcc -m32 -march=i386`
- 1.82: `crypto_stream/rabbit/e/ref`
  using `gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/x86-xmm5`
  using `gcc -funroll-loops -m32 -march=k6-2 -O3 -fomit-frame-pointer`
- 1.16: `crypto_stream/salsa20/e/x86-2`
  using `gcc -funroll-loops -m32 -march=k6-2 -O3 -fomit-frame-pointer`
- 1.16: `crypto_stream/salsa20/e/x86-3`
  using `gcc -funroll-loops -m32 -march=i486 -O -fomit-frame-pointer`
- 1.16: `crypto_stream/salsa20/e/x86-athlon`
  using `gcc -funroll-loops -m32 -march=pentium -O -fomit-frame-pointer`
- 1.20: `crypto_stream/salsa20/e/x86-pm`
  using `cc`
- 1.26: `crypto_stream/salsa20/e/x86-1`
  using `gcc -march=pentium-mmx -Os -fomit-frame-pointer`
- 1.29: `crypto_stream/salsa20/e/x86-xmm4`
  using `gcc -march=i486 -O3 -fomit-frame-pointer`
- 1.34: `crypto_stream/salsa20/e/merged`
  using `gcc -funroll-loops -m32 -march=k8 -O -fomit-frame-pointer`
- 1.40: `crypto_stream/salsa20/e/x86-mmx`
  using `gcc -funroll-loops -march=pentium2 -Os -fomit-frame-pointer`
- 1.46: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -march=nocona -O -fomit-frame-pointer`
- 1.66: `crypto_stream/salsa20/ref`
  using `gcc -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.68: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -march=nocona -O -fomit-frame-pointer`
- 1.90: `crypto_stream/salsa20/e/x86-xmm`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`

- 2.61: `crypto_stream/salsa20/e/x86-xmm2`
  using `gcc -m32 -march=i486 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/x86-xmm5`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.14: `crypto_stream/salsa2012/e/x86-2`
  using `gcc -march=k6 -Os -fomit-frame-pointer`
- 1.15: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -m32 -march=pentium4 -O2 -fomit-frame-pointer`
- 1.15: `crypto_stream/salsa2012/e/x86-athlon`
  using `gcc -funroll-loops -march=i486 -O -fomit-frame-pointer`
- 1.16: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -funroll-loops -m32 -march=i386 -O -fomit-frame-pointer`
- 1.24: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -funroll-loops -march=athlon -O3 -fomit-frame-pointer`
- 1.31: `crypto_stream/salsa2012/e/x86-xmm4`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.34: `crypto_stream/salsa2012/e/x86-mmx`
  using `gcc -m32 -march=k6-3 -Os -fomit-frame-pointer`
- 1.35: `crypto_stream/salsa2012/e/merged`
  using `gcc -m32 -march=k6-2 -O -fomit-frame-pointer`
- 1.57: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium4 -O -fomit-frame-pointer`
- 1.81: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -m32 -march=pentium4 -O -fomit-frame-pointer`
- 1.92: `crypto_stream/salsa2012/ref`
  using `gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 2.12: `crypto_stream/salsa2012/e/x86-xmm`
  using `gcc -m32 -march=pentiumpro -O3 -fomit-frame-pointer`
- 2.49: `crypto_stream/salsa2012/e/x86-xmm2`
  using `gcc -funroll-loops -m32 -march=pentium2 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/x86-xmm5`
  using `gcc -funroll-loops -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa208/e/x86-2`
  using `gcc -m32 -march=pentiumpro -Os -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa208/e/x86-3`
  using `gcc -funroll-loops -m32 -march=nocona -Os -fomit-frame-pointer`

- 1.13: `crypto_stream/salsa208/e/x86-athlon`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.13: `crypto_stream/salsa208/e/x86-pm`
  using `gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer`
- 1.20: `crypto_stream/salsa208/e/x86-1`
  using `gcc -m32 -march=nocona -Os -fomit-frame-pointer`
- 1.28: `crypto_stream/salsa208/e/x86-mmx`
  using `gcc -m32 -march=k8 -Os -fomit-frame-pointer`
- 1.31: `crypto_stream/salsa208/e/x86-xmm4`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 1.32: `crypto_stream/salsa208/e/merged`
  using `gcc -march=pentium -O -fomit-frame-pointer`
- 1.84: `crypto_stream/salsa208/e/regs`
  using `gcc -funroll-loops -m32 -march=nocona -O3 -fomit-frame-pointer`
- 1.86: `crypto_stream/salsa208/e/ref`
  using `gcc -funroll-loops -march=nocona -O -fomit-frame-pointer`
- 2.25: `crypto_stream/salsa208/e/x86-xmm`
  using `gcc -march=k6-3 -O3 -fomit-frame-pointer`
- 2.30: `crypto_stream/salsa208/ref`
  using `gcc -march=pentium -O3 -fomit-frame-pointer`
- 2.39: `crypto_stream/salsa208/e/x86-xmm2`
  using `gcc -march=i386 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -funroll-loops -march=pentium2 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -funroll-loops -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -funroll-loops -march=k6 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -march=athlon -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -m32 -march=nocona -O -fomit-frame-pointer`
- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -march=pentium -Os -fomit-frame-pointer`

5.48 x86, 3000MHz, Intel Xeon (f4a), nmi0090

- 1.00: crypto_dh/claus/gmp
  using g++ -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_dh/curve25519/mpfq
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_dh/surf127eps/mpfq
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_encrypt/ntruees787ep1/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/md5/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/sha256/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/sha512/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/whirlpool/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/md5/x86-1
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.55: crypto_hashblocks/md5/little-1
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.85: crypto_hashblocks/md5/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha256/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha512/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/bls/ref
  using g++ -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes128estream/e/bernstein/x86-mmx-1
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.68: crypto_stream/aes128estream/e/hongjun/v0
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.69: crypto_stream/aes128estream/e/bernstein/little-2
  using gcc -m32 -O3 -fomit-frame-pointer

- 1.71: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.83: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.92: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.10: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.29: `crypto_stream/aes128estream/e/gladman`
  using `gcc -m32`
- 2.77: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.10: `crypto_stream/aes256estream/e/gladman`
  using `gcc -m32`
- 1.00: `crypto_stream/chacha12/e/x86-xmm6`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/chacha12/e/x86-1`
  using `gcc -m32`
- 1.24: `crypto_stream/chacha12/e/x86-mmx`
  using `gcc -m32`
- 1.24: `crypto_stream/chacha12/e/x86-xmm5`
  using `gcc -m32`
- 2.32: `crypto_stream/chacha12/e/x86-xmm`
  using `gcc -m32`
- 2.63: `crypto_stream/chacha12/e/x86-xmm2`
  using `gcc -m32`
- 3.02: `crypto_stream/chacha12/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.66: `crypto_stream/chacha12/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 6.43: `crypto_stream/chacha12/e/ref`
  using `gcc -m32`

- 1.00: `crypto_stream/chacha20/e/x86-1`
  using `gcc -m32`
- 1.03: `crypto_stream/chacha20/e/x86-xmm6`
  using `gcc -m32`
- 1.21: `crypto_stream/chacha20/e/x86-xmm5`
  using `gcc -m32`
- 1.26: `crypto_stream/chacha20/e/x86-mmx`
  using `gcc -m32`
- 2.18: `crypto_stream/chacha20/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.73: `crypto_stream/chacha20/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.13: `crypto_stream/chacha20/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.58: `crypto_stream/chacha20/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 4.97: `crypto_stream/chacha20/e/ref`
  using `gcc -m32`
- 1.00: `crypto_stream/chacha8/e/x86-xmm6`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/chacha8/e/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.20: `crypto_stream/chacha8/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.46: `crypto_stream/chacha8/e/x86-xmm5`
  using `gcc -m32`
- 2.12: `crypto_stream/chacha8/e/x86-xmm`
  using `gcc -m32`
- 2.43: `crypto_stream/chacha8/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.94: `crypto_stream/chacha8/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 3.78: `crypto_stream/chacha8/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 6.41: `crypto_stream/chacha8/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.06: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.12: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.69: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.02: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.10: `crypto_stream/rabbit/e/opt/2/5`
  using `gcc -m32`
- 1.29: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.30: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.39: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.40: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.65: `crypto_stream/rabbit/e/opt/2/4`
  using `gcc -m32`
- 2.12: `crypto_stream/rabbit/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa20/e/x86-xmm5`
  using `gcc -m32`
- 1.12: `crypto_stream/salsa20/e/x86-3`
  using `gcc -m32`
- 1.14: `crypto_stream/salsa20/e/x86-2`
  using `gcc -m32`
- 1.14: `crypto_stream/salsa20/e/x86-athlon`
  using `gcc -m32`
- 1.16: `crypto_stream/salsa20/e/x86-pm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.21: `crypto_stream/salsa20/e/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.28: `crypto_stream/salsa20/e/x86-xmm4`
  using `gcc -m32`
- 1.32: `crypto_stream/salsa20/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.57: `crypto_stream/salsa20/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.88: `crypto_stream/salsa20/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.10: `crypto_stream/salsa20/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.19: `crypto_stream/salsa20/e/x86-xmm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.34: `crypto_stream/salsa20/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.51: `crypto_stream/salsa20/e/x86-xmm2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/x86-xmm5`
  using `gcc -m32`
- 1.03: `crypto_stream/salsa2012/e/x86-2`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.03: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -m32`
- 1.04: `crypto_stream/salsa2012/e/x86-athlon`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.08: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.10: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.18: `crypto_stream/salsa2012/e/x86-mmx`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.25: `crypto_stream/salsa2012/e/x86-xmm4`
  using `gcc -m32`
- 1.61: `crypto_stream/salsa2012/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.91: `crypto_stream/salsa2012/e/x86-xmm`
  using `gcc -m32`
- 1.92: `crypto_stream/salsa2012/e/regs`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.23: `crypto_stream/salsa2012/e/x86-xmm2`
  using `gcc -m32`
- 2.30: `crypto_stream/salsa2012/e/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 2.60: `crypto_stream/salsa2012/ref`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/x86-xmm5`
  using `gcc -m32`
- 1.04: `crypto_stream/salsa208/e/x86-2`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.04: `crypto_stream/salsa208/e/x86-pm`
  using `gcc -m32`
- 1.05: `crypto_stream/salsa208/e/x86-3`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.05: `crypto_stream/salsa208/e/x86-athlon`
  using `gcc -m32`
- 1.11: `crypto_stream/salsa208/e/x86-1`
  using `gcc -m32`

- 1.15: crypto_stream/salsa208/e/x86-mmx
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.26: crypto_stream/salsa208/e/x86-xmm4
  using gcc -m32
- 1.57: crypto_stream/salsa208/e/merged
  using gcc -m32 -O3 -fomit-frame-pointer
- 2.18: crypto_stream/salsa208/e/x86-xmm
  using gcc -m32
- 2.21: crypto_stream/salsa208/e/x86-xmm2
  using gcc -m32
- 2.24: crypto_stream/salsa208/e/regs
  using gcc -m32 -O3 -fomit-frame-pointer
- 2.68: crypto_stream/salsa208/e/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 3.40: crypto_stream/salsa208/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpy/e/tpy
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpy6/e/tpy6
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpypy/e/tpypy
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/trivium/e/submissions/trivium
  using gcc -m32 -O3 -fomit-frame-pointer

5.49 x86, 3000MHz, Intel Xeon (f4a), nmi0102

- 1.00: crypto_dh/claus/gmp
  using g++ -march=pentium3 -O -fomit-frame-pointer
- 2.52: crypto_dh/claus/openssl
  using gcc -march=pentiumpro -Os -fomit-frame-pointer
- 1.00: crypto_dh/curve25519/mpfq
  using gcc -funroll-loops -m32 -march=pentiumpro -O2 -fomit-frame-pointer

- 1.00: `crypto_dh/surf127eps/mpfq`
  using `gcc -funroll-loops -m32 -march=pentium2 -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/mceliece/ref`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -funroll-loops -m32 -march=athlon -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -march=pentium4`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -funroll-loops -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -m32`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -funroll-loops -m32 -march=pentium2 -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `gcc -funroll-loops -m32 -march=athlon -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -funroll-loops -m32 -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -funroll-loops -march=k6-3 -O -fomit-frame-pointer`
- 1.12: `crypto_hash/md5/openssl`
  using `gcc -funroll-loops -m32 -march=i386 -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -march=athlon -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -funroll-loops -m32 -march=pentium -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/ref`
  using `gcc -funroll-loops -m32 -march=pentium-mmx -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/x86-1`
  using `gcc -funroll-loops -m32 -march=k6-2 -Os -fomit-frame-pointer`

- 1.55: crypto_hashblocks/md5/little-1
  using gcc -funroll-loops -m32 -march=athlon -Os -fomit-frame-pointer
- 2.01: crypto_hashblocks/md5/ref
  using gcc -funroll-loops -march=k6 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha256/ref
  using gcc -m32 -march=i486 -Os -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha512/ref
  using gcc -funroll-loops -m32 -march=i386 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/bls/ref
  using g++ -march=pentium4 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/donald1024/openssl
  using gcc -funroll-loops -m32 -march=pentium2 -Os -fomit-frame-pointer
- 1.00: crypto_sign/donald2048/openssl
  using gcc -funroll-loops -m32 -march=i486 -O -fomit-frame-pointer
- 1.00: crypto_sign/donald512/openssl
  using gcc -funroll-loops -march=athlon -Os -fomit-frame-pointer
- 1.00: crypto_sign/ronald1024/openssl
  using gcc -m32 -march=pentium4 -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald1536/openssl
  using gcc -O3 -fomit-frame-pointer
- 1.00: crypto_sign/ronald2048/openssl
  using gcc -m32 -march=athlon -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald3072/openssl
  using gcc -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ronald4096/openssl
  using gcc -march=pentium4 -O2 -fomit-frame-pointer
- 1.00: crypto_sign/ronald512/openssl
  using gcc -m32 -march=pentiumpro -O -fomit-frame-pointer
- 1.00: crypto_sign/ronald768/openssl
  using gcc -m32 -march=i486 -Os -fomit-frame-pointer
- 1.00: crypto_sign/sflashv2/ref
  using gcc -funroll-loops -march=pentium3 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/aes128estream/e/bernstein/x86-mmx-1
  using gcc -funroll-loops -march=k6-3 -O3 -fomit-frame-pointer
- 1.09: crypto_stream/aes128estream/e/hongjun/v1
  using gcc -funroll-loops -m32 -march=pentium4 -O -fomit-frame-pointer

- 1.22: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -march=pentium4 -O -fomit-frame-pointer`
- 1.44: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -march=k6-3 -Os -fomit-frame-pointer`
- 1.57: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -march=i486 -O2 -fomit-frame-pointer`
- 1.66: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -funroll-loops -m32 -march=k6 -Os -fomit-frame-pointer`
- 1.68: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -funroll-loops -march=pentium4 -O2 -fomit-frame-pointer`
- 1.70: `crypto_stream/aes128estream/e/gladman`
  using `gcc -funroll-loops -march=pentiumpro -O -fomit-frame-pointer`
- 1.76: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -m32 -march=pentium2 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -funroll-loops -march=pentiumpro -O -fomit-frame-pointer`
- 1.08: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -funroll-loops -march=pentiumpro -O -fomit-frame-pointer`
- 1.52: `crypto_stream/aes256estream/e/gladman`
  using `gcc -m32 -march=i386 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/x86-xmm6`
  using `gcc -O -fomit-frame-pointer`
- 1.01: `crypto_stream/chacha12/e/x86-1`
  using `gcc -march=k6-2 -O3 -fomit-frame-pointer`
- 1.09: `crypto_stream/chacha12/e/x86-xmm5`
  using `gcc -funroll-loops -march=pentium2 -O -fomit-frame-pointer`
- 1.24: `crypto_stream/chacha12/e/x86-mmx`
  using `gcc -O3 -fomit-frame-pointer`
- 1.88: `crypto_stream/chacha12/e/merged`
  using `gcc -funroll-loops -m32 -march=i386 -O -fomit-frame-pointer`
- 2.25: `crypto_stream/chacha12/e/x86-xmm`
  using `gcc -funroll-loops -m32 -march=athlon -O2 -fomit-frame-pointer`
- 2.27: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -m32 -march=k6-2 -O -fomit-frame-pointer`
- 2.38: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -march=k6-3 -O -fomit-frame-pointer`

- 2.63: crypto_stream/chacha12/e/x86-xmm2
  using gcc -m32 -march=k6-2 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/chacha20/e/x86-xmm6
  using gcc -march=pentium3 -O -fomit-frame-pointer
- 1.02: crypto_stream/chacha20/e/x86-1
  using gcc -m32 -march=pentium2 -O -fomit-frame-pointer
- 1.21: crypto_stream/chacha20/e/x86-xmm5
  using gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer
- 1.29: crypto_stream/chacha20/e/x86-mmx
  using gcc -funroll-loops -m32 -march=pentium2 -O -fomit-frame-pointer
- 1.94: crypto_stream/chacha20/e/merged
  using gcc -funroll-loops -march=pentium -O -fomit-frame-pointer
- 2.16: crypto_stream/chacha20/e/ref
  using gcc -funroll-loops -march=k6-3 -O -fomit-frame-pointer
- 2.23: crypto_stream/chacha20/e/x86-xmm
  using gcc -m32 -march=pentium3 -O2 -fomit-frame-pointer
- 2.28: crypto_stream/chacha20/e/regs
  using gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer
- 2.57: crypto_stream/chacha20/e/x86-xmm2
  using gcc -funroll-loops -march=pentium
- 1.00: crypto_stream/chacha8/e/x86-xmm6
  using gcc -m32 -march=k6-3 -O -fomit-frame-pointer
- 1.01: crypto_stream/chacha8/e/x86-1
  using gcc -m32 -march=pentiumpro -O2 -fomit-frame-pointer
- 1.17: crypto_stream/chacha8/e/x86-xmm5
  using gcc -funroll-loops -O -fomit-frame-pointer
- 1.20: crypto_stream/chacha8/e/x86-mmx
  using gcc -m32 -march=pentium3 -O2 -fomit-frame-pointer
- 1.84: crypto_stream/chacha8/e/merged
  using gcc -funroll-loops -march=pentium -O -fomit-frame-pointer
- 2.07: crypto_stream/chacha8/e/x86-xmm
  using gcc -funroll-loops -march=pentium3 -O -fomit-frame-pointer
- 2.35: crypto_stream/chacha8/e/x86-xmm2
  using gcc -march=i486 -O -fomit-frame-pointer
- 2.39: crypto_stream/chacha8/e/ref
  using gcc -funroll-loops -march=k6-2 -O -fomit-frame-pointer

- 2.55: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -funroll-loops -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -funroll-loops -march=pentium -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -funroll-loops -march=pentium-mmx -Os -fomit-frame-pointer`
- 1.08: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -m32 -march=i386 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -funroll-loops -march=pentium3 -O2 -fomit-frame-pointer`
- 1.02: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -funroll-loops -m32 -march=pentium-mmx -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -funroll-loops -m32 -march=pentium -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -m32 -march=k6 -O3 -fomit-frame-pointer`
- 1.73: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -m32 -march=k6-2 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.10: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.10: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.20: `crypto_stream/rabbit/e/opt/2/5`
  using `gcc -funroll-loops -march=pentiumpro`
- 1.35: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -m32 -march=pentium -O2 -fomit-frame-pointer`
- 1.35: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -m32 -march=pentium -O2 -fomit-frame-pointer`
- 1.48: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -m32 -march=pentium -O2 -fomit-frame-pointer`

- 1.49: crypto_stream/rabbit/e/opt/2/1
  using gcc -funroll-loops -m32 -march=pentium -O2 -fomit-frame-pointer
- 1.75: crypto_stream/rabbit/e/ref
  using gcc -funroll-loops -march=k6 -O3 -fomit-frame-pointer
- 1.81: crypto_stream/rabbit/e/opt/2/4
  using gcc -m32 -march=athlon
- 1.00: crypto_stream/salsa20/e/x86-xmm5
  using gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer
- 1.16: crypto_stream/salsa20/e/x86-2
  using gcc -funroll-loops -march=pentium-mmx -O2 -fomit-frame-pointer
- 1.16: crypto_stream/salsa20/e/x86-3
  using gcc -march=i486
- 1.16: crypto_stream/salsa20/e/x86-athlon
  using gcc -march=i486 -O3 -fomit-frame-pointer
- 1.20: crypto_stream/salsa20/e/x86-pm
  using gcc -funroll-loops -m32 -march=i386 -O3 -fomit-frame-pointer
- 1.26: crypto_stream/salsa20/e/x86-1
  using gcc -funroll-loops -march=pentium3 -Os -fomit-frame-pointer
- 1.29: crypto_stream/salsa20/e/x86-xmm4
  using gcc -funroll-loops -m32 -O -fomit-frame-pointer
- 1.36: crypto_stream/salsa20/e/x86-mmx
  using gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer
- 1.58: crypto_stream/salsa20/e/merged
  using gcc -m32 -march=k6-2 -Os -fomit-frame-pointer
- 1.73: crypto_stream/salsa20/e/regs
  using gcc -funroll-loops -march=pentiumpro -O3 -fomit-frame-pointer
- 1.79: crypto_stream/salsa20/e/ref
  using gcc -funroll-loops -march=pentium4 -O3 -fomit-frame-pointer
- 1.89: crypto_stream/salsa20/e/x86-xmm
  using gcc -m32 -march=athlon
- 2.06: crypto_stream/salsa20/ref
  using gcc -march=pentium-mmx -O3 -fomit-frame-pointer
- 2.59: crypto_stream/salsa20/e/x86-xmm2
  using gcc -funroll-loops -m32 -march=pentium-mmx -O3 -fomit-frame-pointer
- 1.00: crypto_stream/salsa2012/e/x86-xmm5
  using gcc -funroll-loops -m32 -O3 -fomit-frame-pointer

- 1.14: `crypto_stream/salsa2012/e/x86-2`
  using `gcc -m32 -march=i386 -O3 -fomit-frame-pointer`
- 1.14: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -funroll-loops -march=pentium4 -O3 -fomit-frame-pointer`
- 1.14: `crypto_stream/salsa2012/e/x86-athlon`
  using `gcc -m32 -march=k6-2 -O3 -fomit-frame-pointer`
- 1.15: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -funroll-loops -march=pentiumpro -O -fomit-frame-pointer`
- 1.23: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -m32 -march=pentium3 -O3 -fomit-frame-pointer`
- 1.29: `crypto_stream/salsa2012/e/x86-xmm4`
  using `gcc -m32 -march=pentiumpro -O2 -fomit-frame-pointer`
- 1.31: `crypto_stream/salsa2012/e/x86-mmx`
  using `gcc -m32 -march=pentium2 -O -fomit-frame-pointer`
- 1.56: `crypto_stream/salsa2012/e/merged`
  using `gcc -march=k6-3 -Os -fomit-frame-pointer`
- 1.85: `crypto_stream/salsa2012/e/regs`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.95: `crypto_stream/salsa2012/e/ref`
  using `gcc -funroll-loops -m32 -march=pentium2 -Os -fomit-frame-pointer`
- 2.11: `crypto_stream/salsa2012/e/x86-xmm`
  using `gcc -march=pentium-mmx -O2 -fomit-frame-pointer`
- 2.22: `crypto_stream/salsa2012/ref`
  using `gcc -funroll-loops -march=pentium -O3 -fomit-frame-pointer`
- 2.48: `crypto_stream/salsa2012/e/x86-xmm2`
  using `gcc -m32 -march=i486 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa208/e/x86-xmm5`
  using `gcc -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.12: `crypto_stream/salsa208/e/x86-2`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 1.12: `crypto_stream/salsa208/e/x86-3`
  using `gcc -march=pentium2 -O -fomit-frame-pointer`
- 1.12: `crypto_stream/salsa208/e/x86-athlon`
  using `gcc -m32 -march=i486 -O2 -fomit-frame-pointer`
- 1.12: `crypto_stream/salsa208/e/x86-pm`
  using `gcc -m32 -march=pentium2 -O3 -fomit-frame-pointer`

- 1.19: crypto_stream/salsa208/e/x86-1
  using gcc -march=athlon -O -fomit-frame-pointer
- 1.25: crypto_stream/salsa208/e/x86-mmx
  using gcc -march=pentiumpro -O -fomit-frame-pointer
- 1.30: crypto_stream/salsa208/e/x86-xmm4
  using gcc -m32 -march=k6-2 -O2 -fomit-frame-pointer
- 1.53: crypto_stream/salsa208/e/merged
  using gcc -m32 -march=k6 -Os -fomit-frame-pointer
- 1.96: crypto_stream/salsa208/e/regs
  using gcc -funroll-loops -march=i486 -O2 -fomit-frame-pointer
- 2.06: crypto_stream/salsa208/e/x86-xmm
  using gcc -march=pentium4 -O -fomit-frame-pointer
- 2.07: crypto_stream/salsa208/e/ref
  using gcc -funroll-loops -m32 -march=pentiumpro -Os -fomit-frame-pointer
- 2.36: crypto_stream/salsa208/e/x86-xmm2
  using gcc -march=i386 -O -fomit-frame-pointer
- 2.49: crypto_stream/salsa208/ref
  using gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer
- 1.00: crypto_stream/snow20/e/benchmarks/snow-2.0
  using gcc -funroll-loops -march=k6 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/sosemanuk/e/submissions/sosemanuk
  using gcc -funroll-loops -march=pentium2 -O -fomit-frame-pointer
- 1.00: crypto_stream/tpy/e/tpy
  using gcc -funroll-loops -m32 -march=pentium4 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpy6/e/tpy6
  using gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer
- 1.00: crypto_stream/tpypy/e/tpypy
  using gcc -funroll-loops -m32 -march=pentium4 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/trivium/e/submissions/trivium
  using gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer

5.50 x86, 3391MHz, Intel Pentium D (f64), nmi0099

- 1.00: crypto_dh/claus/gmp
  using g++ -m32 -march=pentium4 -O2 -fomit-frame-pointer
- 1.84: crypto_dh/claus/openssl
  using gcc -march=i386 -Os -fomit-frame-pointer

- 1.00: `crypto_dh/curve2251/mpfq`
  using `gcc -funroll-loops -march=pentium-m -O -fomit-frame-pointer`
- 1.00: `crypto_dh/curve25519/mpfq`
  using `gcc -funroll-loops -march=pentium-m -Os -fomit-frame-pointer`
- 1.00: `crypto_dh/hector/ref`
  using `gcc -march=pentium-m -O3 -fomit-frame-pointer`
- 1.00: `crypto_dh/surf127eps/mpfq`
  using `gcc -funroll-loops -march=athlon -O3 -fomit-frame-pointer`
- 1.00: `crypto_dh/surf2113/mpfq`
  using `gcc -funroll-loops -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/mceliece/ref`
  using `gcc -funroll-loops -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -funroll-loops -m32 -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -m32 -march=pentium4 -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -funroll-loops -march=k6-2 -O2 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -m32 -march=pentium`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -m32 -march=athlon -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `gcc -m32 -march=pentium -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -funroll-loops -m32 -march=pentium2`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -funroll-loops -march=pentium4 -O -fomit-frame-pointer`
- 1.12: `crypto_hash/md5/openssl`
  using `gcc -march=pentium-m -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -m32 -march=pentium-mmx -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -m32 -march=k6-2 -O -fomit-frame-pointer`

- 1.00: crypto_hash/sha224/openssl
  using gcc -funroll-loops -march=pentiumpro -Os -fomit-frame-pointer
- 1.00: crypto_hash/sha256/ref
  using gcc -m32 -O3 -fomit-frame-pointer
- 1.59: crypto_hash/sha256/openssl
  using gcc -march=i386 -O3 -fomit-frame-pointer
- 1.00: crypto_hash/sha384/openssl
  using gcc -m32 -march=pentium-mmx -O -fomit-frame-pointer
- 1.00: crypto_hash/sha512/openssl
  using gcc -march=i386 -Os -fomit-frame-pointer
- 3.89: crypto_hash/sha512/ref
  using gcc -funroll-loops -m32 -march=k6-2 -O2 -fomit-frame-pointer
- 1.00: crypto_hash/whirlpool/ref
  using gcc -funroll-loops -m32 -march=athlon -O2 -fomit-frame-pointer
- 1.00: crypto_hashblocks/md5/x86-1
  using gcc -m32 -march=k8 -O3 -fomit-frame-pointer
- 1.10: crypto_hashblocks/md5/little-1
  using gcc -funroll-loops -Os -fomit-frame-pointer
- 1.51: crypto_hashblocks/md5/ref
  using gcc -funroll-loops -march=k6-3 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha256/ref
  using gcc -m32 -march=pentium4 -O2 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha512/ref
  using gcc -funroll-loops -march=nocona -O -fomit-frame-pointer
- 1.00: crypto_sign/bls/ref
  using g++ -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/donald1024/openssl
  using gcc -funroll-loops -m32 -march=i486 -O -fomit-frame-pointer
- 1.00: crypto_sign/donald2048/openssl
  using gcc -funroll-loops -march=pentiumpro -O3 -fomit-frame-pointer
- 1.00: crypto_sign/donald512/openssl
  using gcc -march=pentium-m -Os -fomit-frame-pointer
- 1.00: crypto_sign/hector/ref
  using gcc -funroll-loops -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_sign/rainbow/ref
  using g++ -m32 -march=k8

- 1.00: `crypto_sign/ronald1024/openssl`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1536/openssl`
  using `gcc -funroll-loops -m32 -march=athlon -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald2048/openssl`
  using `gcc -m32 -march=pentium -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald3072/openssl`
  using `gcc -funroll-loops -m32 -march=pentium-m -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald4096/openssl`
  using `gcc -m32 -march=k6 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald512/openssl`
  using `gcc -march=pentiumpro -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald768/openssl`
  using `gcc -funroll-loops -O -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -funroll-loops -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/bernstein/x86-mmx-1`
  using `gcc -m32 -march=k6 -Os -fomit-frame-pointer`
- 1.08: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -funroll-loops -march=nocona -O -fomit-frame-pointer`
- 1.09: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer`
- 1.20: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -m32 -march=pentium-mmx -O -fomit-frame-pointer`
- 1.38: `crypto_stream/aes128estream/e/gladman`
  using `gcc -funroll-loops -march=athlon -O -fomit-frame-pointer`
- 1.40: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -march=k6-3 -O3 -fomit-frame-pointer`
- 1.75: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -funroll-loops -m32 -march=athlon -O -fomit-frame-pointer`
- 1.78: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -m32 -march=prescott -O -fomit-frame-pointer`
- 1.96: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -m32 -march=pentium4 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -funroll-loops -march=prescott -O -fomit-frame-pointer`

- 1.02: crypto_stream/aes256estream/e/hongjun/v1
  using gcc -O -fomit-frame-pointer
- 1.18: crypto_stream/aes256estream/e/gladman
  using gcc -m32 -march=pentium3 -O -fomit-frame-pointer
- 1.00: crypto_stream/chacha12/e/x86-xmm6
  using gcc -march=pentium2 -Os -fomit-frame-pointer
- 1.01: crypto_stream/chacha12/e/x86-1
  using gcc -m32 -march=pentium2 -Os -fomit-frame-pointer
- 1.06: crypto_stream/chacha12/e/merged
  using gcc -m32 -march=k6-2 -O2 -fomit-frame-pointer
- 1.09: crypto_stream/chacha12/e/x86-xmm5
  using gcc -m32 -march=nocona -O2 -fomit-frame-pointer
- 1.24: crypto_stream/chacha12/e/x86-mmx
  using gcc -m32 -march=prescott -O3 -fomit-frame-pointer
- 1.42: crypto_stream/chacha12/e/regs
  using gcc -funroll-loops -m32 -O3 -fomit-frame-pointer
- 1.53: crypto_stream/chacha12/e/ref
  using gcc -funroll-loops -march=prescott -O3 -fomit-frame-pointer
- 2.25: crypto_stream/chacha12/e/x86-xmm
  using gcc -march=pentiumpro -Os -fomit-frame-pointer
- 2.65: crypto_stream/chacha12/e/x86-xmm2
  using gcc -funroll-loops -m32 -march=pentiumpro -O2 -fomit-frame-pointer
- 1.00: crypto_stream/chacha20/e/x86-xmm6
  using gcc -march=pentium-mmx -Os -fomit-frame-pointer
- 1.02: crypto_stream/chacha20/e/x86-1
  using gcc -march=pentium2 -O2 -fomit-frame-pointer
- 1.07: crypto_stream/chacha20/e/merged
  using gcc -funroll-loops -m32 -march=k6 -O3 -fomit-frame-pointer
- 1.11: crypto_stream/chacha20/e/x86-xmm5
  using gcc -funroll-loops -m32 -march=pentium-m -O2 -fomit-frame-pointer
- 1.29: crypto_stream/chacha20/e/x86-mmx
  using gcc -funroll-loops -march=i486 -O2 -fomit-frame-pointer
- 1.30: crypto_stream/chacha20/e/regs
  using gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer
- 1.37: crypto_stream/chacha20/e/ref
  using gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer

- 2.23: `crypto_stream/chacha20/e/x86-xmm`
  using `gcc -m32 -march=k8 -Os -fomit-frame-pointer`
- 2.57: `crypto_stream/chacha20/e/x86-xmm2`
  using `gcc -funroll-loops -m32 -march=i386 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/x86-xmm6`
  using `gcc -m32 -march=i386 -Os -fomit-frame-pointer`
- 1.01: `crypto_stream/chacha8/e/x86-1`
  using `gcc -m32 -march=k8 -O -fomit-frame-pointer`
- 1.07: `crypto_stream/chacha8/e/x86-xmm5`
  using `gcc -m32 -march=pentium-m -O3 -fomit-frame-pointer`
- 1.09: `crypto_stream/chacha8/e/merged`
  using `gcc -m32 -march=k6 -O2 -fomit-frame-pointer`
- 1.20: `crypto_stream/chacha8/e/x86-mmx`
  using `gcc -march=k8 -Os -fomit-frame-pointer`
- 1.60: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -m32 -march=k6 -Os -fomit-frame-pointer`
- 1.77: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer`
- 2.08: `crypto_stream/chacha8/e/x86-xmm`
  using `gcc -march=k6-3 -Os -fomit-frame-pointer`
- 2.35: `crypto_stream/chacha8/e/x86-xmm2`
  using `gcc -m32 -march=k8 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -march=pentium-m -O -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -funroll-loops -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -funroll-loops -march=athlon -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200701a`
  using `gcc -funroll-loops -march=pentium -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -funroll-loops -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200511`
  using `gcc -funroll-loops -m32 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc256/e/hc-256/200701`
  using `gcc -funroll-loops -m32 -march=k8 -O2 -fomit-frame-pointer`

- 1.00: `crypto_stream/lexv2/e/v2/ref`
  using `gcc -funroll-loops -march=prescott -O -fomit-frame-pointer`
- 1.00: `crypto_stream/nlsv2/e/v2/sync/2`
  using `gcc -funroll-loops -m32 -march=pentium3 -Os -fomit-frame-pointer`
- 2.12: `crypto_stream/nlsv2/e/v2/sync/1`
  using `gcc -funroll-loops -march=athlon -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/1/4`
  using `gcc -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/rabbit/e/opt/2/3`
  using `gcc -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.09: `crypto_stream/rabbit/e/opt/1/3`
  using `gcc -funroll-loops -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.30: `crypto_stream/rabbit/e/opt/2/5`
  using `gcc -march=pentium2`
- 1.44: `crypto_stream/rabbit/e/opt/1/2`
  using `gcc -m32 -march=k6-3 -O -fomit-frame-pointer`
- 1.44: `crypto_stream/rabbit/e/opt/2/2`
  using `gcc -m32 -march=i486 -O -fomit-frame-pointer`
- 1.59: `crypto_stream/rabbit/e/opt/1/1`
  using `gcc -march=athlon -O3 -fomit-frame-pointer`
- 1.59: `crypto_stream/rabbit/e/opt/2/1`
  using `gcc -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.70: `crypto_stream/rabbit/e/ref`
  using `gcc -funroll-loops -m32 -march=k6 -O3 -fomit-frame-pointer`
- 1.85: `crypto_stream/rabbit/e/opt/2/4`
  using `gcc -funroll-loops -m32 -march=pentium2`
- 1.00: `crypto_stream/salsa20/e/x86-xmm5`
  using `gcc -funroll-loops -m32 -march=i486 -O -fomit-frame-pointer`
- 1.17: `crypto_stream/salsa20/e/x86-2`
  using `gcc -funroll-loops -m32 -march=k8 -O2 -fomit-frame-pointer`
- 1.17: `crypto_stream/salsa20/e/x86-3`
  using `gcc -m32 -march=i386 -O2 -fomit-frame-pointer`
- 1.17: `crypto_stream/salsa20/e/x86-pm`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O -fomit-frame-pointer`
- 1.18: `crypto_stream/salsa20/e/x86-athlon`
  using `gcc -march=pentiumpro -O -fomit-frame-pointer`

- 1.27: `crypto_stream/salsa20/e/merged`
  using `gcc -m32 -march=pentium-m -Os -fomit-frame-pointer`
- 1.27: `crypto_stream/salsa20/e/x86-1`
  using `gcc -m32 -march=pentium-mmx -O2 -fomit-frame-pointer`
- 1.29: `crypto_stream/salsa20/e/x86-xmm4`
  using `gcc -march=pentium3 -O3 -fomit-frame-pointer`
- 1.41: `crypto_stream/salsa20/e/x86-mmx`
  using `gcc -march=pentium4 -O -fomit-frame-pointer`
- 1.48: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer`
- 1.54: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -march=prescott -O2 -fomit-frame-pointer`
- 1.65: `crypto_stream/salsa20/ref`
  using `gcc -funroll-loops -m32 -Os -fomit-frame-pointer`
- 1.93: `crypto_stream/salsa20/e/x86-xmm`
  using `gcc -m32 -march=prescott -O -fomit-frame-pointer`
- 2.63: `crypto_stream/salsa20/e/x86-xmm2`
  using `gcc -m32 -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/x86-xmm5`
  using `gcc -m32 -march=prescott -O3 -fomit-frame-pointer`
- 1.14: `crypto_stream/salsa2012/e/x86-2`
  using `gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 1.14: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -funroll-loops -march=k6-2 -O2 -fomit-frame-pointer`
- 1.14: `crypto_stream/salsa2012/e/x86-athlon`
  using `gcc -m32 -march=pentium -O2 -fomit-frame-pointer`
- 1.14: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -march=k6-2 -O -fomit-frame-pointer`
- 1.20: `crypto_stream/salsa2012/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`
- 1.23: `crypto_stream/salsa2012/e/x86-1`
  using `gcc -m32 -march=pentium3 -O -fomit-frame-pointer`
- 1.30: `crypto_stream/salsa2012/e/x86-xmm4`
  using `gcc -m32 -march=pentium3 -O -fomit-frame-pointer`
- 1.33: `crypto_stream/salsa2012/e/x86-mmx`
  using `gcc -m32 -march=k6-2 -Os -fomit-frame-pointer`

- 1.56: crypto_stream/salsa2012/e/regs
  using gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer
- 1.62: crypto_stream/salsa2012/e/ref
  using gcc -funroll-loops -O3 -fomit-frame-pointer
- 1.80: crypto_stream/salsa2012/ref
  using gcc -funroll-loops -m32 -Os -fomit-frame-pointer
- 2.09: crypto_stream/salsa2012/e/x86-xmm
  using gcc -m32 -march=pentiumpro -O -fomit-frame-pointer
- 2.47: crypto_stream/salsa2012/e/x86-xmm2
  using gcc -m32 -march=prescott -Os -fomit-frame-pointer
- 1.00: crypto_stream/salsa208/e/x86-xmm5
  using gcc -funroll-loops -m32 -march=k6-2 -Os -fomit-frame-pointer
- 1.14: crypto_stream/salsa208/e/x86-2
  using gcc -march=k8 -O -fomit-frame-pointer
- 1.14: crypto_stream/salsa208/e/x86-3
  using gcc -funroll-loops -m32 -march=pentium4 -O2 -fomit-frame-pointer
- 1.14: crypto_stream/salsa208/e/x86-athlon
  using gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer
- 1.14: crypto_stream/salsa208/e/x86-pm
  using gcc -funroll-loops -m32 -march=k8 -O -fomit-frame-pointer
- 1.21: crypto_stream/salsa208/e/merged
  using gcc -O2 -fomit-frame-pointer
- 1.21: crypto_stream/salsa208/e/x86-1
  using gcc -m32 -march=prescott -O3 -fomit-frame-pointer
- 1.29: crypto_stream/salsa208/e/x86-mmx
  using gcc -m32 -march=k8 -O2 -fomit-frame-pointer
- 1.31: crypto_stream/salsa208/e/x86-xmm4
  using gcc -m32 -march=athlon -O2 -fomit-frame-pointer
- 1.88: crypto_stream/salsa208/e/regs
  using gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer
- 2.02: crypto_stream/salsa208/ref
  using gcc -funroll-loops -m32 -Os -fomit-frame-pointer
- 2.03: crypto_stream/salsa208/e/ref
  using gcc -funroll-loops -march=k6-2 -O -fomit-frame-pointer
- 2.12: crypto_stream/salsa208/e/x86-xmm
  using gcc -m32 -march=k6 -O3 -fomit-frame-pointer

- 2.40: `crypto_stream/salsa208/e/x86-xmm2`
  using `gcc -m32 -march=pentiumpro -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -funroll-loops -march=pentiumpro -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -funroll-loops -m32 -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -funroll-loops -march=k6-2 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -funroll-loops -m32 -march=pentium-m -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -m32 -march=i386 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -m32 -march=nocona -O -fomit-frame-pointer`

5.51 x86, 3392MHz, Intel Pentium D (f64), `nmi0104`

- 1.00: `crypto_dh/claus/openssl`
  using `gcc -m32 -march=i386 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/mceliece/ref`
  using `gcc -funroll-loops -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -funroll-loops -m32 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -funroll-loops -m32 -march=k6-3 -Os -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -funroll-loops -m32 -march=pentium`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -m32 -march=pentium-m`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -m32 -march=pentium -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `gcc -m32 -march=k6-3`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -m32 -march=i386 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -m32 -march=k8 -O -fomit-frame-pointer`

- 1.00: crypto_hash/md5/ref
  using gcc -funroll-loops -m32 -march=pentium -O -fomit-frame-pointer
- 1.11: crypto_hash/md5/openssl
  using gcc -m32 -march=pentium2 -O2 -fomit-frame-pointer
- 1.00: crypto_hash/ripemd160/openssl
  using gcc -m32 -march=pentiumpro -O -fomit-frame-pointer
- 1.00: crypto_hash/sha1/openssl
  using gcc -funroll-loops -m32 -march=i486 -Os -fomit-frame-pointer
- 1.00: crypto_hash/sha224/openssl
  using gcc -m32 -march=i386
- 1.00: crypto_hash/sha256/ref
  using gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer
- 1.56: crypto_hash/sha256/openssl
  using gcc -m32 -march=pentium2 -O -fomit-frame-pointer
- 1.00: crypto_hash/sha384/openssl
  using gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer
- 1.00: crypto_hash/sha512/openssl
  using gcc -funroll-loops -m32 -march=i486
- 3.90: crypto_hash/sha512/ref
  using gcc -m32 -march=pentium-mmx -O -fomit-frame-pointer
- 1.00: crypto_hash/whirlpool/ref
  using gcc -funroll-loops -m32 -march=k8 -O2 -fomit-frame-pointer
- 1.00: crypto_hashblocks/md5/x86-1
  using gcc -m32 -march=k8 -Os -fomit-frame-pointer
- 1.10: crypto_hashblocks/md5/little-1
  using gcc -funroll-loops -m32 -Os -fomit-frame-pointer
- 1.56: crypto_hashblocks/md5/ref
  using gcc -funroll-loops -m32 -march=pentium-m -Os -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha256/ref
  using gcc -m32 -march=pentium4 -O3 -fomit-frame-pointer
- 1.00: crypto_hashblocks/sha512/ref
  using gcc -funroll-loops -m32 -march=athlon -O -fomit-frame-pointer
- 1.00: crypto_sign/bls/ref
  using g++ -m32 -march=k8 -O3 -fomit-frame-pointer
- 1.00: crypto_sign/donald1024/openssl
  using gcc -m32 -march=pentium -O2 -fomit-frame-pointer

- 1.00: `crypto_sign/donald2048/openssl`
  using `gcc -m32 -march=k6 -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/donald512/openssl`
  using `gcc -m32 -march=pentium2 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/rainbow/ref`
  using `g++ -m32 -march=prescott`
- 1.00: `crypto_sign/ronald1024/openssl`
  using `gcc -m32 -march=pentium3 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1536/openssl`
  using `gcc -funroll-loops -m32 -march=prescott -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald2048/openssl`
  using `gcc -m32 -march=pentiumpro -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald3072/openssl`
  using `gcc -m32 -march=athlon -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald4096/openssl`
  using `gcc -m32 -march=pentium4 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald512/openssl`
  using `gcc -m32 -march=pentium-mmx -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald768/openssl`
  using `gcc -funroll-loops -m32 -march=k6 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -funroll-loops -m32 -march=nocona -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/bernstein/x86-mmx-1`
  using `gcc -m32 -march=k6-3 -O2 -fomit-frame-pointer`
- 1.05: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer`
- 1.07: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -m32 -O -fomit-frame-pointer`
- 1.18: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -m32 -march=pentium-mmx -O -fomit-frame-pointer`
- 1.34: `crypto_stream/aes128estream/e/gladman`
  using `gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer`
- 1.37: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -m32 -march=k6 -O3 -fomit-frame-pointer`
- 1.71: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -funroll-loops -m32 -march=pentium2 -O -fomit-frame-pointer`

- 1.76: `crypto_stream/aes128estream/e/bernstein/little-2`
  using `gcc -m32 -march=nocona -O -fomit-frame-pointer`
- 1.92: `crypto_stream/aes128estream/e/bernstein/big-1`
  using `gcc -m32 -march=pentium4 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/aes256estream/e/hongjun/v0`
  using `gcc -funroll-loops -m32 -O -fomit-frame-pointer`
- 1.03: `crypto_stream/aes256estream/e/hongjun/v1`
  using `gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer`
- 1.18: `crypto_stream/aes256estream/e/gladman`
  using `gcc -m32 -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha12/e/x86-xmm6`
  using `gcc -funroll-loops -m32 -march=pentium4 -O -fomit-frame-pointer`
- 1.01: `crypto_stream/chacha12/e/x86-1`
  using `gcc -funroll-loops -m32 -march=pentium3 -O -fomit-frame-pointer`
- 1.06: `crypto_stream/chacha12/e/merged`
  using `gcc -m32 -march=k6 -O2 -fomit-frame-pointer`
- 1.09: `crypto_stream/chacha12/e/x86-xmm5`
  using `gcc -m32 -march=k8 -O2 -fomit-frame-pointer`
- 1.24: `crypto_stream/chacha12/e/x86-mmx`
  using `gcc -m32 -march=k8 -Os -fomit-frame-pointer`
- 1.41: `crypto_stream/chacha12/e/regs`
  using `gcc -funroll-loops -m32 -O3 -fomit-frame-pointer`
- 1.52: `crypto_stream/chacha12/e/ref`
  using `gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer`
- 2.25: `crypto_stream/chacha12/e/x86-xmm`
  using `gcc -m32 -march=athlon -O2 -fomit-frame-pointer`
- 2.64: `crypto_stream/chacha12/e/x86-xmm2`
  using `gcc -m32 -march=k6-2 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha20/e/x86-xmm6`
  using `gcc -m32 -march=prescott -Os -fomit-frame-pointer`
- 1.03: `crypto_stream/chacha20/e/x86-1`
  using `gcc -m32 -march=k8 -O3 -fomit-frame-pointer`
- 1.07: `crypto_stream/chacha20/e/merged`
  using `gcc -m32 -march=pentium -Os -fomit-frame-pointer`
- 1.18: `crypto_stream/chacha20/e/x86-xmm5`
  using `gcc -m32 -march=pentium-m -O -fomit-frame-pointer`

- 1.29: `crypto_stream/chacha20/e/x86-mmx`
  using `gcc -m32 -march=k6 -O2 -fomit-frame-pointer`
- 1.30: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer`
- 1.37: `crypto_stream/chacha20/e/ref`
  using `gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer`
- 2.23: `crypto_stream/chacha20/e/x86-xmm`
  using `gcc -m32 -march=pentium3 -O3 -fomit-frame-pointer`
- 2.57: `crypto_stream/chacha20/e/x86-xmm2`
  using `gcc -m32 -march=k8 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/x86-xmm6`
  using `gcc -m32 -march=k8 -Os -fomit-frame-pointer`
- 1.01: `crypto_stream/chacha8/e/x86-1`
  using `gcc -m32 -march=i386 -O -fomit-frame-pointer`
- 1.07: `crypto_stream/chacha8/e/x86-xmm5`
  using `gcc -m32 -march=k8 -O2 -fomit-frame-pointer`
- 1.09: `crypto_stream/chacha8/e/merged`
  using `gcc -m32 -march=k6-2 -O2 -fomit-frame-pointer`
- 1.20: `crypto_stream/chacha8/e/x86-mmx`
  using `gcc -m32 -march=pentium2 -Os -fomit-frame-pointer`
- 1.68: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -m32 -march=k6-3 -Os -fomit-frame-pointer`
- 1.84: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer`
- 2.10: `crypto_stream/chacha8/e/x86-xmm`
  using `gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer`
- 2.35: `crypto_stream/chacha8/e/x86-xmm2`
  using `gcc -m32 -march=athlon -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -m32 -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200701b`
  using `gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -funroll-loops -m32 -march=athlon -O2 -fomit-frame-pointer`

- 1.01: crypto_stream/hc128/e/hc-128/200701a
  using gcc -funroll-loops -m32 -march=pentium -Os -fomit-frame-pointer
- 1.00: crypto_stream/hc256/e/hc-256/200511
  using gcc -funroll-loops -m32 -march=k8 -O2 -fomit-frame-pointer
- 1.01: crypto_stream/hc256/e/hc-256/200701
  using gcc -funroll-loops -m32 -march=pentium2 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/lexv2/e/v2/ref
  using gcc -funroll-loops -m32 -march=pentium-mmx -O -fomit-frame-pointer
- 1.00: crypto_stream/nlsv2/e/v2/sync/2
  using gcc -funroll-loops -m32 -march=pentiumpro -Os -fomit-frame-pointer
- 2.06: crypto_stream/nlsv2/e/v2/sync/1
  using gcc -funroll-loops -m32 -march=k6-2 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/1/4
  using gcc -m32 -march=k6-3 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/2/3
  using gcc -m32 -march=k6-3 -O3 -fomit-frame-pointer
- 1.09: crypto_stream/rabbit/e/opt/1/3
  using gcc -funroll-loops -m32 -march=pentium-mmx -O3 -fomit-frame-pointer
- 1.31: crypto_stream/rabbit/e/opt/2/5
  using gcc -m32 -march=k6-3
- 1.44: crypto_stream/rabbit/e/opt/1/2
  using gcc -m32 -march=k6-3 -O -fomit-frame-pointer
- 1.44: crypto_stream/rabbit/e/opt/2/2
  using gcc -m32 -march=k6-2 -O -fomit-frame-pointer
- 1.58: crypto_stream/rabbit/e/opt/2/1
  using gcc -m32 -march=k6-3 -O2 -fomit-frame-pointer
- 1.59: crypto_stream/rabbit/e/opt/1/1
  using gcc -m32 -march=k6-2 -O2 -fomit-frame-pointer
- 1.70: crypto_stream/rabbit/e/ref
  using gcc -funroll-loops -m32 -march=k6-3 -O3 -fomit-frame-pointer
- 1.86: crypto_stream/rabbit/e/opt/2/4
  using gcc -m32 -march=pentium-m
- 1.00: crypto_stream/salsa20/e/x86-xmm5
  using gcc -m32 -march=pentiumpro -O3 -fomit-frame-pointer
- 1.11: crypto_stream/salsa20/e/x86-2
  using gcc -funroll-loops -m32 -march=prescott -Os -fomit-frame-pointer

- 1.11: `crypto_stream/salsa20/e/x86-3`
  using `gcc -m32 -march=k8 -Os -fomit-frame-pointer`
- 1.11: `crypto_stream/salsa20/e/x86-athlon`
  using `gcc -m32 -march=nocona -O2 -fomit-frame-pointer`
- 1.11: `crypto_stream/salsa20/e/x86-pm`
  using `gcc -m32 -march=i486 -O3 -fomit-frame-pointer`
- 1.19: `crypto_stream/salsa20/e/merged`
  using `gcc -m32 -march=pentium3 -Os -fomit-frame-pointer`
- 1.20: `crypto_stream/salsa20/e/x86-1`
  using `gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer`
- 1.22: `crypto_stream/salsa20/e/x86-xmm4`
  using `gcc -m32 -march=i386 -O -fomit-frame-pointer`
- 1.33: `crypto_stream/salsa20/e/x86-mmx`
  using `gcc -m32 -march=k8 -O2 -fomit-frame-pointer`
- 1.40: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -m32 -O3 -fomit-frame-pointer`
- 1.46: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -m32 -O2 -fomit-frame-pointer`
- 1.54: `crypto_stream/salsa20/ref`
  using `gcc -funroll-loops -m32 -Os -fomit-frame-pointer`
- 1.81: `crypto_stream/salsa20/e/x86-xmm`
  using `gcc -m32 -march=k6-3 -O2 -fomit-frame-pointer`
- 2.47: `crypto_stream/salsa20/e/x86-xmm2`
  using `gcc -m32 -march=pentiumpro -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/x86-xmm5`
  using `gcc -m32 -march=pentium4 -Os -fomit-frame-pointer`
- 1.08: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -funroll-loops -m32 -march=k6-3 -O2 -fomit-frame-pointer`
- 1.09: `crypto_stream/salsa2012/e/x86-athlon`
  using `gcc -m32 -march=athlon`
- 1.09: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -funroll-loops -m32 -march=k6 -Os -fomit-frame-pointer`
- 1.10: `crypto_stream/salsa2012/e/x86-2`
  using `gcc -m32 -march=pentium2 -Os -fomit-frame-pointer`
- 1.14: `crypto_stream/salsa2012/e/merged`
  using `gcc -m32 -O3 -fomit-frame-pointer`

- 1.17: crypto_stream/salsa2012/e/x86-1
  using gcc -m32 -march=k6 -O3 -fomit-frame-pointer
- 1.23: crypto_stream/salsa2012/e/x86-xmm4
  using gcc -m32 -march=pentium4 -O3 -fomit-frame-pointer
- 1.27: crypto_stream/salsa2012/e/x86-mmx
  using gcc -funroll-loops -m32 -march=prescott -O2 -fomit-frame-pointer
- 1.49: crypto_stream/salsa2012/e/regs
  using gcc -funroll-loops -m32 -march=pentium2 -O3 -fomit-frame-pointer
- 1.55: crypto_stream/salsa2012/e/ref
  using gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer
- 1.72: crypto_stream/salsa2012/ref
  using gcc -funroll-loops -m32 -Os -fomit-frame-pointer
- 2.00: crypto_stream/salsa2012/e/x86-xmm
  using gcc -m32 -march=k8 -O3 -fomit-frame-pointer
- 2.36: crypto_stream/salsa2012/e/x86-xmm2
  using gcc -funroll-loops -m32 -march=k6 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/salsa208/e/x86-xmm5
  using gcc -funroll-loops -m32 -march=k6-2 -Os -fomit-frame-pointer
- 1.14: crypto_stream/salsa208/e/x86-2
  using gcc -m32 -march=pentium-mmx
- 1.14: crypto_stream/salsa208/e/x86-3
  using gcc -m32 -march=k6
- 1.14: crypto_stream/salsa208/e/x86-athlon
  using gcc -funroll-loops -m32 -march=nocona -Os -fomit-frame-pointer
- 1.14: crypto_stream/salsa208/e/x86-pm
  using gcc -funroll-loops -m32 -march=nocona -O2 -fomit-frame-pointer
- 1.21: crypto_stream/salsa208/e/merged
  using gcc -m32 -march=i486 -O2 -fomit-frame-pointer
- 1.21: crypto_stream/salsa208/e/x86-1
  using gcc -m32 -march=k8 -Os -fomit-frame-pointer
- 1.28: crypto_stream/salsa208/e/x86-mmx
  using gcc -m32 -march=athlon -O3 -fomit-frame-pointer
- 1.32: crypto_stream/salsa208/e/x86-xmm4
  using gcc -funroll-loops -m32 -march=pentium3 -O3 -fomit-frame-pointer
- 1.91: crypto_stream/salsa208/e/regs
  using gcc -funroll-loops -m32 -march=pentium2 -O3 -fomit-frame-pointer

- 2.01: `crypto_stream/salsa208/ref`
  using `gcc -funroll-loops -m32 -Os -fomit-frame-pointer`
- 2.08: `crypto_stream/salsa208/e/ref`
  using `gcc -funroll-loops -m32 -march=pentium2 -O3 -fomit-frame-pointer`
- 2.11: `crypto_stream/salsa208/e/x86-xmm`
  using `gcc -m32 -march=k6 -O3 -fomit-frame-pointer`
- 2.40: `crypto_stream/salsa208/e/x86-xmm2`
  using `gcc -m32 -march=k6-3 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -funroll-loops -m32 -march=pentium-m -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -m32 -march=athlon -O -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -funroll-loops -m32 -march=k6 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -funroll-loops -m32 -march=pentium3 -Os -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -m32 -march=pentium4 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer`

5.52 x86, 3392MHz, Intel Pentium D (f64), `nmi0241`

- 1.00: `crypto_dh/claus/gmp`
  using `g++ -m32 -march=prescott -O3 -fomit-frame-pointer`
- 1.13: `crypto_dh/claus/openssl`
  using `gcc -funroll-loops -m32 -march=pentium-mmx -Os -fomit-frame-pointer`
- 1.00: `crypto_dh/curve25519/mpfq`
  using `gcc -funroll-loops -m32 -march=pentium3 -O2 -fomit-frame-pointer`
- 1.00: `crypto_dh/surf127eps/mpfq`
  using `gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/mceliece/ref`
  using `gcc -funroll-loops -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ntruees787ep1/ref`
  using `gcc -funroll-loops -m32 -march=i386 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald1024/openssl`
  using `gcc -m32 -march=pentium3`

- 1.00: `crypto_encrypt/ronald1536/openssl`
  using `gcc -m32 -march=pentium-mmx`
- 1.00: `crypto_encrypt/ronald2048/openssl`
  using `gcc -m32 -march=k6-2 -O -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald3072/openssl`
  using `gcc -m32 -march=i486 -O3 -fomit-frame-pointer`
- 1.00: `crypto_encrypt/ronald4096/openssl`
  using `gcc -funroll-loops -m32 -march=i486 -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/md2/openssl`
  using `gcc -m32 -march=i386 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/md4/openssl`
  using `gcc -m32 -march=k6 -O -fomit-frame-pointer`
- 1.00: `crypto_hash/md5/ref`
  using `gcc -funroll-loops -m32 -march=k8 -O -fomit-frame-pointer`
- 1.12: `crypto_hash/md5/openssl`
  using `gcc -m32 -march=k6-3 -Os -fomit-frame-pointer`
- 1.00: `crypto_hash/ripemd160/openssl`
  using `gcc -m32 -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha1/openssl`
  using `gcc -m32 -march=pentium4 -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha256/ref`
  using `gcc -funroll-loops -m32 -march=athlon -O2 -fomit-frame-pointer`
- 1.00: `crypto_hash/sha512/ref`
  using `gcc -funroll-loops -m32 -march=k6-3 -O3 -fomit-frame-pointer`
- 1.00: `crypto_hash/whirlpool/ref`
  using `gcc -funroll-loops -m32 -march=pentium4 -O -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/md5/x86-1`
  using `gcc -m32 -march=k8 -Os -fomit-frame-pointer`
- 1.52: `crypto_hashblocks/md5/little-1`
  using `gcc -m32 -march=athlon -Os -fomit-frame-pointer`
- 1.92: `crypto_hashblocks/md5/ref`
  using `gcc -m32 -march=nocona -O2 -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha256/ref`
  using `gcc -m32 -march=pentium-m -O -fomit-frame-pointer`
- 1.00: `crypto_hashblocks/sha512/ref`
  using `gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer`

- 1.00: `crypto_sign/bls/ref`
  using `g++ -m32 -march=k8 -O3 -fomit-frame-pointer`
- 1.00: `crypto_sign/donald1024/openssl`
  using `gcc -m32`
- 1.00: `crypto_sign/donald2048/openssl`
  using `gcc -funroll-loops -m32 -march=k6`
- 1.00: `crypto_sign/donald512/openssl`
  using `gcc -funroll-loops -m32 -march=pentium4 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1024/openssl`
  using `gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald1536/openssl`
  using `gcc -funroll-loops -m32 -march=pentium -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald2048/openssl`
  using `gcc -funroll-loops -m32 -march=k8 -O2 -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald3072/openssl`
  using `gcc -funroll-loops -m32 -march=nocona -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald4096/openssl`
  using `gcc -m32 -march=pentium -O -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald512/openssl`
  using `gcc -funroll-loops -m32 -march=pentium-m -Os -fomit-frame-pointer`
- 1.00: `crypto_sign/ronald768/openssl`
  using `gcc -funroll-loops -m32 -march=pentium3 -O -fomit-frame-pointer`
- 1.00: `crypto_sign/sflashv2/ref`
  using `gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/aes128estream/e/bernstein/x86-mmx-1`
  using `gcc -m32 -march=k6-2 -O2 -fomit-frame-pointer`
- 1.07: `crypto_stream/aes128estream/e/hongjun/v1`
  using `gcc -funroll-loops -m32 -O -fomit-frame-pointer`
- 1.22: `crypto_stream/aes128estream/e/hongjun/v0`
  using `gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer`
- 1.29: `crypto_stream/aes128estream/e/bernstein/little-4`
  using `gcc -m32 -O2 -fomit-frame-pointer`
- 1.50: `crypto_stream/aes128estream/e/bernstein/little-3`
  using `gcc -funroll-loops -m32 -march=k6-2 -O3 -fomit-frame-pointer`
- 1.60: `crypto_stream/aes128estream/e/bernstein/little-1`
  using `gcc -funroll-loops -m32 -march=k8 -Os -fomit-frame-pointer`

- 1.62: crypto_stream/aes128estream/e/gladman
  using gcc -funroll-loops -m32 -march=i386 -O -fomit-frame-pointer
- 1.66: crypto_stream/aes128estream/e/bernstein/little-2
  using gcc -funroll-loops -m32 -march=i386 -O2 -fomit-frame-pointer
- 1.74: crypto_stream/aes128estream/e/bernstein/big-1
  using gcc -funroll-loops -m32 -march=k8 -Os -fomit-frame-pointer
- 1.00: crypto_stream/aes256estream/e/hongjun/v1
  using gcc -funroll-loops -m32 -O -fomit-frame-pointer
- 1.06: crypto_stream/aes256estream/e/hongjun/v0
  using gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer
- 1.38: crypto_stream/aes256estream/e/gladman
  using gcc -funroll-loops -m32 -march=i386 -O -fomit-frame-pointer
- 1.00: crypto_stream/chacha12/e/x86-xmm6
  using gcc -m32 -march=pentiumpro -O2 -fomit-frame-pointer
- 1.01: crypto_stream/chacha12/e/x86-1
  using gcc -m32 -march=k8 -O3 -fomit-frame-pointer
- 1.09: crypto_stream/chacha12/e/x86-xmm5
  using gcc -m32 -march=k8 -O2 -fomit-frame-pointer
- 1.11: crypto_stream/chacha12/e/merged
  using gcc -funroll-loops -m32 -march=i386 -O3 -fomit-frame-pointer
- 1.24: crypto_stream/chacha12/e/x86-mmx
  using gcc -funroll-loops -m32 -march=nocona -O3 -fomit-frame-pointer
- 1.68: crypto_stream/chacha12/e/ref
  using gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer
- 1.77: crypto_stream/chacha12/e/regs
  using gcc -funroll-loops -m32 -march=pentium-mmx -O3 -fomit-frame-pointer
- 2.26: crypto_stream/chacha12/e/x86-xmm
  using gcc -m32 -march=k8 -O2 -fomit-frame-pointer
- 2.63: crypto_stream/chacha12/e/x86-xmm2
  using gcc -m32 -march=k6-2
- 1.00: crypto_stream/chacha20/e/x86-xmm6
  using gcc -m32 -march=pentium2 -O2 -fomit-frame-pointer
- 1.02: crypto_stream/chacha20/e/x86-1
  using gcc -m32 -march=k8 -Os -fomit-frame-pointer
- 1.09: crypto_stream/chacha20/e/merged
  using gcc -funroll-loops -m32 -march=i386 -O3 -fomit-frame-pointer

- 1.14: `crypto_stream/chacha20/e/x86-xmm5`
  using `gcc -funroll-loops -m32 -march=i386`
- 1.28: `crypto_stream/chacha20/e/x86-mmx`
  using `gcc -m32 -march=nocona -O -fomit-frame-pointer`
- 1.49: `crypto_stream/chacha20/e/ref`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.56: `crypto_stream/chacha20/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium-mmx -O3 -fomit-frame-pointer`
- 2.22: `crypto_stream/chacha20/e/x86-xmm`
  using `gcc -funroll-loops -m32 -march=pentium4`
- 2.57: `crypto_stream/chacha20/e/x86-xmm2`
  using `gcc -m32 -march=prescott -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/chacha8/e/x86-xmm6`
  using `gcc -m32 -march=prescott -O3 -fomit-frame-pointer`
- 1.01: `crypto_stream/chacha8/e/x86-1`
  using `gcc -funroll-loops -m32 -march=k6-2`
- 1.08: `crypto_stream/chacha8/e/x86-xmm5`
  using `gcc -m32 -march=pentium-m`
- 1.13: `crypto_stream/chacha8/e/merged`
  using `gcc -funroll-loops -m32 -march=i486 -O3 -fomit-frame-pointer`
- 1.20: `crypto_stream/chacha8/e/x86-mmx`
  using `gcc -m32 -march=k6-3 -O2 -fomit-frame-pointer`
- 1.84: `crypto_stream/chacha8/e/ref`
  using `gcc -funroll-loops -m32 -march=prescott -O3 -fomit-frame-pointer`
- 1.98: `crypto_stream/chacha8/e/regs`
  using `gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer`
- 2.07: `crypto_stream/chacha8/e/x86-xmm`
  using `gcc -funroll-loops -m32 -march=pentium-m -O3 -fomit-frame-pointer`
- 2.35: `crypto_stream/chacha8/e/x86-xmm2`
  using `gcc -m32 -march=k6-2 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/cryptmtv3/e/v3`
  using `gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/dragon/e/submissions/dragon`
  using `gcc -funroll-loops -m32 -march=pentium4 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/hc128/e/hc-128/200606`
  using `gcc -funroll-loops -m32 -march=pentium2 -Os -fomit-frame-pointer`

- 1.04: crypto_stream/hc128/e/hc-128/200701a
  using gcc -m32 -march=pentium3 -Os -fomit-frame-pointer
- 1.07: crypto_stream/hc128/e/hc-128/200701b
  using gcc -m32 -march=athlon -O -fomit-frame-pointer
- 1.00: crypto_stream/hc256/e/hc-256/200701
  using gcc -m32 -march=i386 -O -fomit-frame-pointer
- 1.01: crypto_stream/hc256/e/hc-256/200511
  using gcc -m32 -march=k6-2 -O -fomit-frame-pointer
- 1.00: crypto_stream/lexv2/e/v2/ref
  using gcc -funroll-loops -m32 -march=k6-2 -O2 -fomit-frame-pointer
- 1.00: crypto_stream/nlsv2/e/v2/sync/2
  using gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer
- 1.81: crypto_stream/nlsv2/e/v2/sync/1
  using gcc -funroll-loops -m32 -march=k6-3 -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/1/4
  using gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer
- 1.00: crypto_stream/rabbit/e/opt/2/3
  using gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer
- 1.02: crypto_stream/rabbit/e/opt/1/3
  using gcc -funroll-loops -m32 -march=pentium-mmx -O3 -fomit-frame-pointer
- 1.15: crypto_stream/rabbit/e/opt/2/4
  using gcc -m32 -march=pentium-m -O3 -fomit-frame-pointer
- 1.28: crypto_stream/rabbit/e/opt/2/5
  using gcc -m32 -march=nocona
- 1.38: crypto_stream/rabbit/e/opt/1/2
  using gcc -m32 -march=pentium-mmx -O3 -fomit-frame-pointer
- 1.39: crypto_stream/rabbit/e/opt/2/2
  using gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer
- 1.62: crypto_stream/rabbit/e/opt/1/1
  using gcc -funroll-loops -m32 -march=pentium2 -O3 -fomit-frame-pointer
- 1.62: crypto_stream/rabbit/e/opt/2/1
  using gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer
- 1.90: crypto_stream/rabbit/e/ref
  using gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer
- 1.00: crypto_stream/salsa20/e/x86-xmm5
  using gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer

- 1.16: `crypto_stream/salsa20/e/x86-2`
  using `gcc -m32 -march=pentium -O2 -fomit-frame-pointer`
- 1.16: `crypto_stream/salsa20/e/x86-3`
  using `gcc -funroll-loops -m32 -march=pentium4`
- 1.16: `crypto_stream/salsa20/e/x86-athlon`
  using `gcc -m32 -march=i386 -O3 -fomit-frame-pointer`
- 1.20: `crypto_stream/salsa20/e/x86-pm`
  using `gcc -m32 -march=pentium-mmx -O2 -fomit-frame-pointer`
- 1.23: `crypto_stream/salsa20/e/merged`
  using `gcc -m32 -march=i486 -O3 -fomit-frame-pointer`
- 1.26: `crypto_stream/salsa20/e/x86-1`
  using `gcc -m32 -march=nocona -O3 -fomit-frame-pointer`
- 1.29: `crypto_stream/salsa20/e/x86-xmm4`
  using `gcc -m32 -march=pentium-m -O -fomit-frame-pointer`
- 1.39: `crypto_stream/salsa20/e/x86-mmx`
  using `gcc -m32 -march=k8 -O -fomit-frame-pointer`
- 1.60: `crypto_stream/salsa20/e/regs`
  using `gcc -funroll-loops -m32 -march=i386 -O3 -fomit-frame-pointer`
- 1.83: `crypto_stream/salsa20/e/ref`
  using `gcc -funroll-loops -m32 -march=pentium4 -Os -fomit-frame-pointer`
- 1.91: `crypto_stream/salsa20/e/x86-xmm`
  using `gcc -m32 -march=k8 -O3 -fomit-frame-pointer`
- 1.91: `crypto_stream/salsa20/ref`
  using `gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer`
- 2.60: `crypto_stream/salsa20/e/x86-xmm2`
  using `gcc -m32 -march=pentium -O -fomit-frame-pointer`
- 1.00: `crypto_stream/salsa2012/e/x86-xmm5`
  using `gcc -funroll-loops -m32 -march=i486 -O3 -fomit-frame-pointer`
- 1.10: `crypto_stream/salsa2012/e/x86-2`
  using `gcc -funroll-loops -m32 -march=nocona -O2 -fomit-frame-pointer`
- 1.10: `crypto_stream/salsa2012/e/x86-3`
  using `gcc -m32 -march=prescott -O2 -fomit-frame-pointer`
- 1.10: `crypto_stream/salsa2012/e/x86-athlon`
  using `gcc -funroll-loops -m32 -march=nocona -O -fomit-frame-pointer`
- 1.10: `crypto_stream/salsa2012/e/x86-pm`
  using `gcc -m32 -march=pentium3 -O2 -fomit-frame-pointer`

- 1.19: crypto_stream/salsa2012/e/merged
  using gcc -m32 -march=i386 -O3 -fomit-frame-pointer
- 1.19: crypto_stream/salsa2012/e/x86-1
  using gcc -m32 -march=pentium-m -O3 -fomit-frame-pointer
- 1.25: crypto_stream/salsa2012/e/x86-xmm4
  using gcc -funroll-loops -m32 -march=pentium
- 1.28: crypto_stream/salsa2012/e/x86-mmx
  using gcc -m32 -Os -fomit-frame-pointer
- 1.66: crypto_stream/salsa2012/e/regs
  using gcc -funroll-loops -m32 -march=pentiumpro -O3 -fomit-frame-pointer
- 1.87: crypto_stream/salsa2012/e/ref
  using gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer
- 2.03: crypto_stream/salsa2012/e/x86-xmm
  using gcc -funroll-loops -m32
- 2.04: crypto_stream/salsa2012/ref
  using gcc -funroll-loops -m32 -march=pentium -O3 -fomit-frame-pointer
- 2.40: crypto_stream/salsa2012/e/x86-xmm2
  using gcc -m32 -march=i386 -O -fomit-frame-pointer
- 1.00: crypto_stream/salsa208/e/x86-xmm5
  using gcc -m32 -O2 -fomit-frame-pointer
- 1.13: crypto_stream/salsa208/e/x86-2
  using gcc -funroll-loops -m32 -march=nocona -O3 -fomit-frame-pointer
- 1.13: crypto_stream/salsa208/e/x86-3
  using gcc -m32 -march=pentium-m -O2 -fomit-frame-pointer
- 1.13: crypto_stream/salsa208/e/x86-athlon
  using gcc -funroll-loops -m32 -march=k8 -O3 -fomit-frame-pointer
- 1.13: crypto_stream/salsa208/e/x86-pm
  using gcc -m32 -march=k8 -Os -fomit-frame-pointer
- 1.21: crypto_stream/salsa208/e/x86-1
  using gcc -m32 -march=athlon -Os -fomit-frame-pointer
- 1.28: crypto_stream/salsa208/e/merged
  using gcc -funroll-loops -m32 -march=i486 -O3 -fomit-frame-pointer
- 1.28: crypto_stream/salsa208/e/x86-mmx
  using gcc -m32 -march=k8 -O2 -fomit-frame-pointer
- 1.32: crypto_stream/salsa208/e/x86-xmm4
  using gcc -m32 -march=nocona -O2 -fomit-frame-pointer

- 1.86: `crypto_stream/salsa208/e/regs`
  using `gcc -funroll-loops -m32 -march=i486 -O3 -fomit-frame-pointer`
- 2.11: `crypto_stream/salsa208/e/ref`
  using `gcc -funroll-loops -m32 -march=prescott -O -fomit-frame-pointer`
- 2.11: `crypto_stream/salsa208/e/x86-xmm`
  using `gcc -funroll-loops -m32 -march=pentium-mmx`
- 2.39: `crypto_stream/salsa208/e/x86-xmm2`
  using `gcc -m32 -march=k6 -O2 -fomit-frame-pointer`
- 2.45: `crypto_stream/salsa208/ref`
  using `gcc -m32 -march=pentium -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/snow20/e/benchmarks/snow-2.0`
  using `gcc -funroll-loops -m32 -march=pentium4 -O2 -fomit-frame-pointer`
- 1.00: `crypto_stream/sosemanuk/e/submissions/sosemanuk`
  using `gcc -funroll-loops -m32 -march=k8 -O -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy/e/tpy`
  using `gcc -funroll-loops -m32 -march=i386 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpy6/e/tpy6`
  using `gcc -funroll-loops -m32 -march=athlon -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/tpypy/e/tpypy`
  using `gcc -funroll-loops -m32 -march=i386 -O3 -fomit-frame-pointer`
- 1.00: `crypto_stream/trivium/e/submissions/trivium`
  using `gcc -funroll-loops -m32 -march=pentium4 -O -fomit-frame-pointer`

Chapter 6

Measurements of hash functions

6.1 Introduction

This chapter presents a series of graphs, one for each computer. The horizontal axis on each graph is message length, from 0 bytes to 2000 bytes. The vertical axis on each graph is time, from 0 cycles to 20000 cycles. The bottom-left-to-top-right diagonal is 10 cycles/byte.

Each graph is a superimposition of several curves, one curve for each hash function. The stair-step shape of a typical curve reflects the fact that these hash functions handle messages in blocks, typically 64-byte blocks.

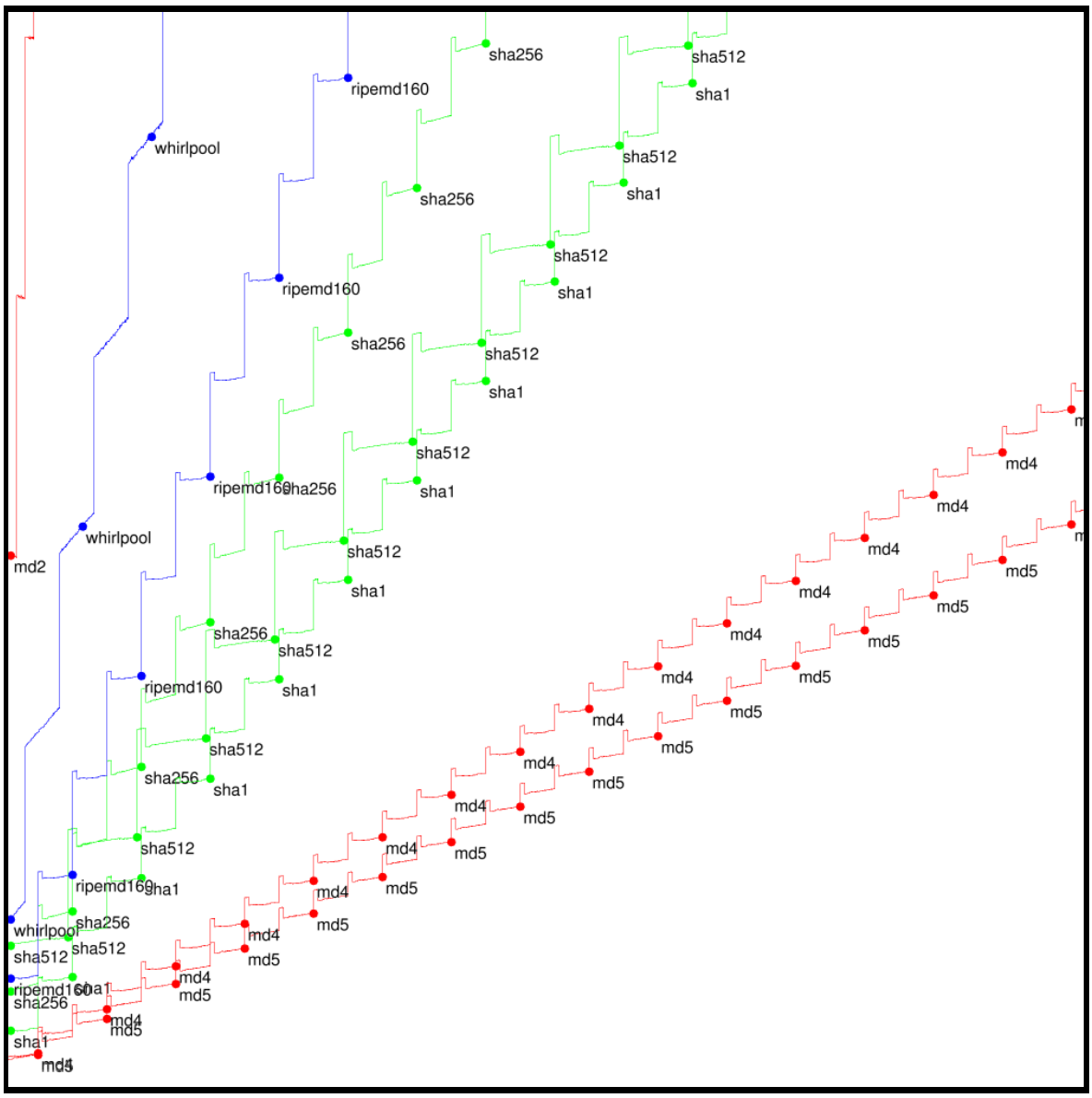
This chapter also presents a series of tables, six tables for each computer. The first table shows the speed, in cycles/byte, of hashing 8-byte messages. Each row of the table lists

- the first quartile of many speed measurements,
- the median of many speed measurements,
- the third quartile of many speed measurements, and
- the name of the hash function.

The second table shows the speed of hashing 64-byte messages. The third table shows the speed of hashing 576-byte messages. The fourth table shows the speed of hashing 1536-byte messages. The fifth table shows the speed of hashing 4096-byte messages. The sixth table shows the speed of hashing long messages; this is computed as 1/2048 of the difference in cycle counts between hashing 4096-byte messages and hashing 2048-byte messages.

SHA-224 and SHA-384 are omitted from this chapter. They have essentially the same performance as, respectively, SHA-256 and SHA-512.

6.2 amd64, 1403MHz, AMD Opteron 240 (f58), `nmisles8amd64`


sha256
sha512
ripemd160
sha1
whirlpool
sha512
sha256
sha1
sha512
ripemd160
sha1
sha256
sha512
sha1
sha512
ripemd160
sha256
sha1
whirlpool
md2
sha512
sha1
sha256
sha512
ripemd160
sha1
sha512
sha256
sha1
sha512
ripemd160
sha1
whirlpool
sha256
sha512
sha256
ripemd160
sha1
sha1
md4
md4
md4
md5
md4
md5
md4
md5

Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
65.00	65.25	65.25	`md5`
72.00	72.00	74.25	`md4`
128.50	130.88	130.88	`sha1`
223.12	223.38	225.88	`sha256`
252.38	252.38	256.62	`ripemd160`
324.00	330.50	330.62	`sha512`
394.00	395.38	397.38	`whirlpool`
1232.38	1236.12	1237.25	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
13.16	13.16	13.53	`md5`
15.44	15.44	15.72	`md4`
30.81	30.81	30.81	`sha1`
42.67	42.81	42.83	`sha512`
48.72	48.75	49.77	`sha256`
60.61	60.61	61.30	`ripemd160`
104.28	104.38	104.48	`whirlpool`
454.58	454.92	455.25	`md2`

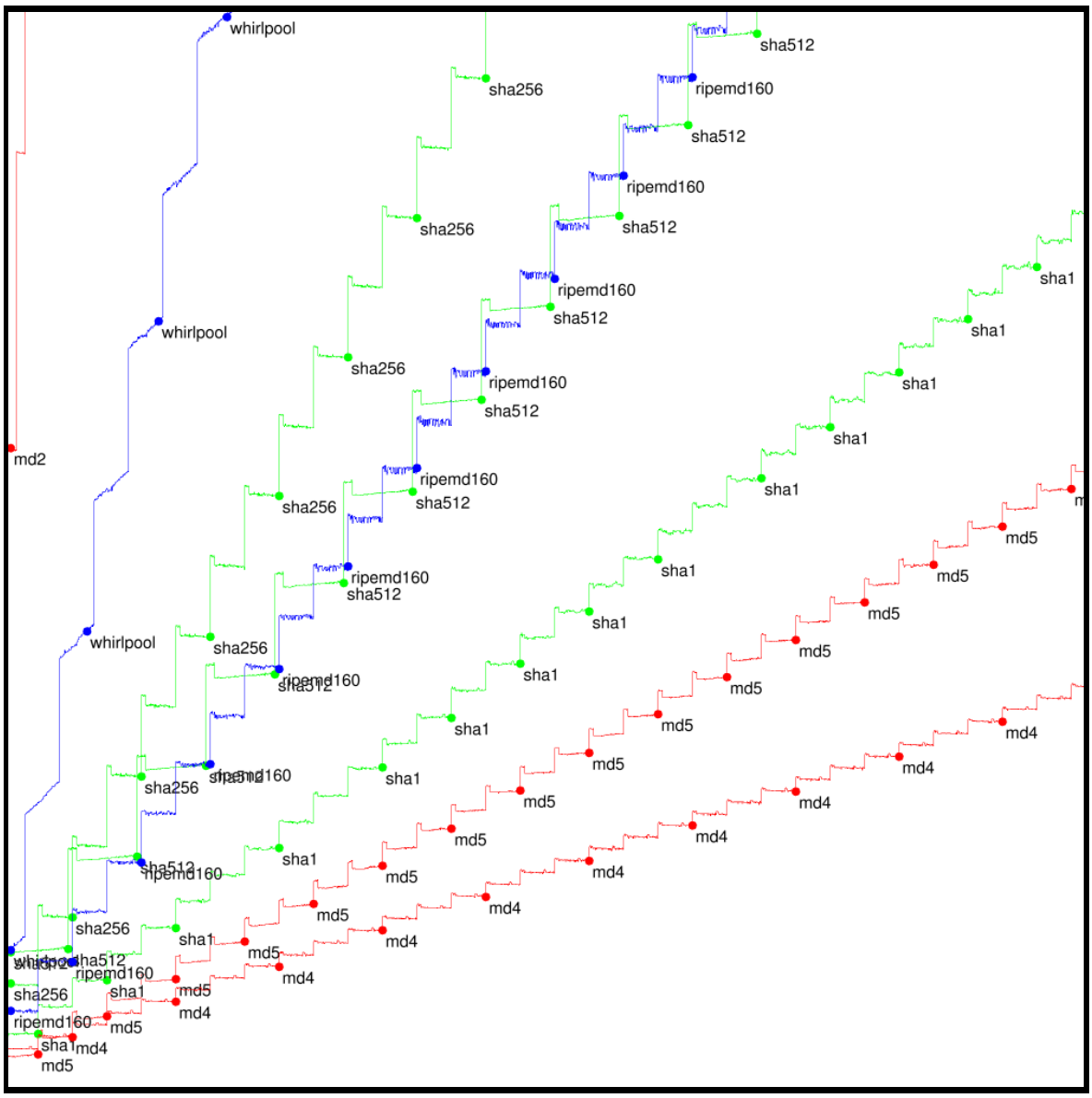
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
6.02	6.02	6.02	`md5`
7.24	7.24	7.27	`md4`
16.26	16.26	16.26	`sha1`
17.57	17.57	17.57	`sha512`
24.11	24.11	24.14	`sha256`
32.48	32.48	32.52	`ripemd160`
61.89	62.04	62.08	`whirlpool`
317.71	317.71	317.92	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
5.47	5.47	5.47	`md5`
6.61	6.61	6.62	`md4`
15.12	15.12	15.12	`sha1`
16.10	16.10	16.10	`sha512`
22.17	22.17	22.19	`sha256`
30.27	30.27	30.29	`ripemd160`
58.60	58.61	58.65	`whirlpool`
307.10	307.10	307.10	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
5.25	5.25	5.25	`md5`
6.37	6.37	6.37	`md4`
14.69	14.69	14.69	`sha1`
15.02	15.02	15.02	`sha512`
21.44	21.44	21.45	`sha256`
29.44	29.44	29.44	`ripemd160`
57.36	57.37	57.40	`whirlpool`
303.04	303.11	303.18	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
5.12	5.12	5.12	`md5`
6.21	6.22	6.23	`md4`
14.38	14.38	14.38	`sha512`
14.43	14.43	14.43	`sha1`
20.99	21.01	21.02	`sha256`
28.93	28.94	28.95	`ripemd160`
56.60	56.67	56.76	`whirlpool`
300.45	300.67	300.94	`md2`

6.3 amd64, 2400MHz, Intel Core 2 Duo (6fb), `utrecht`


whirlpool
sha256
sha512
ripemd160
sha512
ripemd160
sha256
sha512
ripemd160
sha512
whirlpool
sha256
ripemd160
sha512
md2
ripemd160
sha256
sha512
ripemd160
sha512
whirlpool
sha256
sha256
sha1
sha1
sha1
sha1
sha1
sha1
sha1
sha1
sha1
sha1
sha1
sha1
sha1
sha1
sha1
md5
md5
md5
md5
md5
md5
md5
md5
md5
md5
md5
md5
md5
md5
md4
md4
md4

Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
68.62	69.75	73.12	`md5`
87.75	88.88	88.88	`md4`
121.50	122.62	122.62	`sha1`
177.75	178.88	182.25	`ripemd160`
238.50	240.75	255.38	`sha256`
311.62	312.75	315.00	`sha512`
322.88	322.88	328.50	`whirlpool`
1479.38	1483.88	1488.38	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
14.20	14.34	14.48	`md5`
14.48	14.48	14.62	`md4`
23.20	23.20	23.20	`sha1`
36.42	36.42	36.84	`ripemd160`
39.80	39.80	40.08	`sha512`
49.64	49.78	49.78	`sha256`
83.53	83.67	84.09	`whirlpool`
530.72	530.86	531.00	`md2`

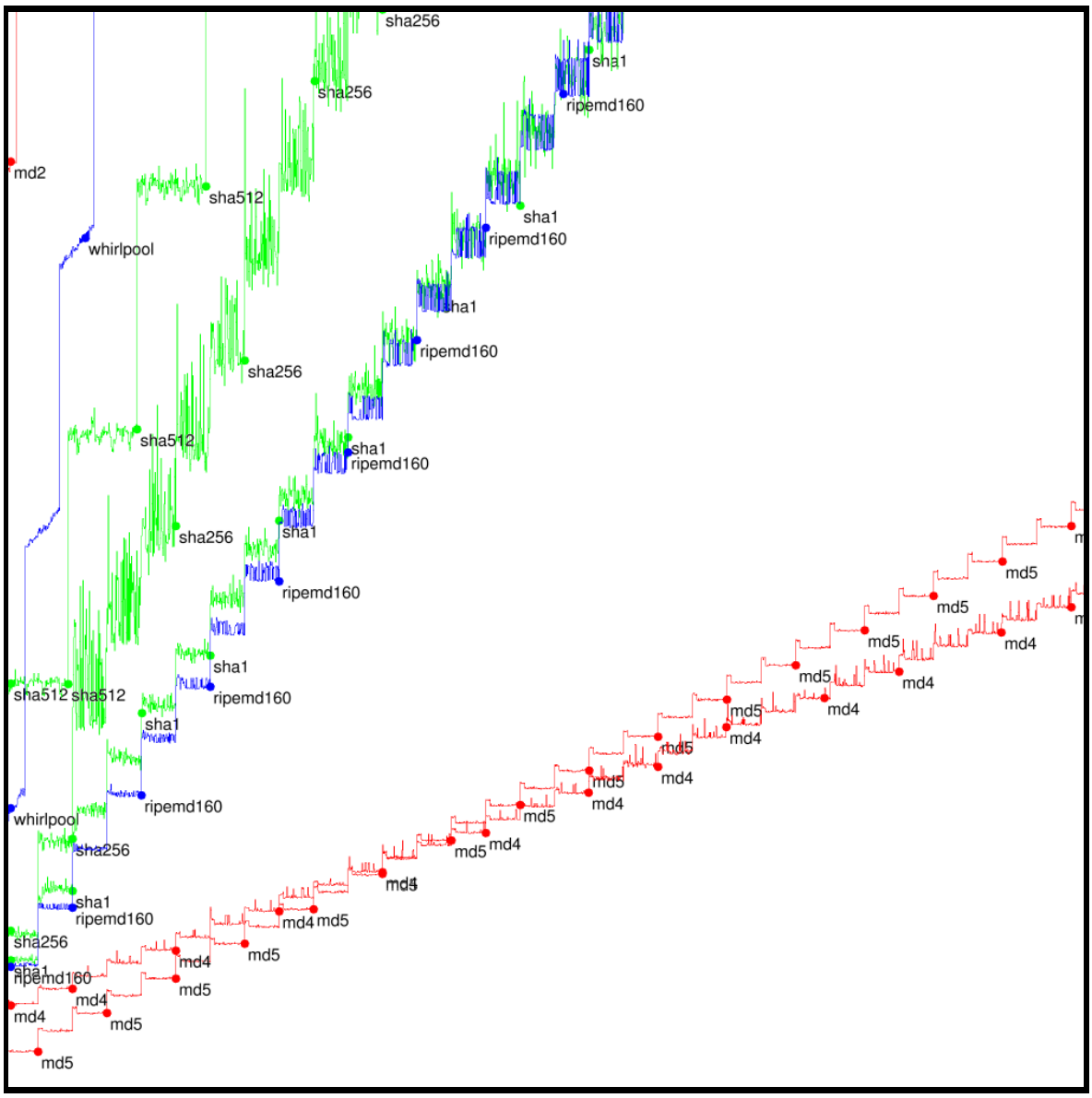
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
4.62	4.64	4.67	`md4`
6.42	6.44	6.44	`md5`
9.39	9.39	9.41	`sha1`
16.23	16.25	16.28	`sha512`
16.64	16.64	16.66	`ripemd160`
23.61	23.62	23.62	`sha256`
49.03	49.08	49.20	`whirlpool`
365.78	365.80	366.05	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
3.84	3.86	3.87	`md4`
5.85	5.85	5.86	`md5`
8.29	8.30	8.35	`sha1`
14.92	14.92	15.02	`sha512`
15.11	15.11	15.12	`ripemd160`
21.52	21.52	21.52	`sha256`
46.29	46.32	46.34	`whirlpool`
352.90	353.02	353.26	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
3.55	3.56	3.57	`md4`
5.61	5.62	5.63	`md5`
7.91	7.92	7.92	`sha1`
13.90	13.91	13.91	`sha512`
14.59	14.59	14.62	`ripemd160`
20.73	20.75	20.75	`sha256`
45.26	45.27	45.28	`whirlpool`
348.15	348.15	348.31	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
3.33	3.39	3.41	`md4`
5.46	5.48	5.49	`md5`
7.62	7.66	7.67	`sha1`
13.19	13.28	13.28	`sha512`
14.22	14.22	14.31	`ripemd160`
20.26	20.29	20.30	`sha256`
44.57	44.60	44.74	`whirlpool`
344.91	345.12	345.56	`md2`

6.4 amd64, 2800MHz, Intel Xeon (f41), nmi0056



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
84.00	85.75	86.62	`md5`
190.75	193.38	194.25	`md4`
280.00	280.00	280.88	`ripemd160`
294.88	299.25	310.62	`sha1`
348.25	353.50	378.88	`sha256`
642.25	646.62	657.12	`whirlpool`
925.75	939.75	951.12	`sha512`
2148.12	2150.75	2151.62	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
16.19	16.52	16.95	`md5`
28.33	28.44	28.44	`md4`
51.41	51.73	52.83	`ripemd160`
57.09	58.19	61.36	`sha1`
68.03	68.69	69.78	`sha256`
112.77	113.75	116.38	`sha512`
161.11	161.55	162.31	`whirlpool`
736.75	737.19	737.52	`md2`

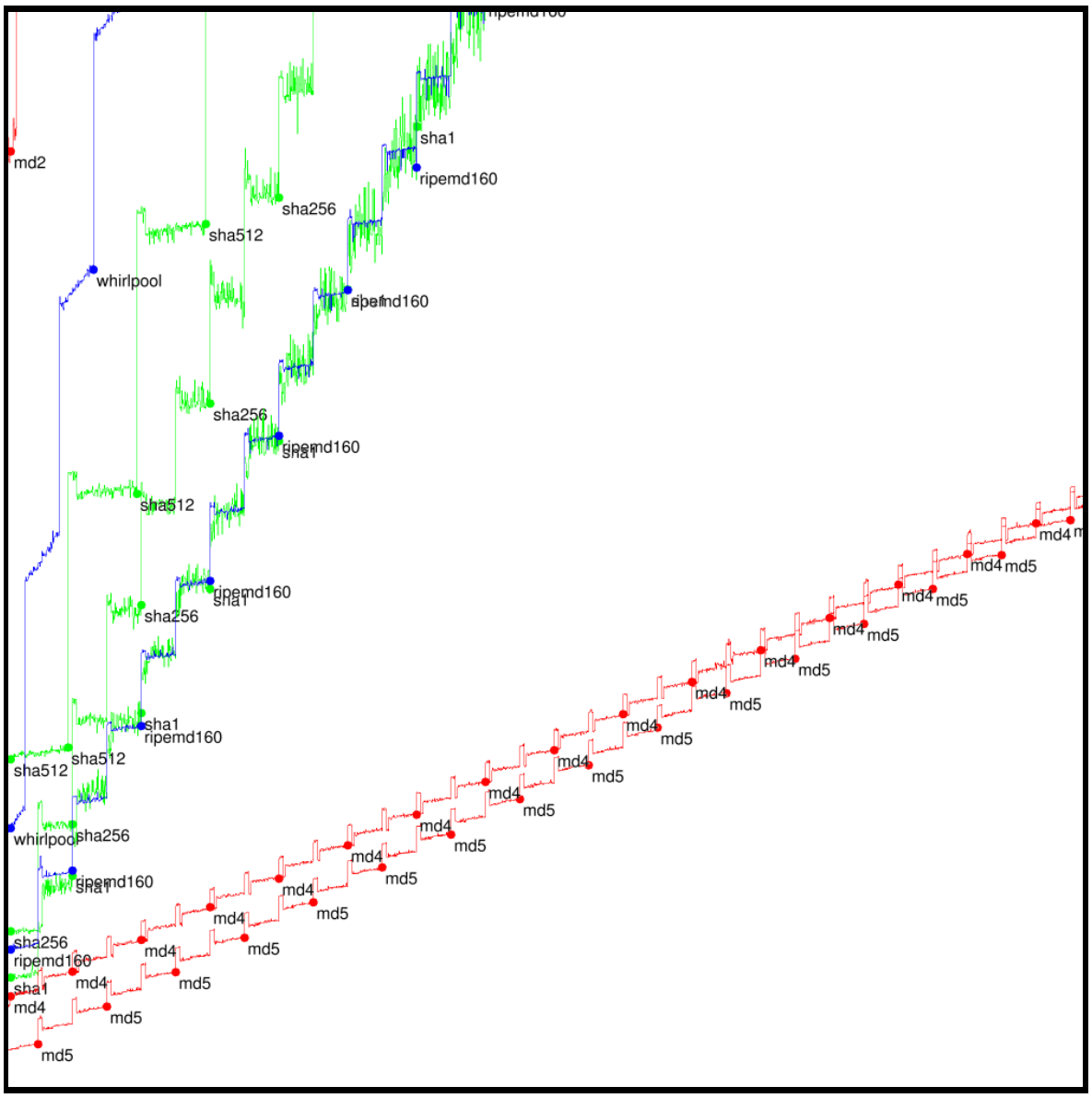
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
6.28	6.34	6.37	`md5`
6.51	6.54	6.78	`md4`
19.78	19.82	20.48	`ripemd160`
19.76	20.38	21.29	`sha1`
32.72	33.13	35.79	`sha256`
44.92	45.10	46.22	`sha512`
90.96	91.18	91.44	`whirlpool`
496.98	497.05	501.98	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
4.87	5.00	5.01	`md4`
5.51	5.53	5.56	`md5`
15.99	16.49	17.19	`sha1`
17.25	17.25	18.30	`ripemd160`
27.13	27.48	28.00	`sha256`
40.59	40.70	40.75	`sha512`
85.23	85.42	85.82	`whirlpool`
478.26	478.99	479.40	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
4.19	4.20	4.23	`md4`
5.21	5.22	5.23	`md5`
15.43	15.70	16.20	`sha1`
16.25	16.94	16.96	`ripemd160`
26.36	26.53	27.02	`sha256`
37.50	37.61	37.87	`sha512`
83.13	83.18	83.34	`whirlpool`
471.28	471.89	472.33	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
3.79	3.80	3.88	`md4`
5.01	5.03	5.07	`md5`
13.94	14.83	16.17	`sha1`
14.96	17.02	17.07	`ripemd160`
23.32	24.74	26.58	`sha256`
35.35	35.69	36.34	`sha512`
81.25	81.80	82.29	`whirlpool`
466.04	468.28	469.20	`md2`

6.5 amd64, 2800MHz, Intel Xeon (f41), nmi0057



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
86.62	88.38	94.50	`md5`
210.00	210.88	211.75	`md4`
243.25	248.50	252.88	`sha1`
319.38	320.25	321.12	`ripemd160`
355.25	362.25	364.88	`sha256`
599.38	604.62	614.25	`whirlpool`
754.25	763.88	787.50	`sha512`
2166.50	2171.75	2179.62	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
16.41	16.52	17.17	`md5`
28.11	28.22	28.66	`md4`
54.47	58.52	58.73	`sha1`
60.81	60.92	61.14	`ripemd160`
75.69	76.02	76.45	`sha256`
96.47	97.34	101.61	`sha512`
152.69	154.44	310.73	`whirlpool`
738.06	749.22	757.97	`md2`

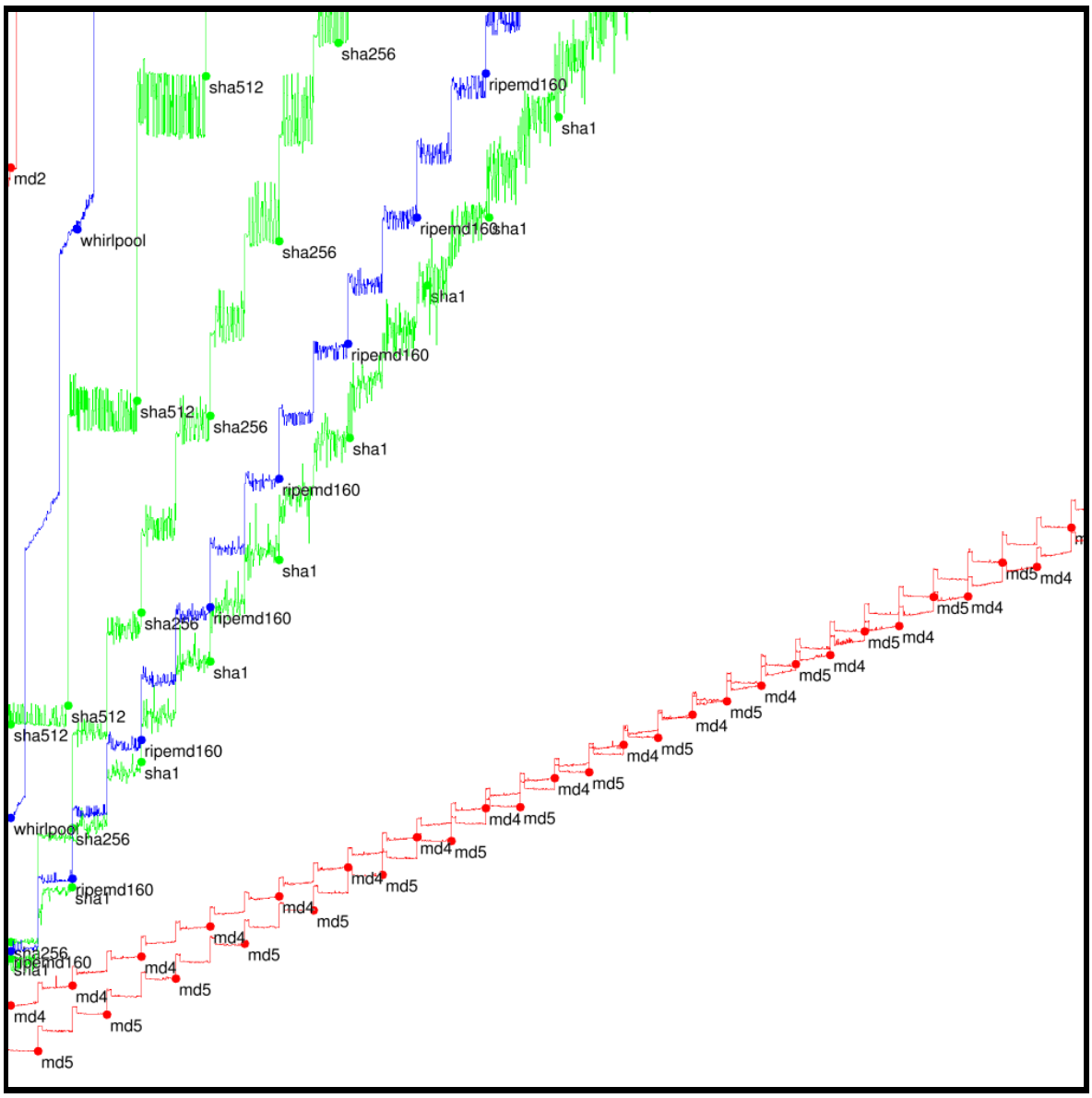
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
6.27	6.30	6.37	`md5`
7.28	7.34	7.46	`md4`
24.34	24.83	24.86	`sha1`
25.52	25.59	25.67	`ripemd160`
35.68	36.35	36.65	`sha256`
43.81	44.04	44.72	`sha512`
86.99	87.12	87.63	`whirlpool`
508.80	514.49	520.69	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
5.52	5.53	5.53	`md5`
5.65	5.68	5.71	`md4`
21.23	21.29	22.15	`sha1`
22.71	22.72	22.75	`ripemd160`
32.29	32.42	33.60	`sha256`
41.45	42.06	60.44	`sha512`
81.78	82.07	82.32	`whirlpool`
492.72	494.75	498.46	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
4.99	5.00	5.01	`md4`
5.22	5.22	5.22	`md5`
20.74	20.91	20.96	`sha1`
21.62	21.70	21.71	`ripemd160`
30.91	31.70	68.23	`sha256`
38.94	39.46	40.12	`sha512`
79.95	80.20	81.61	`whirlpool`
485.16	487.45	488.58	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
4.56	4.59	4.62	`md4`
5.02	5.03	5.04	`md5`
20.65	21.02	21.15	`sha1`
20.89	21.06	21.09	`ripemd160`
-12.33	30.61	104.54	`sha256`
36.72	37.82	39.33	`sha512`
78.57	79.30	82.23	`whirlpool`
472.25	482.15	487.25	`md2`

6.6 amd64, 2800MHz, Intel Xeon (f41), nmi0063



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
84.88	85.75	88.38	`md5`
188.12	189.00	189.88	`md4`
275.62	278.25	304.50	`sha1`
313.25	315.88	321.12	`ripemd160`
330.75	332.50	336.00	`sha256`
627.38	633.50	637.88	`whirlpool`
845.25	868.88	894.25	`sha512`
2123.62	2128.00	2140.25	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
16.30	16.41	16.84	`md5`
28.33	28.33	28.55	`md4`
55.02	56.33	58.52	`sha1`
59.17	59.61	59.94	`ripemd160`
70.33	72.19	76.12	`sha256`
104.89	105.33	110.69	`sha512`
162.42	162.97	163.62	`whirlpool`
728.33	728.98	730.30	`md2`

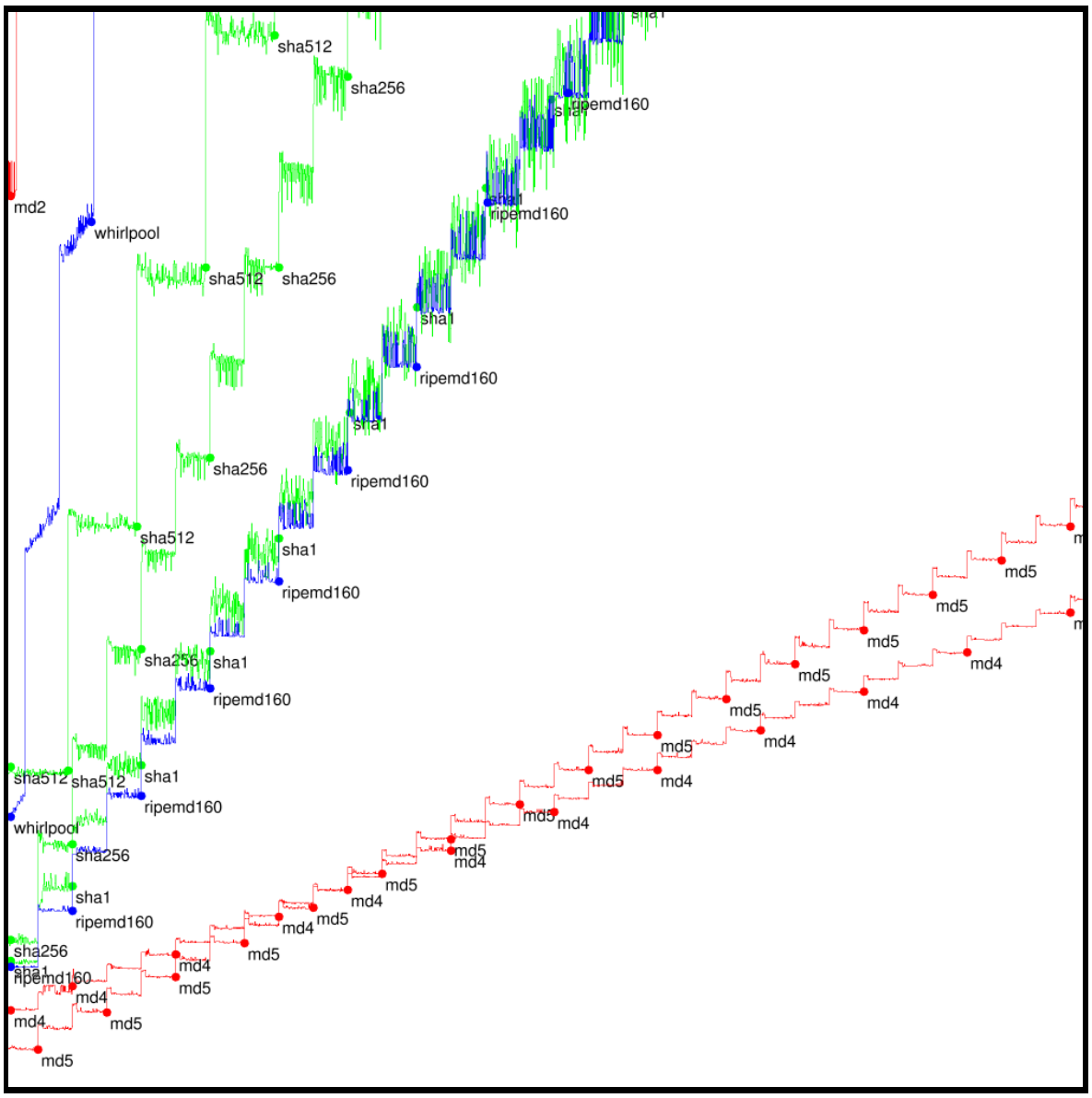
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
6.28	6.30	6.32	`md5`
6.96	6.98	7.00	`md4`
20.79	21.12	22.71	`sha1`
23.44	23.48	23.89	`ripemd160`
33.54	34.47	36.19	`sha256`
49.62	52.33	60.30	`sha512`
94.63	94.84	95.05	`whirlpool`
491.23	492.30	501.61	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
5.34	5.34	8.31	`md4`
5.51	5.53	5.55	`md5`
16.37	17.59	18.00	`sha1`
20.68	20.86	21.23	`ripemd160`
30.78	32.23	32.67	`sha256`
46.98	47.13	50.53	`sha512`
89.51	89.56	89.70	`whirlpool`
473.17	474.26	476.46	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
4.70	4.70	4.71	`md4`
5.22	5.22	5.22	`md5`
15.27	17.15	17.46	`sha1`
19.66	19.67	20.21	`ripemd160`
29.65	29.66	31.44	`sha256`
44.33	47.63	47.63	`sha512`
87.56	87.64	88.87	`whirlpool`
466.92	467.71	468.35	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
4.31	4.32	4.33	`md4`
5.01	5.03	5.03	`md5`
12.91	17.37	18.90	`sha1`
19.03	19.09	20.18	`ripemd160`
28.31	28.98	32.58	`sha256`
39.30	45.90	46.03	`sha512`
86.23	86.51	89.07	`whirlpool`
460.41	464.06	466.32	`md2`

6.7 amd64, 3000MHz, Intel Pentium D (f64), speed



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
90.00	93.75	95.62	`md5`
178.12	178.12	178.12	`md4`
275.62	277.50	286.88	`ripemd160`
279.38	283.12	288.75	`sha1`
341.25	343.12	350.62	`sha256`
633.75	637.50	643.12	`whirlpool`
725.62	731.25	744.38	`sha512`
2070.00	2071.88	2075.62	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
16.64	17.34	18.05	`md5`
26.48	26.72	26.72	`md4`
50.62	50.86	50.86	`ripemd160`
56.02	56.95	57.66	`sha1`
69.61	72.42	72.89	`sha256`
90.70	91.64	92.11	`sha512`
161.02	162.19	163.12	`whirlpool`
746.48	746.95	747.19	`md2`

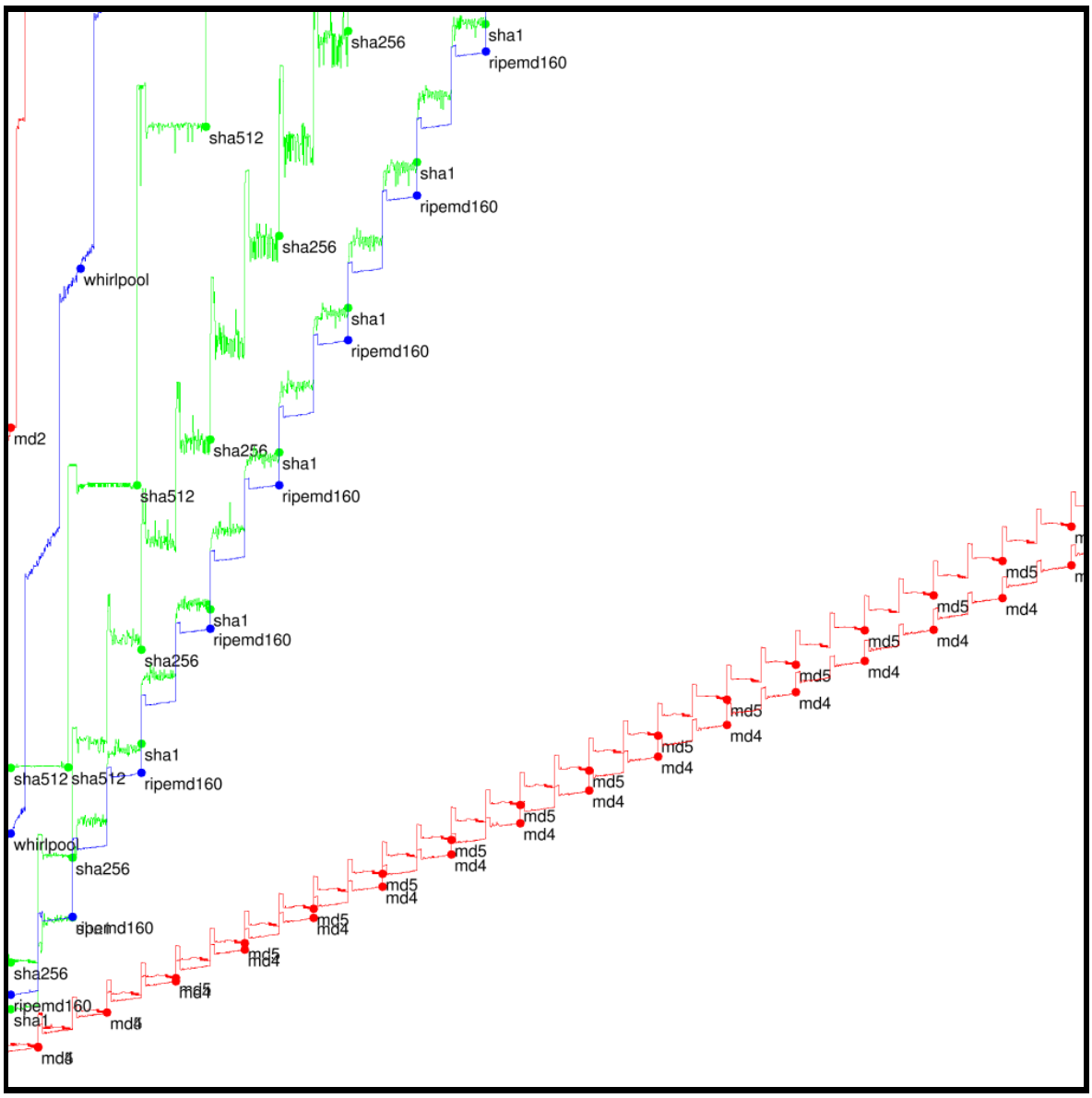
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
6.25	6.33	6.33	`md4`
6.30	6.35	6.46	`md5`
19.77	20.36	20.76	`ripemd160`
19.53	20.65	21.51	`sha1`
31.95	32.71	32.79	`sha256`
40.91	42.08	42.63	`sha512`
92.42	93.31	93.70	`whirlpool`
505.47	505.52	505.55	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
4.78	4.79	4.79	`md4`
5.54	5.55	5.60	`md5`
17.27	17.70	18.23	`ripemd160`
18.29	18.47	18.54	`sha1`
29.66	29.71	29.98	`sha256`
39.54	39.63	39.69	`sha512`
86.61	87.13	87.64	`whirlpool`
486.52	486.57	488.82	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
4.16	4.16	4.17	`md4`
5.22	5.23	5.24	`md5`
14.99	15.11	16.60	`sha1`
16.29	16.30	17.35	`ripemd160`
26.89	28.80	28.80	`sha256`
36.95	37.23	37.23	`sha512`
84.88	85.33	85.75	`whirlpool`
479.49	479.62	481.29	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
3.76	3.78	3.80	`md4`
4.98	5.03	5.08	`md5`
11.98	12.67	15.89	`sha1`
14.68	15.69	17.81	`ripemd160`
24.26	28.84	29.77	`sha256`
35.53	36.34	36.41	`sha512`
81.51	83.45	84.57	`whirlpool`
473.55	475.49	478.94	`md2`

6.8 amd64, 3000MHz, Intel Xeon (f4a), nmi0090


sha256
sha1
ripemd160
sha512
sha1
ripemd160
sha256
whirlpool
sha1
ripemd160
md2
sha256
sha1
sha512
ripemd160
sha1
ripemd160
sha256
sha1
sha512
sha512
ripemd160
whirlpool
sha256
ripemd160
sha256
ripemd160
sha1
md5
md4
md5
md4
md5
md4

Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
83.50	84.38	85.25	`md4`
94.75	95.62	105.88	`md5`
176.25	179.12	185.62	`sha1`
209.12	210.00	214.62	`ripemd160`
289.75	295.25	299.00	`sha256`
595.25	599.12	606.50	`whirlpool`
740.62	741.50	744.38	`sha512`
1531.88	1532.75	1533.75	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
15.47	15.47	15.59	`md4`
17.00	17.34	17.34	`md5`
47.34	48.17	49.69	`sha1`
48.16	48.17	48.28	`ripemd160`
67.73	67.84	67.97	`sha256`
93.16	93.17	93.28	`sha512`
153.75	154.22	155.05	`whirlpool`
547.97	548.09	548.80	`md2`

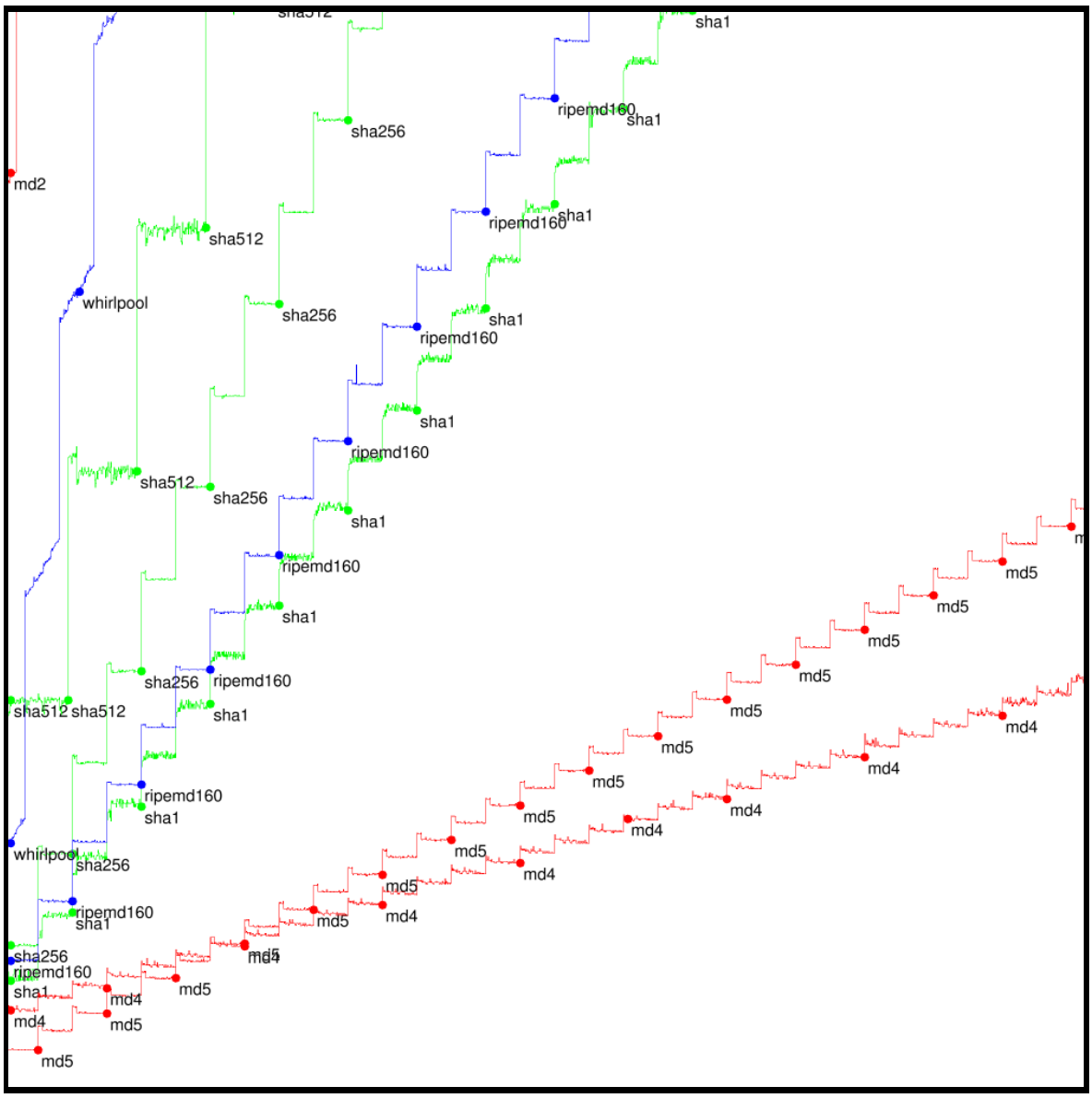
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
5.81	5.82	5.85	`md4`
6.35	6.35	6.35	`md5`
23.96	23.97	23.97	`ripemd160`
24.79	24.88	25.01	`sha1`
32.99	33.54	33.61	`sha256`
46.34	47.29	48.80	`sha512`
89.80	90.04	90.22	`whirlpool`
381.96	382.05	382.11	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
5.08	5.09	5.09	`md4`
5.56	5.56	5.57	`md5`
22.10	22.11	22.11	`ripemd160`
22.55	22.57	22.59	`sha1`
29.92	31.37	33.14	`sha256`
44.26	44.89	45.17	`sha512`
84.79	84.93	85.04	`whirlpool`
368.81	368.83	368.88	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
4.79	4.79	4.79	`md4`
5.23	5.23	5.23	`md5`
21.39	21.39	21.40	`ripemd160`
21.63	21.63	22.33	`sha1`
28.78	29.55	30.22	`sha256`
41.69	41.79	41.99	`sha512`
83.01	83.06	83.11	`whirlpool`
361.35	363.84	363.93	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
4.60	4.61	4.61	`md4`
5.03	5.03	5.04	`md5`
20.97	20.97	20.97	`ripemd160`
21.05	21.08	22.46	`sha1`
26.54	28.12	31.76	`sha256`
39.48	39.72	40.58	`sha512`
81.87	82.07	82.26	`whirlpool`
355.87	362.97	363.17	`md2`

6.9 amd64, 3392MHz, Intel Pentium D (f64), nmi0104



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
87.12	89.25	89.25	`md5`
174.25	178.50	191.25	`md4`
246.50	246.50	246.50	`sha1`
291.12	293.25	295.38	`ripemd160`
325.12	329.38	331.50	`sha256`
573.75	580.12	586.50	`whirlpool`
892.50	894.62	909.50	`sha512`
2125.00	2129.25	2142.00	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
16.47	16.47	17.00	`md5`
26.56	26.56	28.69	`md4`
48.61	49.14	50.20	`sha1`
53.66	53.92	53.92	`ripemd160`
67.47	67.73	68.27	`sha256`
108.91	109.17	109.97	`sha512`
148.48	149.28	149.81	`whirlpool`
727.28	730.73	735.52	`md2`

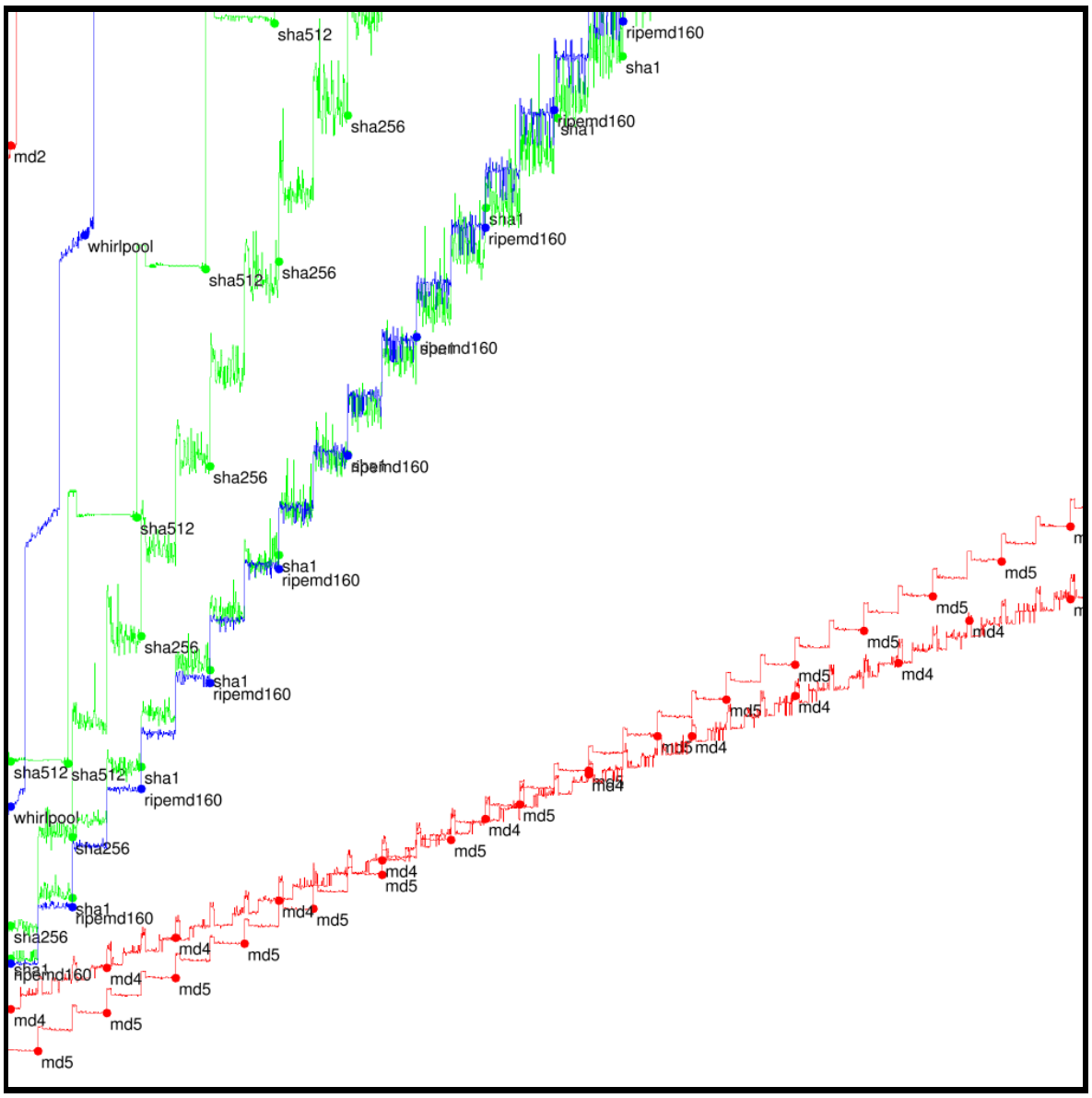
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
5.64	5.67	5.84	`md4`
6.32	6.32	6.38	`md5`
18.65	18.77	18.89	`sha1`
20.84	20.87	20.95	`ripemd160`
31.20	31.20	31.31	`sha256`
42.12	42.23	42.41	`sha512`
87.51	87.69	87.95	`whirlpool`
492.97	494.39	495.10	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
4.02	4.03	4.17	`md4`
5.53	5.54	5.54	`md5`
15.97	16.00	16.09	`sha1`
18.23	18.24	18.25	`ripemd160`
28.41	28.42	28.43	`sha256`
37.34	37.40	37.43	`sha512`
82.62	82.80	82.94	`whirlpool`
477.52	478.89	482.83	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
3.40	3.40	3.46	`md4`
5.22	5.22	5.23	`md5`
14.98	15.00	15.13	`sha1`
17.23	17.23	17.24	`ripemd160`
27.34	27.35	27.36	`sha256`
34.37	34.38	34.40	`sha512`
80.87	80.93	81.00	`whirlpool`
467.71	468.63	470.80	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
2.91	3.02	3.18	`md4`
5.01	5.03	5.06	`md5`
14.29	14.34	14.68	`sha1`
16.54	16.59	16.63	`ripemd160`
26.68	26.72	26.75	`sha256`
32.41	32.57	32.63	`sha512`
79.36	79.83	80.08	`whirlpool`
456.45	460.06	466.31	`md2`

6.10 amd64, 3392MHz, Intel Pentium D (f64), nmi0161



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
85.00	87.12	87.12	`md5`
178.50	180.62	182.75	`md4`
280.50	282.62	286.88	`ripemd160`
282.62	289.00	293.25	`sha1`
348.50	380.38	384.62	`sha256`
648.12	656.62	663.00	`whirlpool`
756.50	756.50	765.00	`sha512`
2167.50	2188.75	2195.12	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
16.73	17.00	17.27	`md5`
26.56	26.83	27.62	`md4`
51.27	51.53	52.06	`ripemd160`
56.31	57.64	57.91	`sha1`
72.25	73.58	73.58	`sha256`
94.83	94.83	95.09	`sha512`
161.50	162.30	163.62	`whirlpool`
744.28	748.27	751.45	`md2`

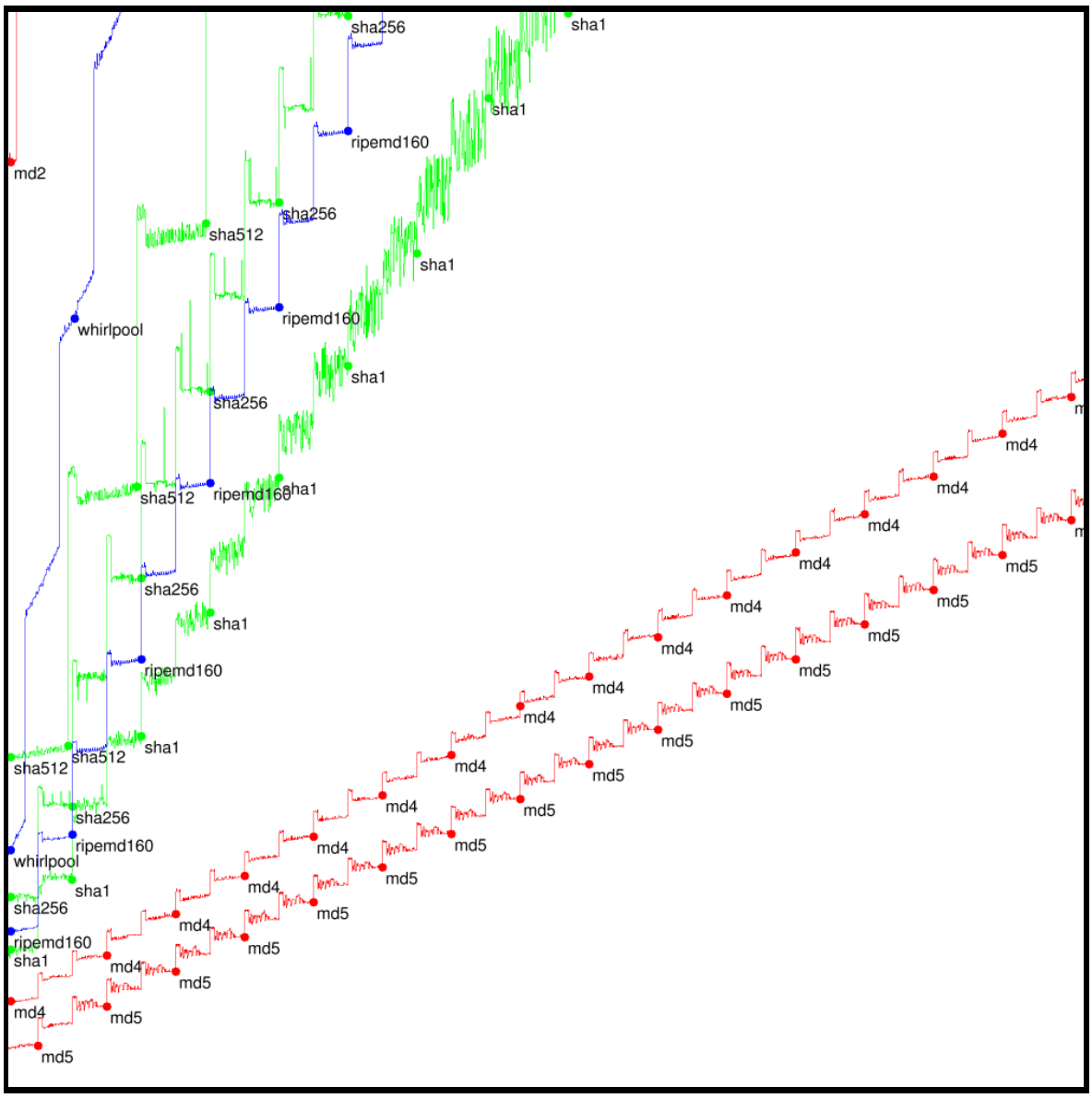
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
6.29	6.32	6.43	`md5`
6.40	6.43	6.46	`md4`
20.57	20.81	20.87	`ripemd160`
20.84	21.22	21.31	`sha1`
31.26	31.28	32.47	`sha256`
42.38	42.41	42.41	`sha512`
90.90	91.29	91.76	`whirlpool`
509.82	510.44	511.21	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
4.80	4.80	4.81	`md4`
5.52	5.56	5.56	`md5`
16.93	17.71	18.22	`sha1`
17.28	17.92	17.94	`ripemd160`
27.78	27.79	28.16	`sha256`
39.88	39.88	39.89	`sha512`
85.25	85.45	85.85	`whirlpool`
473.03	487.99	493.39	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
4.18	4.18	4.19	`md4`
5.22	5.23	5.23	`md5`
13.75	16.41	16.61	`sha1`
16.28	16.98	17.37	`ripemd160`
26.70	26.80	26.88	`sha256`
37.34	37.34	37.34	`sha512`
83.00	83.23	83.48	`whirlpool`
465.49	468.22	486.36	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
3.80	3.81	3.82	`md4`
5.01	5.04	5.06	`md5`
9.60	16.57	16.98	`sha1`
14.66	17.08	17.86	`ripemd160`
25.47	25.93	26.41	`sha256`
35.82	35.82	35.82	`sha512`
81.29	81.96	82.69	`whirlpool`
440.34	447.64	501.34	`md2`

6.11 amd64, 3392MHz, Intel Pentium D (f64), nmi0241



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
91.38	91.38	93.50	`md5`
195.50	195.50	197.62	`md4`
306.00	312.38	325.12	`sha1`
363.38	363.38	365.50	`ripemd160`
435.62	442.00	444.12	`sha256`
554.62	561.00	563.12	`whirlpool`
756.50	760.75	796.88	`sha512`
2146.25	2150.50	2163.25	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
17.00	17.27	17.80	`md5`
30.81	30.81	30.81	`md4`
59.50	60.03	61.62	`sha1`
71.19	71.19	71.45	`ripemd160`
84.20	84.73	85.27	`sha256`
96.69	97.48	98.55	`sha512`
144.77	145.56	146.09	`whirlpool`
747.20	749.33	754.38	`md2`

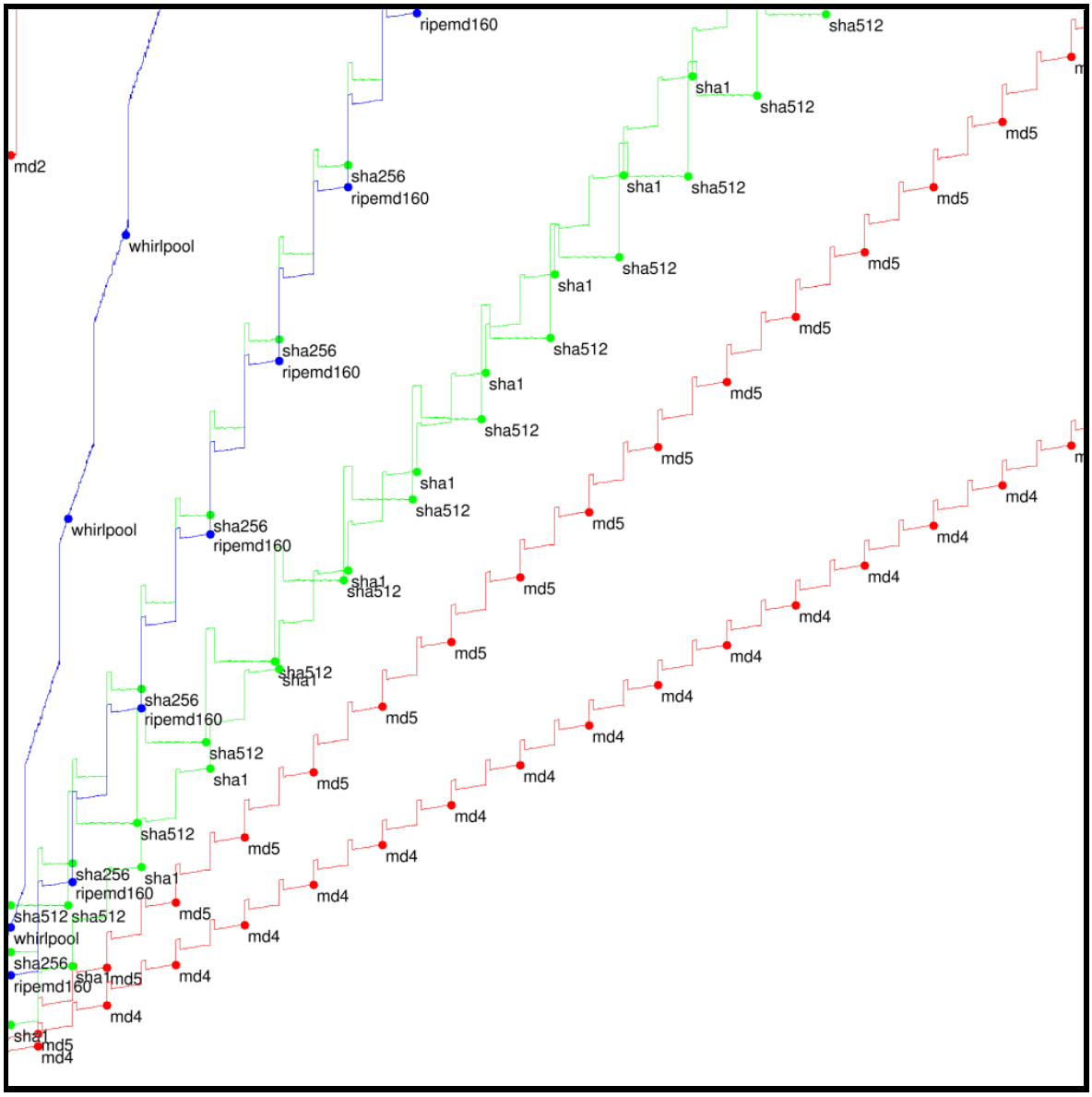
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
6.35	6.40	6.46	`md5`
8.62	8.62	8.65	`md4`
22.58	22.78	23.40	`sha1`
30.64	30.81	30.84	`ripemd160`
34.65	34.68	34.68	`sha256`
43.86	43.86	44.24	`sha512`
87.21	87.57	88.22	`whirlpool`
506.34	506.87	514.19	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
5.56	5.58	5.59	`md5`
6.84	6.85	6.86	`md4`
18.72	18.93	20.45	`sha1`
27.54	27.55	27.56	`ripemd160`
30.07	30.10	30.90	`sha256`
41.33	41.98	42.27	`sha512`
82.27	82.53	82.85	`whirlpool`
489.74	493.34	499.41	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
5.23	5.24	5.27	`md5`
6.17	6.17	6.17	`md4`
17.90	18.14	19.32	`sha1`
26.34	26.35	26.37	`ripemd160`
28.33	29.00	30.04	`sha256`
39.37	39.52	39.56	`sha512`
80.61	80.79	80.98	`whirlpool`
484.22	487.58	490.24	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
5.01	5.05	5.10	`md5`
5.74	5.76	5.77	`md4`
16.47	18.08	20.53	`sha1`
25.58	25.63	25.68	`ripemd160`
27.27	28.63	30.71	`sha256`
37.61	38.12	38.74	`sha512`
78.98	79.49	80.03	`whirlpool`
473.14	487.54	495.26	`md2`

6.12 ia64, 900MHz, HP Itanium II, nmi0025



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
84.00	84.00	84.00	`md4`
112.62	112.62	113.50	`md5`
143.88	143.88	144.12	`sha1`
256.12	257.25	257.50	`ripemd160`
311.12	311.12	311.50	`sha256`
378.50	382.50	390.88	`whirlpool`
418.12	418.50	419.00	`sha512`
2162.88	2164.00	2164.00	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
16.05	16.05	16.05	`md4`
23.20	23.20	23.20	`md5`
33.55	33.59	33.83	`sha1`
52.25	52.33	52.39	`sha512`
57.70	57.83	57.88	`ripemd160`
64.27	64.30	64.34	`sha256`
108.36	108.81	109.38	`whirlpool`
794.17	794.39	794.78	`md2`

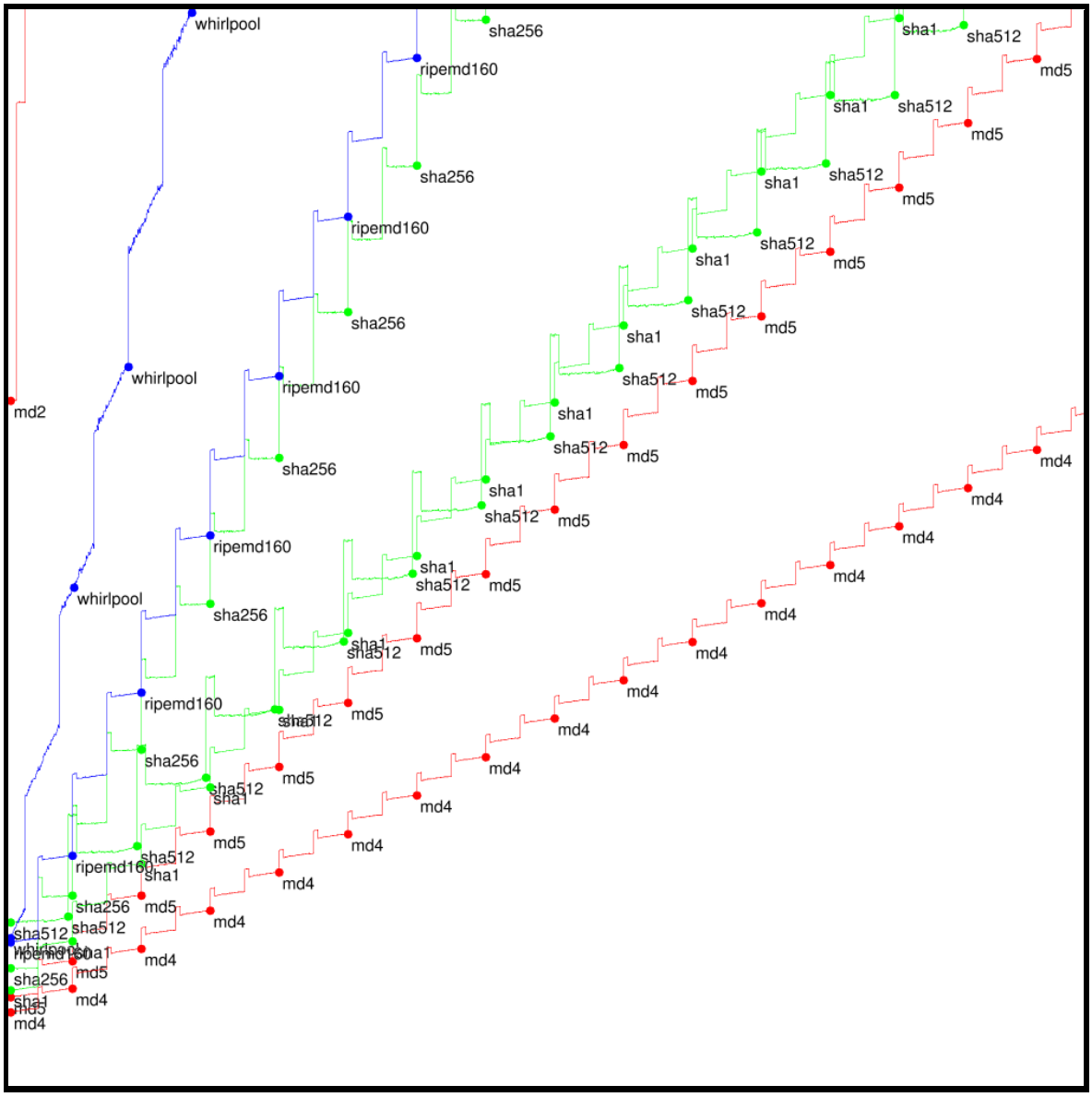
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
6.97	6.97	6.97	`md4`
11.00	11.00	11.00	`md5`
16.28	16.28	16.29	`sha512`
16.49	16.50	16.52	`sha1`
28.84	28.85	28.86	`ripemd160`
29.63	29.64	29.65	`sha256`
68.86	68.88	68.98	`whirlpool`
553.30	553.42	555.91	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
6.24	6.24	6.24	`md4`
10.02	10.02	10.02	`md5`
13.94	13.94	13.94	`sha512`
15.14	15.15	15.15	`sha1`
26.58	26.58	26.59	`ripemd160`
26.91	26.92	26.93	`sha256`
65.56	65.67	65.79	`whirlpool`
534.64	535.43	535.55	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
5.96	5.96	5.96	`md4`
9.66	9.66	9.66	`md5`
12.56	12.56	12.57	`sha512`
14.63	14.63	14.64	`sha1`
25.73	25.73	25.73	`ripemd160`
25.89	25.91	25.91	`sha256`
64.48	64.51	64.91	`whirlpool`
528.10	528.25	528.46	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
5.80	5.80	5.80	`md4`
9.44	9.44	9.44	`md5`
11.74	11.74	11.74	`sha512`
14.32	14.33	14.34	`sha1`
25.21	25.22	25.23	`ripemd160`
25.25	25.31	25.32	`sha256`
63.69	63.82	64.68	`whirlpool`
523.57	524.10	524.59	`md2`

6.13 ia64, 997MHz, HP Itanium II, nmi0020



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
172.50	172.50	172.50	`md4`
206.75	207.25	207.75	`md5`
221.62	222.38	222.88	`sha1`
271.62	272.88	273.50	`sha256`
333.25	334.00	335.00	`ripemd160`
354.38	354.62	358.88	`whirlpool`
380.50	381.00	382.38	`sha512`
1591.75	1592.50	1592.50	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
26.89	26.89	26.89	`md4`
34.89	35.05	35.11	`md5`
40.59	40.69	40.80	`sha1`
48.03	48.19	48.28	`sha512`
54.72	54.81	54.95	`sha256`
65.36	65.56	65.66	`ripemd160`
94.20	94.36	95.50	`whirlpool`
545.00	545.19	545.19	`md2`

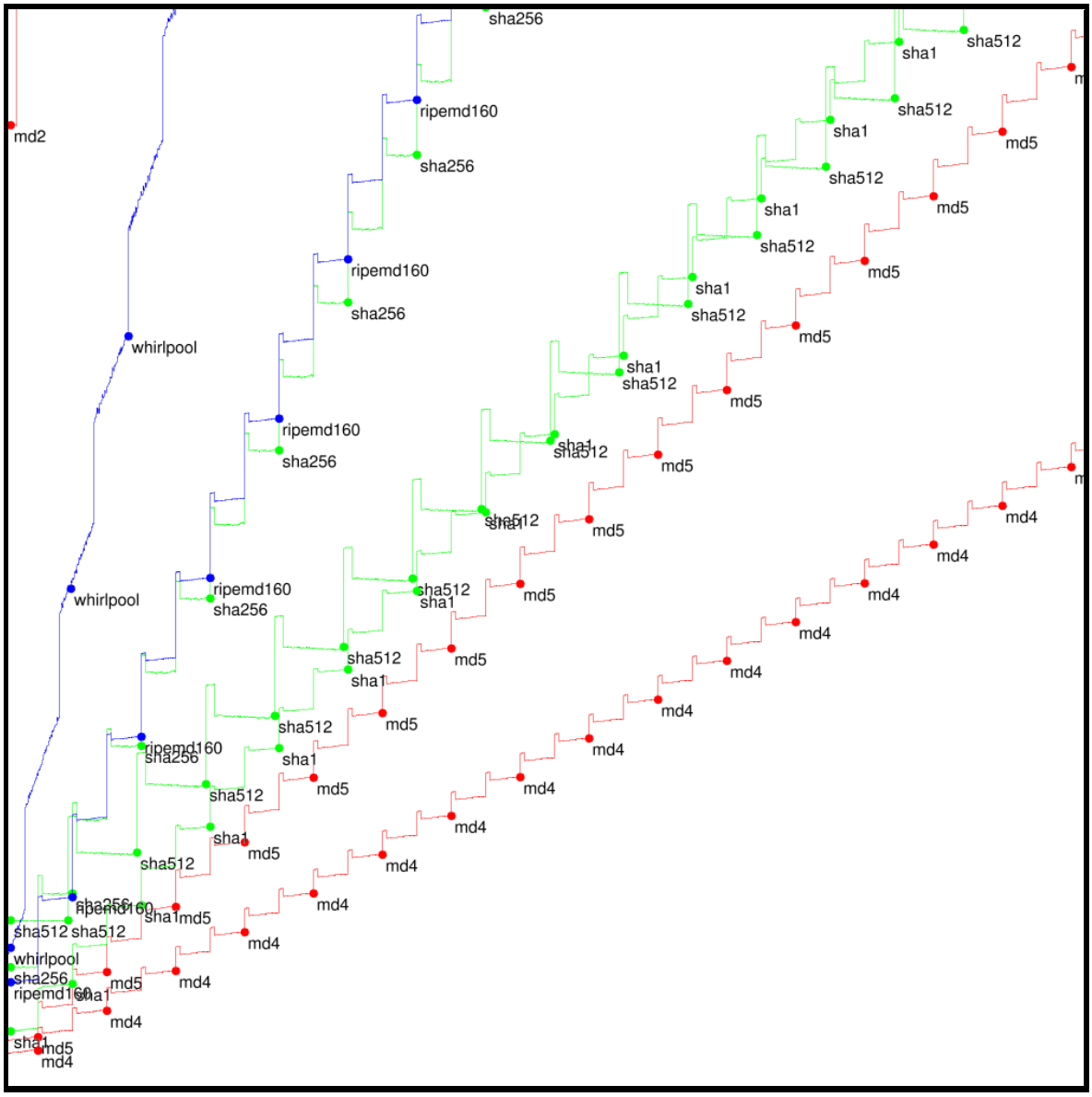
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
7.97	7.97	7.97	`md4`
12.21	12.23	12.23	`md5`
14.17	14.19	14.20	`sha512`
14.46	14.47	14.48	`sha1`
24.93	24.94	24.95	`sha256`
27.87	27.88	27.89	`ripemd160`
56.98	57.03	57.49	`whirlpool`
368.13	368.25	369.16	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
6.48	6.48	6.48	`md4`
10.42	10.43	10.43	`md5`
11.91	11.92	11.93	`sha512`
12.40	12.40	12.40	`sha1`
22.58	22.59	22.62	`sha256`
24.88	24.89	24.89	`ripemd160`
54.28	54.33	54.35	`whirlpool`
354.42	355.72	356.12	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
5.92	5.92	5.92	`md4`
9.75	9.75	9.75	`md5`
10.66	10.66	10.67	`sha512`
11.62	11.62	11.62	`sha1`
21.72	21.72	21.74	`sha256`
23.76	23.77	23.77	`ripemd160`
53.23	53.26	53.52	`whirlpool`
349.83	350.17	350.34	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
5.58	5.58	5.58	`md4`
9.34	9.34	9.35	`md5`
9.88	9.90	9.92	`sha512`
11.15	11.16	11.16	`sha1`
21.18	21.20	21.27	`sha256`
23.09	23.09	23.10	`ripemd160`
52.45	52.64	53.19	`whirlpool`
345.64	346.69	348.03	`md2`

6.14 ia64, 997MHz, HP Itanium II, nmi0058



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
78.38	78.38	78.38	`md4`
108.00	108.00	108.00	`md5`
126.38	127.00	127.50	`sha1`
240.00	240.88	241.88	`ripemd160`
275.50	275.75	277.62	`sha256`
330.62	330.88	337.25	`whirlpool`
383.38	384.00	384.38	`sha512`
2229.25	2229.75	2230.25	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
15.22	15.22	15.22	`md4`
22.62	22.62	22.62	`md5`
28.75	28.78	28.95	`sha1`
47.69	47.73	47.81	`sha512`
53.48	53.67	53.78	`ripemd160`
55.55	55.69	55.73	`sha256`
93.83	94.58	95.88	`whirlpool`
824.91	825.06	825.34	`md2`

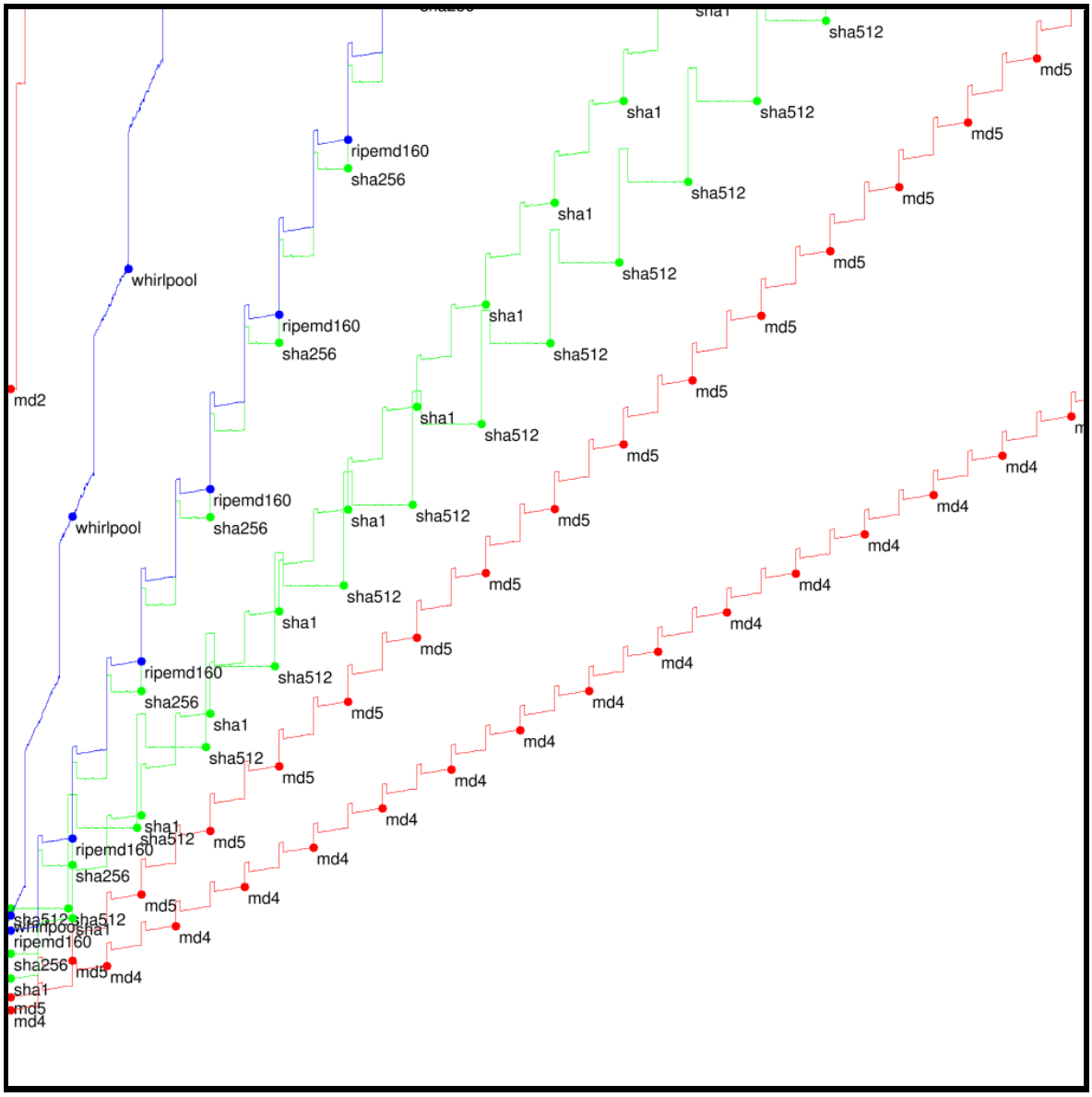
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
6.73	6.73	6.73	`md4`
10.88	10.88	10.88	`md5`
13.34	13.36	13.37	`sha1`
14.09	14.09	14.11	`sha512`
25.22	25.24	25.25	`sha256`
26.52	26.54	26.55	`ripemd160`
59.84	59.89	60.34	`whirlpool`
576.58	576.67	579.35	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
6.04	6.04	6.04	`md4`
9.94	9.94	9.94	`md5`
11.94	11.95	11.95	`sha512`
12.12	12.13	12.13	`sha1`
22.84	22.85	22.86	`sha256`
24.40	24.40	24.41	`ripemd160`
57.27	57.33	57.46	`whirlpool`
558.14	558.20	559.28	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
5.78	5.78	5.78	`md4`
9.59	9.59	9.59	`md5`
10.69	10.69	10.70	`sha512`
11.66	11.67	11.67	`sha1`
21.92	21.94	21.95	`sha256`
23.60	23.61	23.61	`ripemd160`
56.40	56.43	56.66	`whirlpool`
551.56	552.02	552.49	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
5.62	5.62	5.63	`md4`
9.38	9.38	9.38	`md5`
9.92	9.94	9.98	`sha512`
11.38	11.39	11.40	`sha1`
21.35	21.39	21.42	`sha256`
23.12	23.13	23.14	`ripemd160`
55.73	55.82	56.35	`whirlpool`
546.65	548.13	549.97	`md2`

6.15 ia64, 1396MHz, HP Itanium II, nmi0065



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
177.50	177.50	178.62	`md4`
207.38	207.38	207.62	`md5`
249.25	249.88	250.00	`sha1`
306.38	307.12	308.25	`sha256`
361.62	362.00	362.88	`ripemd160`
403.50	405.00	407.50	`whirlpool`
411.00	412.38	413.88	`sha512`
1618.25	1618.25	1618.88	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
27.67	27.67	27.77	`md4`
35.03	35.05	35.06	`md5`
47.56	47.81	47.83	`sha1`
51.47	51.58	51.66	`sha512`
63.72	63.91	64.02	`sha256`
70.42	70.52	70.62	`ripemd160`
107.83	108.30	108.38	`whirlpool`
557.03	557.12	557.25	`md2`

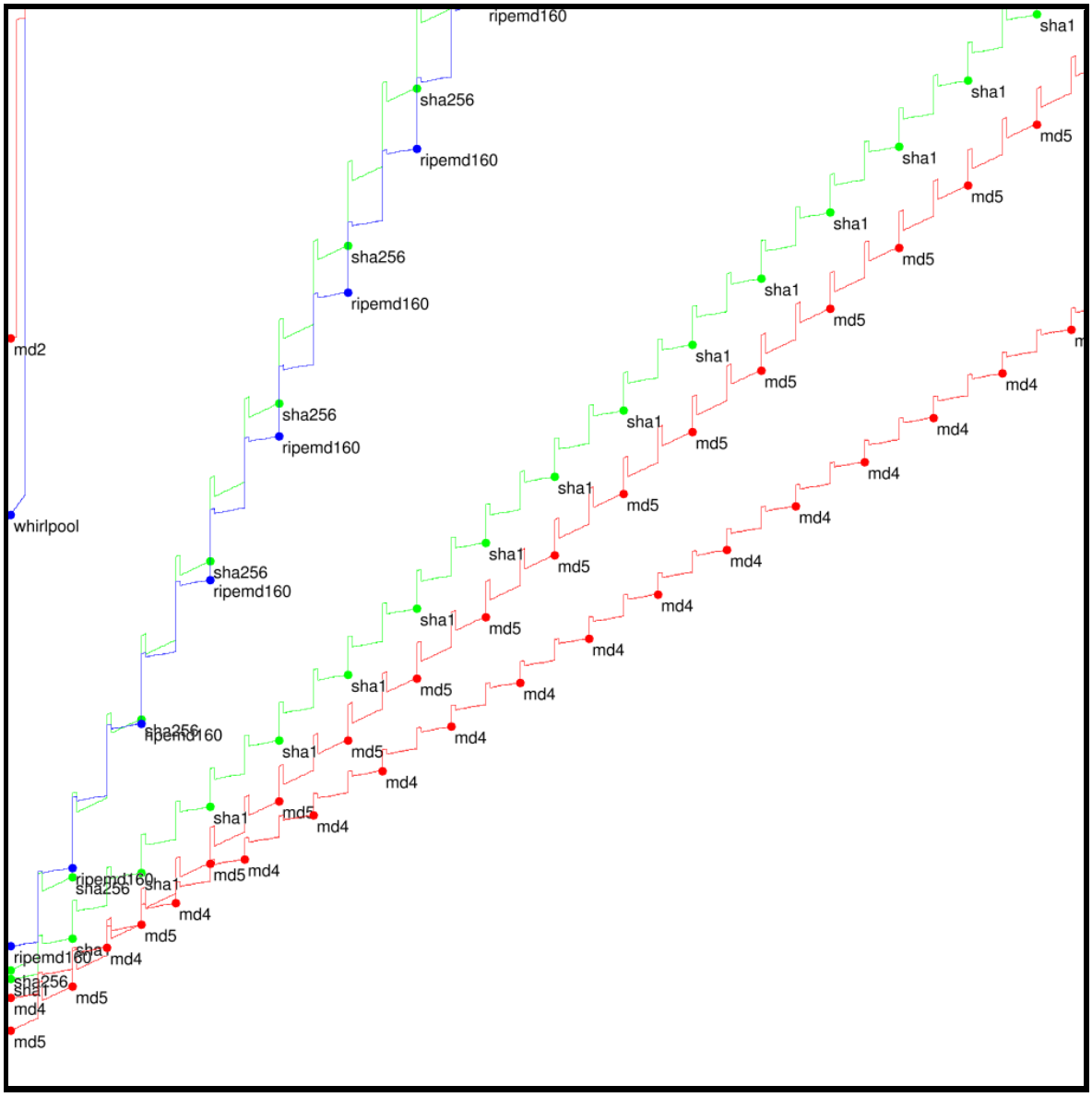
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
8.16	8.16	8.17	`md4`
12.23	12.23	12.23	`md5`
16.11	16.13	16.16	`sha512`
18.40	18.47	18.48	`sha1`
29.47	29.56	29.58	`sha256`
30.36	30.36	30.36	`ripemd160`
65.13	65.19	65.38	`whirlpool`
377.24	377.30	377.45	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
6.61	6.61	6.62	`md4`
10.42	10.43	10.43	`md5`
13.85	13.86	13.87	`sha512`
16.13	16.18	16.19	`sha1`
26.81	26.81	26.89	`sha256`
27.23	27.23	27.24	`ripemd160`
61.82	61.84	61.93	`whirlpool`
363.26	363.36	364.71	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
6.04	6.04	6.04	`md4`
9.75	9.75	9.75	`md5`
12.51	12.51	12.52	`sha512`
15.23	15.27	15.31	`sha1`
25.89	25.90	25.90	`sha256`
26.06	26.06	26.07	`ripemd160`
60.52	60.55	60.56	`whirlpool`
358.50	358.60	358.68	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
5.68	5.69	5.69	`md4`
9.34	9.34	9.35	`md5`
11.69	11.71	11.72	`sha512`
14.66	14.77	14.85	`sha1`
25.36	25.36	25.37	`ripemd160`
25.29	25.38	25.39	`sha256`
59.65	59.75	59.83	`whirlpool`
354.92	355.24	356.18	`md2`

6.16 ppc32, 400MHz, Motorola PowerPC G4 7400, nmi0042


ripemd160
sha256
ripemd160
sha256
ripemd160
md2
sha256
ripemd160
whirlpool
sha256
ripemd160
sha256
ripemd160
sha1
sha1
md5
sha1
md5
sha1
md5

Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
130.00	130.00	130.00	`md5`
204.00	204.00	204.00	`md4`
248.00	250.00	250.00	`sha1`
270.00	270.00	272.00	`sha256`
324.00	324.00	324.00	`ripemd160`
1332.00	1332.00	1334.00	`whirlpool`
1736.00	1738.00	1738.00	`md2`
4314.00	4316.00	4316.00	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
24.75	24.75	24.75	`md5`
32.25	32.25	32.25	`md4`
41.00	41.25	41.25	`sha1`
56.50	56.50	56.50	`sha256`
61.75	61.75	61.75	`ripemd160`
337.00	337.00	337.25	`whirlpool`
543.25	543.25	543.50	`sha512`
587.25	587.25	587.25	`md2`

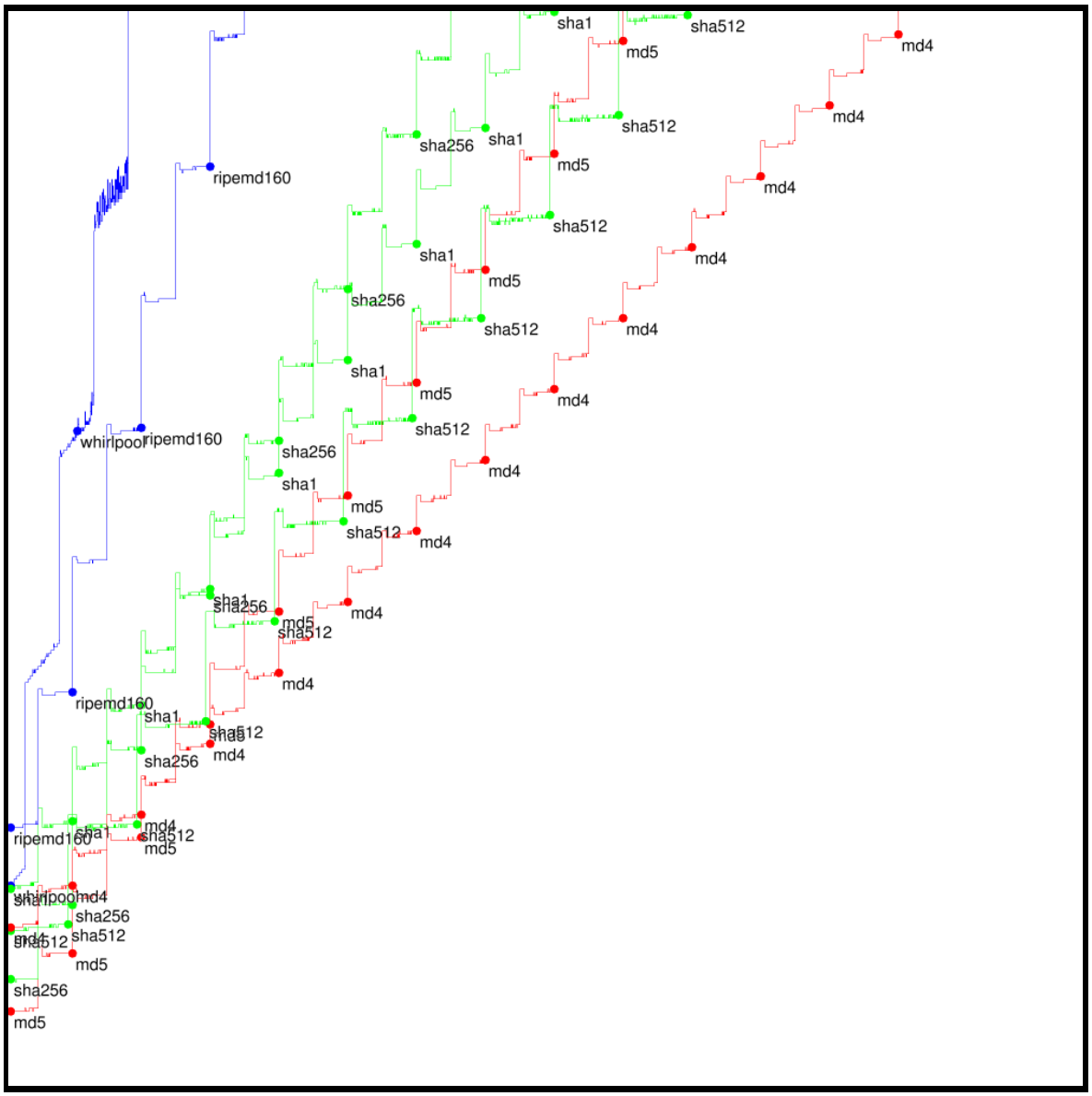
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
9.28	9.28	9.28	`md4`
10.69	10.72	10.72	`md5`
13.08	13.08	13.08	`sha1`
25.39	25.42	25.42	`ripemd160`
26.64	26.64	26.67	`sha256`
190.33	190.33	190.36	`whirlpool`
285.67	285.69	285.69	`sha512`
394.19	394.19	394.19	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
7.48	7.48	7.49	`md4`
9.60	9.60	9.60	`md5`
10.89	10.90	10.90	`sha1`
22.56	22.56	22.57	`ripemd160`
24.30	24.31	24.31	`sha256`
178.88	178.88	178.88	`whirlpool`
275.54	275.54	275.54	`sha512`
379.13	379.13	379.15	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
6.81	6.81	6.81	`md4`
9.19	9.19	9.19	`md5`
10.07	10.07	10.07	`sha1`
21.50	21.50	21.50	`ripemd160`
23.43	23.43	23.43	`sha256`
174.58	174.59	174.60	`whirlpool`
261.39	261.39	261.95	`sha512`
373.46	373.47	373.66	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
6.40	6.41	6.41	`md4`
8.94	8.94	8.94	`md5`
9.57	9.58	9.59	`sha1`
20.86	20.86	20.86	`ripemd160`
22.90	22.91	22.91	`sha256`
171.99	172.03	172.05	`whirlpool`
252.89	252.89	254.02	`sha512`
370.05	370.07	370.44	`md2`

6.17 ppc32, 2000MHz, IBM PowerPC G5 970, geespaz



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
172.50	172.50	172.50	`md5`
240.00	247.50	247.50	`sha256`
360.00	360.00	360.00	`sha512`
367.50	367.50	367.50	`md4`
457.50	457.50	465.00	`sha1`
465.00	472.50	480.00	`whirlpool`
600.00	600.00	600.00	`ripemd160`
3262.50	3270.00	3270.00	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
37.50	37.50	38.44	`md5`
45.94	45.94	45.94	`sha512`
52.50	52.50	52.50	`sha256`
56.25	56.25	57.19	`md4`
75.00	75.00	75.94	`sha1`
112.50	113.44	113.44	`ripemd160`
121.88	122.81	131.25	`whirlpool`
1105.31	1106.25	1108.12	`md2`

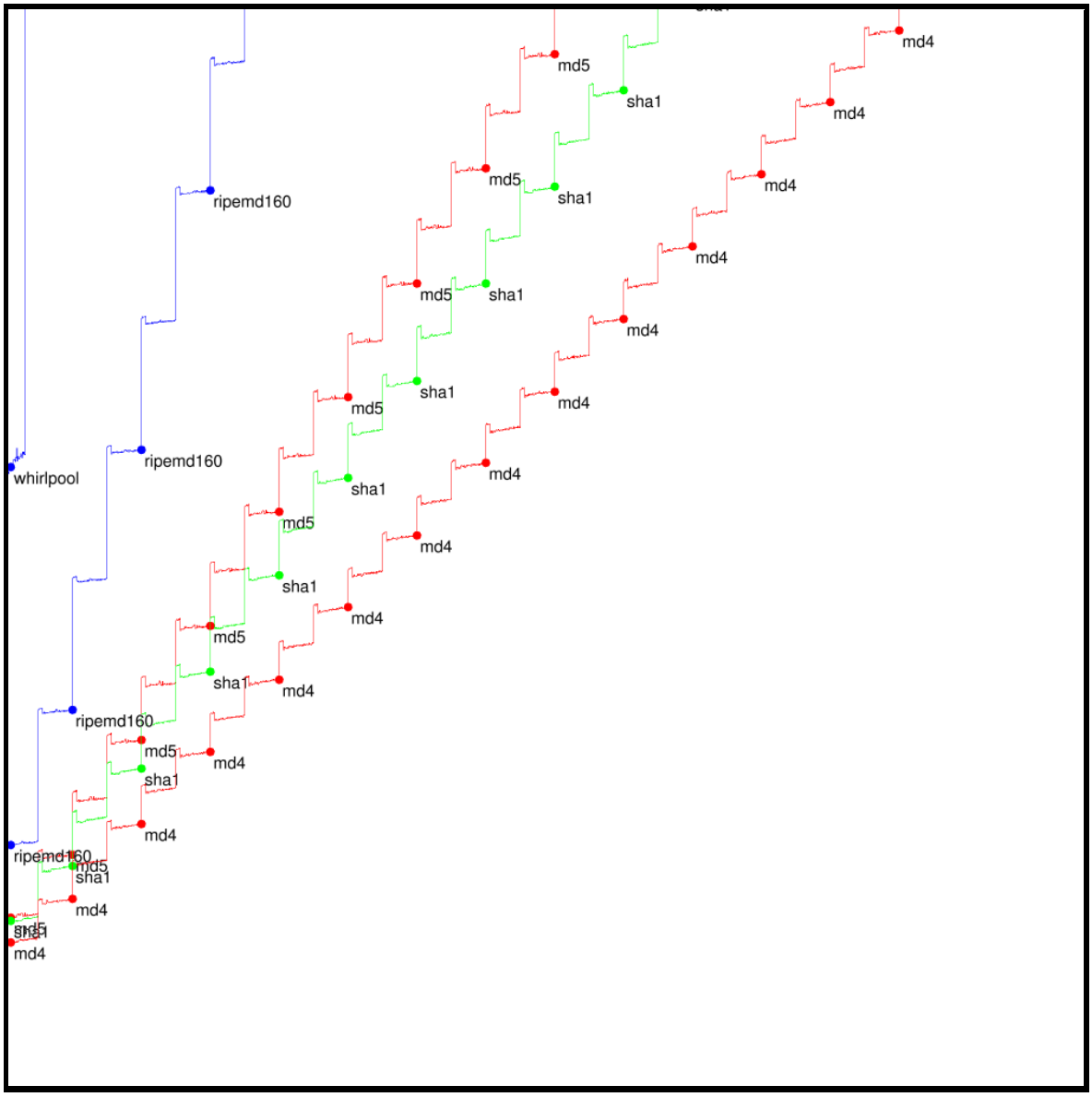
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
15.42	15.42	15.52	`md4`
18.12	18.12	18.23	`sha512`
18.85	18.96	18.96	`md5`
23.23	23.33	23.44	`sha1`
25.62	25.73	25.73	`sha256`
46.46	46.46	46.56	`ripemd160`
72.71	73.65	75.31	`whirlpool`
741.77	742.40	743.12	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
12.23	12.23	12.23	`md4`
16.52	16.60	16.68	`sha512`
17.42	17.42	17.46	`md5`
19.22	19.26	19.30	`sha1`
23.52	23.55	23.63	`sha256`
41.29	41.29	41.29	`ripemd160`
69.45	70.00	70.66	`whirlpool`
713.28	713.98	714.77	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
11.02	11.02	11.03	`md4`
15.35	15.38	15.47	`sha512`
16.86	16.88	16.88	`md5`
17.71	17.72	17.74	`sha1`
22.75	22.76	22.78	`sha256`
39.32	39.33	39.35	`ripemd160`
68.03	68.58	69.02	`whirlpool`
702.96	703.68	704.44	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
10.25	10.28	10.34	`md4`
14.56	14.65	14.88	`sha512`
16.49	16.55	16.55	`md5`
16.76	16.82	16.88	`sha1`
22.18	22.27	22.32	`sha256`
38.12	38.17	38.20	`ripemd160`
65.98	68.00	69.43	`whirlpool`
695.13	697.50	699.93	`md2`

6.18 ppc32, 2097MHz, IBM POWER5, nmi0154



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
330.00	332.50	336.00	`md4`
378.50	381.00	385.00	`sha1`
387.50	391.00	392.50	`md5`
557.00	559.50	562.00	`ripemd160`
1429.00	1437.00	1452.50	`whirlpool`
2994.00	3000.00	3008.50	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
52.31	52.69	53.31	`md4`
61.81	62.00	62.62	`sha1`
65.38	65.75	66.00	`md5`
107.75	108.00	108.44	`ripemd160`
359.19	360.88	363.44	`whirlpool`
1017.50	1018.50	1020.06	`md2`

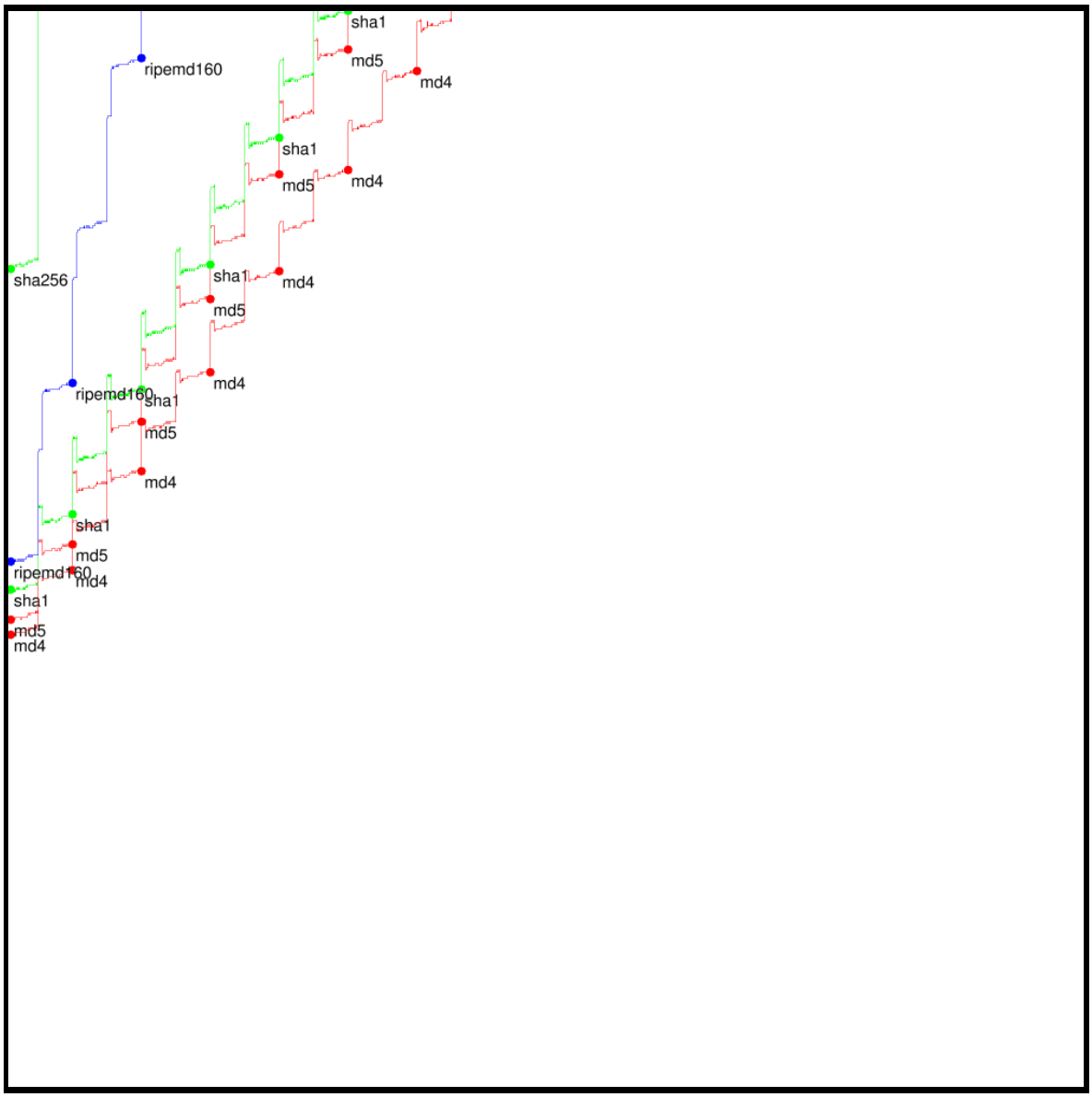
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
15.15	15.23	15.34	`md4`
19.37	19.41	19.44	`sha1`
22.01	22.05	22.10	`md5`
45.39	45.42	45.48	`ripemd160`
202.44	203.49	204.54	`whirlpool`
684.28	684.84	685.90	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
12.24	12.25	12.30	`md4`
16.05	16.06	16.08	`sha1`
18.62	18.63	18.65	`md5`
40.51	40.53	40.56	`ripemd160`
189.57	190.05	190.96	`whirlpool`
658.61	659.38	659.77	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
11.13	11.14	11.15	`md4`
14.80	14.81	14.83	`sha1`
17.35	17.36	17.37	`md5`
38.67	38.69	38.71	`ripemd160`
185.78	186.13	186.66	`whirlpool`
649.14	649.32	649.50	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
10.41	10.46	10.51	`md4`
14.02	14.06	14.10	`sha1`
16.56	16.60	16.63	`md5`
37.51	37.59	37.64	`ripemd160`
181.29	182.94	185.16	`whirlpool`
642.74	643.28	644.27	`md2`

6.19 ppc32, 3192MHz, IBM Cell PPE, nmips3



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
1050.00	1050.00	1050.00	`md4`
1080.00	1085.00	1085.00	`md5`
1155.00	1155.00	1155.00	`sha1`
1215.00	1220.00	1220.00	`ripemd160`
1900.00	1905.00	1905.00	`sha256`
5325.00	5325.00	8530.00	`whirlpool`
7360.00	7360.00	7365.00	`md2`
7755.00	7760.00	7765.00	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
146.88	146.88	146.88	`md4`
154.38	154.38	154.38	`md5`
162.50	163.12	163.12	`sha1`
200.62	201.25	201.25	`ripemd160`
330.00	330.00	330.62	`sha256`
969.38	969.38	970.00	`sha512`
1517.50	1518.12	1518.12	`whirlpool`
2376.25	2376.25	2376.25	`md2`

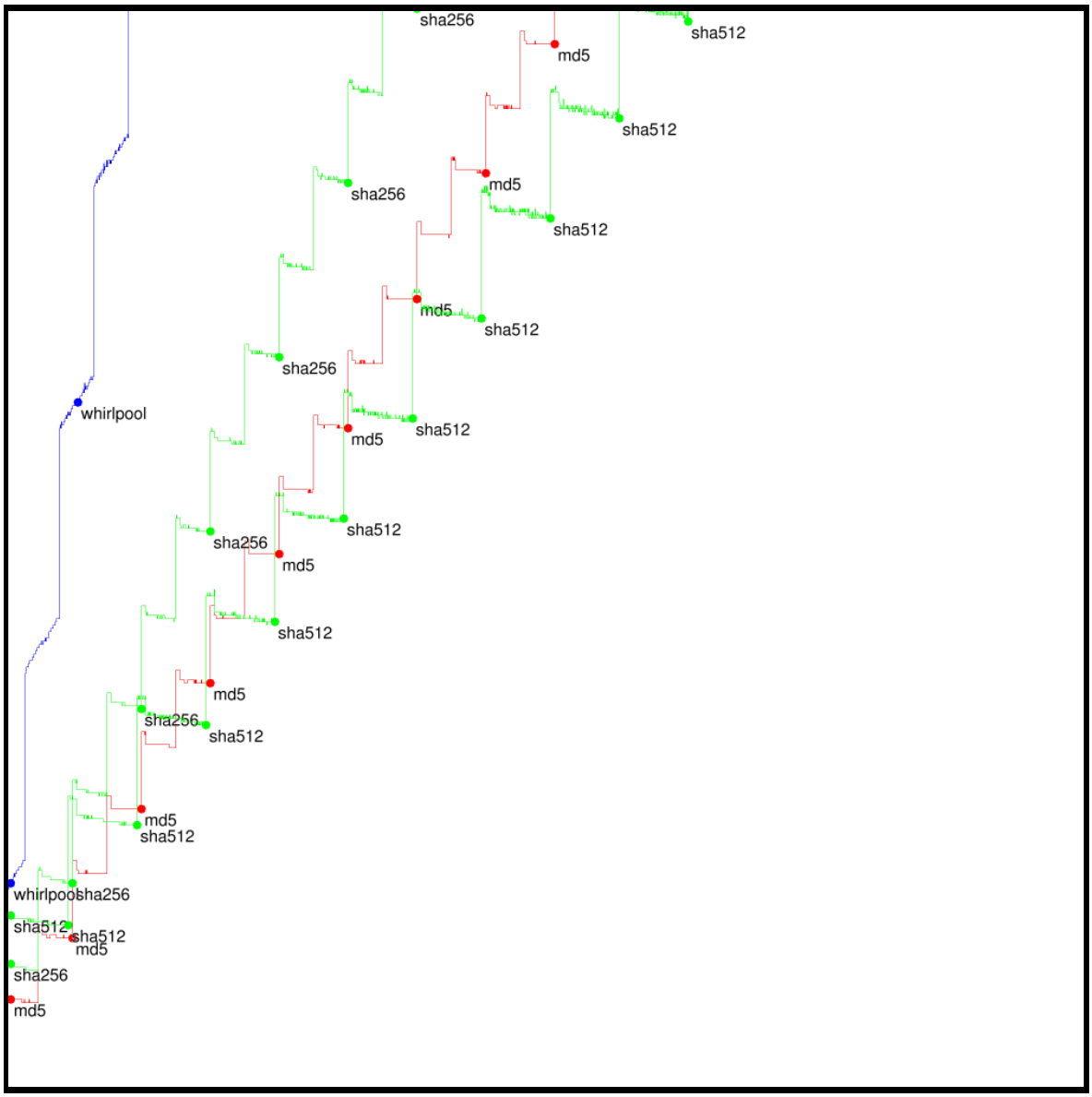
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
29.17	29.24	29.24	`md4`
33.12	33.12	33.19	`md5`
34.31	34.38	34.38	`sha1`
64.31	64.31	64.31	`ripemd160`
116.94	116.94	117.01	`sha256`
418.61	418.68	418.75	`sha512`
960.90	1307.57	1414.65	`whirlpool`
1557.64	1560.42	1573.33	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
20.00	20.00	20.00	`md4`
23.65	23.65	27.99	`md5`
24.27	24.30	24.30	`sha1`
53.57	53.59	53.59	`ripemd160`
100.31	100.31	100.31	`sha256`
388.25	388.28	390.00	`sha512`
916.88	921.04	941.35	`whirlpool`
1493.67	1495.13	1498.83	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
16.55	16.55	16.56	`md4`
20.08	20.08	20.08	`md5`
20.52	20.52	20.53	`sha1`
49.61	49.62	61.64	`ripemd160`
94.06	94.07	94.07	`sha256`
362.52	363.10	365.01	`sha512`
902.13	904.08	969.35	`whirlpool`
1471.87	1472.59	1472.99	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
11.35	14.49	14.51	`md4`
17.93	17.95	17.95	`md5`
18.24	18.26	18.28	`sha1`
47.23	47.27	71.31	`ripemd160`
90.23	90.33	90.33	`sha256`
346.02	348.22	352.07	`sha512`
888.55	895.62	1028.14	`whirlpool`
1454.61	1457.85	1461.80	`md2`

6.20 ppc64, 2000MHz, IBM PowerPC G5 970, geespaz



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
195.00	202.50	202.50	`md5`
277.50	277.50	285.00	`sha256`
390.00	390.00	397.50	`sha512`
472.50	480.00	480.00	`whirlpool`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
44.06	44.06	44.06	`md5`
47.81	47.81	48.75	`sha512`
60.94	60.94	60.94	`sha256`
127.50	128.44	129.38	`whirlpool`

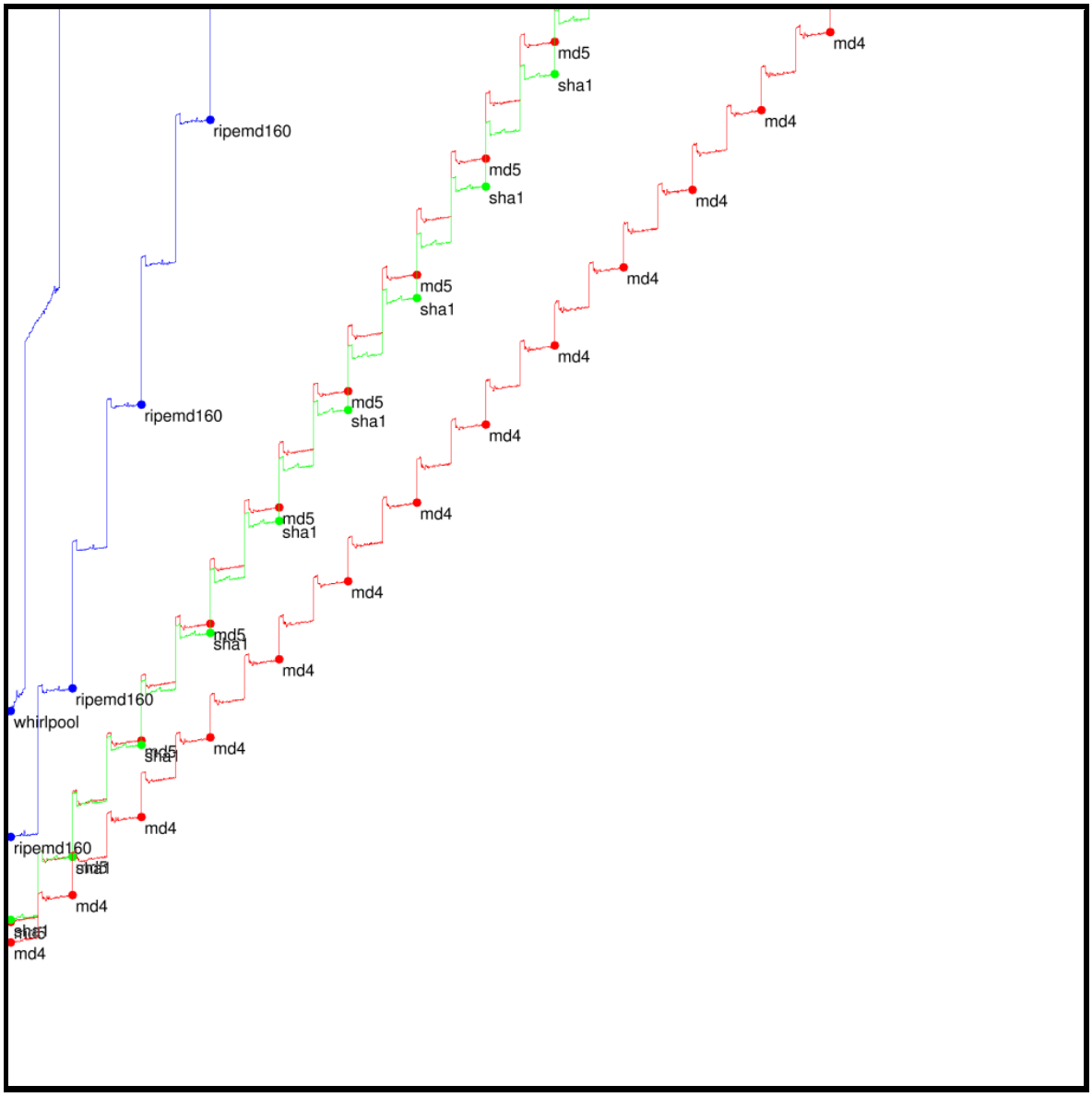
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
18.33	18.44	18.54	`sha512`
21.25	21.35	21.35	`md5`
29.38	29.38	29.58	`sha256`
76.46	76.67	76.88	`whirlpool`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
16.68	16.72	16.84	`sha512`
19.57	19.57	19.61	`md5`
26.84	26.91	26.99	`sha256`
72.38	72.58	72.77	`whirlpool`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
15.41	15.45	15.53	`sha512`
18.93	18.93	18.93	`md5`
25.93	25.96	26.02	`sha256`
70.91	71.16	71.37	`whirlpool`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
14.41	14.62	14.85	`sha512`
18.52	18.52	18.54	`md5`
25.25	25.37	25.55	`sha256`
69.84	70.55	71.02	`whirlpool`

6.21 ppc64, 2097MHz, IBM POWER5, nmi0154



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
331.50	333.50	336.00	`md4`
379.50	381.00	385.00	`md5`
384.00	385.50	388.00	`sha1`
576.00	578.50	580.50	`ripemd160`
877.50	882.50	889.00	`whirlpool`
2873.00	2879.00	2885.00	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
53.88	54.25	55.00	`md4`
64.81	65.12	65.50	`sha1`
65.00	65.94	66.62	`md5`
113.81	114.06	114.38	`ripemd160`
223.38	224.31	226.94	`whirlpool`
980.12	981.44	982.81	`md2`

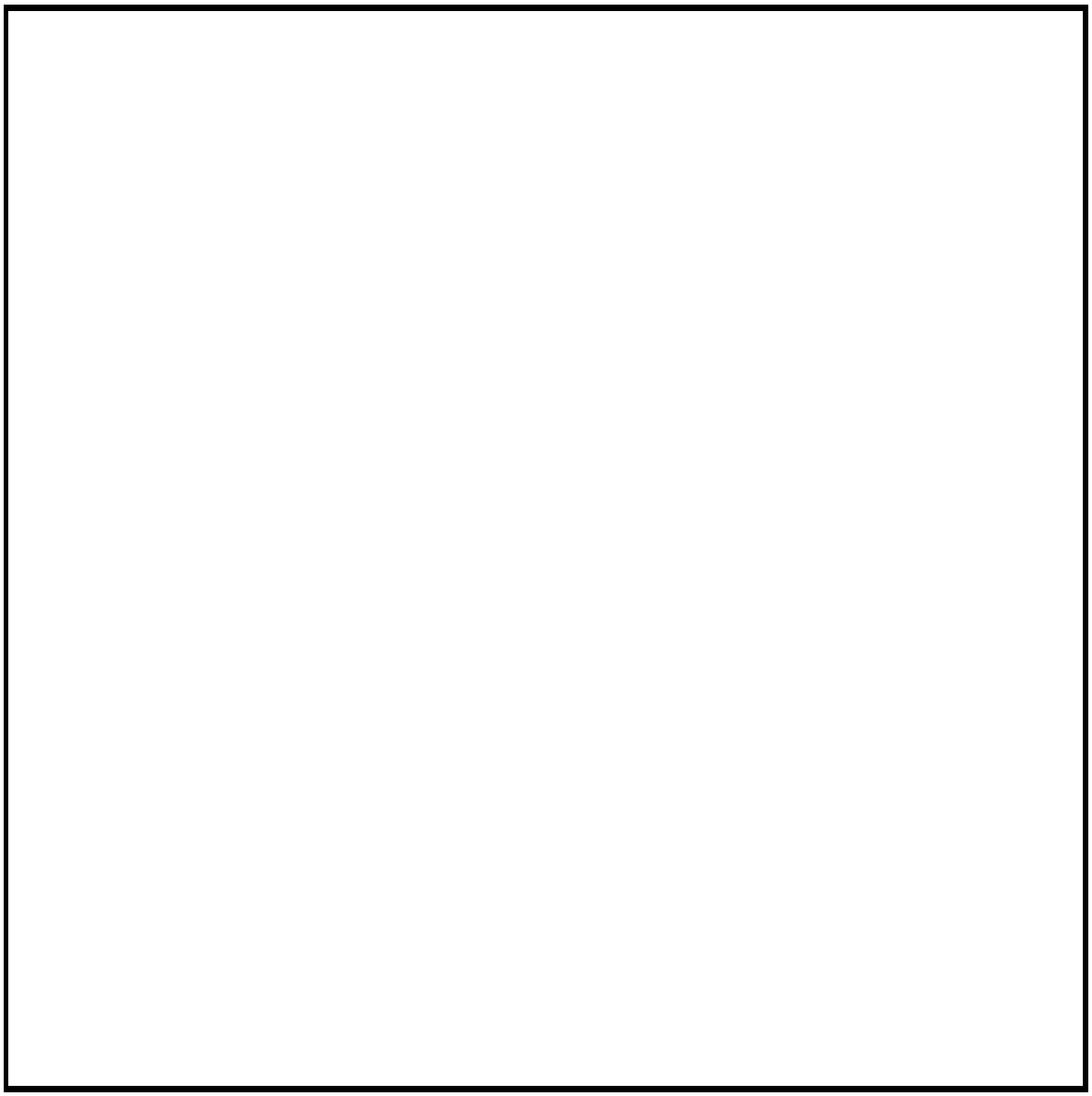
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
16.11	16.19	16.26	`md4`
21.58	21.60	21.64	`sha1`
22.24	22.31	22.40	`md5`
49.31	49.34	49.40	`ripemd160`
128.11	128.60	128.78	`whirlpool`
660.32	660.69	661.35	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
13.14	13.18	13.20	`md4`
18.23	18.24	18.25	`sha1`
18.89	18.92	18.95	`md5`
44.28	44.30	44.33	`ripemd160`
120.84	121.08	122.25	`whirlpool`
635.51	636.09	636.69	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
12.05	12.06	12.08	`md4`
16.97	16.97	16.98	`sha1`
17.64	17.64	17.66	`md5`
42.41	42.43	42.47	`ripemd160`
118.06	118.40	118.80	`whirlpool`
626.50	626.69	626.97	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
11.34	11.39	11.46	`md4`
16.19	16.21	16.24	`sha1`
16.84	16.87	16.91	`md5`
41.25	41.30	41.39	`ripemd160`
115.70	116.74	117.78	`whirlpool`
620.21	620.82	621.89	`md2`

6.22 ppc64, 3192MHz, IBM Cell PPE, `nmips3`



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
4585.00	4590.00	4600.00	`whirlpool`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
1351.25	1351.88	1353.75	`whirlpool`

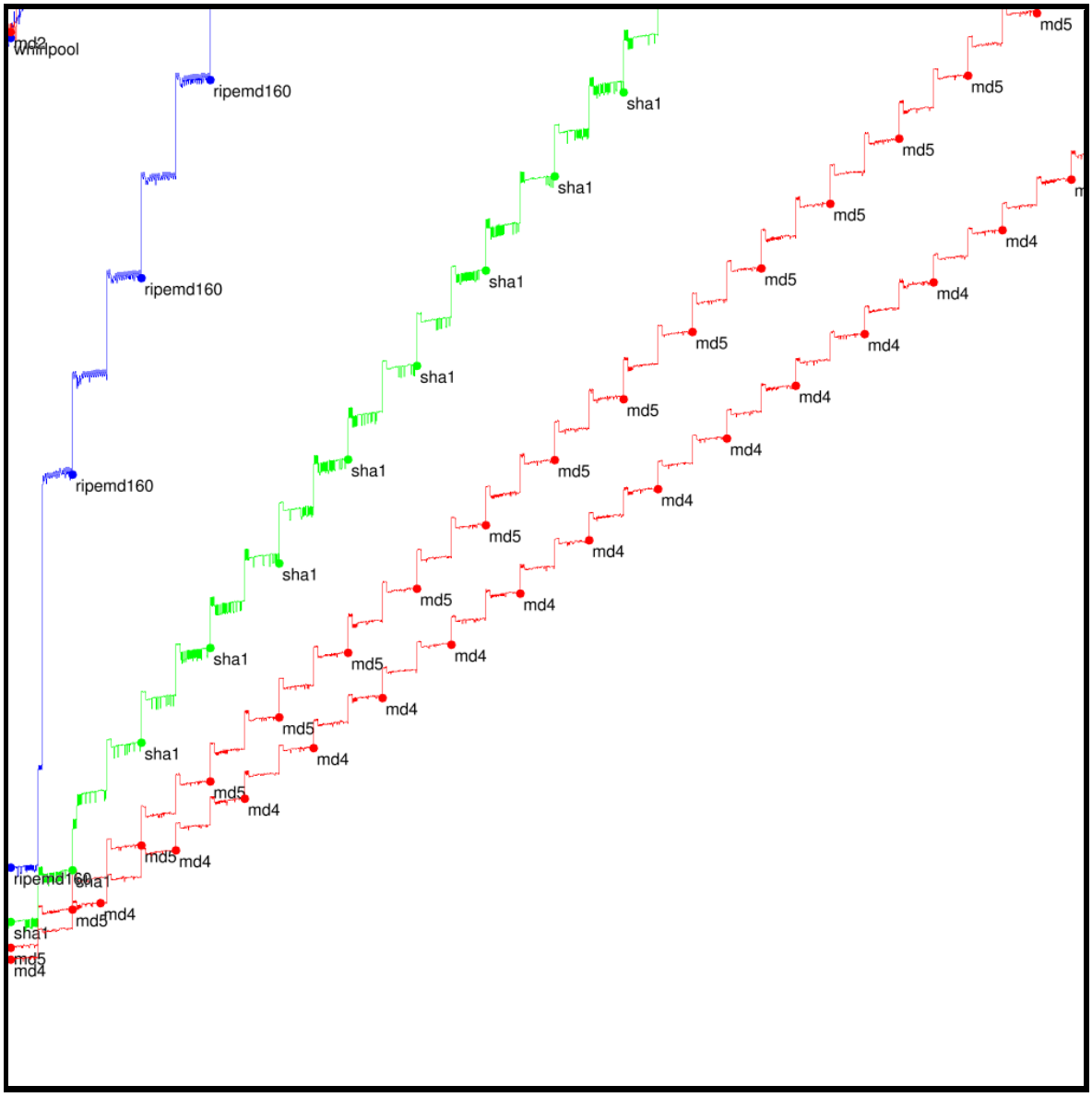
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
878.96	879.17	879.38	`whirlpool`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
842.29	842.42	844.09	`whirlpool`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
828.98	830.53	831.24	`whirlpool`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
817.32	824.12	825.88	`whirlpool`

6.23 sparcv9, 300MHz, Sun UltraSPARC IIi, nmi0096



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
294.50	295.00	296.25	`md4`
313.75	322.00	322.75	`md5`
381.75	382.25	383.00	`sha1`
508.00	508.75	510.00	`ripemd160`
2433.50	2457.50	2458.75	`whirlpool`
2462.50	2464.25	2473.00	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
44.44	44.53	44.59	`md4`
49.66	49.72	49.81	`md5`
58.75	58.81	59.00	`sha1`
173.19	174.66	174.94	`ripemd160`
614.78	622.81	628.75	`whirlpool`
823.72	824.88	828.94	`md2`

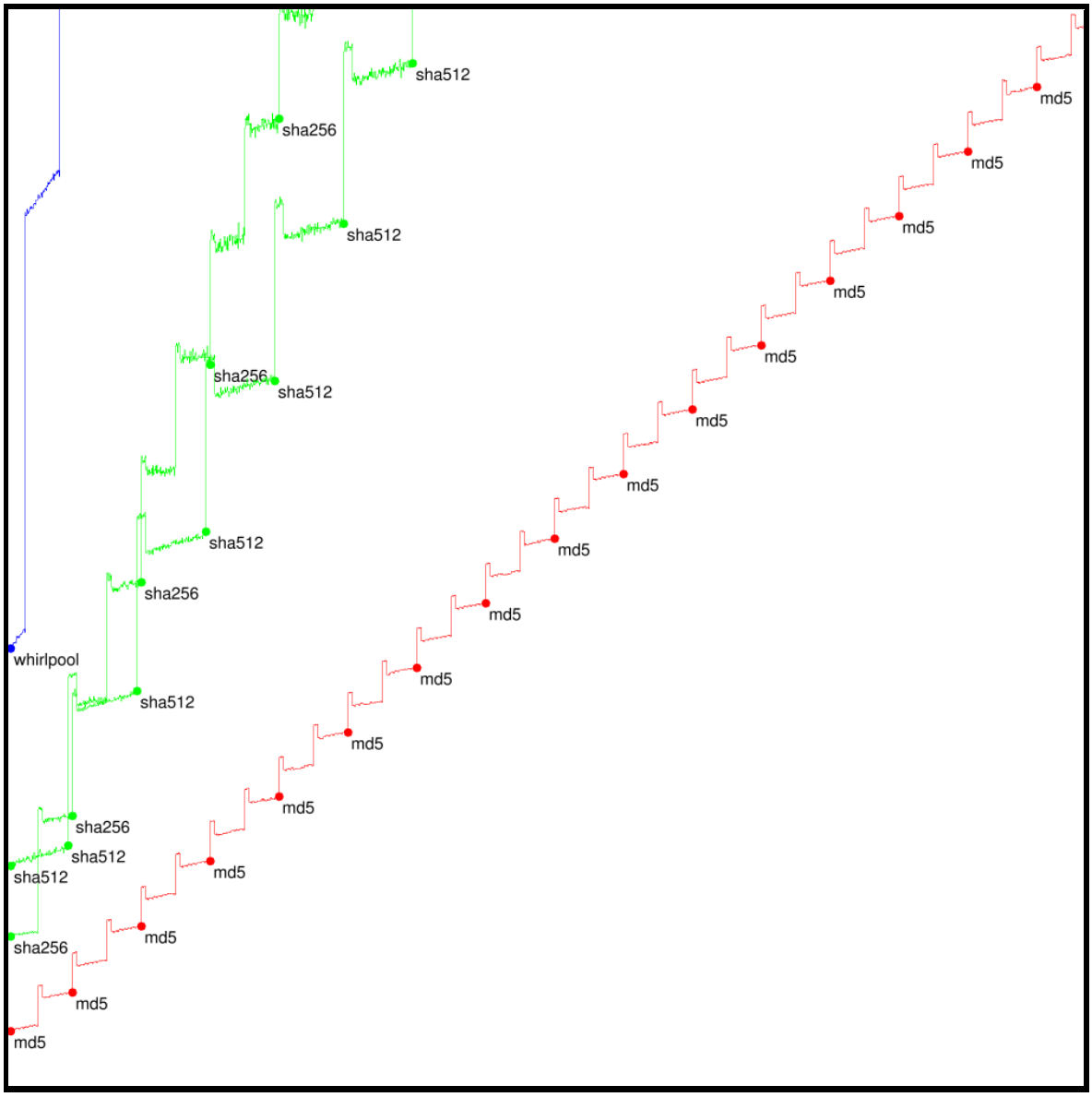
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
11.58	11.60	11.61	`md4`
13.80	13.81	13.81	`md5`
19.77	19.78	19.79	`sha1`
44.86	44.86	44.87	`ripemd160`
352.78	354.01	354.96	`whirlpool`
549.30	550.16	552.69	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
9.04	9.05	9.05	`md4`
11.01	11.01	11.02	`md5`
16.09	16.09	16.10	`sha1`
34.76	34.77	34.77	`ripemd160`
332.60	332.66	333.24	`whirlpool`
529.02	533.74	553.71	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
8.08	8.09	8.09	`md4`
9.95	9.95	9.96	`md5`
14.60	14.60	14.60	`sha1`
30.94	30.94	30.94	`ripemd160`
325.01	325.33	337.72	`whirlpool`
526.89	530.52	532.73	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
7.50	7.51	7.53	`md4`
9.32	9.32	9.33	`md5`
13.70	13.71	13.71	`sha1`
28.64	28.65	28.65	`ripemd160`
303.30	321.41	346.49	`whirlpool`
511.98	532.34	539.48	`md2`

6.24 sparcv9, 900MHz, Sun UltraSPARC III, nmi0051



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
127.12	128.62	130.38	`md5`
347.50	348.50	357.25	`sha256`
506.88	515.00	604.38	`sha512`
1017.38	1023.62	1031.62	`whirlpool`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
25.55	25.64	26.22	`md5`
66.03	66.61	76.86	`sha512`
76.73	77.31	77.67	`sha256`
258.30	259.09	260.08	`whirlpool`

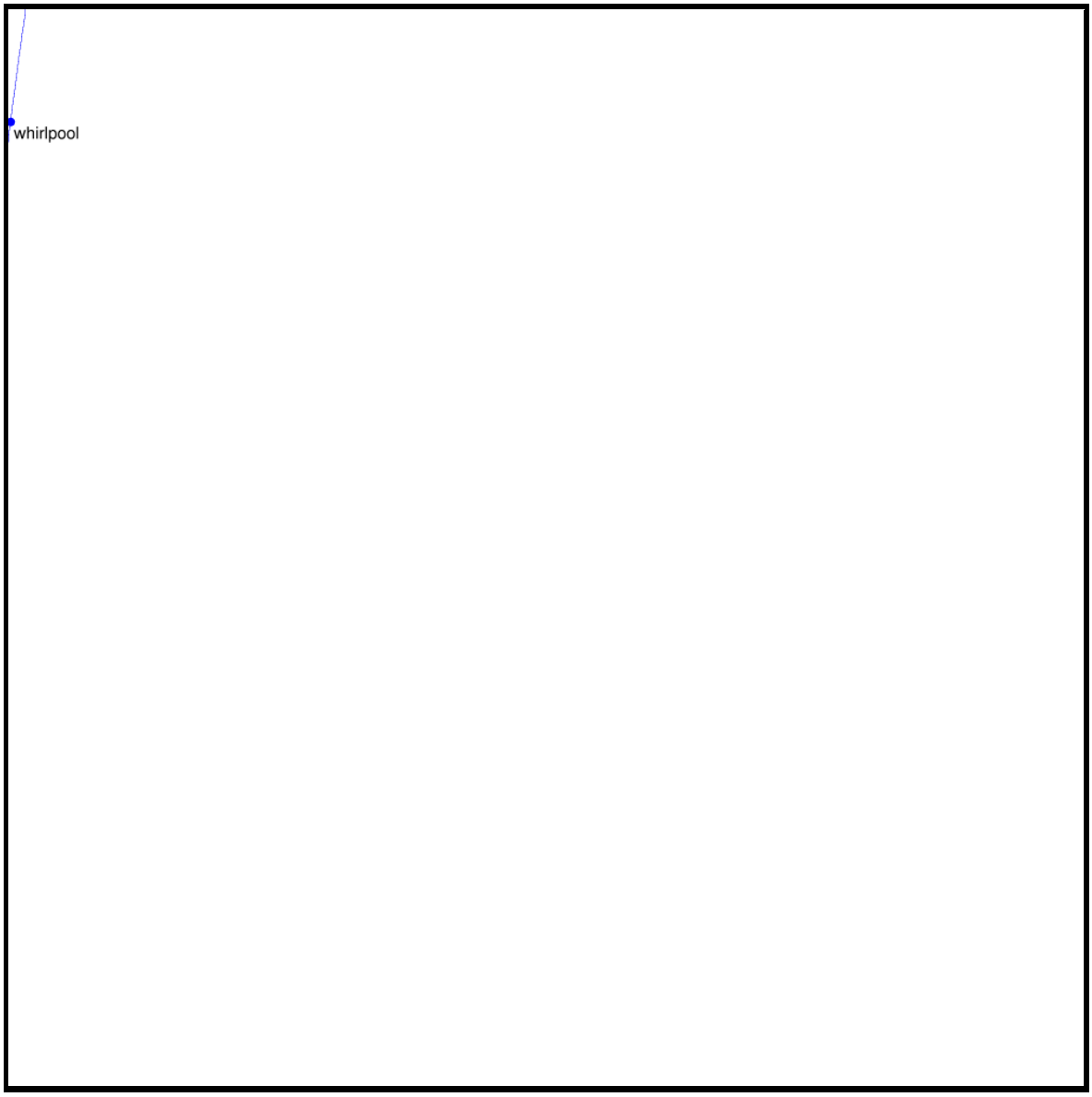
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
11.22	11.23	11.27	`md5`
27.43	27.65	27.84	`sha512`
38.07	38.25	38.34	`sha256`
146.26	146.31	146.48	`whirlpool`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
10.06	10.07	10.07	`md5`
25.43	25.50	25.62	`sha512`
35.06	35.20	35.82	`sha256`
137.55	137.69	137.79	`whirlpool`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
9.62	9.62	9.63	`md5`
23.74	23.79	23.93	`sha512`
33.49	33.87	34.09	`sha256`
134.09	134.28	134.35	`whirlpool`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
9.34	9.36	9.36	`md5`
22.49	22.68	22.98	`sha512`
32.42	33.34	33.79	`sha256`
131.68	132.19	132.46	`whirlpool`

6.25 sparcv9, 1200MHz, Sun UltraSPARC III, nmisolaris10



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
2277.50	2278.25	2282.50	`whirlpool`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
601.47	601.92	608.19	`whirlpool`

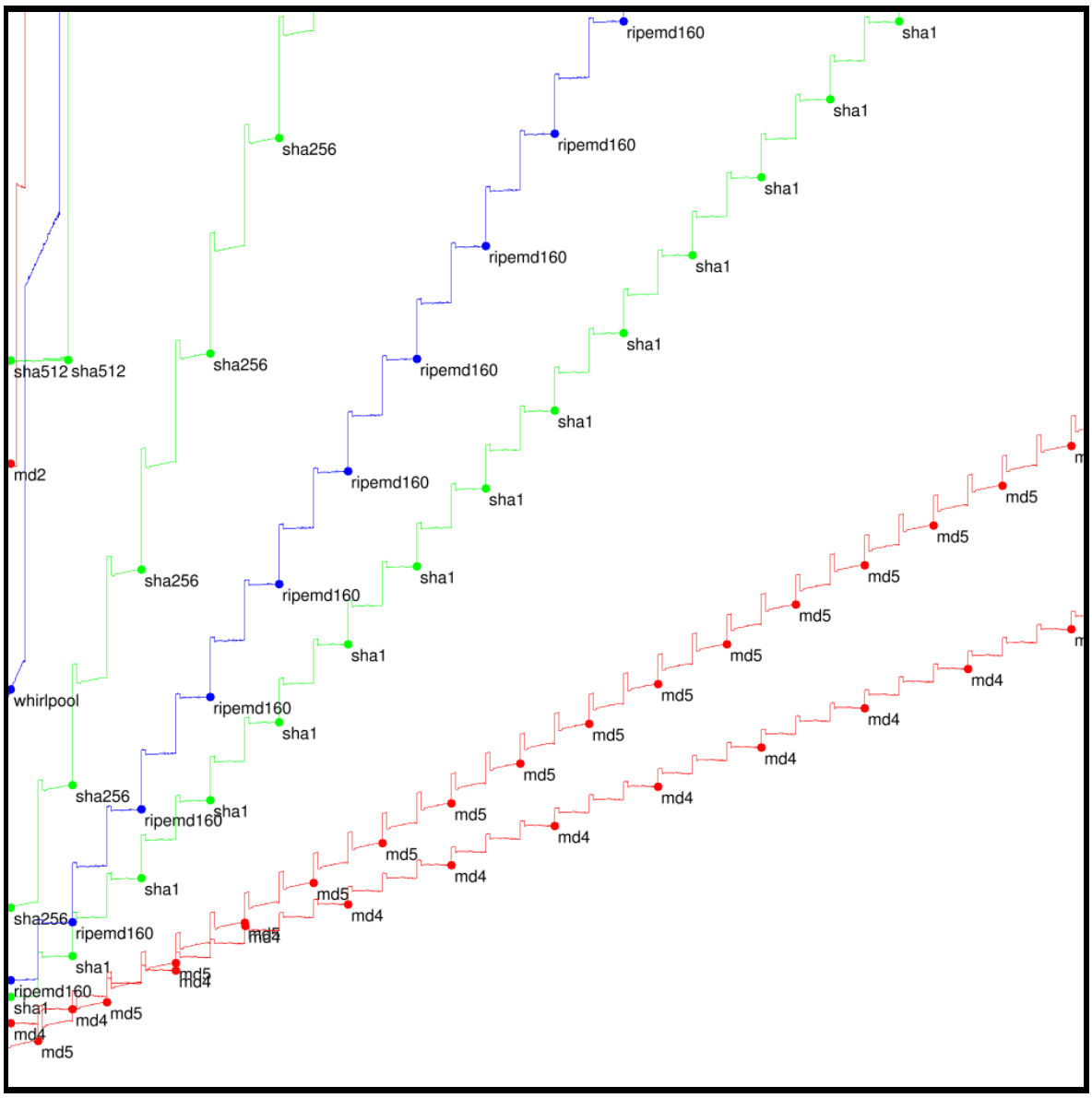
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
356.04	356.05	356.08	`whirlpool`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
336.80	336.81	337.00	`whirlpool`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
329.49	329.59	329.74	`whirlpool`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
324.16	325.27	325.64	`whirlpool`

6.26 x86, 1196MHz, Intel Celeron (6b1), `vieux`



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
96.25	96.25	96.25	`md5`
147.38	147.38	147.38	`md4`
208.88	208.88	208.88	`sha1`
247.50	247.50	247.50	`ripemd160`
420.12	420.12	420.12	`sha256`
928.25	930.62	931.00	`whirlpool`
1447.38	1448.62	1448.75	`md2`
1689.25	1689.25	1689.25	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
17.25	17.25	17.25	`md5`
22.36	22.36	22.36	`md4`
37.52	37.52	37.52	`sha1`
47.27	47.27	47.27	`ripemd160`
86.27	86.27	86.27	`sha256`
210.97	210.97	211.11	`sha512`
242.81	243.33	243.73	`whirlpool`
504.94	505.03	505.41	`md2`

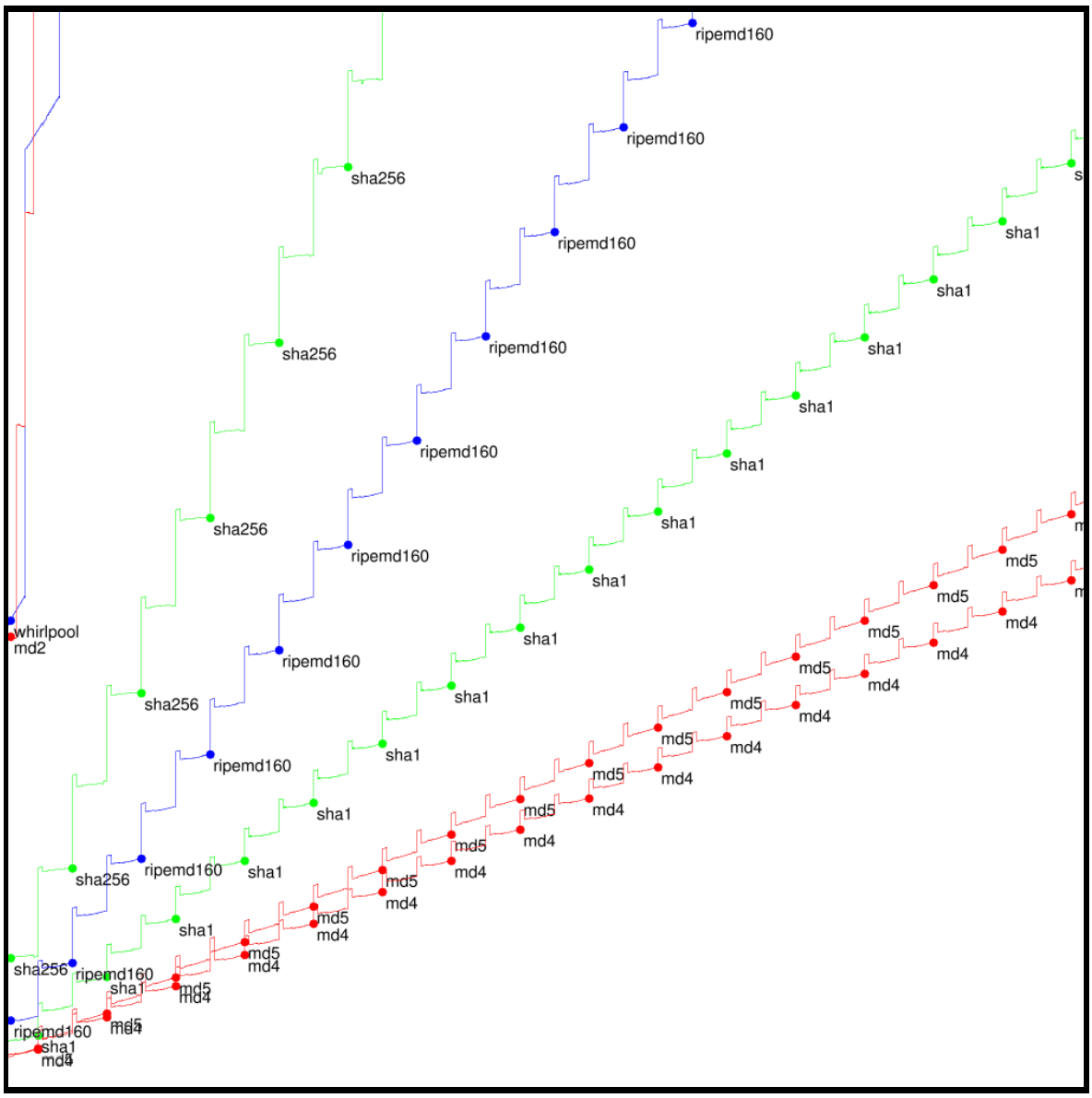
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
5.88	5.88	5.88	`md4`
7.04	7.04	7.04	`md5`
14.24	14.24	14.24	`sha1`
19.82	19.82	19.86	`ripemd160`
37.45	37.45	37.45	`sha256`
98.64	98.64	98.69	`sha512`
141.65	141.68	141.73	`whirlpool`
343.90	344.04	344.13	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
4.58	4.58	4.58	`md4`
6.24	6.24	6.24	`md5`
12.41	12.41	12.41	`sha1`
17.66	17.66	17.67	`ripemd160`
33.63	33.63	33.63	`sha256`
93.10	93.10	93.14	`sha512`
133.60	133.66	133.77	`whirlpool`
331.35	331.39	331.45	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
4.10	4.10	4.10	`md4`
5.95	5.95	5.95	`md5`
11.72	11.72	11.73	`sha1`
16.85	16.85	16.85	`ripemd160`
32.19	32.19	32.19	`sha256`
87.49	87.49	87.51	`sha512`
130.79	130.82	130.88	`whirlpool`
326.70	326.71	327.89	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
3.80	3.80	3.80	`md4`
5.77	5.77	5.77	`md5`
11.31	11.31	11.31	`sha1`
16.36	16.37	16.37	`ripemd160`
31.33	31.33	31.33	`sha256`
84.11	84.11	84.16	`sha512`
128.97	129.06	129.22	`whirlpool`
323.72	323.90	326.30	`md2`

6.27 x86, 1403MHz, AMD Opteron 240 (f58), nmisles8amd64


ripemd160
ripemd160
sha256
ripemd160
sha1
sha1
sha256
ripemd160
sha1
sha1
ripemd160
sha1
sha256
ripemd160
sha1
whirlpool
md2
ripemd160
sha1
sha256
sha1
ripemd160
sha1
sha256
ripemd160
sha1
sha1
sha256
ripemd160
sha1
md5
md4
md5
md4
md5
md4

Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
67.75	71.75	71.75	`md5`
69.38	76.50	76.50	`md4`
108.62	109.00	110.38	`sha1`
154.75	154.75	154.88	`ripemd160`
299.88	299.88	299.88	`sha256`
1044.75	1045.12	1045.38	`md2`
1092.50	1092.62	1092.75	`whirlpool`
3556.00	3558.25	3561.62	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
13.64	13.73	13.94	`md5`
14.12	14.12	14.12	`md4`
21.98	22.00	22.31	`sha1`
34.48	34.48	34.52	`ripemd160`
62.56	62.56	62.58	`sha256`
279.55	279.56	279.88	`whirlpool`
377.47	377.52	377.66	`md2`
452.23	452.47	452.94	`sha512`

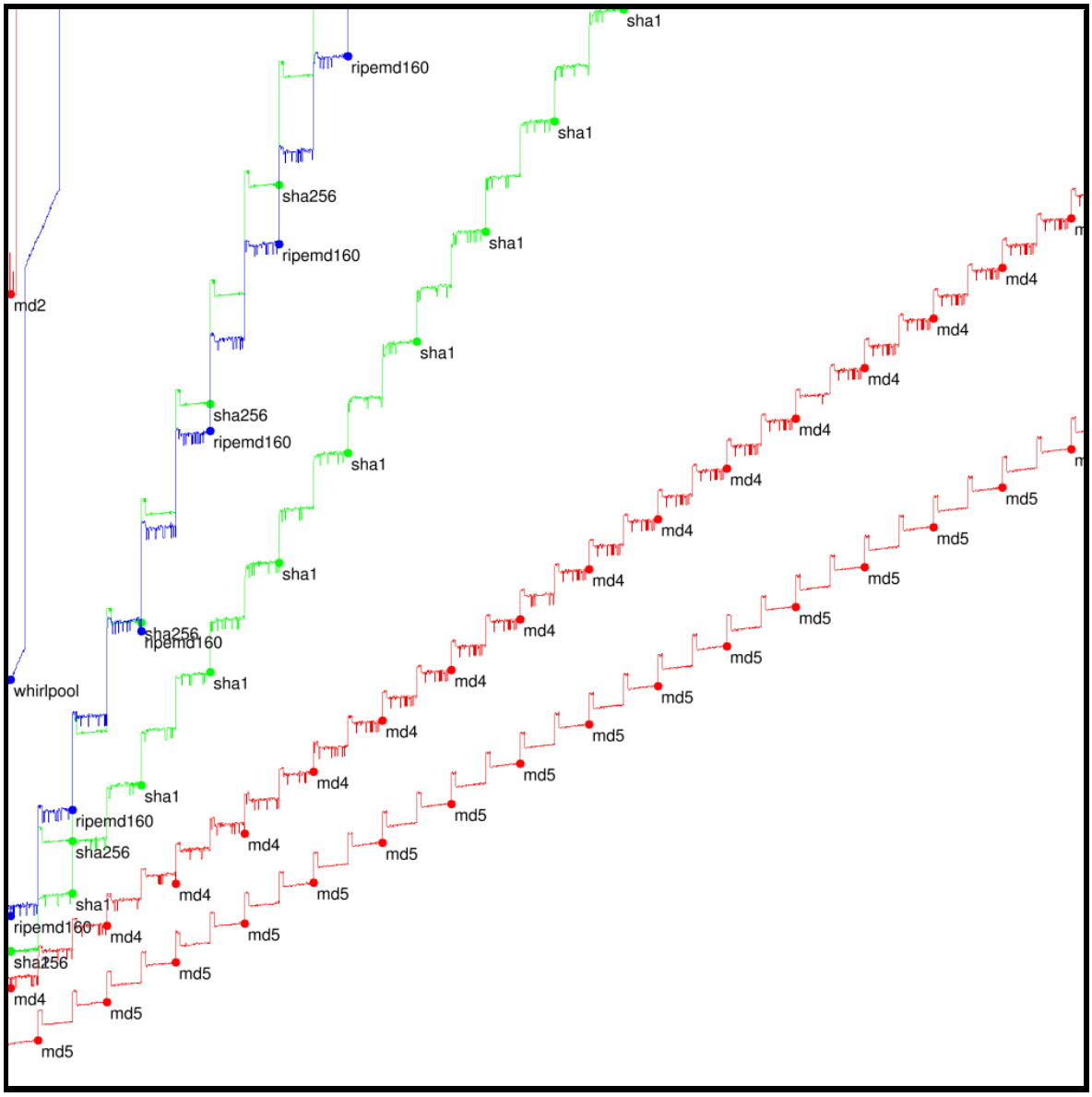
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
5.59	5.60	5.60	`md4`
6.06	6.12	6.12	`md5`
9.91	9.94	9.94	`sha1`
17.34	17.34	17.34	`ripemd160`
29.50	29.50	29.50	`sha256`
160.27	160.32	160.33	`whirlpool`
226.41	226.44	226.49	`sha512`
260.81	260.84	260.86	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
4.94	4.94	4.94	`md4`
5.51	5.54	5.54	`md5`
9.01	9.02	9.02	`sha1`
15.98	15.98	15.98	`ripemd160`
26.90	26.90	26.90	`sha256`
151.01	151.01	151.02	`whirlpool`
213.97	213.99	214.01	`sha512`
251.70	251.75	251.76	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
4.68	4.68	4.68	`md4`
5.31	5.31	5.31	`md5`
8.65	8.65	8.65	`sha1`
15.48	15.48	15.48	`ripemd160`
26.00	26.00	26.00	`sha256`
147.44	147.45	147.50	`whirlpool`
201.57	201.58	201.59	`sha512`
248.33	248.33	248.36	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
4.53	4.53	4.53	`md4`
5.17	5.17	5.19	`md5`
8.44	8.44	8.44	`sha1`
15.17	15.17	15.17	`ripemd160`
25.45	25.45	25.45	`sha256`
145.27	145.29	145.43	`whirlpool`
194.11	194.13	194.16	`sha512`
246.25	246.29	246.40	`md2`

6.28 x86, 1833MHz, Intel Core Duo, nmi0068



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
97.62	99.00	99.00	`md5`
251.62	253.00	255.75	`md4`
310.75	312.12	312.12	`sha256`
313.50	313.50	313.50	`sha1`
418.00	418.00	418.00	`ripemd160`
950.12	950.12	950.12	`whirlpool`
1839.75	1839.75	1841.12	`md2`
3564.00	3564.00	3564.00	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
17.70	17.70	17.70	`md5`
38.67	38.84	38.84	`md4`
54.83	54.83	55.17	`sha1`
70.30	70.47	70.47	`sha256`
76.14	76.31	76.31	`ripemd160`
249.22	249.73	249.91	`whirlpool`
453.23	453.23	453.41	`sha512`
618.23	618.23	620.12	`md2`

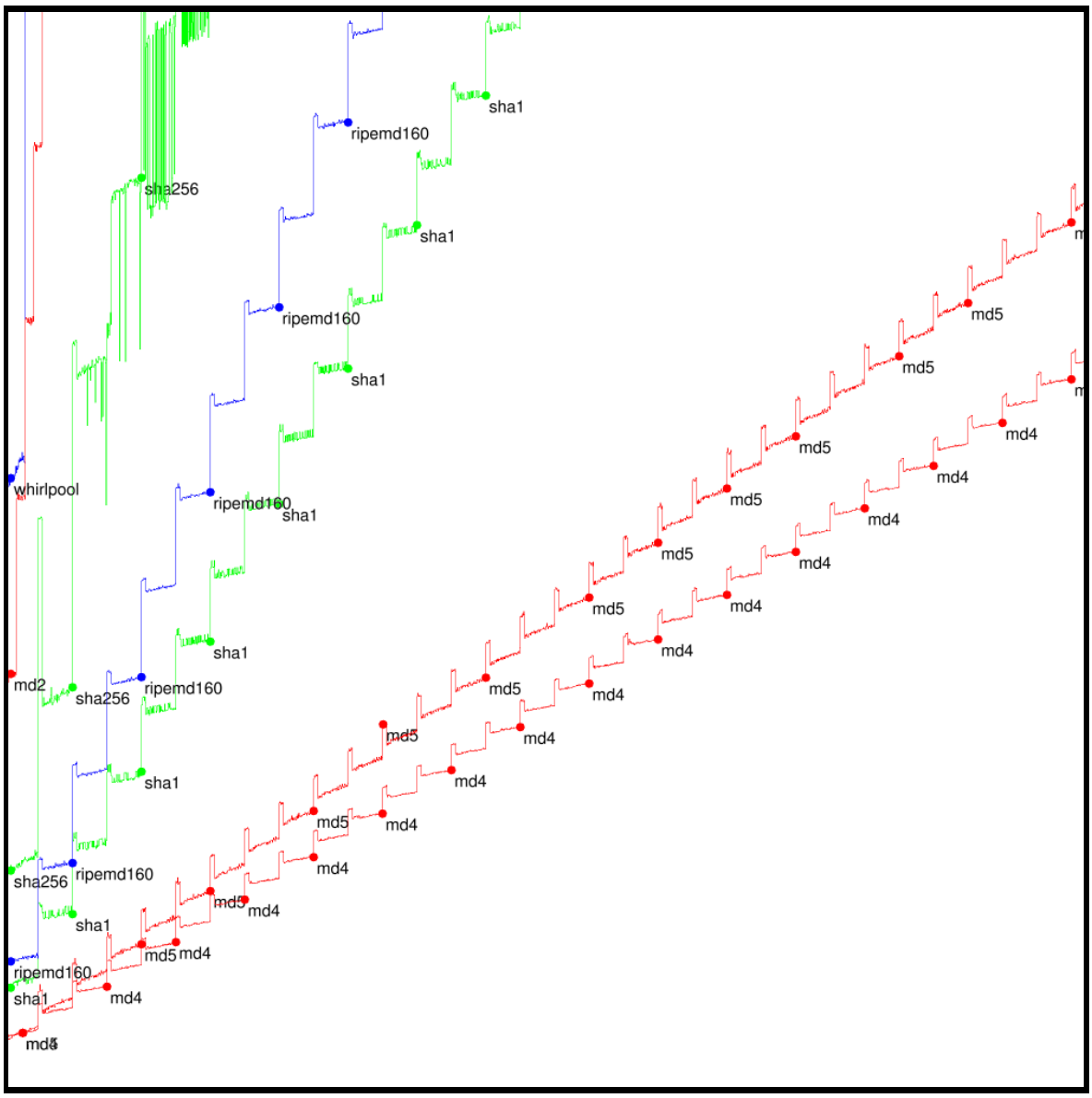
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
7.07	7.07	7.07	`md5`
10.92	10.94	10.94	`md4`
20.26	20.26	20.28	`sha1`
33.15	33.15	33.17	`ripemd160`
36.02	36.04	36.04	`sha256`
145.18	145.22	145.48	`whirlpool`
241.50	241.50	241.50	`sha512`
408.07	408.09	413.82	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
6.24	6.24	6.24	`md5`
8.65	8.65	8.65	`md4`
17.69	17.69	17.69	`sha1`
29.53	29.53	29.53	`ripemd160`
33.37	33.37	33.37	`sha256`
137.04	137.06	137.09	`whirlpool`
233.42	233.43	233.43	`sha512`
391.70	391.70	391.79	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
5.91	5.91	5.91	`md5`
7.80	7.80	7.80	`md4`
16.66	16.66	16.66	`sha1`
28.14	28.14	28.14	`ripemd160`
32.35	32.35	32.35	`sha256`
134.04	134.09	134.14	`whirlpool`
221.81	221.81	221.81	`sha512`
385.84	386.08	389.25	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
5.70	5.70	5.71	`md5`
7.29	7.30	7.30	`md4`
16.06	16.06	16.08	`sha1`
27.31	27.31	27.31	`ripemd160`
31.73	31.73	31.74	`sha256`
132.19	132.31	132.44	`whirlpool`
214.84	214.85	214.86	`sha512`
382.18	382.93	389.27	`md2`

6.29 x86, 2400MHz, Intel Pentium 4 (f24), `nmitest4`


sha1
ripemd160
sha256
sha1
ripemd160
sha1
whirlpool
ripemd160
sha1
sha1
md2
sha256
ripemd160
sha1
sha256
ripemd160
sha1
ripemd160
sha1
md5
md5
md5
md5
md5
md5
md5
md5
md5
md5
md5
md4
md4
md4

Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
117.00	117.50	119.50	`md5`
120.50	120.50	121.50	`md4`
231.00	231.00	241.00	`sha1`
292.50	294.00	295.50	`ripemd160`
507.50	511.00	517.00	`sha256`
956.50	957.00	963.50	`md2`
1405.00	1407.00	1409.00	`whirlpool`
3090.50	3091.00	3094.00	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
21.19	21.44	22.06	`md4`
21.81	21.88	21.94	`md5`
48.56	50.50	50.94	`sha1`
62.88	63.25	63.94	`ripemd160`
109.81	110.56	111.50	`sha256`
324.81	324.94	325.94	`md2`
351.69	353.06	357.06	`whirlpool`
389.88	389.88	390.25	`sha512`

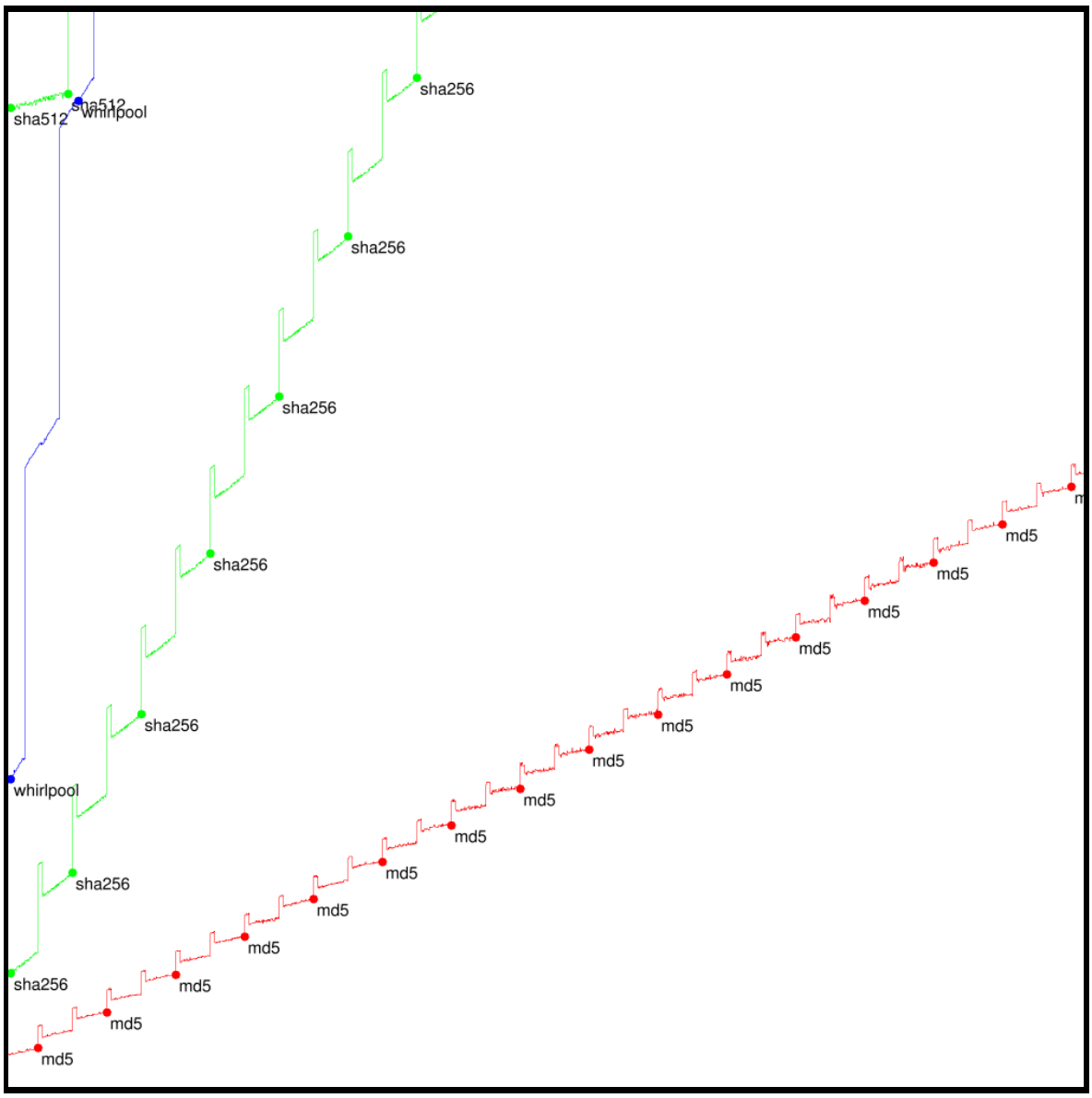
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
7.92	7.96	7.96	`md4`
9.31	9.31	9.37	`md5`
23.02	23.24	23.30	`sha1`
30.90	30.99	31.10	`ripemd160`
54.18	58.81	60.78	`sha256`
190.48	190.49	190.53	`sha512`
199.01	199.18	199.64	`whirlpool`
215.22	215.41	215.55	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
6.92	6.94	6.96	`md4`
8.35	8.35	8.35	`md5`
21.05	21.10	21.12	`sha1`
28.47	28.53	28.57	`ripemd160`
51.91	52.23	53.15	`sha256`
181.32	181.33	181.34	`sha512`
186.92	187.01	187.08	`whirlpool`
207.08	207.71	208.37	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
6.58	6.58	6.61	`md4`
7.98	7.98	7.98	`md5`
20.25	20.28	20.29	`sha1`
27.43	27.51	27.55	`ripemd160`
49.11	49.77	50.38	`sha256`
171.19	171.19	171.20	`sha512`
182.41	182.45	182.71	`whirlpool`
203.78	203.84	205.69	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
6.37	6.40	6.45	`md4`
7.74	7.74	7.76	`md5`
19.71	19.76	19.80	`sha1`
26.69	26.97	27.06	`ripemd160`
46.24	48.55	49.99	`sha256`
165.09	165.11	165.13	`sha512`
179.56	179.69	180.37	`whirlpool`
200.04	200.67	205.72	`md2`

6.30 x86, 2400MHz, Intel Core 2 Duo (6fb), utrecht



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
77.62	78.75	79.88	`md5`
274.50	274.50	277.88	`sha256`
722.25	723.38	724.50	`whirlpool`
2266.88	2279.25	2287.12	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
14.34	14.34	14.48	`md5`
55.41	55.41	55.41	`sha256`
186.61	186.75	186.89	`whirlpool`
285.05	287.02	288.00	`sha512`

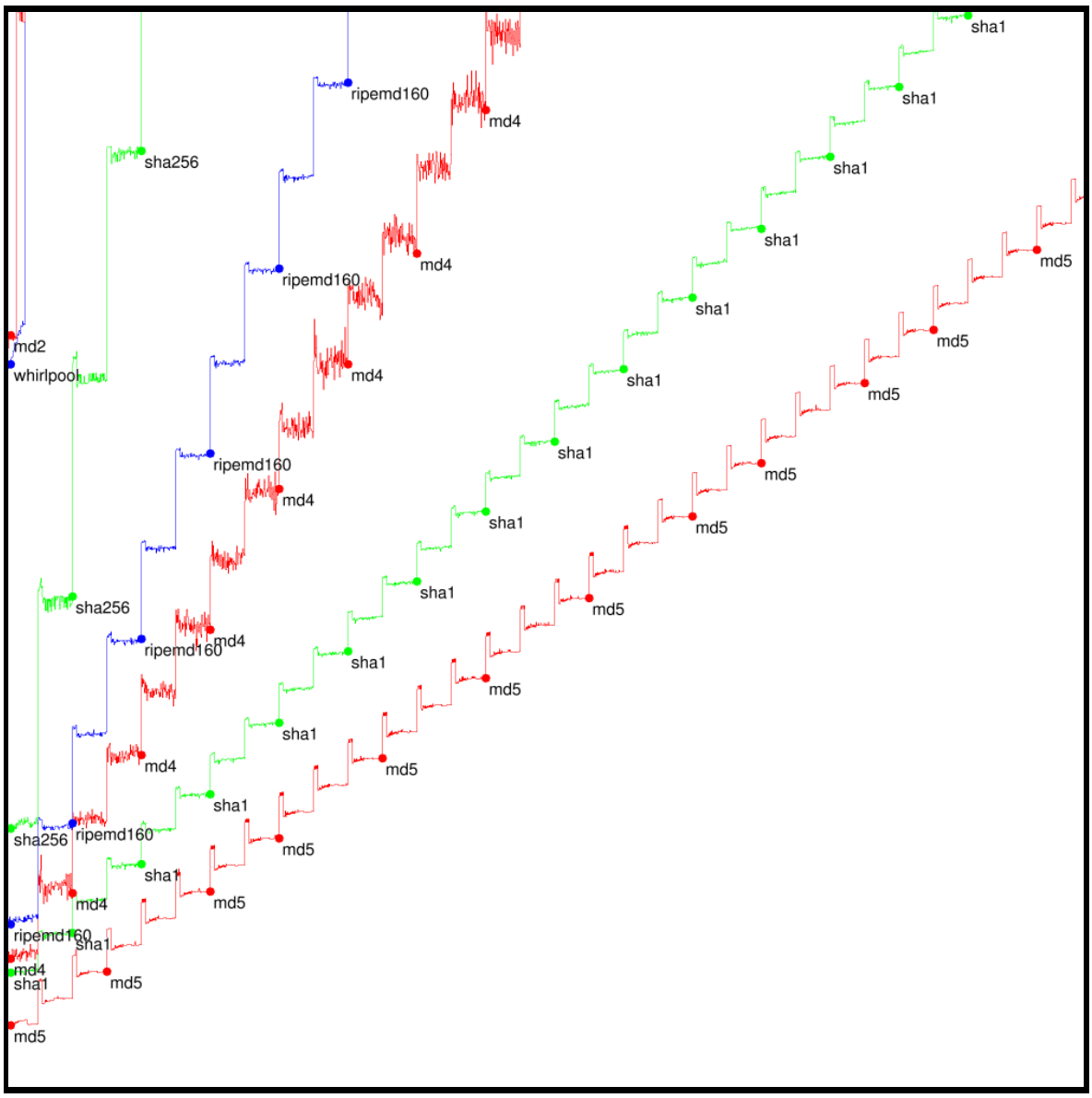
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
6.44	6.44	6.52	`md5`
26.72	26.72	26.72	`sha256`
108.22	108.23	108.25	`whirlpool`
140.20	140.34	140.53	`sha512`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
5.79	5.82	5.87	`md5`
24.57	24.57	24.57	`sha256`
102.02	102.03	102.03	`whirlpool`
133.73	133.80	133.88	`sha512`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
5.58	5.58	5.59	`md5`
23.82	23.83	23.83	`sha256`
99.77	99.77	99.78	`whirlpool`
126.28	126.30	126.32	`sha512`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
5.44	5.44	5.48	`md5`
23.38	23.39	23.39	`sha256`
98.43	98.44	98.58	`whirlpool`
121.71	121.79	121.89	`sha512`

6.31 x86, 2401MHz, Intel Pentium 4 (f24), nmi0086


sha1
sha1
sha1

Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
143.00	143.50	144.50	`md5`
265.00	267.00	268.00	`sha1`
307.50	320.00	337.50	`md4`
386.00	387.00	387.00	`ripemd160`
600.50	605.00	606.00	`sha256`
1695.00	1698.50	1706.50	`whirlpool`
1742.00	1748.00	1757.50	`md2`
2891.50	2891.50	2891.50	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
24.19	24.19	24.19	`md5`
43.12	43.31	44.44	`sha1`
55.56	57.56	60.44	`md4`
75.19	75.19	75.69	`ripemd160`
139.25	142.19	143.25	`sha256`
364.94	364.94	364.94	`sha512`
431.00	431.50	431.88	`whirlpool`
591.31	593.00	593.25	`md2`

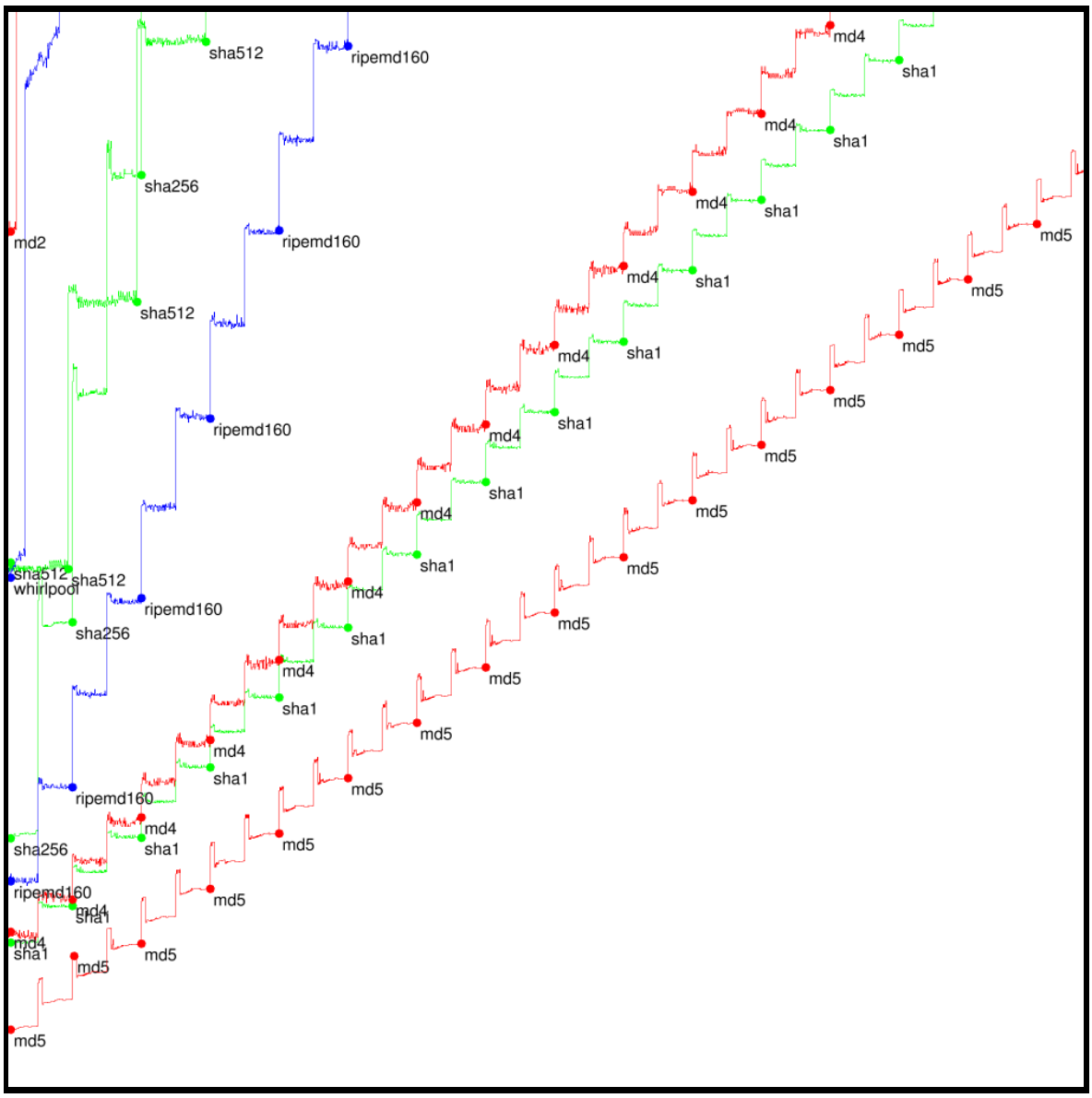
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
9.58	9.58	9.58	`md5`
13.81	13.94	13.97	`sha1`
22.60	23.03	23.75	`md4`
32.29	32.34	32.51	`ripemd160`
72.49	72.97	73.81	`sha256`
189.76	189.76	189.76	`sha512`
243.06	243.38	243.51	`whirlpool`
394.76	394.76	395.67	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
8.45	8.45	8.45	`md5`
11.63	11.63	11.64	`sha1`
20.10	20.25	20.76	`md4`
28.98	28.99	29.01	`ripemd160`
67.15	67.26	68.81	`sha256`
182.86	182.86	182.96	`sha512`
228.69	228.88	231.20	`whirlpool`
379.44	381.19	389.46	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
8.01	8.01	8.01	`md5`
10.74	10.77	10.77	`sha1`
19.56	19.80	19.98	`md4`
27.73	27.73	27.76	`ripemd160`
65.01	65.67	66.11	`sha256`
173.46	174.42	176.84	`sha512`
223.49	224.46	226.97	`whirlpool`
374.93	376.42	377.99	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
7.75	7.75	7.75	`md5`
10.19	10.25	10.26	`sha1`
18.39	19.18	19.98	`md4`
26.96	26.97	27.04	`ripemd160`
62.35	64.92	65.96	`sha256`
165.91	169.74	174.57	`sha512`
218.06	221.96	227.34	`whirlpool`
366.89	374.54	378.88	`md2`

6.32 x86, 2658MHz, Intel Xeon (f25), nmi0013



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
131.00	133.00	133.50	`md5`
334.50	336.50	337.00	`sha1`
345.00	350.00	354.00	`md4`
474.50	484.00	488.00	`ripemd160`
579.50	579.50	580.50	`sha256`
1198.50	1200.50	1211.50	`whirlpool`
1215.50	1220.50	1220.50	`sha512`
1981.50	1987.00	1989.00	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
23.94	23.94	23.94	`md5`
52.12	52.12	52.25	`sha1`
53.81	54.25	54.31	`md4`
86.19	86.31	86.94	`ripemd160`
134.00	134.19	134.38	`sha256`
150.19	150.75	150.75	`sha512`
297.31	298.00	298.75	`whirlpool`
647.25	649.12	649.12	`md2`

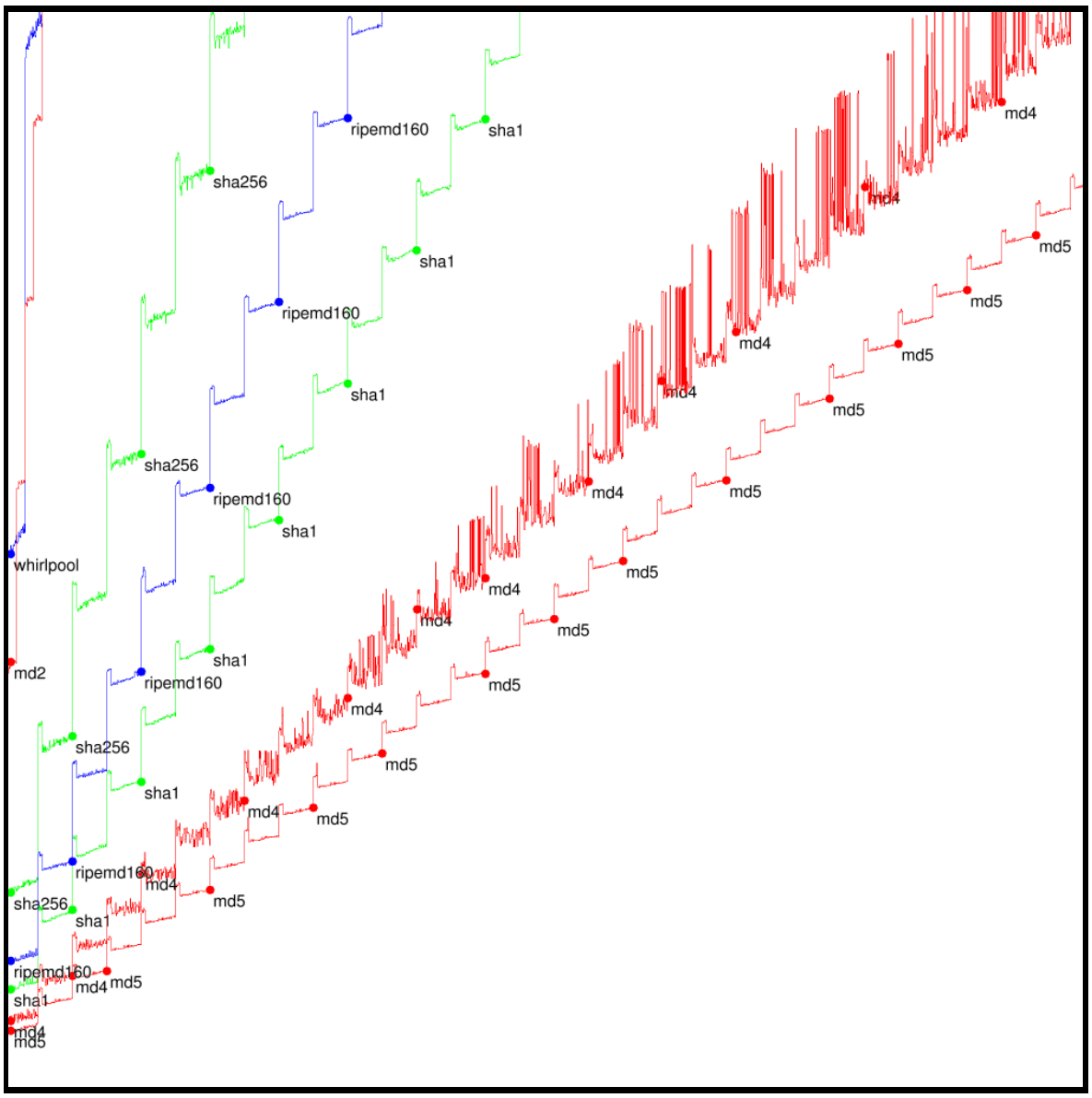
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
9.77	9.77	9.85	`md5`
14.85	14.85	14.95	`sha1`
15.93	16.19	16.42	`md4`
33.52	33.52	33.72	`ripemd160`
50.38	50.38	50.44	`sha512`
69.93	70.49	71.45	`sha256`
168.44	168.89	169.09	`whirlpool`
429.24	429.24	433.83	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
8.71	8.71	8.71	`md5`
11.99	12.01	12.01	`sha1`
13.22	13.24	13.34	`md4`
29.33	29.36	29.40	`ripemd160`
43.79	43.83	43.84	`sha512`
64.50	64.71	66.42	`sha256`
158.52	158.61	158.72	`whirlpool`
412.06	412.06	412.06	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
8.29	8.29	8.29	`md5`
10.86	10.86	10.86	`sha1`
12.12	12.12	12.13	`md4`
27.81	27.82	27.82	`ripemd160`
39.82	39.83	39.84	`sha512`
62.52	62.82	64.49	`sha256`
154.66	154.73	154.82	`whirlpool`
405.38	405.62	407.34	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
8.03	8.03	8.03	`md5`
10.17	10.17	10.18	`sha1`
11.36	11.38	11.48	`md4`
26.86	26.89	26.93	`ripemd160`
37.42	37.43	37.51	`sha512`
59.39	61.72	65.27	`sha256`
151.96	152.19	152.44	`whirlpool`
401.22	401.76	405.22	`md2`

6.33 x86, 2658MHz, Intel Xeon (f25), `nmibuild15`



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
130.00	131.50	133.00	`md5`
153.50	156.00	167.50	`md4`
227.50	229.00	229.00	`sha1`
298.00	299.00	301.50	`ripemd160`
461.50	462.50	464.50	`sha256`
981.50	985.50	991.50	`md2`
1249.00	1250.00	1254.00	`whirlpool`
2727.50	2728.00	2733.50	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
23.94	23.94	24.44	`md5`
29.50	30.69	31.56	`md4`
47.62	47.75	48.25	`sha1`
62.75	62.88	62.94	`ripemd160`
96.06	97.31	98.25	`sha256`
314.44	314.81	318.44	`whirlpool`
331.88	332.31	334.69	`md2`
346.25	346.31	346.31	`sha512`

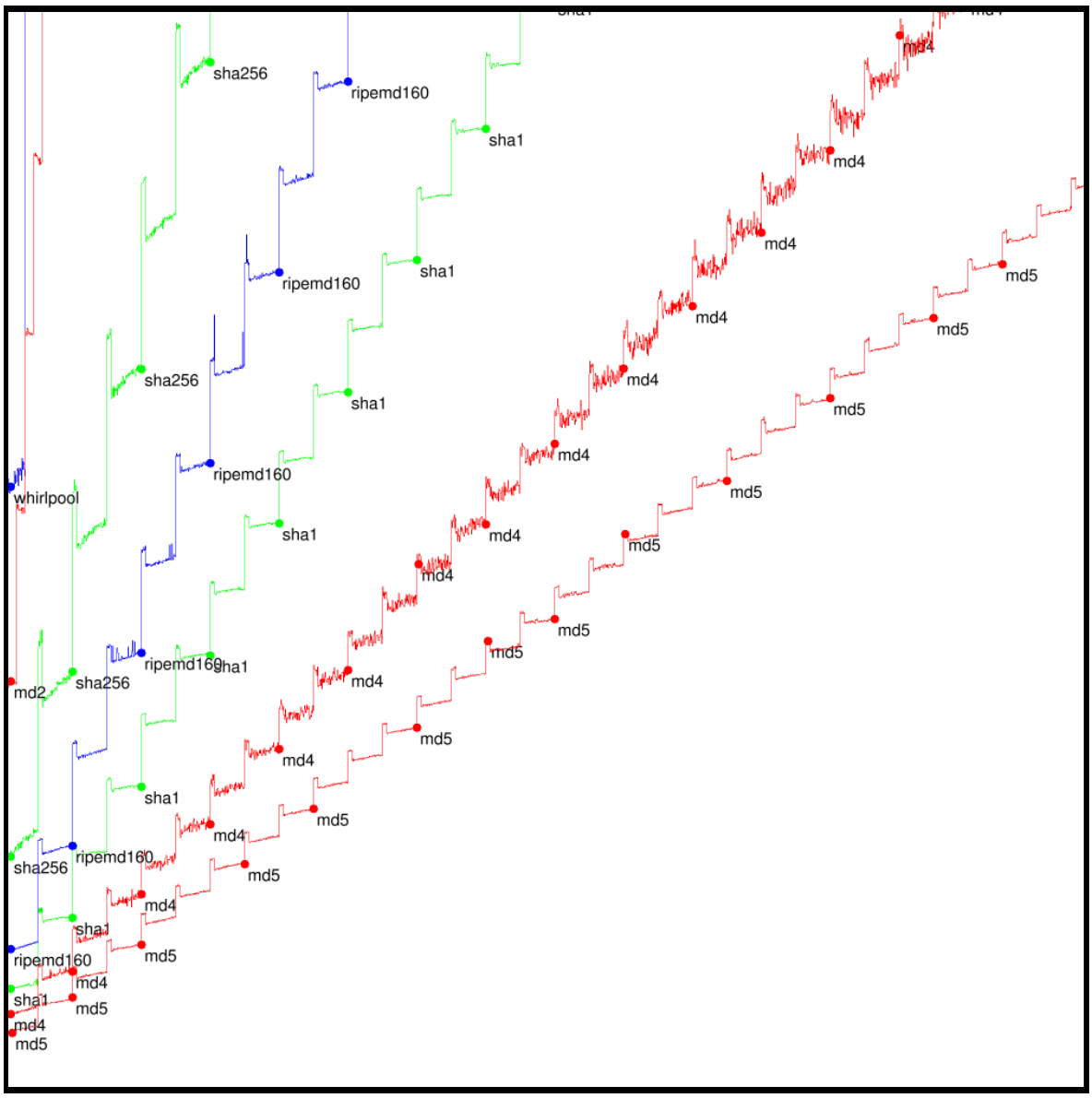
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
9.67	9.67	9.67	`md5`
11.96	11.97	12.53	`md4`
22.38	22.38	22.39	`sha1`
30.99	31.01	31.21	`ripemd160`
46.84	47.53	47.60	`sha256`
175.96	175.99	176.03	`sha512`
177.30	177.91	178.20	`whirlpool`
222.08	222.16	222.82	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
8.58	8.58	8.58	`md5`
10.23	10.37	11.99	`md4`
20.35	20.35	20.36	`sha1`
28.43	28.43	28.48	`ripemd160`
42.89	43.65	43.70	`sha256`
167.00	167.12	167.31	`whirlpool`
168.51	168.54	168.55	`sha512`
214.44	215.18	215.50	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
8.15	8.15	8.15	`md5`
9.73	9.73	9.81	`md4`
19.57	19.57	19.57	`sha1`
27.42	27.45	27.46	`ripemd160`
42.17	42.33	42.37	`sha256`
159.55	159.55	159.56	`sha512`
163.51	163.66	163.78	`whirlpool`
212.13	212.43	214.34	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
7.89	7.89	7.89	`md5`
9.38	9.45	9.61	`md4`
19.09	19.09	19.10	`sha1`
26.80	26.86	26.91	`ripemd160`
41.13	41.58	41.67	`sha256`
154.15	154.15	154.20	`sha512`
160.64	161.42	161.96	`whirlpool`
183.52	210.88	215.63	`md2`

6.34 x86, 2658MHz, Intel Xeon (f25), `nmibuild16`



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
129.50	130.00	132.50	`md5`
141.00	172.00	179.00	`md4`
228.00	230.50	231.50	`sha1`
304.00	322.50	327.00	`ripemd160`
536.00	543.50	552.50	`sha256`
933.50	940.00	1299.50	`md2`
1376.50	1389.00	2188.50	`whirlpool`
2859.50	2865.50	2874.00	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
23.44	23.44	23.88	`md5`
28.81	31.00	32.50	`md4`
48.12	48.69	49.69	`sha1`
62.44	67.62	67.88	`ripemd160`
109.25	110.38	111.62	`sha256`
317.19	320.19	448.81	`md2`
342.94	348.69	570.94	`whirlpool`
362.88	363.19	364.19	`sha512`

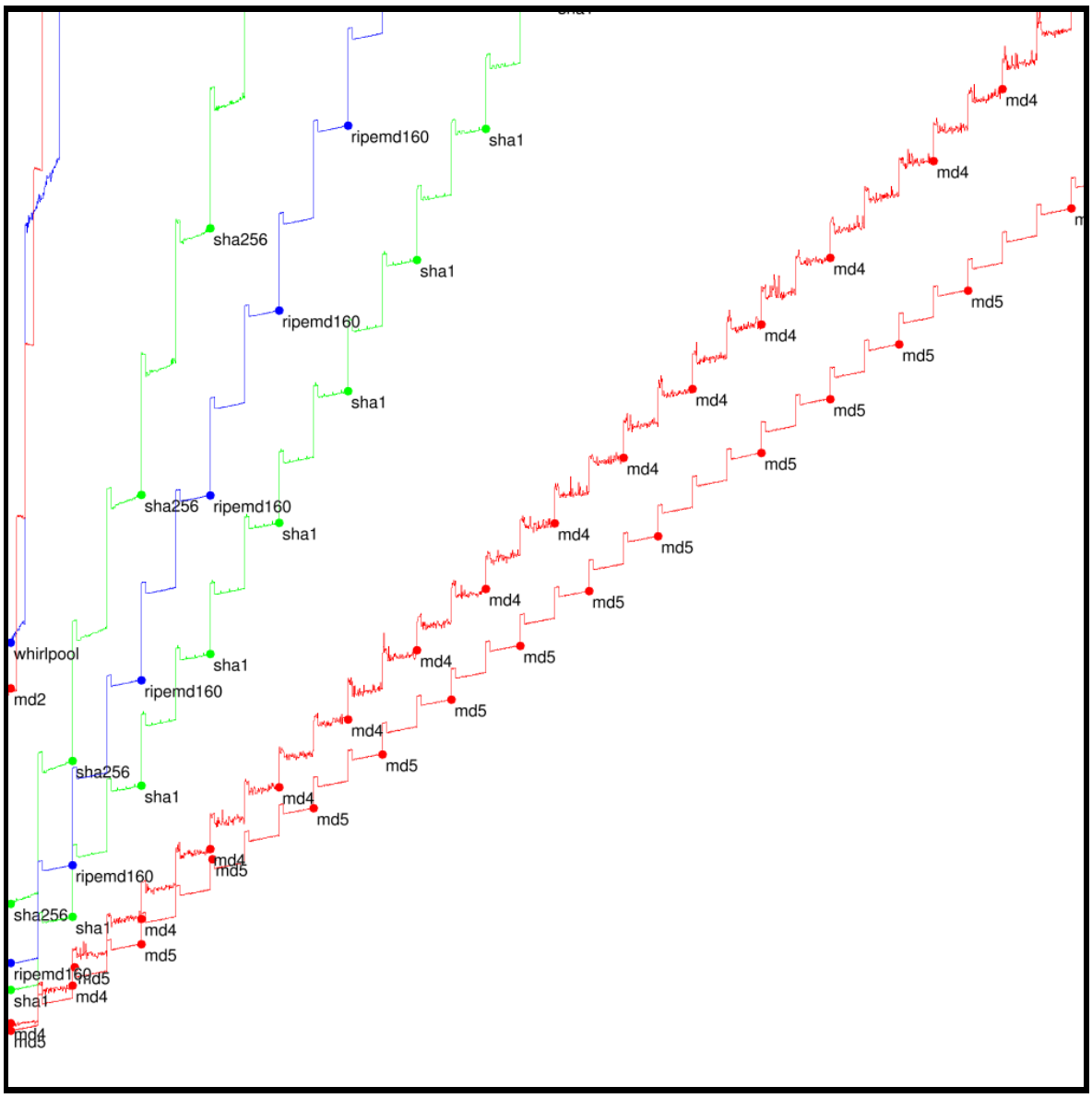
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
9.65	9.67	9.68	`md5`
12.25	12.92	13.35	`md4`
22.29	22.32	22.42	`sha1`
31.00	32.23	32.29	`ripemd160`
52.14	52.30	52.46	`sha256`
188.37	188.52	188.81	`sha512`
192.77	193.73	328.59	`whirlpool`
214.74	215.77	302.92	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
8.57	8.57	8.58	`md5`
11.16	11.72	11.98	`md4`
20.32	20.33	20.37	`sha1`
28.43	29.45	29.50	`ripemd160`
47.55	47.63	47.74	`sha256`
164.08	164.11	181.86	`sha512`
181.02	181.59	182.16	`whirlpool`
205.77	206.74	293.50	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
8.15	8.15	8.15	`md5`
10.70	10.76	11.18	`md4`
19.57	19.58	19.61	`sha1`
27.45	27.55	28.38	`ripemd160`
45.73	45.87	58.41	`sha256`
155.76	172.44	172.57	`sha512`
176.30	176.51	176.79	`whirlpool`
203.72	205.41	205.72	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
7.88	7.90	7.90	`md5`
9.82	10.26	11.41	`md4`
19.07	19.11	19.21	`sha1`
25.81	26.06	28.65	`ripemd160`
44.44	44.80	69.94	`sha256`
109.49	173.03	174.25	`whirlpool`
133.53	183.92	184.39	`sha512`
200.21	205.04	206.50	`md2`

6.35 x86, 2658MHz, Intel Xeon (f25), `nmibuild22`



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
130.50	132.00	132.00	`md5`
142.00	143.50	145.00	`md4`
226.50	226.50	227.00	`sha1`
286.50	287.50	291.00	`ripemd160`
428.00	430.50	434.00	`sha256`
924.50	924.50	927.50	`md2`
1035.50	1048.50	1054.00	`whirlpool`
2686.50	2686.50	2686.50	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
23.94	24.00	24.00	`md5`
27.06	27.06	28.00	`md4`
47.69	47.75	47.94	`sha1`
62.75	62.81	63.81	`ripemd160`
90.94	91.44	92.06	`sha256`
257.31	258.12	260.94	`whirlpool`
316.19	316.56	316.56	`md2`
339.38	339.38	339.44	`sha512`

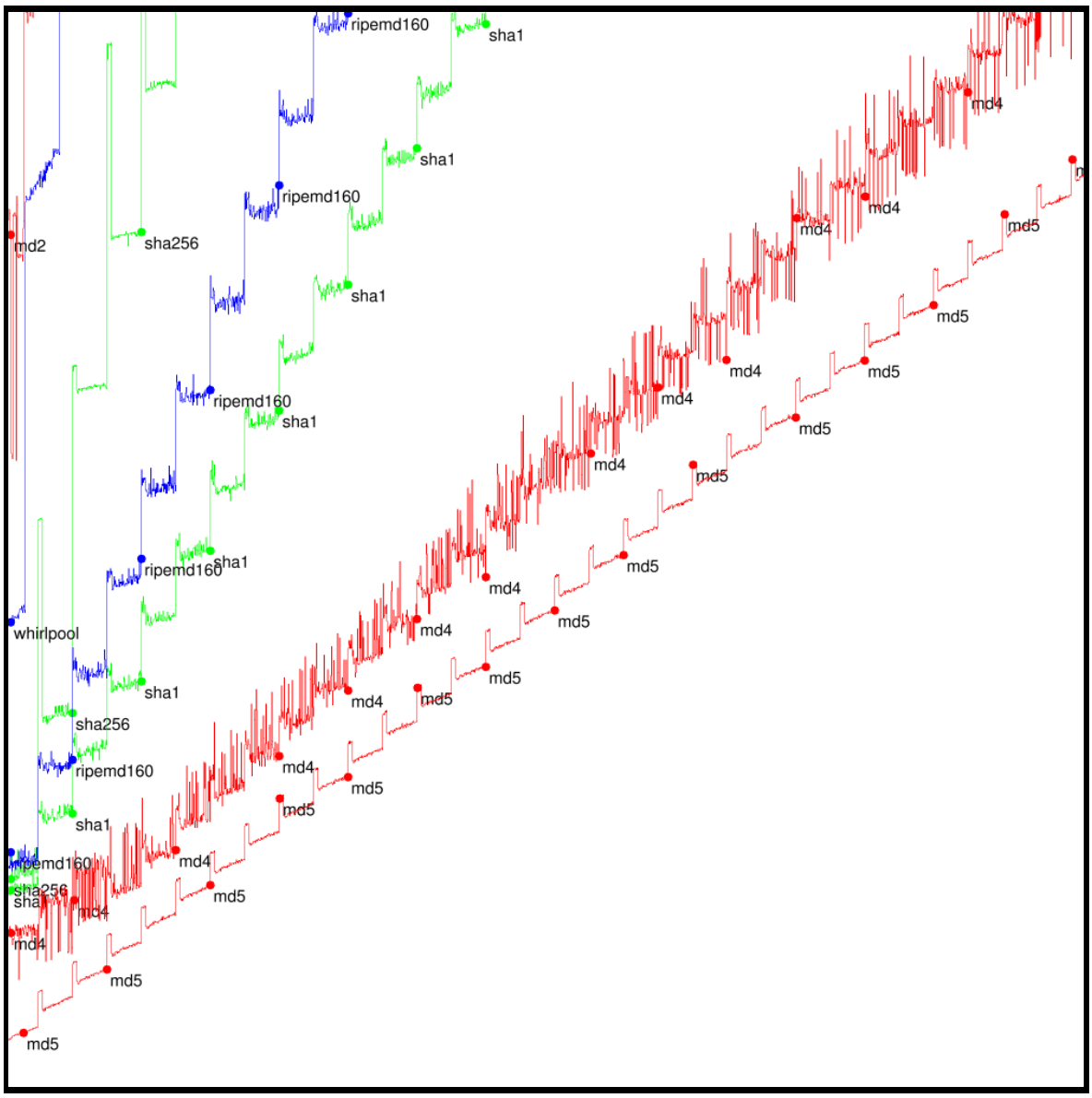
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
9.69	9.69	9.69	`md5`
11.61	11.68	11.71	`md4`
22.27	22.29	22.30	`sha1`
30.85	30.86	30.94	`ripemd160`
44.32	44.42	44.54	`sha256`
147.58	147.76	147.97	`whirlpool`
171.69	171.72	206.75	`sha512`
212.80	212.80	212.91	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
8.59	8.59	9.84	`md5`
10.33	10.35	10.40	`md4`
20.31	20.31	20.32	`sha1`
28.38	28.39	28.40	`ripemd160`
40.68	40.69	40.76	`sha256`
139.01	139.23	139.44	`whirlpool`
164.33	164.34	164.34	`sha512`
204.69	204.69	204.75	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
8.15	8.15	8.15	`md5`
9.82	9.83	9.84	`md4`
19.55	19.55	19.56	`sha1`
27.43	27.43	27.44	`ripemd160`
39.27	39.34	39.38	`sha256`
137.73	137.78	137.91	`whirlpool`
155.53	155.53	155.54	`sha512`
201.66	201.70	201.93	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
7.89	7.89	7.89	`md5`
9.49	9.50	9.54	`md4`
19.08	19.09	19.11	`sha1`
26.84	26.86	26.88	`ripemd160`
38.34	38.50	38.60	`sha256`
137.32	137.59	138.00	`whirlpool`
150.23	150.25	150.27	`sha512`
199.78	199.91	200.37	`md2`

6.36 x86, 2659MHz, Intel Xeon (f25), `nmibuild21`



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
117.00	118.00	121.50	`md5`
233.00	330.50	365.00	`md4`
457.50	468.00	482.00	`sha1`
481.50	483.50	483.50	`sha256`
501.00	522.50	559.00	`ripemd160`
1083.00	1097.00	1107.50	`whirlpool`
1370.50	1461.00	1986.00	`md2`
2979.50	2985.50	2989.00	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
22.44	22.44	22.50	`md5`
37.56	50.56	53.31	`md4`
77.06	77.81	80.25	`sha1`
91.69	93.88	97.31	`ripemd160`
105.75	107.44	110.19	`sha256`
263.44	264.75	267.81	`whirlpool`
376.81	377.25	377.25	`sha512`
454.50	485.12	699.94	`md2`

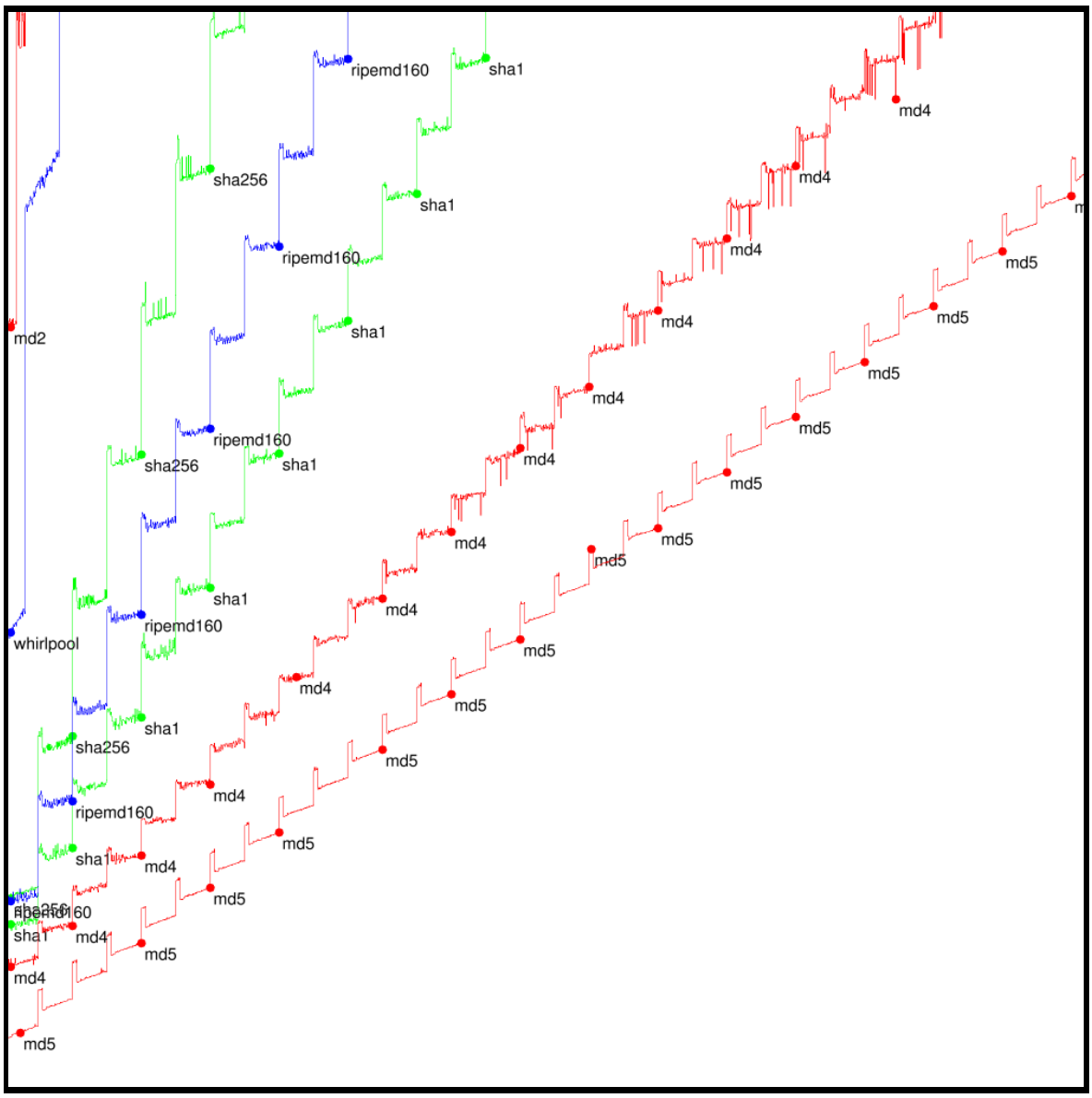
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
9.63	9.64	9.72	`md5`
12.51	12.75	13.59	`md4`
25.49	25.90	25.96	`sha1`
34.03	34.25	34.58	`ripemd160`
51.16	55.49	56.57	`sha256`
148.78	149.05	149.38	`whirlpool`
192.06	192.11	192.11	`sha512`
320.17	473.44	473.49	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
8.62	8.63	8.65	`md5`
10.86	10.88	10.97	`md4`
21.49	21.56	21.70	`sha1`
29.54	29.55	29.85	`ripemd160`
46.57	47.91	48.87	`sha256`
140.10	140.37	140.78	`whirlpool`
183.91	183.93	183.95	`sha512`
312.67	454.98	456.01	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
8.25	8.26	8.26	`md5`
10.15	10.28	10.46	`md4`
19.99	20.03	20.07	`sha1`
27.86	27.88	27.93	`ripemd160`
44.58	44.99	45.69	`sha256`
136.99	138.75	140.14	`whirlpool`
174.09	174.13	175.67	`sha512`
449.63	450.55	451.41	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
8.00	8.04	8.04	`md5`
9.68	9.96	10.32	`md4`
18.96	19.11	19.24	`sha1`
26.69	26.87	26.98	`ripemd160`
41.12	43.20	46.13	`sha256`
134.71	138.45	141.41	`whirlpool`
168.07	168.27	171.35	`sha512`
443.30	448.02	451.31	`md2`

6.37 x86, 2659MHz, Intel Xeon (f25), `nmibuild26`



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
121.00	121.50	122.50	`md5`
282.00	286.50	289.00	`md4`
364.00	370.00	378.00	`sha1`
432.50	436.50	444.00	`ripemd160`
441.00	443.50	458.50	`sha256`
1057.50	1068.00	1072.00	`whirlpool`
1744.50	1768.50	1776.00	`md2`
2848.00	2868.00	2868.00	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
22.19	22.38	22.56	`md5`
44.56	44.75	46.06	`md4`
65.69	67.69	68.12	`sha1`
80.44	81.62	84.00	`ripemd160`
98.31	98.44	99.12	`sha256`
260.81	261.88	263.88	`whirlpool`
360.12	362.19	362.56	`sha512`
569.38	588.06	588.62	`md2`

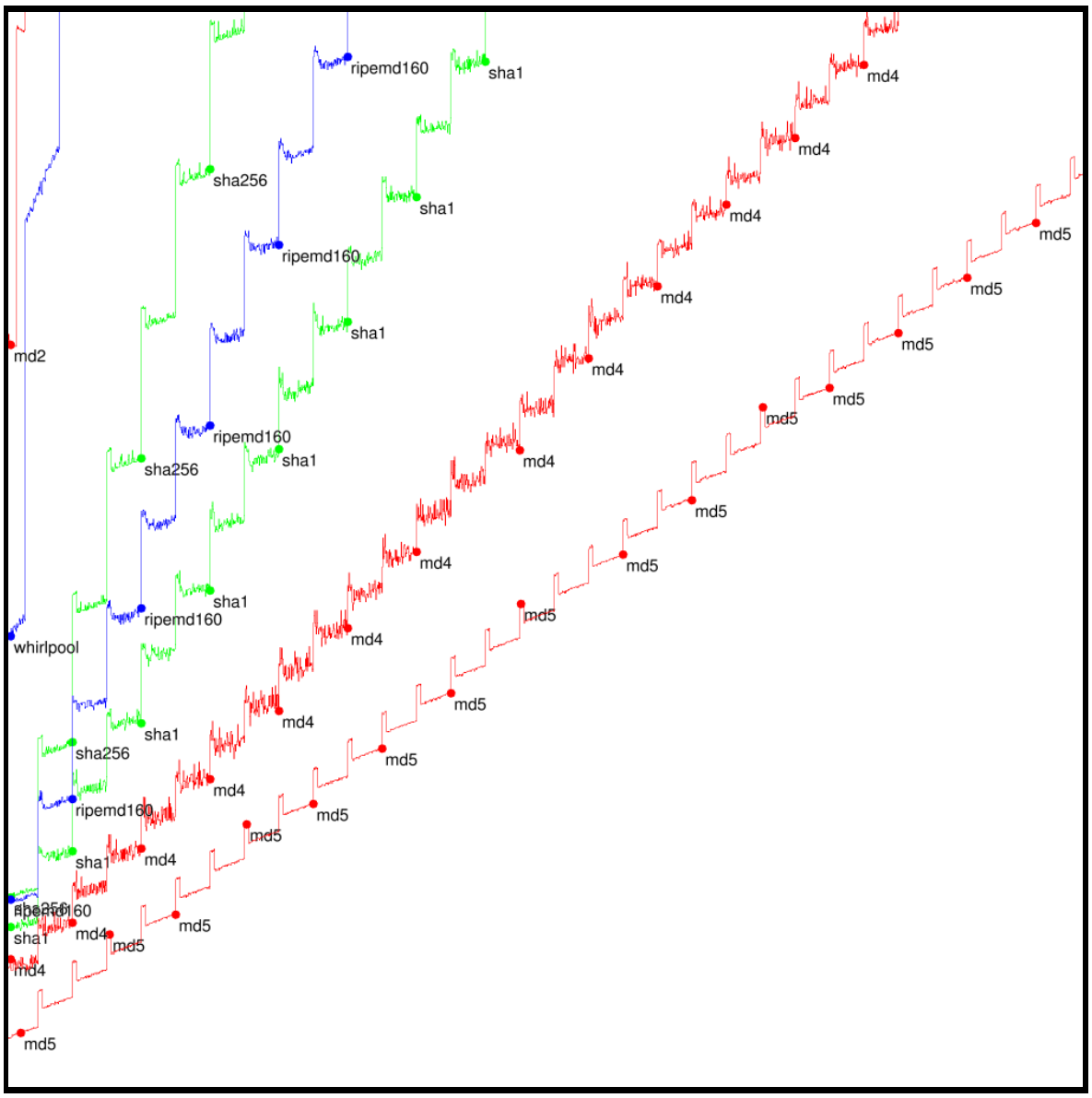
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
9.60	9.61	9.62	`md5`
14.37	14.44	14.46	`md4`
24.33	24.47	24.73	`sha1`
33.01	33.07	33.16	`ripemd160`
47.87	47.88	47.94	`sha256`
147.74	148.15	148.38	`whirlpool`
176.14	176.14	176.15	`sha512`
379.53	379.54	379.69	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
8.64	8.64	8.64	`md5`
11.90	11.94	12.05	`md4`
21.08	21.12	21.21	`sha1`
29.16	29.21	29.27	`ripemd160`
43.92	43.95	43.96	`sha256`
139.07	139.21	139.58	`whirlpool`
167.41	167.42	167.51	`sha512`
365.65	365.90	369.33	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
8.26	8.26	8.26	`md5`
10.98	11.00	11.00	`md4`
19.85	19.86	19.86	`sha1`
27.71	27.73	27.78	`ripemd160`
42.45	42.83	44.40	`sha256`
135.83	135.91	137.61	`whirlpool`
158.06	158.07	159.81	`sha512`
360.54	361.69	362.28	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
8.03	8.03	8.04	`md5`
10.36	10.44	10.46	`md4`
19.06	19.10	19.14	`sha1`
26.73	26.86	27.00	`ripemd160`
40.05	41.76	45.13	`sha256`
133.48	133.77	137.33	`whirlpool`
151.53	152.47	155.94	`sha512`
354.65	359.62	361.00	`md2`

6.38 x86, 2667MHz, Intel Xeon (f25), nmi0036



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
118.50	120.00	120.50	`md5`
270.50	270.50	283.50	`md4`
364.00	370.00	370.50	`sha1`
429.50	431.00	438.00	`ripemd160`
443.50	445.00	447.50	`sha256`
1055.00	1061.00	1064.00	`whirlpool`
1722.00	1723.00	1730.00	`md2`
2868.00	2870.00	2875.50	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
22.88	22.94	23.00	`md5`
49.56	50.00	50.00	`md4`
67.25	67.25	68.69	`sha1`
80.81	82.25	83.06	`ripemd160`
95.94	96.06	97.06	`sha256`
261.75	263.38	266.44	`whirlpool`
363.00	363.12	363.31	`sha512`
566.81	580.12	580.19	`md2`

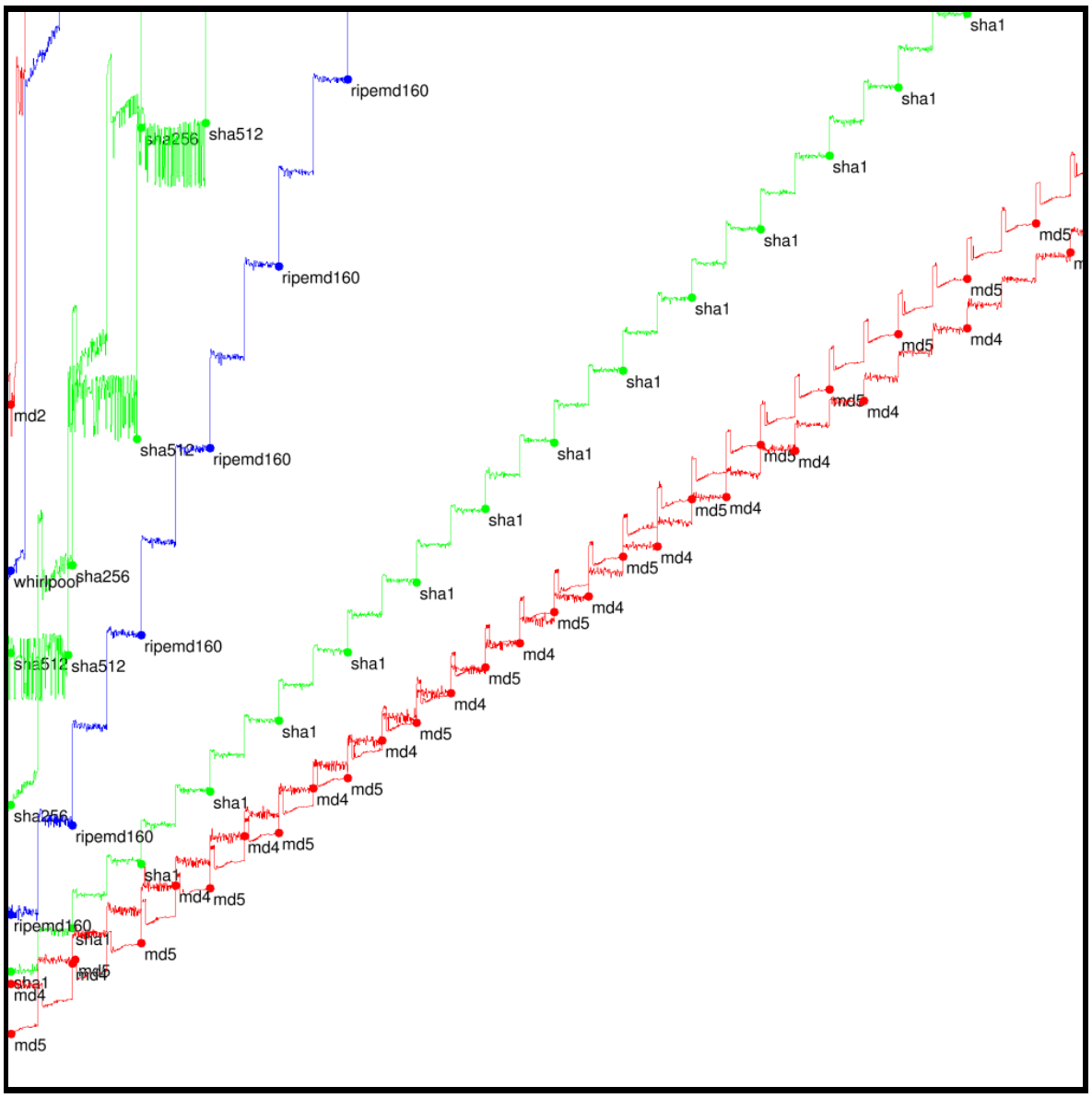
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
9.65	9.67	9.69	`md5`
14.33	14.81	14.84	`md4`
24.48	24.52	24.52	`sha1`
33.19	33.31	33.57	`ripemd160`
47.68	47.71	47.81	`sha256`
149.60	149.90	151.52	`whirlpool`
176.12	176.12	176.14	`sha512`
386.25	387.80	387.83	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
8.65	8.66	8.67	`md5`
12.12	12.35	12.47	`md4`
21.11	21.11	21.32	`sha1`
29.14	29.22	29.30	`ripemd160`
43.77	43.80	43.82	`sha256`
140.87	141.17	141.42	`whirlpool`
167.36	167.36	167.50	`sha512`
372.76	372.81	374.50	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
8.27	8.27	8.27	`md5`
11.50	11.52	11.56	`md4`
19.84	19.85	20.01	`sha1`
27.74	27.77	27.83	`ripemd160`
42.64	43.23	43.53	`sha256`
137.65	138.65	139.04	`whirlpool`
157.98	158.04	159.18	`sha512`
367.21	368.51	373.64	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
8.02	8.03	8.04	`md5`
11.07	11.14	11.26	`md4`
18.75	19.08	19.41	`sha1`
26.79	26.91	27.05	`ripemd160`
42.02	43.19	43.85	`sha256`
135.35	137.54	138.50	`whirlpool`
152.24	152.47	154.74	`sha512`
362.26	366.46	376.77	`md2`

6.39 x86, 2791MHz, Intel Xeon (f27), nmi0024



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
128.00	128.50	130.50	`md5`
229.00	234.50	247.00	`md4`
269.50	269.50	270.00	`sha1`
392.50	396.00	414.50	`ripemd160`
655.50	662.00	664.00	`sha256`
1000.00	1031.00	1043.50	`sha512`
1191.00	1196.00	1203.00	`whirlpool`
1527.50	1581.50	1658.50	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
23.56	23.69	23.75	`md5`
35.38	36.38	36.69	`md4`
44.38	46.00	46.00	`sha1`
76.81	77.25	77.94	`ripemd160`
112.56	130.50	131.00	`sha512`
141.69	141.69	143.75	`sha256`
300.38	301.50	302.75	`whirlpool`
531.00	555.06	565.25	`md2`

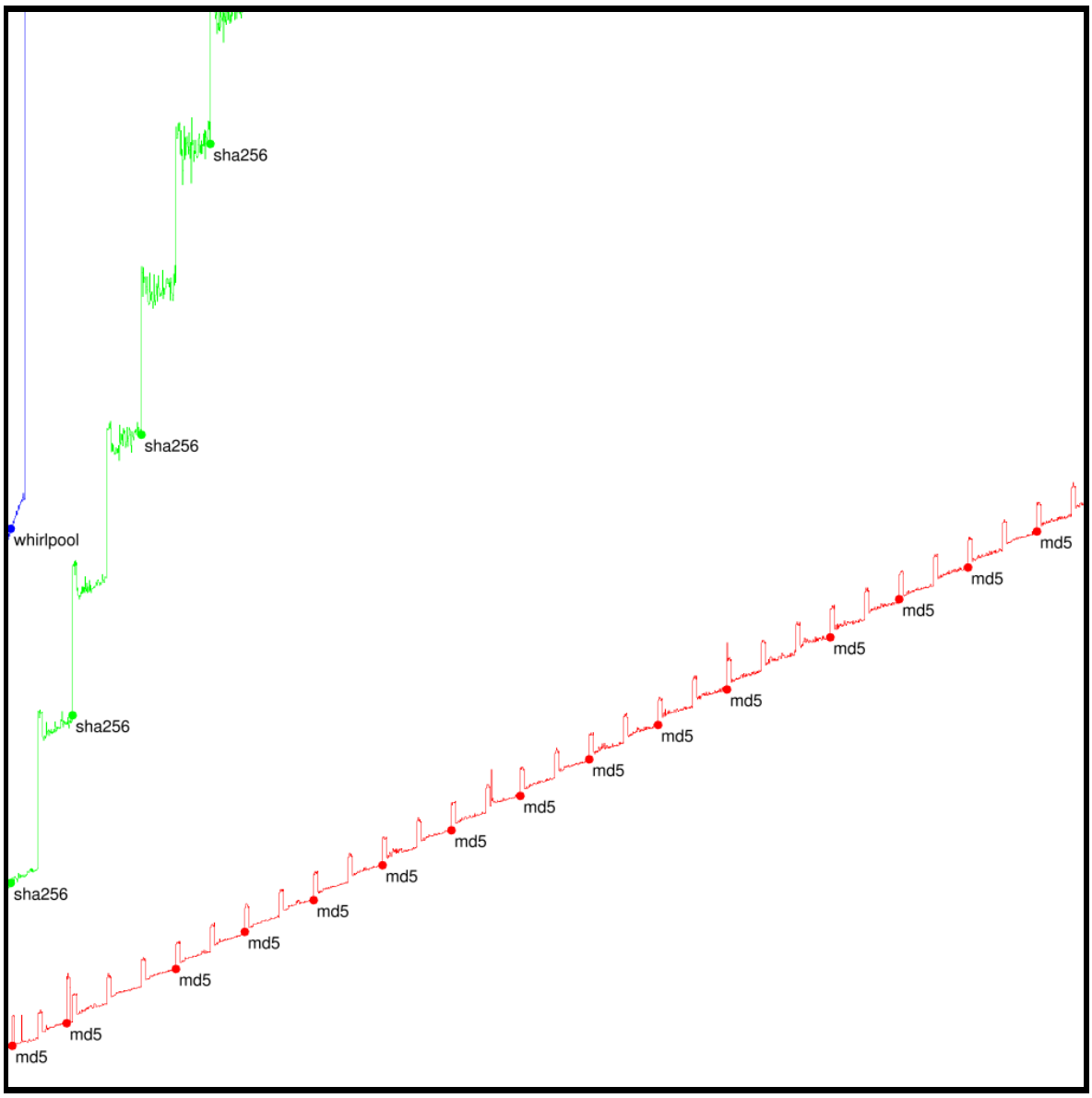
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
9.72	9.72	9.74	`md5`
10.33	10.38	10.44	`md4`
14.08	14.08	14.08	`sha1`
32.56	32.56	32.67	`ripemd160`
47.38	47.67	47.67	`sha512`
74.80	75.40	75.40	`sha256`
168.86	169.09	169.46	`whirlpool`
370.17	370.17	370.17	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
8.23	8.24	8.29	`md4`
8.68	8.68	8.70	`md5`
11.70	11.70	11.70	`sha1`
28.92	28.99	29.04	`ripemd160`
41.71	42.43	42.46	`sha512`
69.61	69.61	69.78	`sha256`
158.53	158.82	159.03	`whirlpool`
355.70	355.73	355.73	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
7.47	7.48	7.48	`md4`
8.28	8.28	8.28	`md5`
10.76	10.76	10.76	`sha1`
27.67	27.68	27.70	`ripemd160`
39.01	39.02	39.02	`sha512`
67.65	67.65	67.65	`sha256`
154.84	155.03	155.13	`whirlpool`
350.37	350.39	350.43	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
6.93	6.96	7.00	`md4`
8.01	8.03	8.03	`md5`
10.17	10.22	10.22	`sha1`
26.88	26.94	27.02	`ripemd160`
36.93	36.96	37.01	`sha512`
66.50	66.50	66.50	`sha256`
152.23	152.72	153.04	`whirlpool`
347.18	347.23	350.26	`md2`

6.40 x86, 2800MHz, Intel Xeon (f41), nmi0057



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
98.88	164.50	171.50	`md5`
474.25	487.38	917.00	`sha256`
1304.62	1308.12	1316.00	`whirlpool`
3024.00	3030.12	3037.12	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
15.75	16.08	16.30	`md5`
100.95	101.72	102.48	`sha256`
336.44	337.53	400.64	`whirlpool`
381.06	382.05	383.14	`sha512`

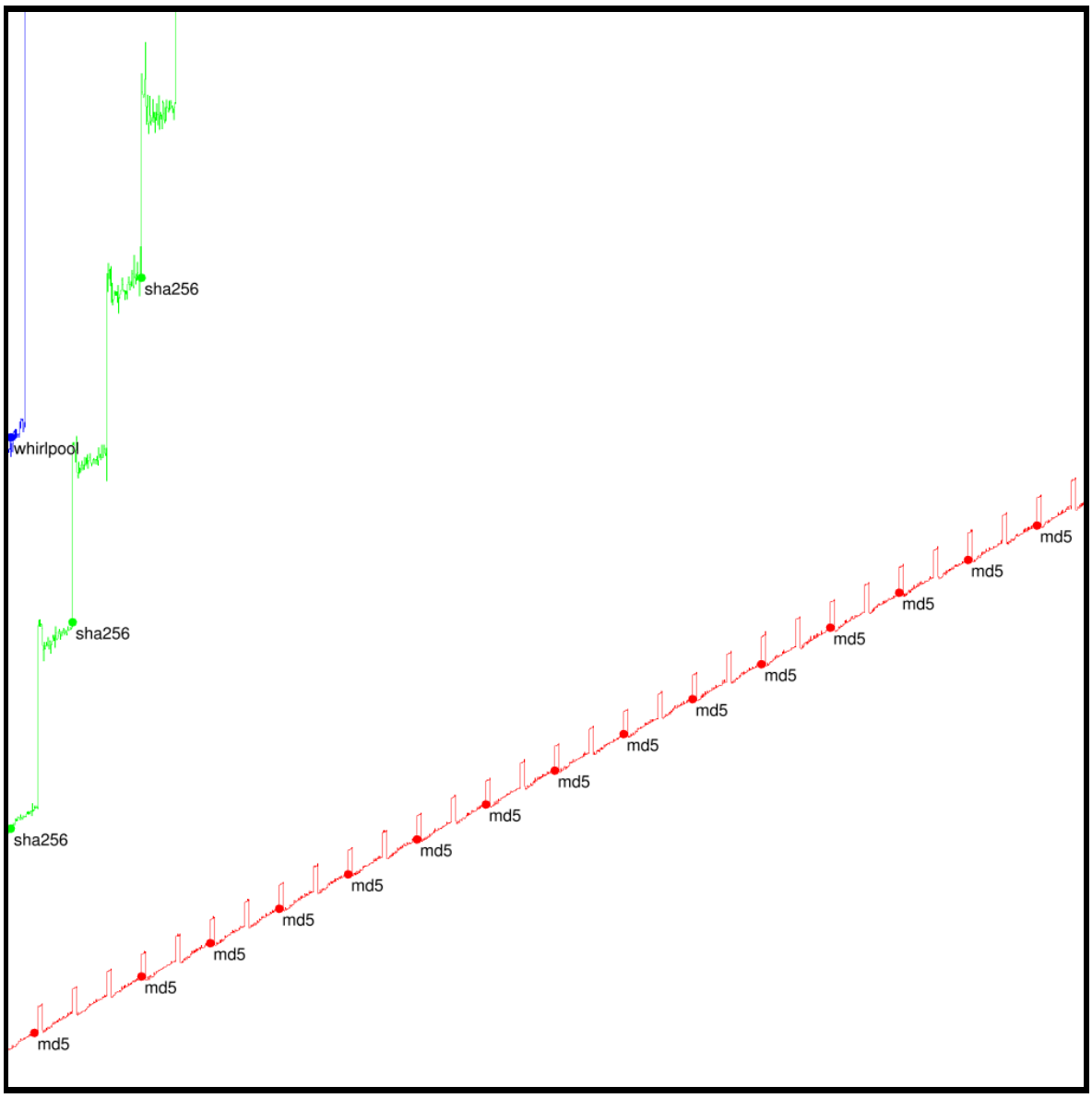
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
6.26	6.30	6.37	`md5`
47.83	48.25	48.51	`sha256`
185.90	186.01	186.21	`sha512`
193.85	194.38	195.16	`whirlpool`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
5.53	5.54	5.57	`md5`
43.12	45.66	88.22	`sha256`
177.04	177.08	177.34	`sha512`
182.51	183.44	185.11	`whirlpool`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
5.24	5.24	5.25	`md5`
43.20	43.69	44.21	`sha256`
167.54	169.56	197.70	`sha512`
178.61	180.76	186.95	`whirlpool`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
5.04	5.06	5.09	`md5`
42.19	43.47	44.66	`sha256`
159.38	165.61	222.28	`sha512`
173.63	179.83	192.89	`whirlpool`

6.41 x86, 2800MHz, Intel Xeon (f41), nmi0063



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
94.50	96.25	98.00	`md5`
602.88	609.00	623.88	`sha256`
1471.75	1477.00	1512.88	`whirlpool`
3019.62	3027.50	3034.50	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
15.86	16.41	16.73	`md5`
127.64	128.41	129.39	`sha256`
374.06	374.83	375.48	`whirlpool`
384.89	385.44	385.77	`sha512`

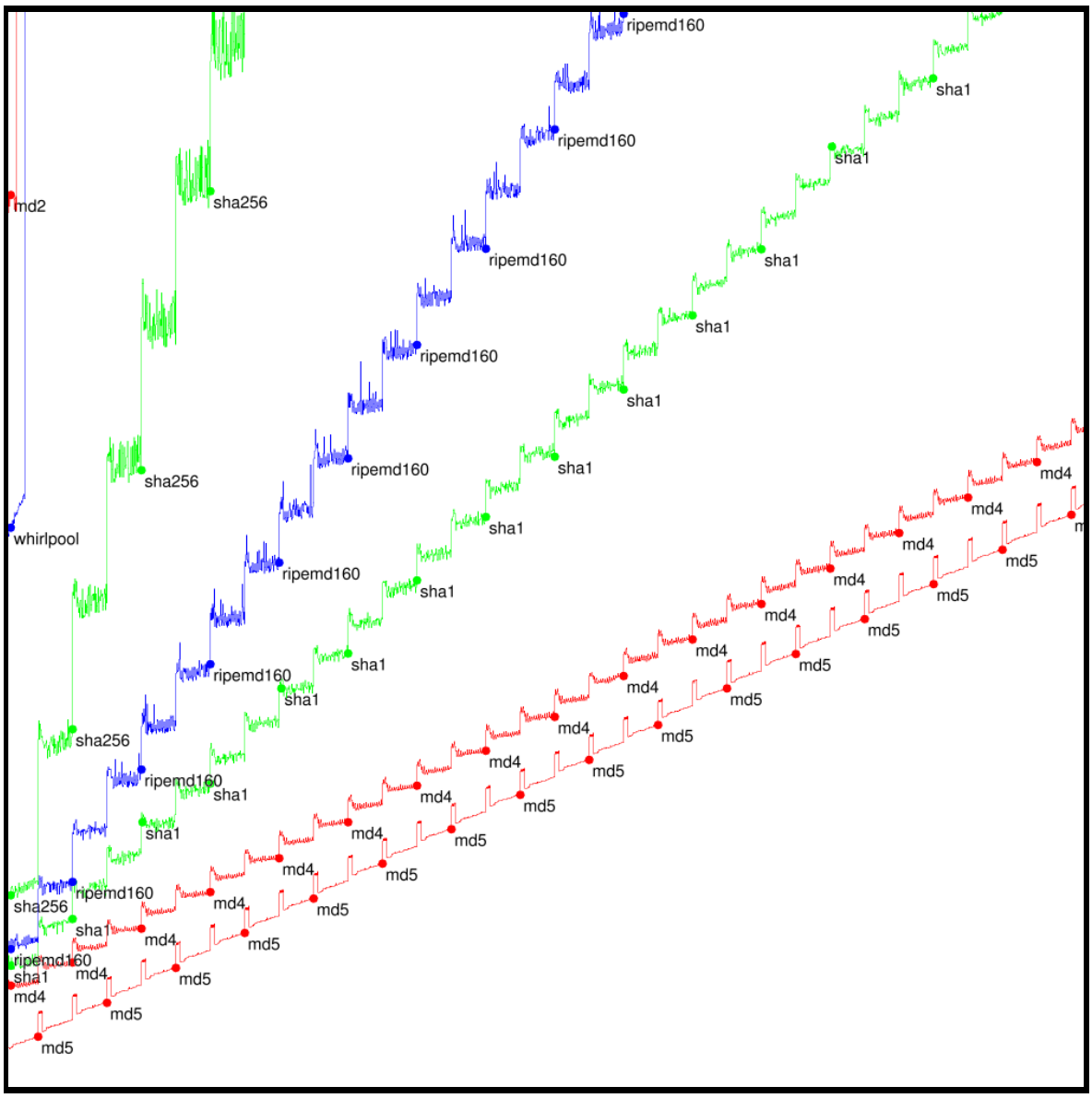
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
6.23	6.25	6.40	`md5`
56.50	58.21	58.45	`sha256`
186.16	186.21	186.22	`sha512`
210.52	211.40	212.20	`whirlpool`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
5.52	5.53	5.56	`md5`
54.17	54.62	54.77	`sha256`
176.97	176.97	177.40	`sha512`
198.29	198.95	199.86	`whirlpool`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
5.22	5.22	5.23	`md5`
50.71	52.11	53.13	`sha256`
166.99	166.99	168.06	`sha512`
192.34	194.04	196.52	`whirlpool`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
5.02	5.04	5.07	`md5`
48.09	51.94	54.80	`sha256`
158.77	160.97	163.15	`sha512`
186.34	191.72	198.04	`whirlpool`

6.42 x86, 2801MHz, Intel Xeon (f41), nmi0060



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
91.00	93.62	94.50	`md5`
239.75	242.38	244.12	`md4`
276.50	292.25	308.00	`sha1`
318.50	324.62	328.12	`ripemd160`
445.38	461.12	469.00	`sha256`
1312.50	1316.88	1322.12	`whirlpool`
2037.88	2069.38	2076.38	`md2`
3017.00	3028.38	3028.38	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
15.86	16.08	16.19	`md5`
35.11	35.77	35.98	`md4`
44.08	47.14	47.25	`sha1`
55.23	55.67	55.89	`ripemd160`
98.77	100.52	102.59	`sha256`
336.11	337.20	338.41	`whirlpool`
381.28	381.28	381.28	`sha512`
698.91	699.89	704.59	`md2`

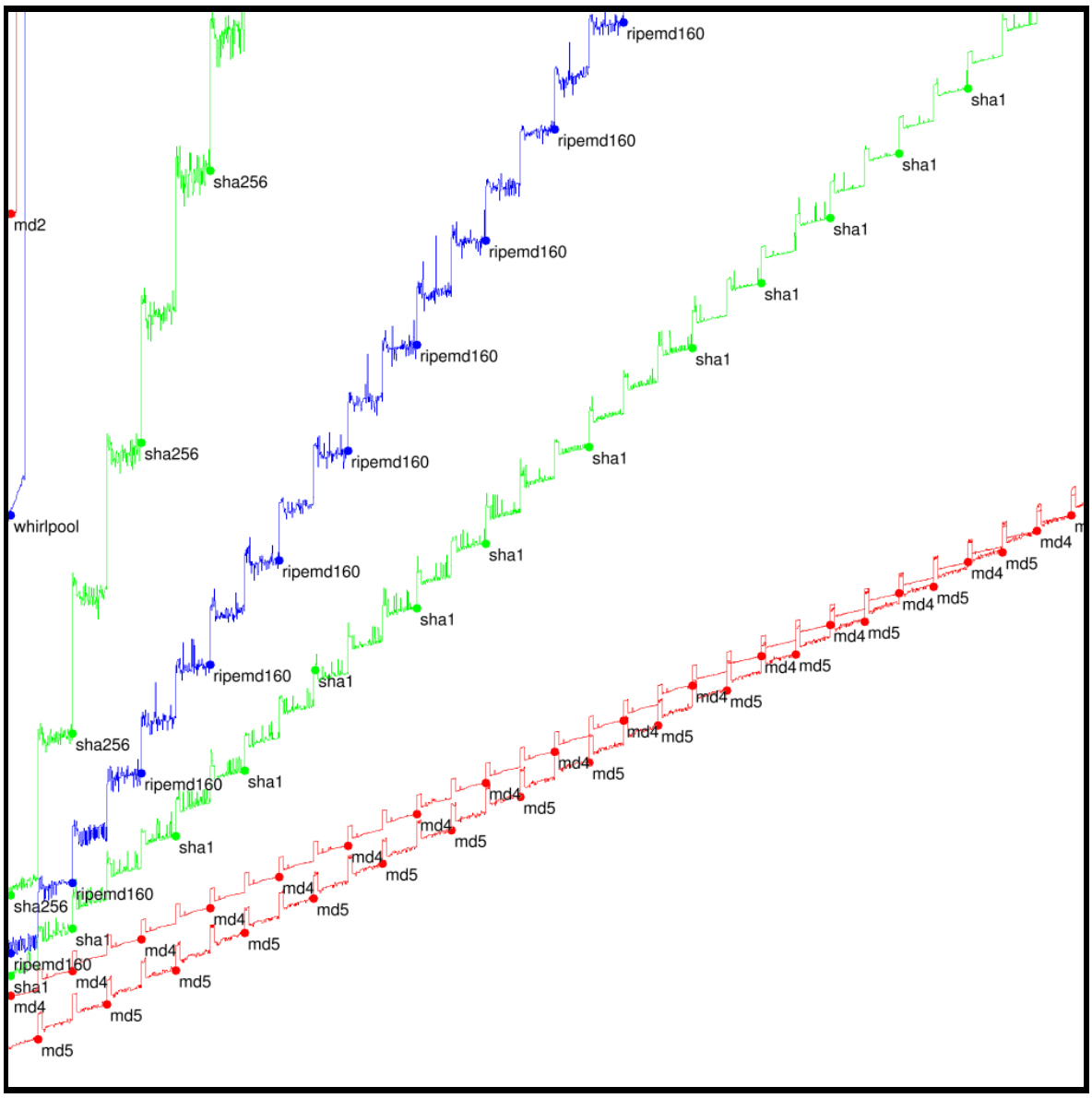
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
6.27	6.28	6.30	`md5`
8.48	8.52	8.57	`md4`
13.74	13.84	13.95	`sha1`
19.97	20.02	21.15	`ripemd160`
45.65	46.18	47.69	`sha256`
186.18	186.18	186.19	`sha512`
193.38	193.98	194.42	`whirlpool`
470.56	470.86	471.44	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
5.53	5.53	5.53	`md5`
6.44	6.47	6.49	`md4`
11.12	11.24	11.36	`sha1`
17.24	17.36	17.38	`ripemd160`
43.46	44.17	45.64	`sha256`
177.27	177.28	177.55	`sha512`
182.56	182.89	183.26	`whirlpool`
452.79	453.14	455.43	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
5.22	5.22	5.22	`md5`
5.64	5.64	5.64	`md4`
10.24	10.27	10.35	`sha1`
16.15	16.16	16.17	`ripemd160`
41.26	41.39	42.61	`sha256`
167.35	167.35	169.49	`sha512`
178.61	179.15	181.09	`whirlpool`
446.39	447.90	449.38	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
5.04	5.04	5.04	`md5`
5.13	5.14	5.15	`md4`
9.18	9.66	9.85	`sha1`
15.25	15.45	15.55	`ripemd160`
38.78	40.02	42.90	`sha256`
161.21	161.40	165.67	`sha512`
175.34	176.81	181.26	`whirlpool`
439.26	445.29	448.50	`md2`

6.43 x86, 2801MHz, Intel Xeon (f41), nmi0061



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
91.88	95.38	98.88	`md5`
211.75	211.75	212.62	`md4`
260.75	264.25	268.62	`sha1`
306.25	329.00	340.38	`ripemd160`
456.75	461.12	462.00	`sha256`
1344.00	1348.38	1352.75	`whirlpool`
2029.12	2029.12	2030.00	`md2`
2989.00	2998.62	3010.00	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
16.73	16.73	17.06	`md5`
31.17	31.28	31.39	`md4`
42.22	42.22	42.33	`sha1`
57.64	57.75	58.41	`ripemd160`
96.03	99.31	100.19	`sha256`
339.50	340.70	341.25	`whirlpool`
377.89	378.11	378.66	`sha512`
686.98	688.52	688.84	`md2`

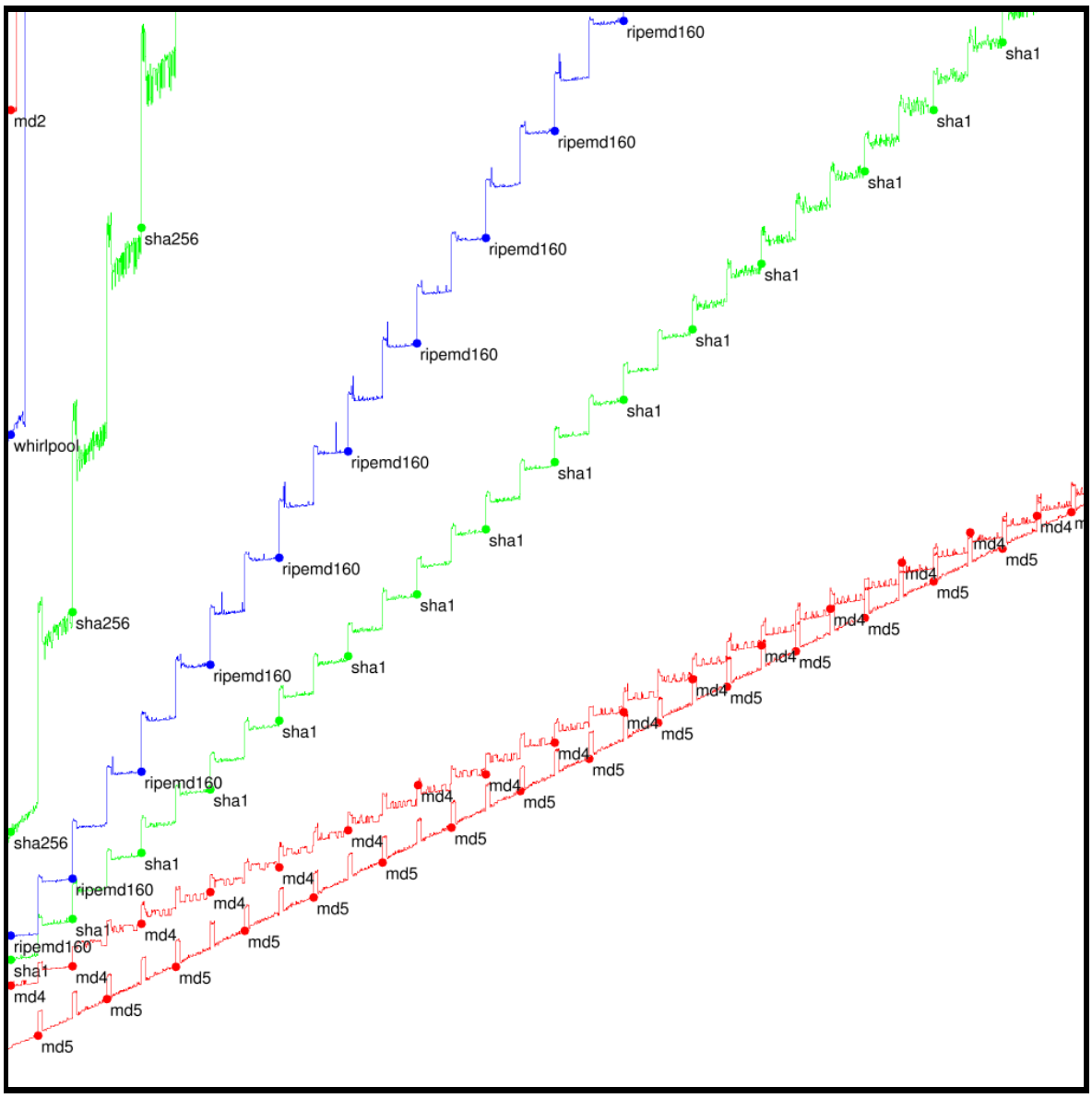
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
6.31	6.33	6.44	`md5`
7.51	7.51	7.52	`md4`
13.14	13.16	13.62	`sha1`
19.78	20.03	20.45	`ripemd160`
47.49	47.58	47.64	`sha256`
183.62	183.62	183.63	`sha512`
196.16	196.64	197.01	`whirlpool`
460.31	460.46	462.74	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
5.55	5.55	5.56	`md5`
5.70	5.71	5.71	`md4`
10.82	10.83	10.87	`sha1`
17.28	17.35	17.64	`ripemd160`
43.60	44.05	44.50	`sha256`
174.73	174.73	174.76	`sha512`
184.50	184.71	185.92	`whirlpool`
442.56	444.58	447.16	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
4.98	4.98	4.98	`md4`
5.23	5.24	5.24	`md5`
9.96	9.96	9.96	`sha1`
16.19	16.20	16.31	`ripemd160`
41.08	42.09	42.14	`sha256`
164.95	164.95	166.74	`sha512`
180.40	181.21	183.06	`whirlpool`
437.71	438.98	440.81	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
4.55	4.55	4.55	`md4`
5.04	5.06	5.09	`md5`
9.43	9.44	9.44	`sha1`
15.14	15.52	15.77	`ripemd160`
39.15	41.22	41.74	`sha256`
159.08	159.08	162.68	`sha512`
174.83	178.71	183.18	`whirlpool`
431.28	435.12	441.66	`md2`

6.44 x86, 2801MHz, Intel Xeon (f41), nmi0062



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
96.25	97.12	98.88	`md5`
234.50	235.38	245.00	`md4`
296.62	297.50	298.38	`sha1`
346.50	348.25	350.88	`ripemd160`
605.50	611.62	619.50	`sha256`
1519.00	1525.12	1533.88	`whirlpool`
2269.75	2273.25	2274.12	`md2`
3031.00	3031.88	3032.75	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
15.86	16.30	16.52	`md5`
33.91	34.02	34.34	`md4`
46.81	46.92	47.14	`sha1`
59.28	59.39	59.83	`ripemd160`
128.62	129.50	129.94	`sha256`
375.38	377.56	378.77	`whirlpool`
382.48	383.36	383.47	`sha512`
777.66	777.88	778.42	`md2`

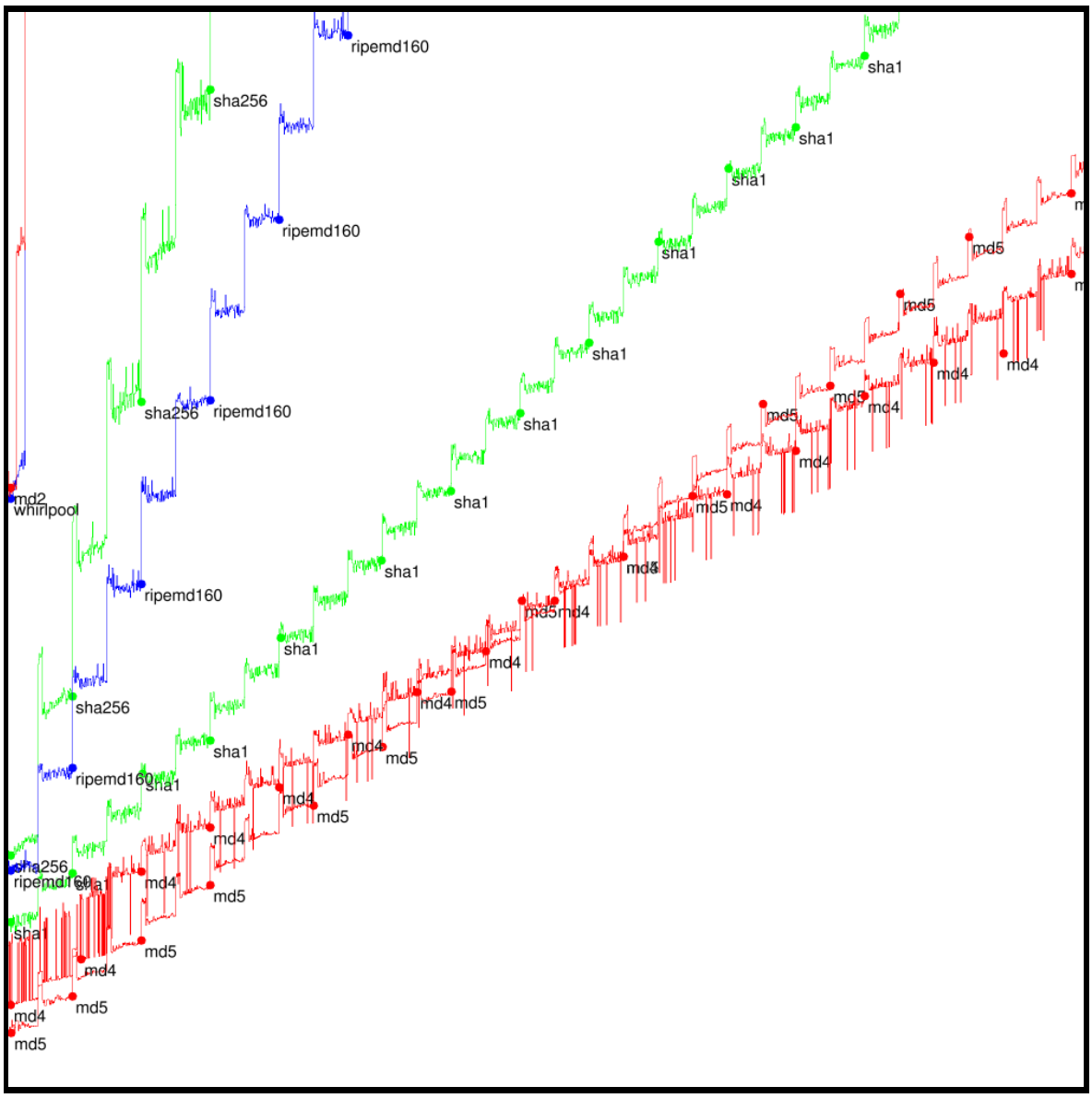
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
6.20	6.23	6.33	`md5`
7.96	7.96	8.03	`md4`
13.57	13.59	13.60	`sha1`
20.40	20.43	21.97	`ripemd160`
60.91	63.18	63.21	`sha256`
185.90	185.96	185.97	`sha512`
212.54	213.29	213.91	`whirlpool`
523.23	523.50	523.89	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
5.51	5.53	5.55	`md5`
5.84	5.84	5.86	`md4`
10.96	11.07	11.07	`sha1`
17.37	17.38	17.40	`ripemd160`
55.69	58.14	58.14	`sha256`
176.97	176.97	176.97	`sha512`
199.18	199.44	199.89	`whirlpool`
503.34	503.69	504.52	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
5.01	5.02	5.02	`md4`
5.22	5.23	5.24	`md5`
9.97	10.04	10.05	`sha1`
16.21	16.21	16.22	`ripemd160`
56.17	56.25	56.25	`sha256`
167.09	167.09	167.09	`sha512`
194.93	195.13	195.54	`whirlpool`
496.20	496.84	497.25	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
4.51	4.52	4.54	`md4`
5.02	5.06	5.08	`md5`
9.28	9.44	9.53	`sha1`
15.49	15.51	15.52	`ripemd160`
54.95	55.12	55.23	`sha256`
161.15	161.16	161.17	`sha512`
192.37	193.18	194.30	`whirlpool`
490.84	492.99	494.17	`md2`

6.45 x86, 2802MHz, Intel Xeon (f29), `nmibuild40`



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
138.50	139.00	156.00	`md5`
189.50	191.50	193.00	`md4`
363.50	370.50	370.50	`sha1`
497.50	515.50	517.50	`ripemd160`
508.00	544.50	563.00	`sha256`
1359.50	1372.50	1394.50	`whirlpool`
1388.00	1392.00	1402.50	`md2`
2873.50	2873.50	2878.00	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
23.69	25.25	27.88	`md5`
30.12	30.25	47.94	`md4`
56.81	56.81	59.81	`sha1`
88.81	89.31	89.56	`ripemd160`
106.88	108.19	112.19	`sha256`
334.12	336.19	338.75	`whirlpool`
361.81	361.81	362.75	`sha512`
454.38	457.12	460.06	`md2`

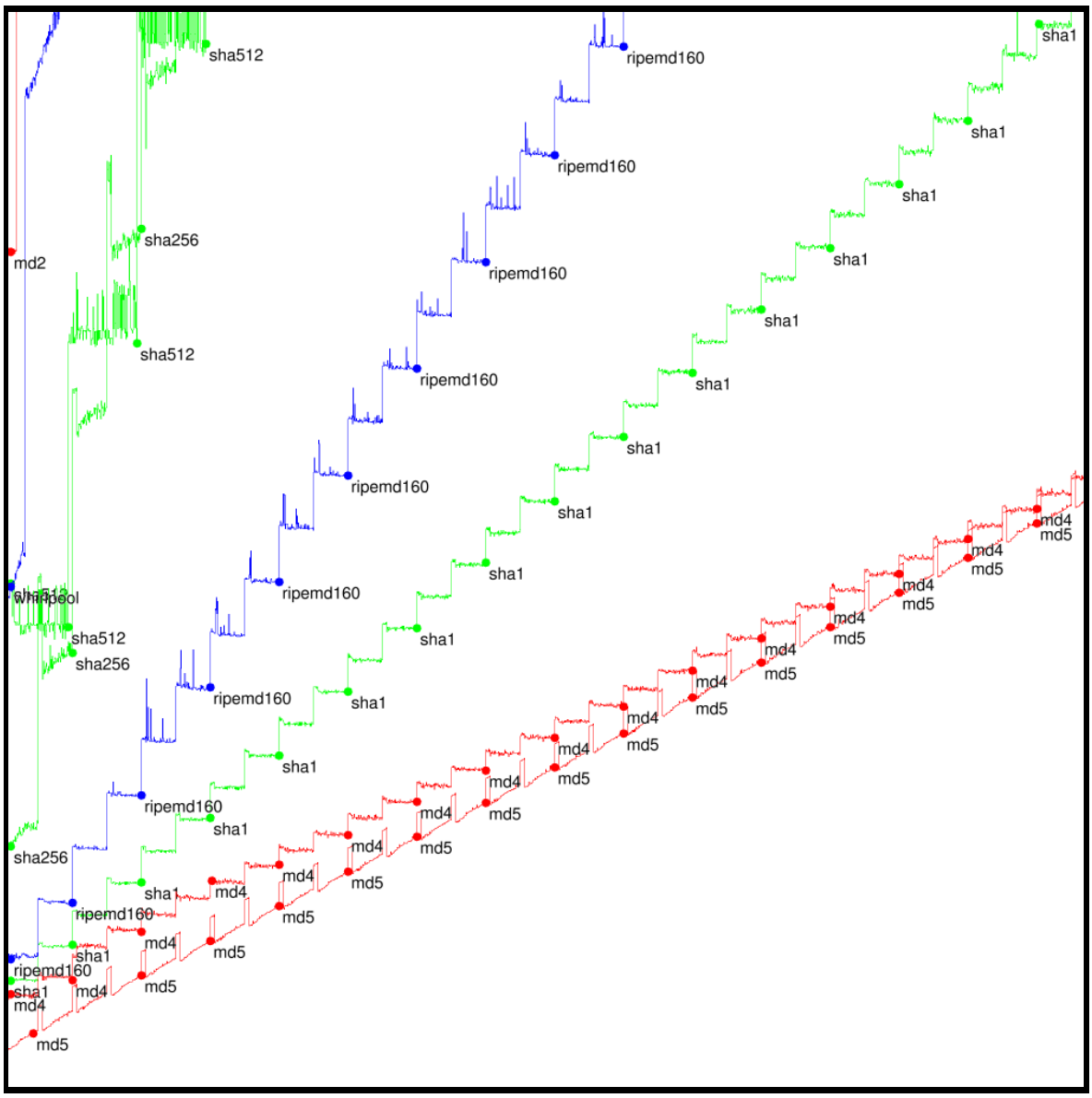
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
9.68	9.68	9.70	`md5`
11.14	11.15	11.43	`md4`
15.48	15.66	15.78	`sha1`
33.74	34.26	34.26	`ripemd160`
49.67	49.83	53.08	`sha256`
188.66	189.53	190.31	`whirlpool`
191.35	191.35	191.44	`sha512`
301.17	302.56	305.46	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
8.28	8.29	8.34	`md4`
8.67	8.67	8.68	`md5`
12.27	12.32	12.36	`sha1`
29.43	29.57	29.57	`ripemd160`
45.26	45.89	46.17	`sha256`
178.05	178.48	179.41	`whirlpool`
185.06	185.07	185.21	`sha512`
288.75	289.75	290.44	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
7.06	7.08	7.08	`md4`
8.29	8.29	8.29	`md5`
11.06	11.09	11.11	`sha1`
27.82	27.89	27.89	`ripemd160`
44.40	44.51	44.69	`sha256`
173.85	174.17	176.33	`whirlpool`
175.72	175.78	178.92	`sha512`
283.48	284.30	287.19	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
6.40	6.43	6.43	`md4`
8.06	8.07	8.08	`md5`
10.23	10.31	10.34	`sha1`
26.67	26.89	26.92	`ripemd160`
43.29	43.70	45.00	`sha256`
170.01	170.22	176.51	`sha512`
171.26	172.36	176.89	`whirlpool`
276.02	280.02	286.51	`md2`

6.46 x86, 2995MHz, Intel Xeon (f41), nmi0079



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
91.00	92.75	94.75	`md5`
213.75	213.75	219.38	`md4`
245.62	246.50	246.62	`sha1`
300.88	305.62	309.38	`ripemd160`
561.50	570.88	582.12	`sha256`
1079.12	1094.00	1159.62	`sha512`
1160.62	1174.75	1185.00	`whirlpool`
1935.88	1937.88	1939.75	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
16.30	16.41	16.64	`md5`
30.81	30.94	30.94	`md4`
40.67	40.91	42.66	`sha1`
52.97	54.38	54.61	`ripemd160`
116.95	118.48	119.89	`sha256`
131.72	132.55	134.30	`sha512`
297.19	300.12	306.45	`whirlpool`
661.17	662.69	664.56	`md2`

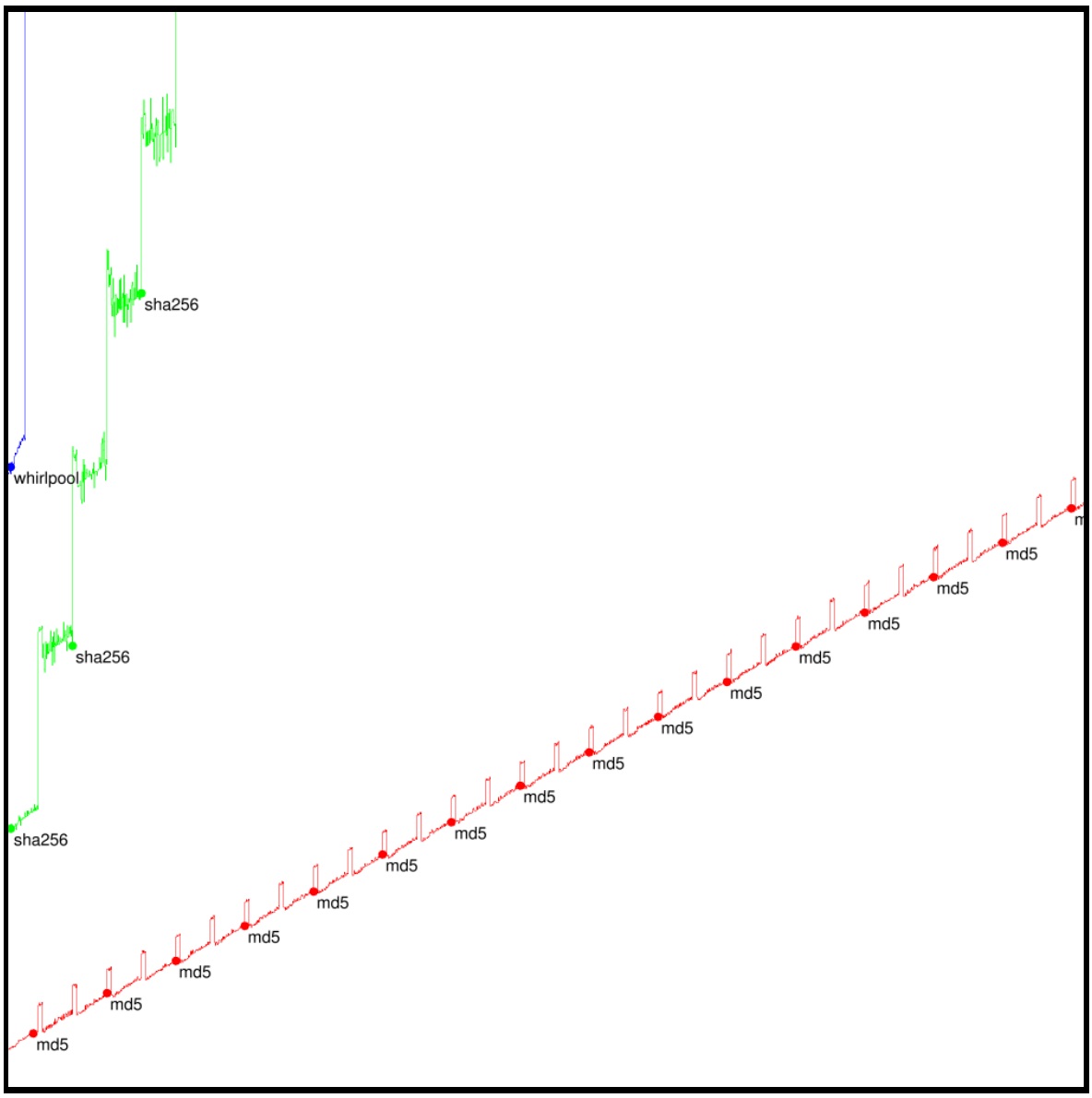
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
6.29	6.32	6.33	`md5`
8.07	8.12	8.15	`md4`
12.75	12.80	12.80	`sha1`
19.71	19.86	20.90	`ripemd160`
53.39	55.17	56.52	`sha512`
59.68	60.96	83.98	`sha256`
173.18	173.59	173.92	`whirlpool`
442.90	443.25	444.08	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
5.53	5.54	5.55	`md5`
6.02	6.03	6.04	`md4`
10.50	10.53	10.56	`sha1`
17.11	17.11	17.13	`ripemd160`
46.44	46.49	47.60	`sha512`
52.63	53.08	54.09	`sha256`
161.20	163.06	163.39	`whirlpool`
425.96	426.37	429.05	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
5.17	5.18	5.19	`md4`
5.23	5.23	5.24	`md5`
9.69	9.71	9.75	`sha1`
16.11	16.11	16.12	`ripemd160`
42.13	44.35	44.44	`sha512`
49.24	50.34	51.71	`sha256`
157.45	159.69	160.12	`whirlpool`
419.77	420.19	423.28	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
4.65	4.67	4.72	`md4`
5.04	5.05	5.08	`md5`
9.09	9.20	9.29	`sha1`
15.50	15.52	15.53	`ripemd160`
37.37	42.97	44.61	`sha512`
45.42	48.69	51.95	`sha256`
153.03	157.90	159.08	`whirlpool`
215.31	415.96	425.55	`md2`

6.47 x86, 2996MHz, Intel Xeon (f41), nmi0076



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
91.00	93.75	96.62	`md5`
602.75	604.62	617.88	`sha256`
1435.38	1443.75	1446.50	`whirlpool`
3028.12	3038.38	3039.38	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
15.70	16.05	16.88	`md5`
124.33	124.81	125.16	`sha256`
367.03	368.20	369.84	`whirlpool`
385.78	386.25	386.38	`sha512`

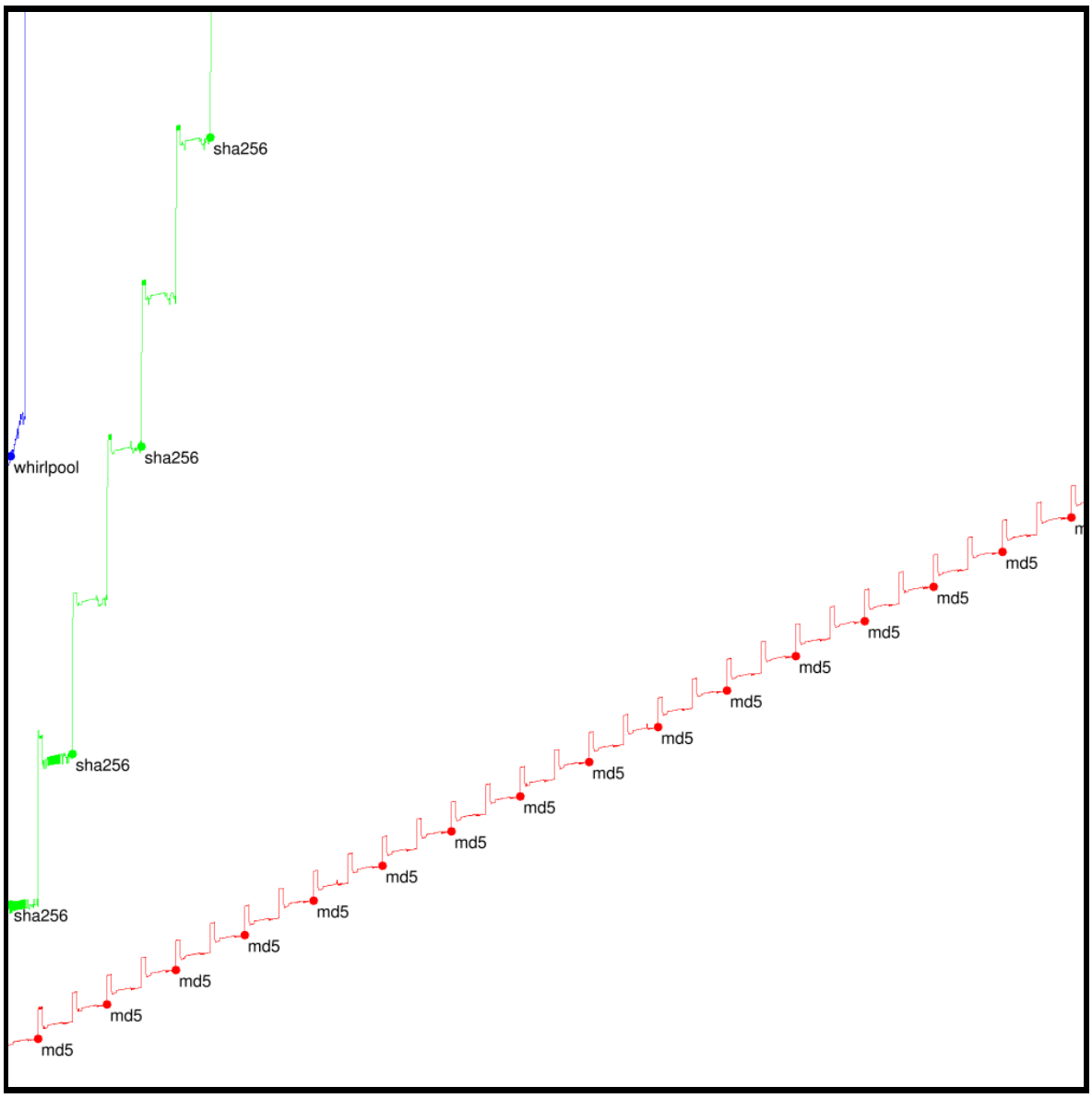
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
6.24	6.26	6.37	`md5`
57.85	57.86	57.88	`sha256`
186.17	186.19	186.24	`sha512`
210.69	210.95	211.30	`whirlpool`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
5.52	5.54	5.57	`md5`
52.60	52.93	55.58	`sha256`
176.80	176.80	176.93	`sha512`
198.38	198.61	198.98	`whirlpool`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
5.22	5.22	5.23	`md5`
50.68	51.89	53.86	`sha256`
166.87	166.91	167.48	`sha512`
193.72	194.00	197.56	`whirlpool`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
5.01	5.04	5.06	`md5`
49.50	51.95	55.90	`sha256`
160.80	160.99	162.13	`sha512`
189.76	191.24	198.60	`whirlpool`

6.48 x86, 3000MHz, Intel Xeon (f4a), nmi0090



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
97.50	98.38	98.50	`md5`
425.62	426.62	432.12	`sha256`
1462.50	1467.25	1481.25	`whirlpool`
2908.12	2910.00	2910.88	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
17.69	17.70	17.81	`md5`
93.62	93.64	94.09	`sha256`
365.50	365.52	365.62	`sha512`
375.58	376.17	377.58	`whirlpool`

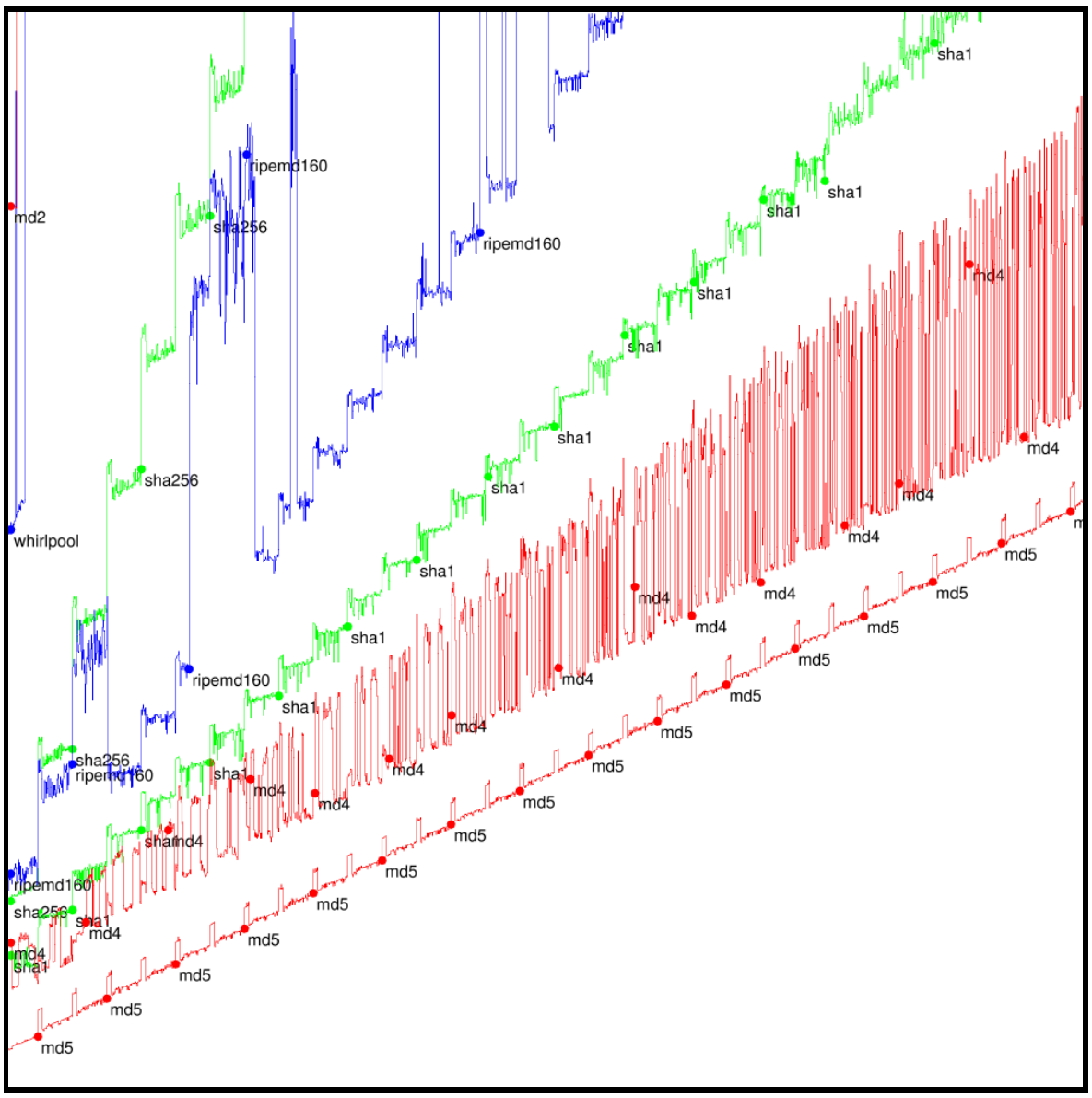
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
6.43	6.43	6.45	`md5`
50.09	50.09	50.09	`sha256`
192.92	192.93	192.93	`sha512`
217.59	218.11	218.67	`whirlpool`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
5.57	5.60	5.60	`md5`
46.82	46.83	46.86	`sha256`
186.55	186.56	186.56	`sha512`
204.84	205.05	205.36	`whirlpool`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
5.24	5.25	5.25	`md5`
42.33	45.65	45.67	`sha256`
177.10	177.10	177.10	`sha512`
199.98	200.17	200.32	`whirlpool`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
5.01	5.04	5.06	`md5`
38.29	44.95	44.98	`sha256`
171.42	171.42	171.43	`sha512`
196.73	197.40	197.96	`whirlpool`

6.49 x86, 3000MHz, Intel Xeon (f4a), nmi0102



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
93.75	94.75	106.00	`md5`
221.25	226.88	337.50	`md4`
309.38	310.38	315.00	`sha1`
436.88	442.50	447.12	`sha256`
310.25	493.12	523.12	`ripemd160`
1293.75	1301.25	2670.00	`whirlpool`
2042.75	2048.38	2604.38	`md2`
3073.12	3075.00	3084.38	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
16.75	16.77	17.23	`md5`
33.52	33.75	34.34	`md4`
48.75	49.11	50.28	`sha1`
54.38	83.44	91.41	`ripemd160`
90.58	92.58	93.98	`sha256`
330.59	331.53	582.42	`whirlpool`
388.36	388.47	388.59	`sha512`
692.69	693.28	989.64	`md2`

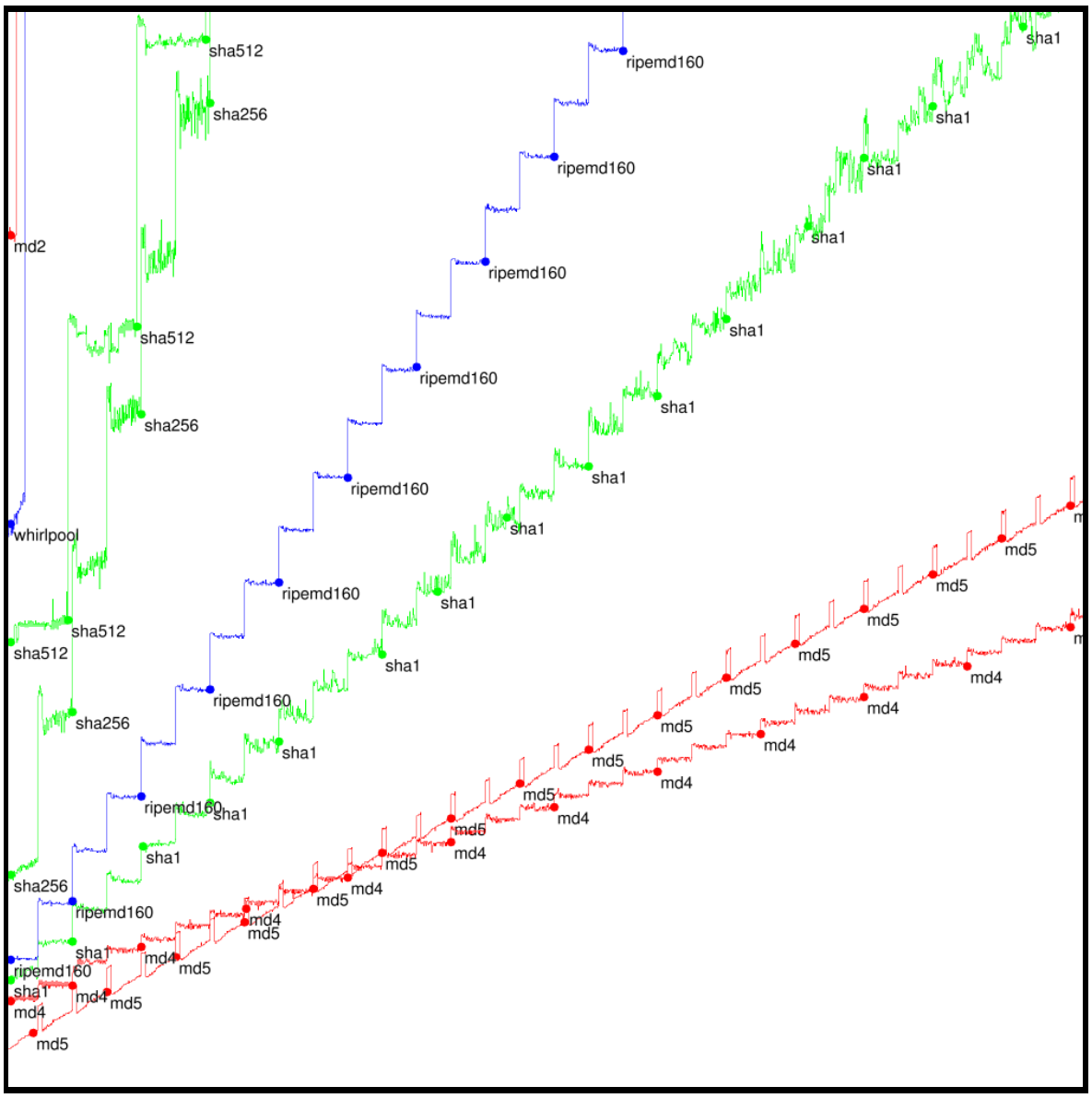
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
6.33	6.34	6.43	`md5`
9.02	12.28	12.93	`md4`
13.54	13.79	14.00	`sha1`
19.83	19.96	34.67	`ripemd160`
44.24	44.41	94.01	`sha256`
190.95	191.48	348.92	`whirlpool`
195.59	195.61	195.90	`sha512`
464.12	465.08	634.22	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
5.51	5.52	5.55	`md5`
8.47	9.34	9.47	`md4`
11.56	11.63	24.22	`sha1`
17.16	17.18	17.23	`ripemd160`
40.92	41.69	85.68	`sha256`
179.34	180.03	372.02	`whirlpool`
187.09	187.09	187.12	`sha512`
445.74	446.76	614.82	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
5.22	5.22	5.23	`md5`
5.76	7.61	8.91	`md4`
10.41	10.45	10.50	`sha1`
29.23	29.65	30.11	`ripemd160`
39.48	40.06	40.22	`sha256`
176.26	176.54	341.88	`whirlpool`
177.01	177.02	177.09	`sha512`
438.90	440.02	440.75	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
5.02	5.04	5.06	`md5`
5.17	8.91	11.51	`md4`
-2.00	9.51	9.84	`sha1`
-3.72	38.48	40.71	`sha256`
28.26	42.52	43.46	`ripemd160`
170.96	170.98	171.12	`sha512`
-14.30	173.90	504.95	`whirlpool`
270.72	435.40	437.83	`md2`

6.50 x86, 3391MHz, Intel Pentium D (f64), nmi0099


sha512
sha256
md2
sha512
sha256
whirlpool
sha512
sha256
ripemd160
sha256
ripemd160
ripemd160
ripemd160
ripemd160
ripemd160
ripemd160
ripemd160
ripemd160
sha1
sha1
sha1
sha1
sha1
sha1
sha1
sha1
sha1
sha1
sha1
sha1
sha1
sha1
sha1
md5
md5
md5
md5
md5
md5
md5
md5
md5
md5
md5
md5
md5
md5
md4
md4
md4
md4
md4
md4
md4
md4
md4
md4
md4
md4
md4
md4

Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
91.38	93.50	99.88	`md5`
197.62	201.88	204.00	`md4`
250.75	259.25	276.25	`sha1`
295.38	299.62	312.38	`ripemd160`
493.00	497.25	501.50	`sha256`
1026.38	1028.50	1041.25	`sha512`
1279.25	1287.75	1296.25	`whirlpool`
1967.75	1978.38	1986.88	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
15.94	16.20	16.73	`md5`
28.42	28.95	29.48	`md4`
40.91	41.44	42.50	`sha1`
52.59	52.86	53.92	`ripemd160`
103.33	106.78	108.91	`sha256`
133.08	133.88	134.41	`sha512`
324.06	326.45	329.11	`whirlpool`
668.84	670.70	673.89	`md2`

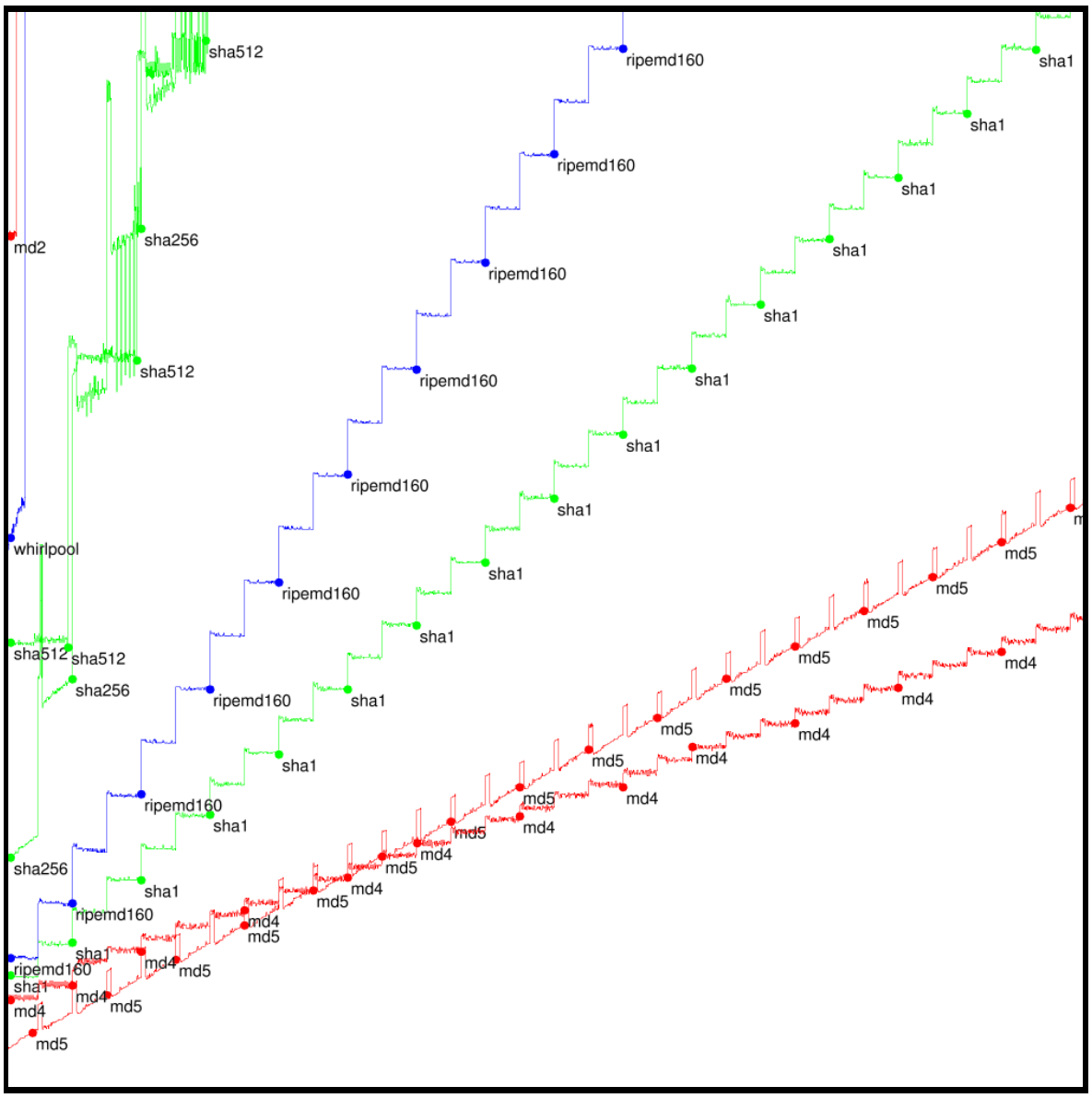
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
6.23	6.29	6.35	`md5`
6.70	6.73	6.79	`md4`
12.69	12.78	13.78	`sha1`
19.69	19.72	19.86	`ripemd160`
51.00	51.94	52.39	`sha256`
52.53	52.62	52.80	`sha512`
189.51	189.95	190.72	`whirlpool`
452.04	455.16	455.93	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
4.63	4.66	4.69	`md4`
5.54	5.57	5.60	`md5`
10.64	10.80	11.47	`sha1`
17.10	17.12	17.24	`ripemd160`
46.50	46.78	47.37	`sha256`
47.47	47.65	47.80	`sha512`
177.33	177.75	178.52	`whirlpool`
438.27	438.76	440.93	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
3.89	3.90	3.91	`md4`
5.22	5.23	5.25	`md5`
9.95	9.99	10.10	`sha1`
16.10	16.12	16.16	`ripemd160`
43.99	44.13	44.24	`sha512`
44.06	45.88	46.79	`sha256`
174.20	174.34	175.38	`whirlpool`
430.40	431.99	434.59	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
3.40	3.44	3.49	`md4`
5.00	5.05	5.09	`md5`
9.06	9.43	9.88	`sha1`
15.32	15.51	15.62	`ripemd160`
41.53	42.23	42.47	`sha512`
42.53	46.29	48.93	`sha256`
172.00	172.53	175.83	`whirlpool`
420.29	427.03	433.17	`md2`

6.51 x86, 3392MHz, Intel Pentium D (f64), nmi0104



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
95.62	95.62	102.00	`md5`
201.88	201.88	204.00	`md4`
255.00	255.00	257.12	`sha1`
297.50	299.62	299.62	`ripemd160`
537.62	539.75	544.00	`sha256`
1020.00	1032.75	1037.00	`sha512`
1281.38	1287.75	1296.25	`whirlpool`
1969.88	1972.00	1984.75	`md2`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
15.94	16.73	17.27	`md5`
28.42	28.69	29.22	`md4`
40.91	41.17	41.70	`sha1`
53.12	53.39	53.39	`ripemd160`
109.17	110.23	112.09	`sha256`
128.83	129.09	129.36	`sha512`
329.38	332.03	334.42	`whirlpool`
669.11	670.17	672.83	`md2`

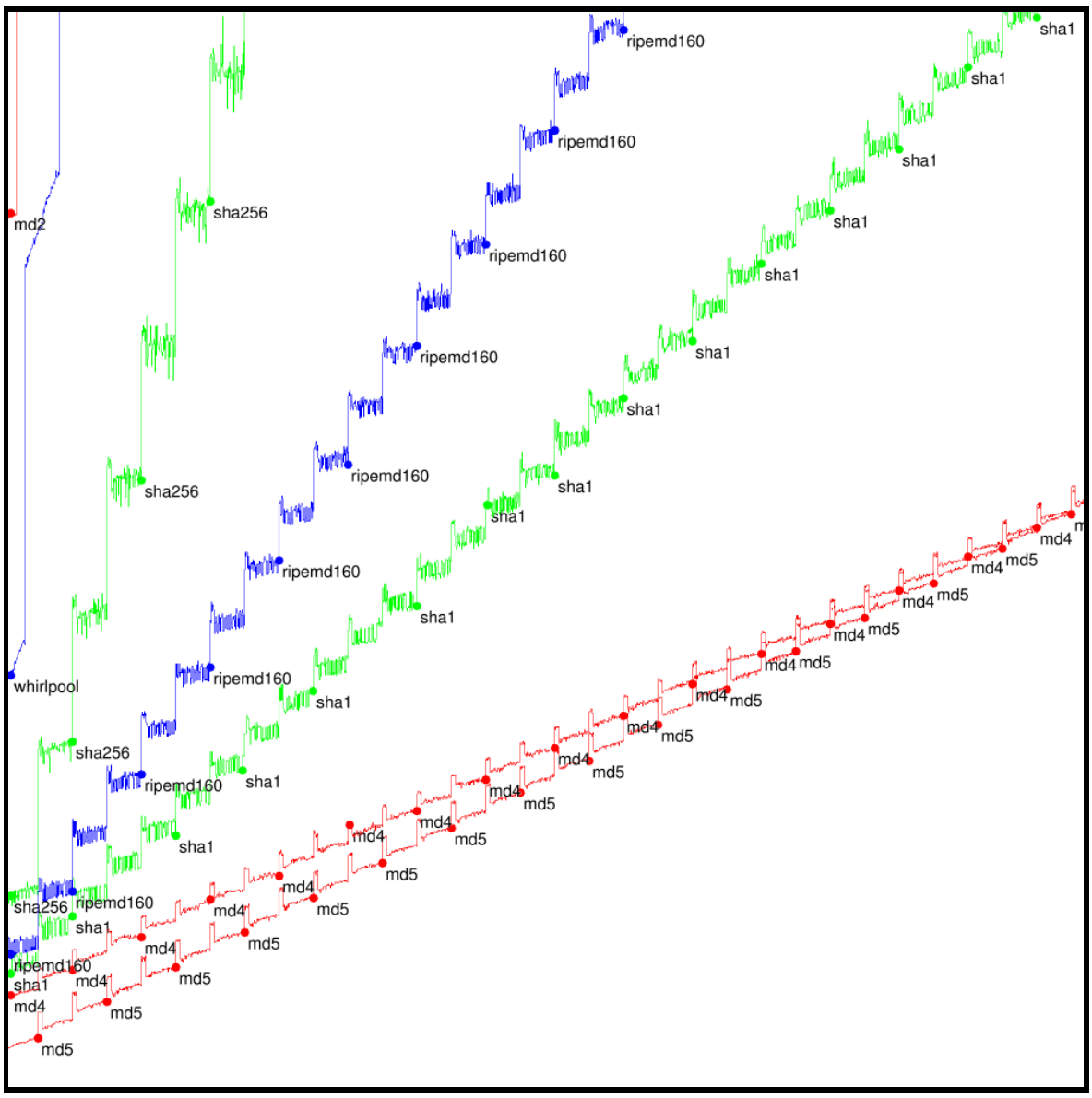
Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
6.26	6.35	6.38	`md5`
6.64	6.64	6.73	`md4`
12.81	12.84	12.93	`sha1`
19.77	19.80	19.80	`ripemd160`
51.89	52.03	52.24	`sha512`
55.72	56.52	57.85	`sha256`
188.18	188.62	189.07	`whirlpool`
452.42	453.21	455.10	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
4.65	4.66	4.68	`md4`
5.52	5.57	5.57	`md5`
10.62	10.62	10.62	`sha1`
17.11	17.12	17.12	`ripemd160`
44.87	46.67	46.95	`sha512`
46.72	48.04	49.09	`sha256`
177.64	177.92	178.27	`whirlpool`
435.06	438.13	438.76	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
3.90	3.91	3.99	`md4`
5.22	5.22	5.24	`md5`
9.77	9.78	9.87	`sha1`
16.11	16.12	16.12	`ripemd160`
41.66	42.33	43.19	`sha512`
44.67	45.05	45.97	`sha256`
172.72	173.72	174.71	`whirlpool`
431.95	433.11	437.29	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
3.43	3.45	3.63	`md4`
5.00	5.04	5.08	`md5`
9.26	9.27	9.45	`sha1`
15.49	15.51	15.51	`ripemd160`
37.99	40.39	42.97	`sha512`
41.47	42.79	45.27	`sha256`
168.79	171.86	174.28	`whirlpool`
428.03	433.12	441.58	`md2`

6.52 x86, 3392MHz, Intel Pentium D (f64), nmi0241



Cycles/byte to hash 8 bytes			
quartile	median	quartile	hash
91.38	93.50	99.88	`md5`
212.50	214.62	216.75	`md4`
261.38	265.62	269.88	`sha1`
308.12	310.25	337.88	`ripemd160`
433.50	446.25	595.00	`sha256`
964.75	969.00	975.38	`whirlpool`
2029.38	2031.50	2035.75	`md2`
3100.38	3106.75	3111.00	`sha512`

Cycles/byte to hash 64 bytes			
quartile	median	quartile	hash
15.94	16.73	17.27	`md5`
31.34	31.88	32.14	`md4`
47.28	47.55	47.81	`sha1`
53.92	54.45	57.64	`ripemd160`
92.17	94.03	97.22	`sha256`
251.02	252.08	254.20	`whirlpool`
391.80	392.06	392.06	`sha512`
687.17	687.70	687.97	`md2`

Cycles/byte to hash 576 bytes			
quartile	median	quartile	hash
6.35	6.38	6.46	`md5`
7.56	7.61	7.64	`md4`
13.58	13.64	13.72	`sha1`
19.86	20.31	21.43	`ripemd160`
45.75	45.81	45.86	`sha256`
149.22	149.84	150.02	`whirlpool`
190.07	190.07	190.10	`sha512`
461.63	461.95	463.52	`md2`

Cycles/byte to hash 1536 bytes			
quartile	median	quartile	hash
5.53	5.57	5.59	`md5`
5.72	5.74	5.74	`md4`
10.87	10.88	10.99	`sha1`
17.14	17.19	17.25	`ripemd160`
41.73	41.90	42.01	`sha256`
141.35	141.56	142.02	`whirlpool`
180.90	180.90	180.91	`sha512`
444.20	445.80	448.50	`md2`

Cycles/byte to hash 4096 bytes			
quartile	median	quartile	hash
5.00	5.00	5.01	`md4`
5.23	5.23	5.25	`md5`
10.01	10.06	10.09	`sha1`
16.13	16.14	16.19	`ripemd160`
38.66	39.88	40.97	`sha256`
138.21	138.44	139.50	`whirlpool`
170.80	170.80	172.15	`sha512`
438.22	439.03	440.96	`md2`

Cycles/byte to hash long messages			
quartile	median	quartile	hash
4.53	4.56	4.59	`md4`
5.01	5.02	5.06	`md5`
9.30	9.40	9.64	`sha1`
15.35	15.42	15.61	`ripemd160`
34.79	38.25	40.93	`sha256`
135.56	136.31	138.78	`whirlpool`
164.73	164.74	167.44	`sha512`
432.01	435.26	440.26	`md2`

Chapter 7

Measurements of secret-key stream ciphers

7.1 Introduction

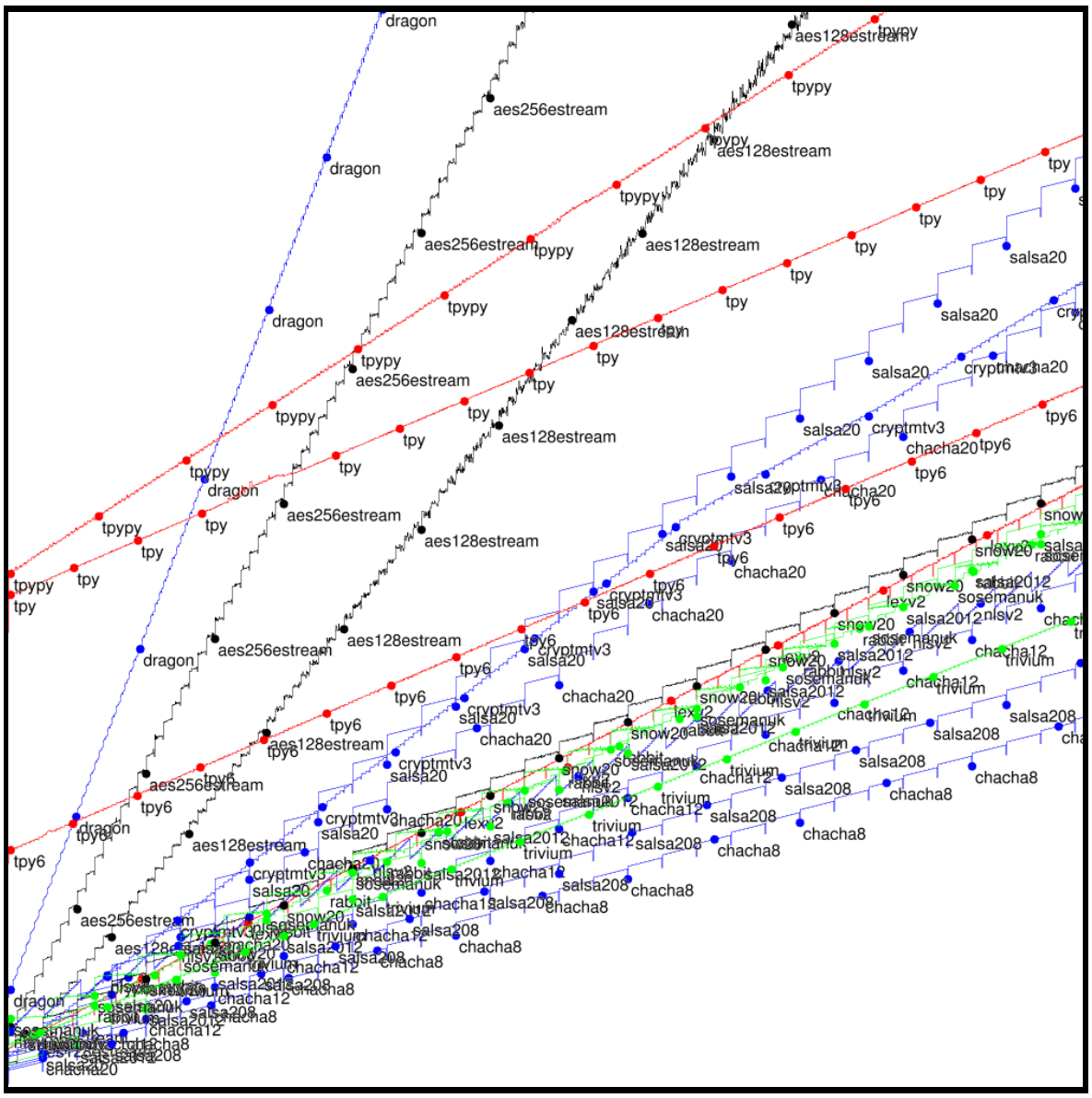
This chapter presents a series of graphs, one for each computer. The horizontal axis on each graph is message length, from 0 bytes to 2000 bytes. The vertical axis on each graph is time, from 0 cycles to 20000 cycles. The bottom-left-to-top-right diagonal is 10 cycles/byte. Each graph is a superimposition of several curves, one curve for each stream cipher.

This chapter also presents a series of tables, six tables for each computer. The first table shows the speed, in cycles/byte, of encrypting 8-byte messages. Each row of the table lists

- the first quartile of many speed measurements,
- the median of many speed measurements,
- the third quartile of many speed measurements, and
- the name of the stream cipher.

The second table shows the speed of encrypting 64-byte messages. The third table shows the speed of encrypting 576-byte messages. The fourth table shows the speed of encrypting 1536-byte messages. The fifth table shows the speed of encrypting 4096-byte messages. The sixth table shows the speed of encrypting long messages; this is computed as 1/2048 of the difference in cycle counts between encrypting 4096-byte messages and encrypting 2048-byte messages.

7.2 amd64, 1403MHz, AMD Opteron 240 (f58), nmisles8amd64



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
41.12	41.12	41.12	chacha8
45.75	45.75	45.88	salsa208
51.62	51.62	51.88	chacha12
56.38	56.88	56.88	aes128estream
58.00	58.00	58.12	salsa2012
72.62	72.62	72.62	chacha20
75.38	75.38	77.00	cryptmtv3
82.12	82.12	83.62	salsa20
93.00	93.50	93.62	lexv2
95.75	95.75	95.75	trivium
101.62	103.75	105.00	rabbit
118.88	119.38	120.75	snow20
135.50	136.38	137.38	nlsv2
141.00	142.12	142.88	aes256estream
158.62	159.00	160.25	sosemanuk
233.50	233.88	235.62	dragon
548.88	550.50	551.12	tpy6
1140.88	1142.25	1143.75	tpy
1193.88	1197.00	1197.75	tpypy
2587.50	2588.62	2589.88	hc128
9230.12	9254.38	9260.12	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
4.41	4.41	4.64	chacha8
4.92	4.92	5.17	salsa208
5.72	5.72	5.95	chacha12
6.45	6.45	6.45	salsa2012
8.34	8.34	8.53	chacha20
9.48	9.64	9.75	salsa20
15.09	15.20	15.33	snow20
15.47	15.47	15.47	trivium
15.78	15.78	16.06	cryptmtv3
16.38	16.41	16.53	rabbit
16.41	16.41	16.42	lexv2
16.91	16.94	17.08	aes128estream
20.16	20.17	20.22	sosemanuk
25.61	25.66	25.67	nlsv2
31.84	31.98	32.08	aes256estream
52.55	52.59	52.78	dragon
72.64	72.66	72.86	tpy6
146.34	146.58	146.70	tpy
155.03	155.50	155.75	tpypy
323.84	323.84	324.20	hc128
1153.77	1158.09	1158.28	hc256

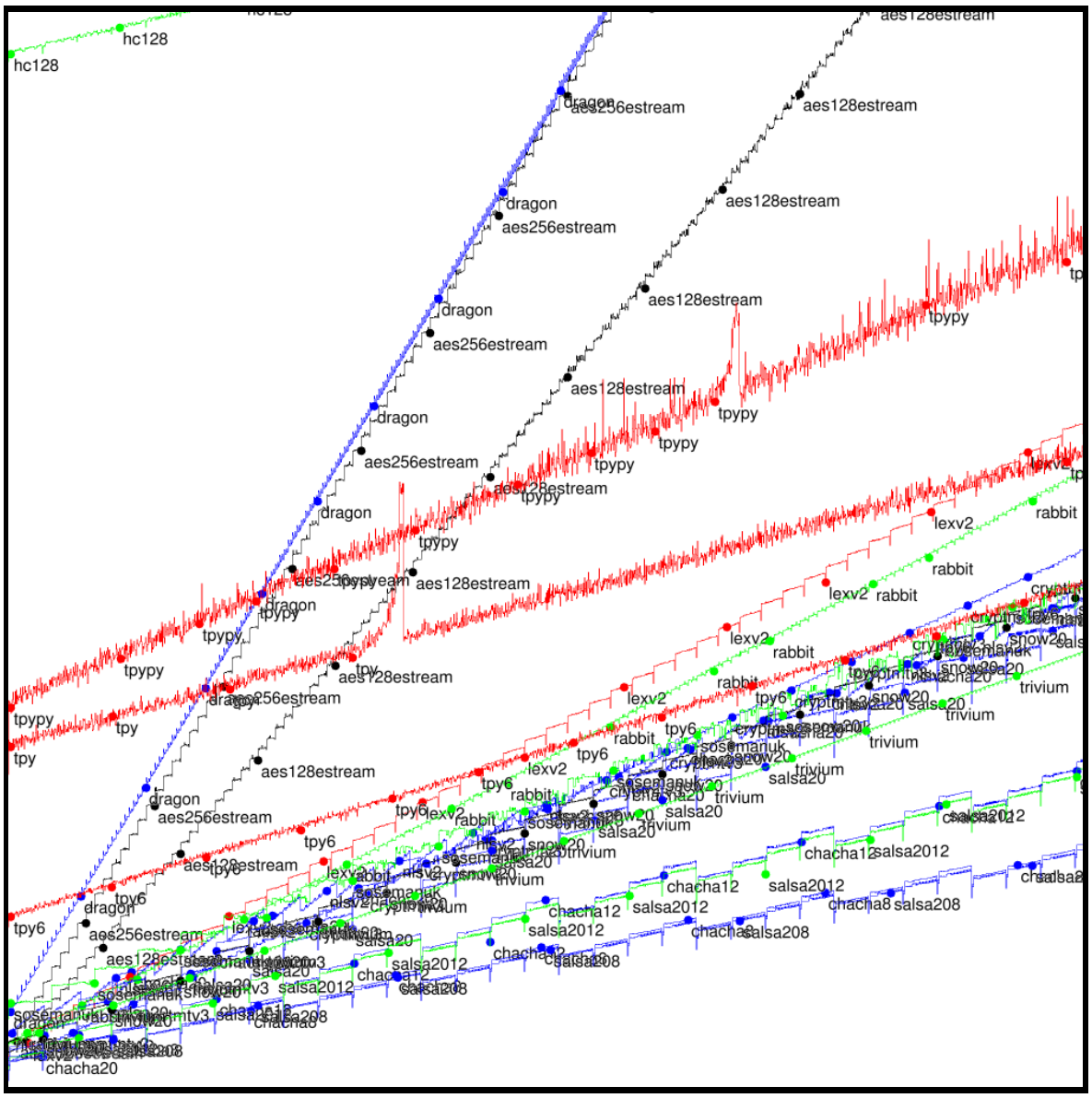
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
3.43	3.43	3.45	chacha8
3.94	3.94	3.96	salsa208
4.74	4.74	4.77	chacha12
5.30	5.30	5.30	trivium
5.47	5.47	5.48	salsa2012
6.18	6.18	6.19	rabbit
6.32	6.33	6.34	nlsv2
6.44	6.44	6.47	snow20
6.49	6.50	6.51	lexv2
6.88	6.89	6.89	sosemanuk
7.37	7.37	7.40	chacha20
8.53	8.55	8.55	salsa20
8.83	8.85	8.87	cryptmtv3
11.92	11.93	11.95	tpy6
13.64	13.65	13.74	aes128estream
20.11	20.13	20.14	tpy
21.03	21.05	21.07	aes256estream
22.93	22.98	22.98	tpypy
29.28	29.29	29.31	dragon
38.40	38.40	38.44	hc128
133.66	133.70	133.72	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
3.34	3.34	3.35	chacha8
3.84	3.84	3.85	salsa208
4.49	4.49	4.49	trivium
4.65	4.65	4.66	chacha12
5.10	5.10	5.11	nlsv2
5.37	5.37	5.37	salsa2012
5.37	5.37	5.38	rabbit
5.56	5.56	5.56	sosemanuk
5.71	5.71	5.72	lexv2
5.74	5.74	5.75	snow20
7.18	7.18	7.18	tpy6
7.28	7.28	7.29	chacha20
7.89	7.89	7.90	cryptmtv3
8.43	8.44	8.44	salsa20
10.23	10.23	10.24	tpy
12.61	12.62	12.63	tpypy
13.40	13.52	13.54	aes128estream
16.16	16.17	16.18	hc128
20.15	20.16	20.21	aes256estream
27.47	27.47	27.48	dragon
53.63	53.64	53.66	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
3.30	3.30	3.31	chacha8
3.80	3.80	3.81	salsa208
4.18	4.18	4.18	trivium
4.56	4.56	4.56	nlsv2
4.61	4.62	4.62	chacha12
5.06	5.06	5.06	rabbit
5.06	5.07	5.07	sosemanuk
5.33	5.33	5.34	salsa2012
5.39	5.39	5.40	tpy6
5.40	5.40	5.42	lexv2
5.48	5.48	5.48	snow20
6.52	6.52	6.52	tpy
6.81	6.81	6.81	cryptmtv3
7.24	7.24	7.24	chacha20
7.74	7.74	7.74	hc128
8.40	8.40	8.40	salsa20
8.73	8.73	8.73	tpypy
13.21	13.26	13.37	aes128estream
19.84	19.84	19.86	aes256estream
23.62	23.62	23.63	hc256
26.79	26.80	26.80	dragon

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
2.66	2.67	2.68	hc128
3.27	3.28	3.29	chacha8
3.77	3.78	3.79	salsa208
4.00	4.00	4.00	trivium
4.28	4.29	4.30	tpy
4.31	4.31	4.32	nlsv2
4.30	4.32	4.32	tpy6
4.59	4.60	4.60	chacha12
4.80	4.82	4.85	sosemanuk
4.87	4.88	4.88	rabbit
5.23	5.23	5.27	lexv2
5.31	5.31	5.32	salsa2012
5.28	5.31	5.33	snow20
5.60	5.61	5.64	hc256
6.17	6.17	6.18	cryptmtv3
6.38	6.40	6.40	tpypy
7.21	7.22	7.23	chacha20
8.37	8.38	8.38	salsa20
13.13	13.24	13.48	aes128estream
19.60	19.62	19.68	aes256estream
26.38	26.39	26.40	dragon

7.3 amd64, 2400MHz, Intel Core 2 Duo (6fb), `utrecht`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
57.38	59.62	60.75	salsa208
59.62	60.75	60.75	chacha8
60.75	61.88	61.88	cryptmtv3
65.25	67.50	69.75	salsa2012
72.00	72.00	72.00	chacha12
82.12	83.25	84.38	aes128estream
84.38	87.75	87.75	salsa20
92.25	93.38	93.38	chacha20
99.00	99.00	100.12	trivium
103.50	105.75	110.25	lexv2
105.75	105.75	106.88	rabbit
106.88	106.88	106.88	aes256estream
109.12	109.12	110.25	snow20
127.12	127.12	128.25	nlsv2
178.88	178.88	180.00	dragon
194.62	195.75	195.75	sosemanuk
384.75	397.12	408.38	tpy6
781.88	783.00	796.50	tpy
879.75	901.12	914.62	tpypy
2405.25	2410.88	2413.12	hc128
6139.12	6141.38	6144.75	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
4.78	4.78	4.92	chacha8
4.92	4.92	4.92	salsa208
5.91	5.91	5.91	salsa2012
6.19	6.19	6.33	chacha12
8.30	8.30	8.30	salsa20
8.72	8.72	8.86	chacha20
11.11	11.25	11.25	cryptmtv3
13.64	13.78	13.78	snow20
15.47	15.61	15.61	trivium
16.88	17.02	17.16	rabbit
17.44	17.58	17.86	lexv2
18.98	19.12	19.12	aes128estream
23.06	23.06	23.06	nlsv2
24.47	24.47	24.75	sosemanuk
25.73	25.88	25.88	aes256estream
36.70	36.70	36.98	dragon
51.75	52.73	54.14	tpy6
99.42	102.38	102.52	tpy
111.80	114.19	116.58	tpypy
300.23	300.38	301.22	hc128
767.53	767.95	767.95	hc256

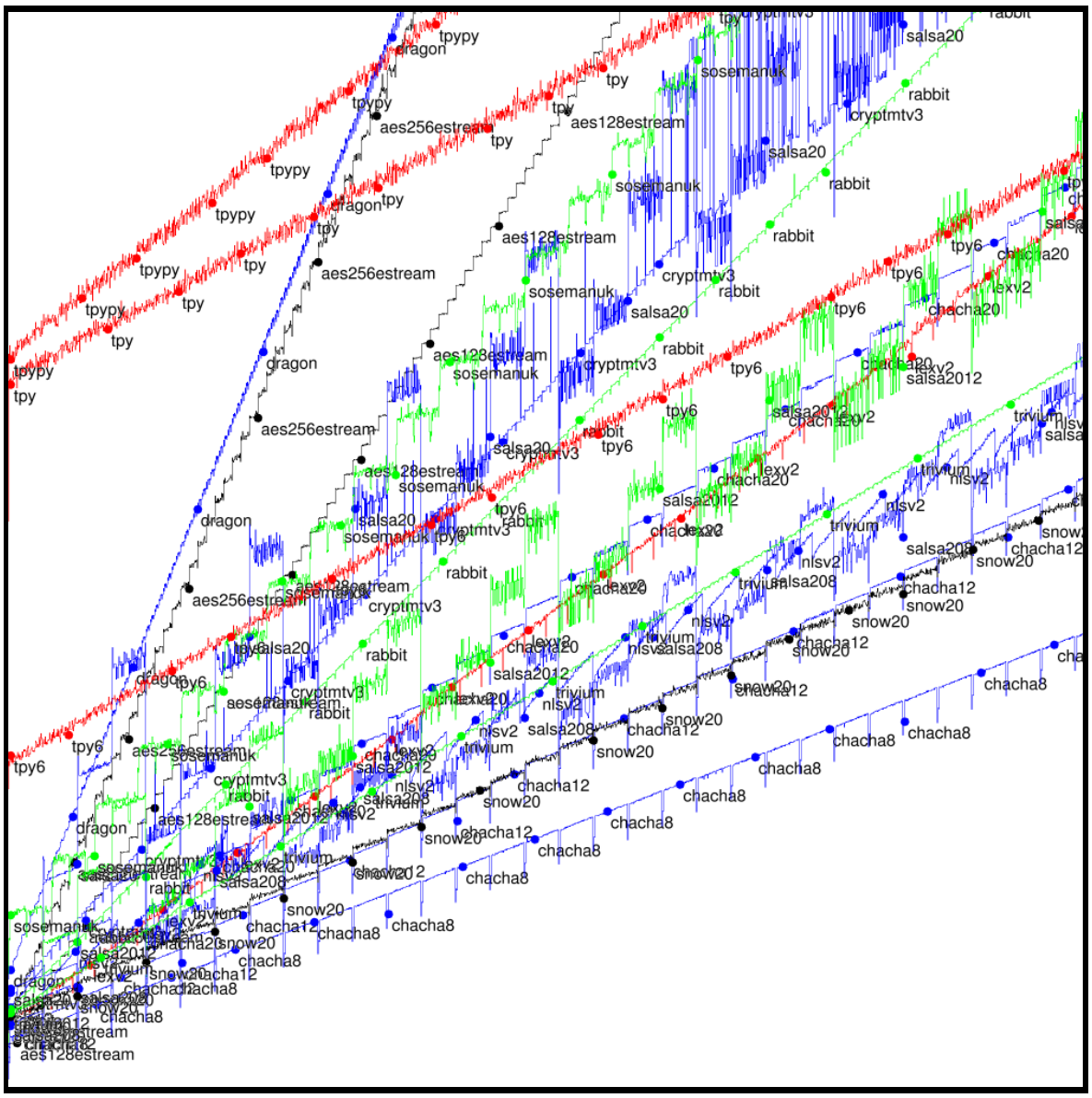
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
2.23	2.25	2.25	salsa208
2.27	2.27	2.28	chacha8
2.92	2.95	2.97	salsa2012
3.00	3.00	3.02	chacha12
4.39	4.42	4.47	salsa20
4.58	4.59	4.59	chacha20
4.95	4.95	4.95	trivium
5.34	5.34	5.34	snow20
5.55	5.55	5.56	cryptmtv3
6.06	6.08	6.14	nlsv2
6.45	6.52	6.64	sosemanuk
6.58	6.58	6.58	rabbit
7.23	7.23	7.27	lexv2
8.48	8.52	8.72	tpy6
12.94	12.94	12.95	aes128estream
13.78	13.94	13.97	tpy
16.34	16.56	16.73	tpypy
18.11	18.12	18.14	aes256estream
18.94	18.97	19.00	dragon
35.58	35.59	35.62	hc128
88.64	88.73	88.73	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
1.98	1.98	1.99	salsa208
2.00	2.00	2.03	chacha8
2.64	2.66	2.66	salsa2012
2.68	2.68	2.68	chacha12
3.99	3.99	4.00	salsa20
4.11	4.11	4.11	chacha20
4.15	4.15	4.15	trivium
4.67	4.68	4.68	snow20
4.76	4.78	4.79	nlsv2
4.98	4.99	5.00	sosemanuk
5.04	5.06	5.06	cryptmtv3
5.10	5.14	5.19	tpy6
5.79	5.80	5.80	rabbit
6.32	6.33	6.33	lexv2
6.84	6.90	7.04	tpy
8.77	8.81	9.43	tpypy
12.47	12.48	12.49	aes128estream
14.82	14.85	14.86	hc128
17.54	17.55	17.61	aes256estream
17.57	17.58	17.60	dragon
35.56	35.58	35.60	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
1.92	1.92	1.93	`salsa208`
1.94	1.94	1.94	`chacha8`
2.60	2.60	2.60	`salsa2012`
2.62	2.62	2.64	`chacha12`
3.61	3.62	3.62	`cryptmtv3`
3.83	3.83	3.83	`trivium`
3.85	3.87	3.90	`tpy6`
3.94	3.94	3.94	`salsa20`
4.05	4.06	4.06	`chacha20`
4.21	4.22	4.22	`nlsv2`
4.27	4.28	4.29	`tpy`
4.35	4.36	4.36	`sosemanuk`
4.43	4.43	4.45	`snow20`
5.50	5.50	5.50	`rabbit`
5.99	5.99	5.99	`lexv2`
5.99	6.04	6.05	`tpypy`
7.06	7.06	7.09	`hc128`
12.30	12.30	12.31	`aes128estream`
15.68	15.69	15.74	`hc256`
16.97	16.99	17.00	`dragon`
17.33	17.34	17.35	`aes256estream`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
1.89	1.89	1.89	`salsa208`
1.89	1.89	1.90	`chacha8`
2.25	2.26	2.28	`cryptmtv3`
2.39	2.40	2.47	`hc128`
2.57	2.58	2.58	`salsa2012`
2.58	2.59	2.63	`chacha12`
2.64	2.72	2.78	`tpy`
3.03	3.12	3.21	`tpy6`
3.64	3.64	3.64	`trivium`
3.71	3.72	3.84	`hc256`
3.89	3.91	3.92	`salsa20`
3.91	3.93	3.94	`nlsv2`
4.01	4.02	4.03	`sosemanuk`
4.01	4.03	4.03	`chacha20`
4.01	4.24	4.30	`tpypy`
4.27	4.28	4.31	`snow20`
5.30	5.30	5.34	`rabbit`
5.77	5.77	5.79	`lexv2`
12.16	12.20	12.22	`aes128estream`
16.58	16.64	16.68	`dragon`
17.15	17.17	17.23	`aes256estream`

7.4 amd64, 2800MHz, Intel Xeon (f41), nmi0056



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
101.50	101.50	103.25	aes128estream
105.88	106.75	115.50	chacha8
116.38	117.25	117.25	chacha12
140.88	140.88	141.75	chacha20
147.00	147.88	148.75	salsa208
152.25	155.75	156.62	lexv2
161.00	162.75	163.62	aes256estream
162.75	165.38	173.25	snow20
165.38	166.25	168.00	trivium
172.38	172.38	173.25	salsa2012
183.75	183.75	188.12	rabbit
190.75	190.75	192.50	nlsv2
213.50	214.38	217.88	cryptmtv3
228.38	228.38	228.38	salsa20
275.62	277.38	278.25	dragon
392.88	398.12	399.88	sosemanuk
742.88	751.62	757.75	tpy6
1622.25	1628.38	1638.88	tpy
1694.00	1710.62	1716.75	tpypy
3801.88	3804.50	3810.62	hc128
9783.38	9845.50	9870.88	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
6.67	7.44	7.77	chacha8
8.86	8.97	9.08	chacha12
11.92	12.03	12.25	chacha20
16.19	16.19	16.19	salsa208
20.23	21.44	21.88	snow20
22.20	22.75	22.86	salsa2012
24.94	25.16	25.48	aes128estream
25.27	25.38	25.38	lexv2
26.14	26.36	26.47	trivium
29.97	30.08	30.08	rabbit
33.91	34.12	34.12	salsa20
33.91	34.23	34.34	cryptmtv3
34.45	34.45	34.56	nlsv2
37.73	38.06	38.83	aes256estream
43.42	44.62	45.06	sosemanuk
56.77	57.09	57.86	dragon
98.22	98.88	99.64	tpy6
210.11	211.09	211.97	tpy
219.62	220.50	225.20	tpypy
475.02	475.89	476.77	hc128
1227.19	1228.94	1233.86	hc256

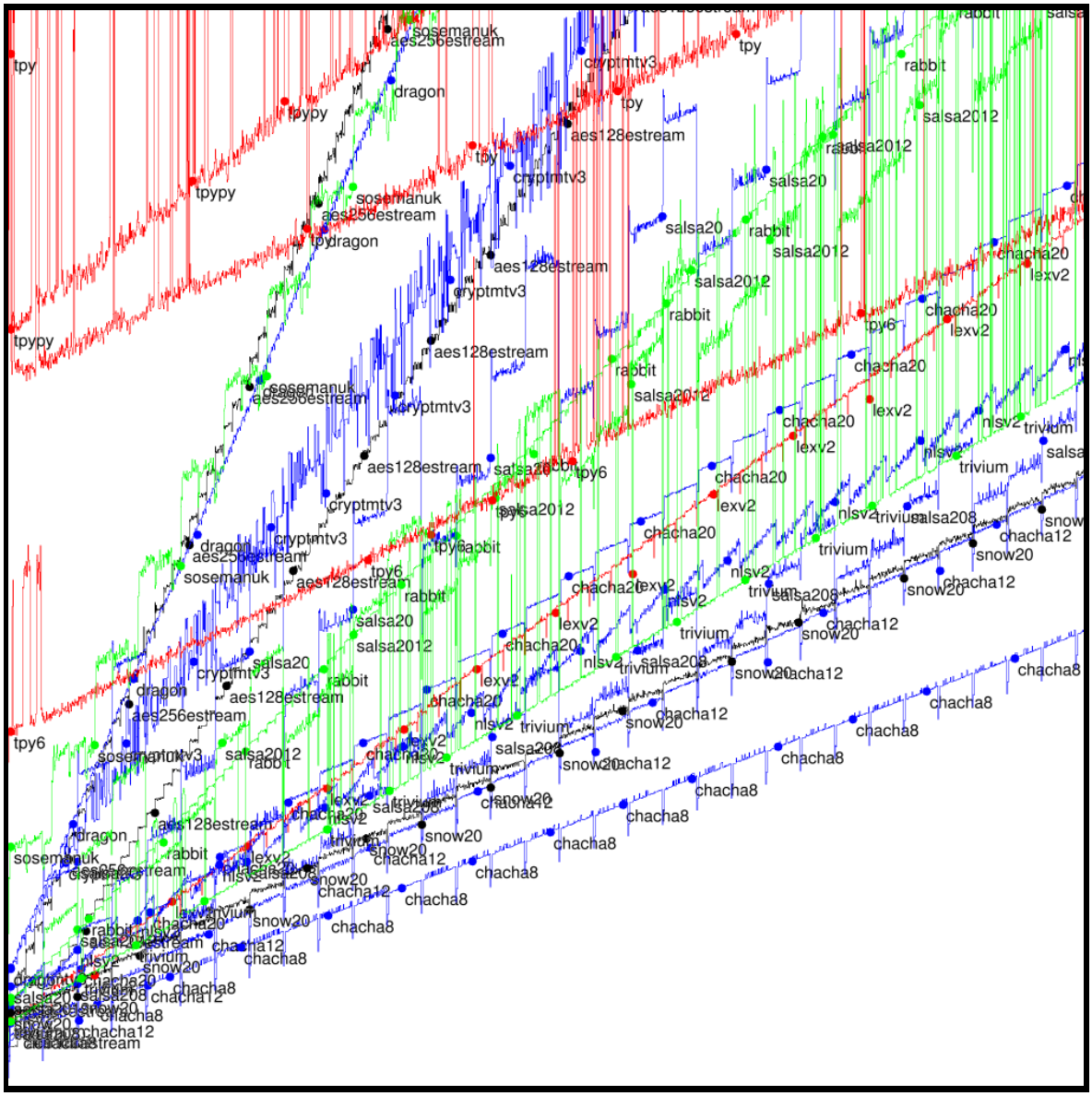
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
4.28	4.29	4.30	chacha8
5.69	5.70	5.70	chacha12
6.10	6.36	6.72	salsa208
6.55	6.60	6.72	snow20
8.42	8.45	8.46	trivium
8.54	8.56	8.57	chacha20
8.63	8.64	8.66	nlsv2
8.63	8.80	9.94	salsa2012
9.44	9.45	9.49	lexv2
11.91	11.98	12.48	salsa20
12.61	12.61	12.61	rabbit
13.99	14.02	14.04	cryptmtv3
15.84	15.90	16.19	tpy6
17.89	17.93	17.94	aes128estream
18.00	18.11	18.12	sosemanuk
26.40	26.64	26.66	aes256estream
28.15	28.16	28.22	dragon
28.26	28.43	28.75	tpy
31.23	31.35	31.82	tpypy
57.13	57.19	57.32	hc128
141.66	141.85	141.87	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
3.93	3.94	3.95	chacha8
5.32	5.34	5.36	chacha12
5.54	5.56	5.59	snow20
5.73	5.89	5.95	salsa208
6.76	6.76	6.78	nlsv2
6.95	6.97	6.98	trivium
7.43	7.57	7.59	salsa2012
8.21	8.21	8.22	chacha20
8.31	8.33	8.34	lexv2
9.47	9.50	9.59	tpy6
10.46	10.54	11.20	salsa20
11.19	11.19	11.50	rabbit
11.68	11.68	11.70	cryptmtv3
13.85	13.98	14.10	tpy
14.67	14.67	14.98	sosemanuk
16.65	16.92	16.94	tpypy
17.28	17.29	17.29	aes128estream
24.52	24.53	24.54	hc128
25.38	25.53	25.62	aes256estream
25.81	25.82	25.88	dragon
56.51	56.52	56.64	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
3.82	3.82	3.82	`chacha8`
5.15	5.16	5.18	`snow20`
5.23	5.23	5.23	`chacha12`
5.68	5.68	5.68	`salsa208`
5.95	5.96	5.96	`nlsv2`
6.42	6.42	6.43	`trivium`
7.09	7.15	7.18	`tpy6`
7.26	7.26	7.39	`salsa2012`
7.87	7.90	7.94	`lexv2`
8.02	8.04	8.04	`cryptmtv3`
8.07	8.08	8.08	`chacha20`
8.62	8.72	8.73	`tpy`
10.64	10.64	10.64	`rabbit`
10.83	10.90	10.90	`salsa20`
11.28	11.34	11.36	`tpypy`
12.25	12.26	12.29	`hc128`
13.44	13.46	13.47	`sosemanuk`
17.05	17.10	17.12	`aes128estream`
24.59	24.60	24.60	`hc256`
24.93	25.00	25.02	`dragon`
25.20	25.20	25.35	`aes256estream`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
3.73	3.74	3.75	`chacha8`
4.86	4.90	5.00	`snow20`
4.88	4.91	4.98	`hc128`
3.51	5.12	5.13	`cryptmtv3`
5.15	5.16	5.16	`chacha12`
5.26	5.52	5.75	`hc256`
5.55	5.57	5.58	`nlsv2`
5.38	5.58	5.70	`tpy`
5.63	5.68	5.74	`salsa208`
5.51	5.70	5.82	`tpy6`
6.09	6.10	6.11	`trivium`
6.86	7.02	7.41	`salsa2012`
7.54	7.59	7.68	`lexv2`
7.99	8.00	8.01	`chacha20`
7.90	8.08	8.20	`tpypy`
10.31	10.31	10.32	`rabbit`
10.62	10.76	10.77	`salsa20`
12.85	12.90	12.92	`sosemanuk`
16.90	17.01	17.10	`aes128estream`
24.40	24.54	24.59	`dragon`
24.94	24.96	25.43	`aes256estream`

7.5 amd64, 2800MHz, Intel Xeon (f41), `nmi0057`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
91.00	91.00	91.88	aes128estream
105.88	106.75	106.75	chacha8
120.75	120.75	121.62	chacha12
142.62	143.50	231.00	chacha20
143.50	146.12	147.88	trivium
139.12	147.00	147.88	salsa208
154.00	154.88	163.62	lexv2
162.75	168.88	169.75	snow20
185.50	187.25	191.62	nlsv2
196.00	197.75	198.62	rabbit
200.38	202.12	203.88	aes256estream
199.50	203.00	205.62	salsa2012
223.12	230.12	231.00	salsa20
269.50	270.38	271.25	dragon
275.62	276.50	280.00	cryptmtv3
535.50	546.88	560.00	sosemanuk
823.38	1114.75	1149.75	tpy6
1756.12	1778.00	2677.50	tpypy
1639.75	2349.38	2522.62	tpy
3985.62	3989.12	4287.50	hc128
14703.50	15192.60	15257.40	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
6.67	7.33	7.55	chacha8
8.09	8.64	9.41	chacha12
10.83	12.03	20.56	chacha20
16.08	16.08	16.08	salsa208
20.12	20.23	21.11	snow20
23.19	23.62	23.84	trivium
21.22	23.73	26.36	salsa2012
23.84	23.95	23.95	aes128estream
25.16	25.48	25.92	lexv2
32.05	32.16	32.48	rabbit
33.36	33.80	33.91	salsa20
33.91	34.23	59.94	nlsv2
44.08	44.41	44.84	aes256estream
51.84	53.59	53.70	cryptmtv3
55.23	55.34	55.45	dragon
62.12	64.20	67.16	sosemanuk
107.08	108.28	152.91	tpy6
208.36	210.66	210.88	tpy
224.00	226.52	228.59	tpypy
498.64	500.28	514.50	hc128
1826.23	1889.56	1903.78	hc256

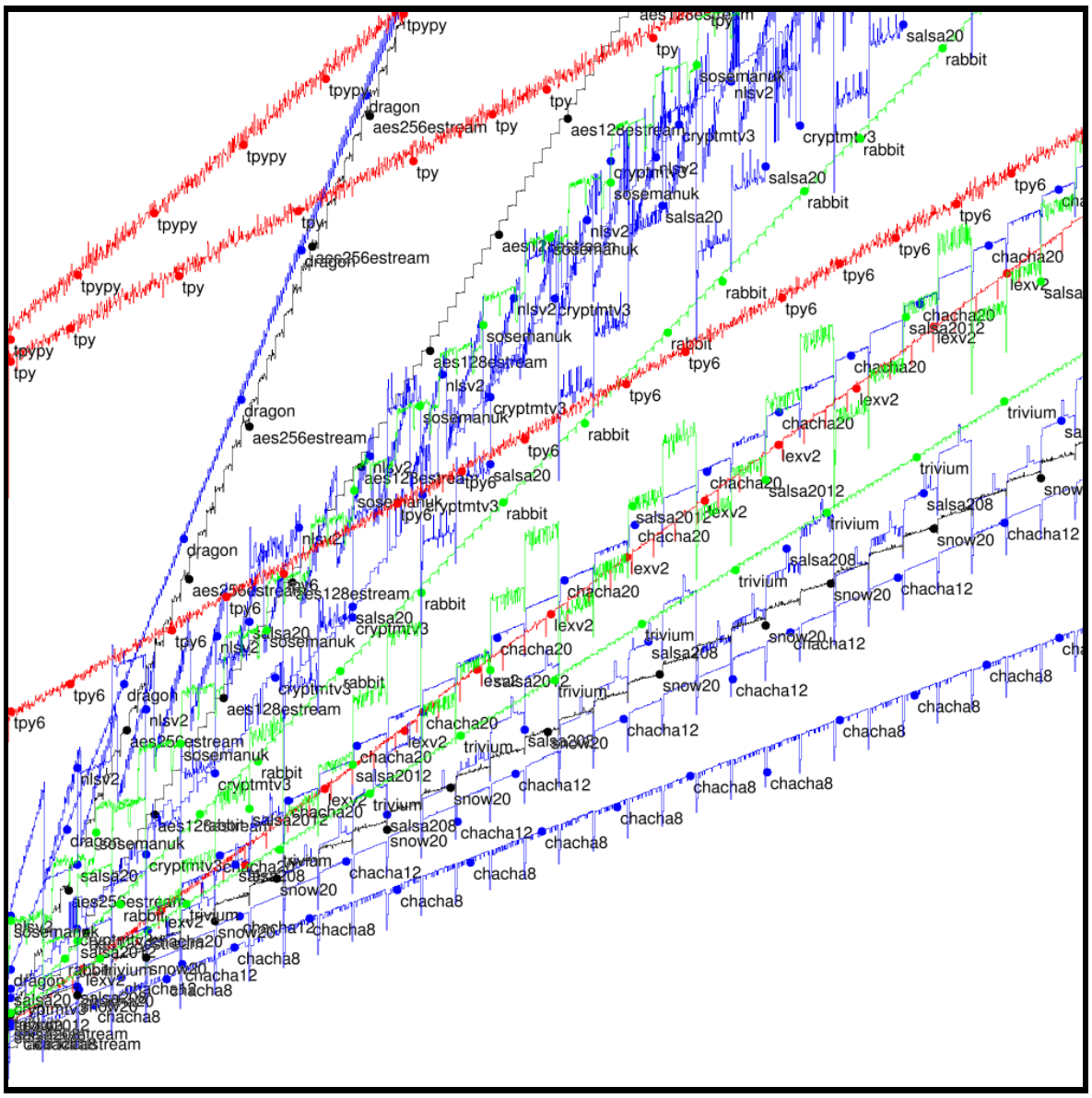
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
4.31	4.33	4.34	chacha8
5.68	5.75	5.77	chacha12
5.93	6.00	6.20	salsa208
6.78	6.81	6.83	snow20
8.02	8.06	8.08	trivium
8.53	8.58	8.60	chacha20
8.77	8.90	8.99	nlsv2
9.41	9.44	9.56	lexv2
10.01	10.33	10.74	salsa2012
11.81	12.03	12.20	salsa20
13.16	13.16	13.17	rabbit
16.09	16.18	16.33	tpy6
17.69	17.69	17.72	aes128estream
19.93	21.13	21.18	cryptmtv3
27.17	27.23	27.25	dragon
27.38	27.49	27.65	tpy
28.36	28.47	28.51	aes256estream
28.38	28.83	29.39	sosemanuk
31.63	31.82	32.06	tpypy
59.32	63.38	63.57	hc128
208.42	215.71	218.47	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
3.96	3.96	3.96	chacha8
5.35	5.36	5.37	chacha12
5.51	5.65	5.76	salsa208
5.72	5.74	5.79	snow20
6.72	6.72	6.74	trivium
7.05	7.07	7.12	nlsv2
8.19	8.21	8.23	chacha20
8.23	8.24	8.26	lexv2
9.05	9.11	9.19	tpy6
9.33	9.49	10.01	salsa2012
10.76	10.84	10.94	salsa20
11.58	11.58	11.59	rabbit
13.06	13.24	13.32	tpy
15.46	16.46	16.88	cryptmtv3
16.77	16.92	34.73	tpypy
17.04	17.06	17.23	aes128estream
23.43	23.67	24.31	sosemanuk
24.92	24.98	24.99	dragon
25.41	26.43	26.51	hc128
26.96	26.98	27.04	aes256estream
80.99	83.35	84.98	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
3.83	3.83	3.83	`chacha8`
5.23	5.24	5.24	`chacha12`
5.34	5.36	5.37	`snow20`
5.41	5.43	5.45	`salsa208`
6.23	6.23	6.23	`trivium`
6.34	6.37	6.42	`nlsv2`
6.47	6.49	6.53	`tpy6`
7.84	7.85	7.88	`lexv2`
7.93	7.98	8.22	`tpy`
8.08	8.09	16.09	`chacha20`
9.30	9.45	9.82	`salsa2012`
10.65	10.67	10.73	`salsa20`
10.86	10.86	10.98	`rabbit`
11.88	11.92	12.48	`hc128`
12.24	12.60	12.98	`cryptmtv3`
16.88	16.89	16.89	`aes128estream`
11.28	18.38	19.96	`tpypy`
21.73	22.10	22.34	`sosemanuk`
24.04	24.06	24.16	`dragon`
26.68	26.84	26.89	`aes256estream`
33.88	34.85	34.98	`hc256`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
2.86	2.99	5.25	`hc128`
3.74	3.75	3.75	`chacha8`
-0.71	4.75	5.34	`tpy`
4.77	4.88	5.01	`tpy6`
5.13	5.15	5.17	`chacha12`
5.11	5.17	5.20	`snow20`
5.22	5.28	5.38	`salsa208`
2.76	5.49	7.57	`hc256`
5.66	5.94	5.94	`trivium`
5.87	6.02	6.14	`nlsv2`
7.60	7.64	7.72	`lexv2`
7.99	8.01	24.04	`chacha20`
8.71	9.35	10.26	`salsa2012`
8.19	9.82	10.67	`cryptmtv3`
10.37	10.38	10.62	`rabbit`
10.44	10.57	10.75	`salsa20`
16.68	16.79	16.84	`aes128estream`
20.04	21.48	22.30	`sosemanuk`
7.92	22.21	25.40	`tpypy`
23.44	23.52	23.76	`dragon`
26.19	26.60	26.98	`aes256estream`

7.6 amd64, 2800MHz, Intel Xeon (f41), nmi0063



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
91.00	91.00	91.88	aes128estream
105.88	106.75	107.62	chacha8
116.38	116.38	116.38	chacha12
140.88	141.75	141.75	chacha20
147.00	147.00	147.88	salsa208
151.38	152.25	155.75	lexv2
161.00	163.62	163.62	aes256estream
165.38	167.12	169.75	trivium
168.88	169.75	169.75	salsa2012
171.50	172.38	172.38	rabbit
171.50	174.12	177.62	snow20
205.62	210.88	211.75	cryptmtv3
225.75	227.50	229.25	salsa20
288.75	290.50	291.38	dragon
371.00	383.25	385.00	sosemanuk
410.38	423.50	435.75	nlsv2
853.12	861.00	870.62	tpy6
1666.88	1686.12	1694.00	tpy
1736.00	1763.12	1782.38	tpypy
3632.12	3830.75	3848.25	hc128
11549.10	11727.60	11779.20	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
7.22	7.22	7.44	chacha8
8.97	8.97	9.41	chacha12
11.92	12.03	12.36	chacha20
16.19	16.19	16.19	salsa208
20.89	21.11	21.44	snow20
22.42	22.64	23.08	salsa2012
23.84	23.84	23.95	aes128estream
25.38	25.38	25.38	lexv2
26.03	26.47	27.02	trivium
28.55	28.66	28.77	rabbit
33.03	33.25	36.64	cryptmtv3
33.80	34.12	34.12	salsa20
37.73	37.84	38.06	aes256estream
40.80	41.56	43.86	sosemanuk
57.64	57.75	58.08	dragon
81.48	83.56	87.72	nlsv2
110.58	111.89	114.08	tpy6
215.03	215.47	217.22	tpy
227.72	228.81	232.09	tpypy
455.11	477.09	482.67	hc128
1446.38	1468.58	1500.41	hc256

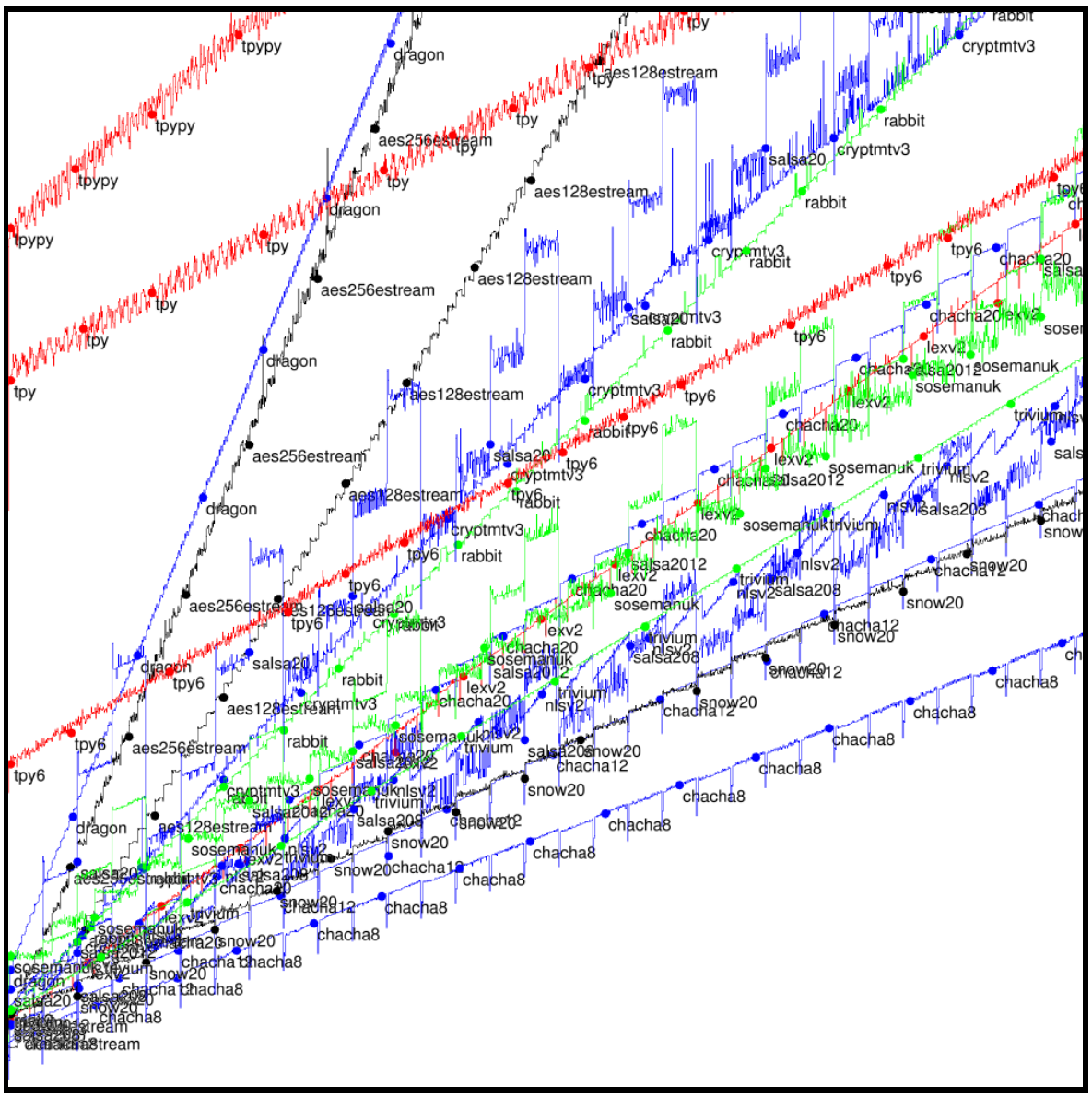
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
4.24	4.25	4.29	chacha8
5.71	5.72	5.72	chacha12
6.10	6.11	6.21	salsa208
7.05	7.15	7.19	snow20
7.86	8.09	8.39	salsa2012
8.40	8.45	8.46	trivium
8.51	8.54	8.54	chacha20
9.41	9.42	9.43	lexv2
12.01	12.09	12.10	salsa20
12.52	12.53	12.54	rabbit
14.92	14.92	14.94	cryptmtv3
16.67	17.27	18.16	nlsv2
17.27	17.45	17.84	tpy6
17.69	17.69	17.69	aes128estream
18.12	18.17	18.23	sosemanuk
26.95	27.08	27.08	aes256estream
28.52	28.60	28.73	tpy
28.34	28.69	28.70	dragon
32.50	32.61	32.72	tpypy
53.59	56.40	56.69	hc128
170.55	171.91	174.21	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
3.94	3.95	3.95	chacha8
5.35	5.35	5.37	chacha12
5.61	5.64	5.74	salsa208
6.04	6.05	6.11	snow20
7.00	7.00	7.01	trivium
6.95	7.02	7.05	salsa2012
8.20	8.21	8.23	chacha20
8.28	8.28	8.34	lexv2
9.82	9.88	9.95	tpy6
10.80	10.83	10.87	salsa20
11.16	11.17	11.17	rabbit
13.23	13.45	14.00	nlsv2
13.84	13.89	14.09	tpy
13.28	13.98	14.18	cryptmtv3
14.98	15.03	15.04	sosemanuk
17.16	17.16	17.17	aes128estream
17.31	17.34	17.41	tpypy
22.39	22.43	23.47	hc128
26.13	26.15	26.27	aes256estream
26.29	26.30	26.31	dragon
68.57	68.57	69.57	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
3.82	3.82	3.82	chacha8
5.23	5.23	5.23	chacha12
5.46	5.46	5.50	salsa208
5.63	5.64	5.64	snow20
6.45	6.46	6.46	trivium
6.86	6.89	6.93	salsa2012
7.09	7.11	7.15	tpy6
7.83	7.84	7.85	lexv2
8.07	8.07	8.08	chacha20
8.43	8.46	8.49	tpy
8.72	8.73	8.79	cryptmtv3
10.65	10.65	10.65	rabbit
10.65	10.68	10.72	salsa20
10.65	10.80	11.01	hc128
11.57	11.62	11.63	tpypy
11.53	11.75	12.01	nlsv2
13.74	13.75	13.76	sosemanuk
17.01	17.02	17.05	aes128estream
25.04	25.40	25.41	dragon
25.96	25.99	26.00	aes256estream
30.15	30.16	30.57	hc256

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
3.74	3.75	3.75	chacha8
2.79	3.89	4.32	hc128
5.15	5.15	5.16	chacha12
5.12	5.21	5.28	tpy
4.60	5.24	5.39	cryptmtv3
5.35	5.35	5.52	salsa208
5.32	5.40	5.53	tpy6
5.39	5.41	5.43	snow20
6.11	6.13	6.13	trivium
6.66	6.83	6.92	salsa2012
7.57	7.58	7.62	lexv2
6.30	7.82	8.64	hc256
7.99	8.00	8.00	chacha20
8.06	8.27	8.33	tpypy
10.34	10.34	10.35	rabbit
10.46	10.54	10.73	salsa20
10.15	11.15	11.95	nlsv2
13.10	13.12	13.16	sosemanuk
16.94	16.97	17.01	aes128estream
24.13	24.87	24.88	dragon
25.85	25.91	25.97	aes256estream

7.7 amd64, 3000MHz, Intel Pentium D (f64), speed



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
90.00	91.88	91.88	aes128estream
105.00	108.75	116.25	chacha8
116.25	116.25	116.25	chacha12
140.62	142.50	146.25	chacha20
146.25	146.25	146.25	salsa208
161.25	161.25	161.25	lexv2
157.50	163.12	168.75	cryptmtv3
159.38	166.88	180.00	aes256estream
168.75	168.75	170.62	salsa2012
170.62	172.50	172.50	trivium
172.50	172.50	176.25	snow20
183.75	185.62	193.12	rabbit
187.50	193.12	196.88	nlsv2
225.00	226.88	226.88	salsa20
273.75	275.62	279.38	dragon
288.75	294.38	309.38	sosemanuk
753.75	766.88	774.38	tpy6
1663.12	1668.75	1680.00	tpy
1976.25	1987.50	1996.88	tpypy
3780.00	3781.88	3785.62	hc128
9780.00	9789.38	9860.62	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
6.33	6.56	7.50	chacha8
7.73	7.97	8.91	chacha12
11.48	11.95	12.42	chacha20
16.17	16.17	16.17	salsa208
20.86	21.80	22.97	snow20
22.27	22.27	22.73	salsa2012
23.67	23.91	23.91	aes128estream
26.25	26.25	26.72	lexv2
26.48	26.72	26.95	trivium
27.89	29.53	31.64	cryptmtv3
30.00	30.23	30.94	rabbit
33.98	34.22	34.22	salsa20
33.98	34.22	35.16	nlsv2
37.03	37.73	40.08	sosemanuk
38.91	39.38	39.38	aes256estream
56.72	57.19	57.89	dragon
98.20	99.38	100.55	tpy6
210.23	211.41	211.88	tpy
251.02	254.77	257.81	tpypy
473.44	473.91	477.19	hc128
1222.50	1222.50	1222.73	hc256

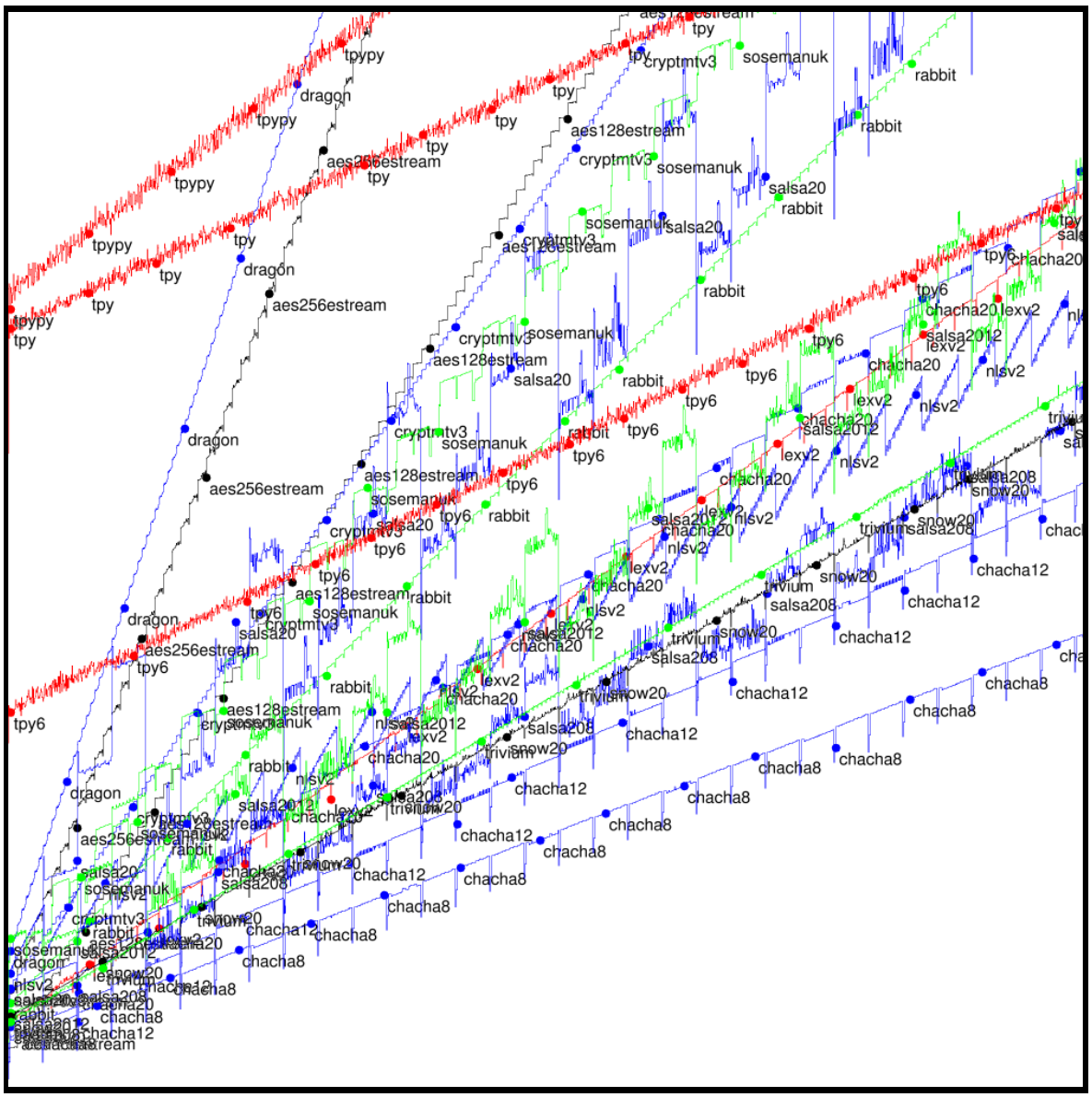
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
4.27	4.30	4.30	chacha8
5.65	5.68	5.68	chacha12
5.78	6.38	6.43	salsa208
6.77	6.85	6.93	snow20
8.41	8.44	8.52	nlsv2
8.39	8.46	8.46	trivium
8.44	8.52	8.52	chacha20
8.07	8.59	8.65	salsa2012
9.51	9.56	9.61	lexv2
10.52	10.83	11.04	sosemanuk
12.55	12.60	12.63	salsa20
12.63	12.63	12.94	rabbit
13.15	13.23	13.41	cryptmtv3
15.96	16.12	16.22	tpy6
17.66	17.68	17.71	aes128estream
26.33	26.48	27.08	aes256estream
28.15	28.18	28.28	dragon
28.44	28.54	28.59	tpy
35.52	35.76	35.83	tpypy
56.35	56.48	56.67	hc128
140.78	140.81	140.86	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
3.91	3.93	3.94	chacha8
5.35	5.35	5.35	chacha12
5.55	5.59	5.60	salsa208
5.60	5.60	5.66	snow20
6.72	6.73	6.74	nlsv2
6.95	6.98	6.99	trivium
7.63	7.63	7.64	salsa2012
7.97	8.07	8.10	sosemanuk
8.11	8.12	8.14	chacha20
8.28	8.29	8.29	lexv2
9.51	9.59	9.72	tpy6
11.04	11.04	11.06	salsa20
11.18	11.18	11.19	rabbit
11.46	11.53	11.88	cryptmtv3
13.90	13.93	14.00	tpy
17.00	17.07	17.19	aes128estream
18.72	18.94	18.95	tpypy
23.91	23.95	23.98	hc128
25.06	25.31	26.06	aes256estream
25.90	25.91	25.95	dragon
56.32	56.34	56.37	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
3.81	3.81	3.81	`chacha8`
5.13	5.15	5.15	`snow20`
5.23	5.23	5.23	`chacha12`
5.55	5.57	5.58	`salsa208`
5.96	5.97	5.99	`nlsv2`
6.42	6.43	6.43	`trivium`
7.06	7.12	7.26	`sosemanuk`
7.11	7.16	7.19	`tpy6`
7.38	7.38	7.38	`salsa2012`
7.80	7.81	7.90	`lexv2`
8.00	8.01	8.01	`chacha20`
8.52	8.55	8.57	`tpy`
8.71	8.71	8.74	`cryptmtv3`
10.64	10.64	10.96	`rabbit`
10.78	10.81	10.86	`salsa20`
11.53	11.55	11.59	`hc128`
12.36	12.40	12.50	`tpypy`
16.96	17.05	17.11	`aes128estream`
24.63	24.64	24.64	`hc256`
24.76	24.77	24.78	`aes256estream`
25.02	25.02	25.06	`dragon`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
3.75	3.75	3.76	`chacha8`
3.99	4.04	4.16	`hc128`
4.86	4.89	4.91	`snow20`
5.16	5.16	5.16	`chacha12`
5.24	5.32	5.38	`tpy`
5.43	5.48	5.49	`salsa208`
5.59	5.62	5.66	`hc256`
5.58	5.63	5.68	`nlsv2`
5.60	5.79	5.90	`tpy6`
6.06	6.09	6.11	`trivium`
6.62	6.79	7.21	`sosemanuk`
6.59	6.80	6.91	`cryptmtv3`
7.23	7.24	7.24	`salsa2012`
7.51	7.56	7.73	`lexv2`
7.91	7.92	7.95	`chacha20`
8.47	8.62	8.89	`tpypy`
9.99	10.31	10.95	`rabbit`
10.59	10.66	10.77	`salsa20`
16.92	17.10	17.29	`aes128estream`
23.66	24.38	24.59	`aes256estream`
24.48	24.51	24.59	`dragon`

7.8 amd64, 3000MHz, Intel Xeon (f4a), nmi0090



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
90.88	91.00	91.00	aes128estream
106.88	107.75	107.88	chacha8
115.38	116.25	116.25	chacha12
138.75	138.75	139.62	chacha20
147.12	147.12	147.25	salsa208
147.25	151.88	155.62	trivium
152.88	154.75	158.38	lexv2
162.25	165.88	166.88	snow20
171.50	171.50	171.62	salsa2012
196.88	196.88	206.25	rabbit
226.88	227.75	227.88	salsa20
227.88	228.75	228.75	cryptmtv3
232.50	237.12	239.00	aes256estream
273.75	274.75	278.38	nlsv2
321.50	322.50	324.38	dragon
344.12	349.62	349.75	sosemanuk
829.75	861.50	864.38	tpy6
1733.38	1748.38	1776.62	tpy
1820.62	1841.25	1852.50	tpypy
4746.50	4746.62	4746.62	hc128
13159.60	13174.80	13197.10	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
6.91	7.03	7.27	chacha8
8.55	9.02	9.14	chacha12
11.59	11.84	12.42	chacha20
16.06	16.17	16.17	salsa208
20.62	20.75	21.22	snow20
22.27	22.73	22.86	salsa2012
23.80	23.91	24.02	trivium
24.25	24.27	24.95	aes128estream
25.44	25.55	25.67	lexv2
31.77	31.88	32.00	rabbit
33.98	34.22	34.45	salsa20
37.27	38.31	38.44	sosemanuk
41.25	41.25	41.25	cryptmtv3
48.16	48.17	48.28	aes256estream
50.75	51.09	51.09	nlsv2
67.39	67.84	67.97	dragon
112.16	113.31	167.69	tpy6
221.14	224.30	225.12	tpy
234.72	237.55	237.66	tpypy
592.86	592.97	592.97	hc128
1644.38	1646.02	1647.31	hc256

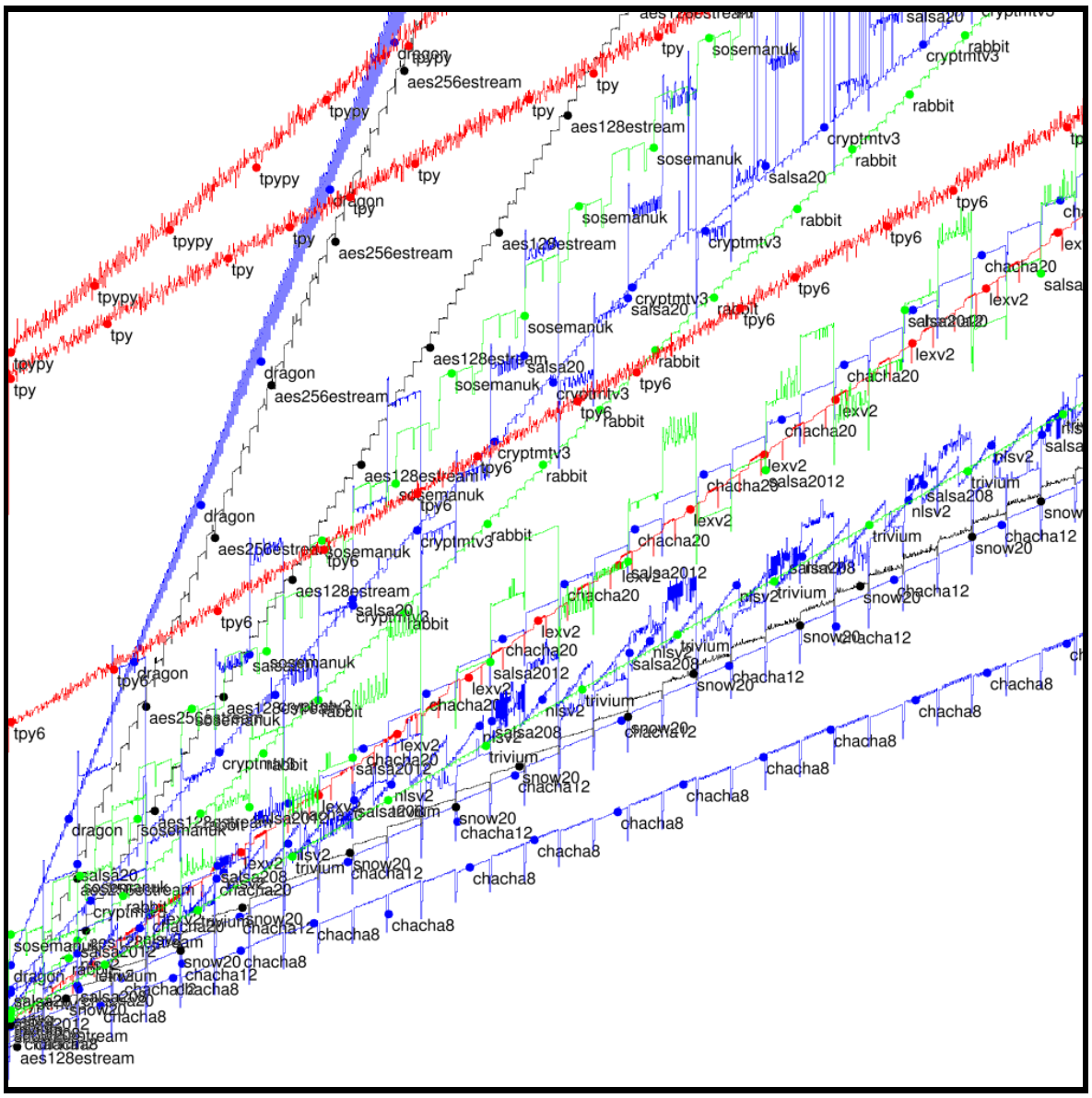
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
4.14	4.22	4.23	chacha8
5.65	5.69	5.69	chacha12
5.48	5.76	6.46	salsa208
7.36	7.36	7.37	snow20
7.44	7.54	7.92	salsa2012
7.99	8.02	8.05	trivium
8.46	8.48	8.49	chacha20
9.47	9.49	9.58	lexv2
10.44	10.48	10.55	nlsv2
11.77	11.86	11.97	salsa20
12.95	12.96	12.97	rabbit
17.02	17.02	17.10	tpy6
17.40	17.49	17.49	sosemanuk
17.68	17.73	17.75	aes128estream
17.86	17.90	17.90	cryptmtv3
28.71	29.36	29.53	tpy
29.43	29.47	29.64	aes256estream
32.83	33.49	33.62	tpypy
34.22	34.24	34.26	dragon
68.97	68.98	68.98	hc128
187.38	187.43	187.70	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
3.93	3.93	3.93	chacha8
5.35	5.36	5.36	chacha12
5.52	5.53	5.53	salsa208
6.24	6.24	6.30	snow20
6.71	6.72	6.73	trivium
7.17	7.18	7.27	salsa2012
7.64	7.65	7.65	nlsv2
8.18	8.18	8.18	chacha20
8.30	8.30	8.30	lexv2
9.27	9.27	9.40	tpy6
10.36	10.51	10.55	salsa20
11.40	11.41	11.41	rabbit
13.72	13.84	13.95	tpy
14.59	14.59	14.61	sosemanuk
14.71	14.88	14.89	cryptmtv3
17.01	17.13	17.21	tpypy
17.18	17.19	17.19	aes128estream
27.92	27.92	27.93	aes256estream
28.23	28.25	28.26	hc128
31.58	31.59	31.60	dragon
73.53	73.66	73.73	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
3.82	3.82	3.82	chacha8
5.22	5.23	5.23	chacha12
5.40	5.40	5.40	salsa208
5.89	5.91	5.93	snow20
6.23	6.23	6.23	trivium
6.46	6.47	6.47	nlsv2
6.53	6.54	6.59	tpy6
7.13	7.13	7.13	salsa2012
7.83	7.84	7.87	lexv2
8.07	8.07	8.07	chacha20
8.06	8.10	8.15	tpy
10.29	10.34	10.39	salsa20
10.82	10.82	10.82	rabbit
11.13	11.14	11.14	cryptmtv3
11.12	11.14	11.20	tpypy
12.89	12.90	12.92	hc128
13.49	13.49	13.50	sosemanuk
17.02	17.03	17.03	aes128estream
27.53	27.54	27.55	aes256estream
30.59	30.60	30.60	dragon
30.90	30.92	30.93	hc256

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
3.68	3.70	3.74	hc128
3.75	3.75	3.75	chacha8
4.65	4.75	4.84	tpy
4.74	4.85	5.05	tpy6
5.14	5.15	5.15	chacha12
5.14	5.20	5.29	hc256
5.31	5.33	5.34	salsa208
5.71	5.75	5.80	snow20
5.92	5.94	5.94	trivium
5.92	5.95	5.96	nlsv2
7.10	7.10	7.12	salsa2012
7.49	7.54	7.70	tpypy
7.57	7.57	7.64	lexv2
7.99	8.00	8.01	chacha20
8.94	8.94	8.96	cryptmtv3
10.06	10.23	10.45	salsa20
10.47	10.47	10.47	rabbit
4.28	12.98	13.00	sosemanuk
16.93	16.95	16.97	aes128estream
27.29	27.32	27.40	aes256estream
29.99	30.00	30.01	dragon

7.9 amd64, 3392MHz, Intel Pentium D (f64), `nmi0104`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
95.62	95.62	97.75	aes128estream
104.12	106.25	108.38	chacha8
114.75	116.88	116.88	chacha12
140.25	140.25	140.25	chacha20
144.50	146.62	146.62	snow20
148.75	148.75	148.75	salsa208
148.75	150.88	150.88	aes256estream
155.12	155.12	157.25	lexv2
155.12	157.25	157.25	trivium
170.00	170.00	172.12	salsa2012
180.62	182.75	182.75	rabbit
184.88	184.88	193.38	nlsv2
218.88	221.00	235.88	cryptmtv3
223.12	225.25	225.25	salsa20
291.12	291.12	291.12	dragon
352.75	354.88	354.88	sosemanuk
833.00	835.12	837.25	tpy6
1653.25	1657.50	1670.25	tpy
1712.75	1717.00	1723.38	tpypy
3678.38	3686.88	3797.38	hc128
12048.80	12106.10	12121.00	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
6.38	7.44	7.70	chacha8
8.77	9.03	9.03	chacha12
11.16	11.69	11.69	chacha20
15.94	16.20	16.20	salsa208
18.59	18.86	18.86	snow20
22.31	22.31	22.31	salsa2012
24.44	24.70	24.70	trivium
24.70	24.97	25.23	aes128estream
25.23	25.50	25.50	lexv2
29.48	29.75	30.55	rabbit
33.73	33.73	34.00	nlsv2
33.73	34.00	34.27	salsa20
35.86	35.86	36.12	aes256estream
35.86	36.12	36.12	cryptmtv3
38.78	38.78	39.05	sosemanuk
59.23	59.23	59.23	dragon
109.70	110.77	112.89	tpy6
211.17	212.50	214.09	tpy
220.20	223.39	225.78	tpypy
459.80	474.94	475.47	hc128
1498.66	1510.88	1520.97	hc256

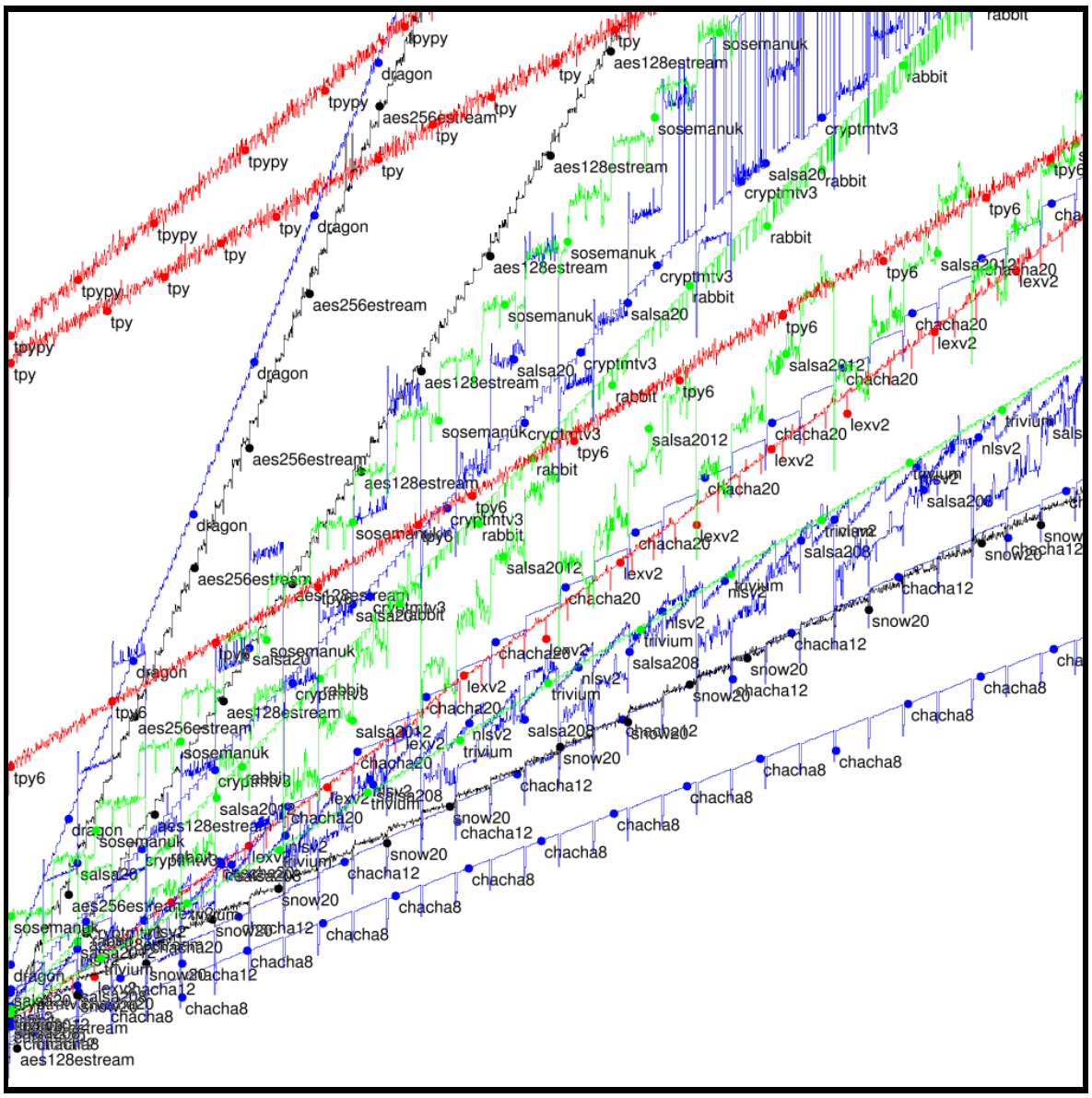
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
4.28	4.31	4.31	chacha8
5.64	5.64	5.67	chacha12
6.43	6.43	6.46	salsa208
6.70	6.70	6.73	snow20
7.91	7.91	7.94	trivium
8.23	8.23	8.26	nlsv2
8.23	8.35	8.38	salsa2012
8.35	8.44	8.44	chacha20
9.47	9.50	9.50	lexv2
12.31	12.40	12.69	salsa20
12.45	12.48	12.48	rabbit
14.23	14.23	14.26	cryptmtv3
17.00	17.27	17.41	tpy6
17.59	17.62	17.62	sosemanuk
17.77	17.80	17.80	aes128estream
25.91	25.94	25.94	aes256estream
28.45	28.48	28.60	tpy
28.86	29.07	29.13	dragon
31.28	31.93	31.96	tpypy
54.66	54.72	56.19	hc128
172.48	173.16	173.69	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
3.90	3.91	3.91	chacha8
5.35	5.35	5.35	chacha12
5.42	5.42	5.57	salsa208
5.78	5.82	5.84	snow20
6.53	6.54	6.54	trivium
6.61	6.63	6.64	nlsv2
7.54	7.54	7.54	salsa2012
8.07	8.08	8.08	chacha20
8.27	8.27	8.28	lexv2
9.96	10.06	10.13	tpy6
11.05	11.05	11.05	rabbit
11.08	11.09	11.10	salsa20
13.77	13.82	13.93	tpy
11.65	14.01	14.02	cryptmtv3
14.73	14.73	14.73	sosemanuk
16.61	16.79	16.86	tpypy
17.19	17.20	17.21	aes128estream
22.94	23.02	23.08	hc128
25.12	25.13	25.21	aes256estream
26.37	26.39	26.67	dragon
68.49	68.89	69.08	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
3.79	3.81	3.82	`chacha8`
5.02	5.06	5.07	`salsa208`
5.23	5.23	5.23	`chacha12`
5.45	5.45	5.45	`snow20`
5.83	5.84	5.84	`nlsv2`
6.03	6.03	6.03	`trivium`
7.35	7.36	7.36	`salsa2012`
7.33	7.39	7.43	`tpy6`
7.81	7.82	7.84	`lexv2`
7.98	7.98	7.98	`chacha20`
8.51	8.57	8.61	`tpy`
8.06	8.62	8.62	`cryptmtv3`
10.51	10.51	10.51	`rabbit`
10.85	10.87	10.87	`salsa20`
11.11	11.14	11.34	`hc128`
11.27	11.28	11.29	`tpypy`
13.65	13.65	13.65	`sosemanuk`
17.04	17.04	17.05	`aes128estream`
24.88	24.89	24.90	`aes256estream`
25.46	25.46	25.77	`dragon`
29.31	29.43	29.63	`hc256`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
3.73	3.77	3.79	`chacha8`
3.56	4.00	4.49	`hc128`
4.76	4.83	4.87	`salsa208`
5.16	5.16	5.17	`chacha12`
5.22	5.26	5.28	`snow20`
5.13	5.37	5.47	`tpy`
5.44	5.46	5.47	`nlsv2`
5.71	5.72	5.73	`trivium`
5.64	5.83	5.93	`tpy6`
5.56	5.94	6.90	`hc256`
3.54	6.37	6.46	`cryptmtv3`
7.22	7.25	7.26	`salsa2012`
7.51	7.55	7.59	`lexv2`
7.89	7.92	7.93	`chacha20`
8.00	8.05	8.08	`tpypy`
10.19	10.19	10.19	`rabbit`
10.69	10.73	10.78	`salsa20`
13.16	13.16	13.17	`sosemanuk`
16.95	16.96	16.98	`aes128estream`
24.69	24.71	24.80	`aes256estream`
24.90	24.91	25.52	`dragon`

7.10 amd64, 3392MHz, Intel Pentium D (f64), nmi0161



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
91.38	99.88	110.50	aes128estream
104.12	106.25	106.25	chacha8
116.88	116.88	116.88	chacha12
140.25	140.25	140.25	chacha20
146.62	146.62	150.88	salsa208
153.00	155.12	157.25	lexv2
165.75	167.88	167.88	trivium
170.00	170.00	172.12	salsa2012
170.00	174.25	176.38	aes256estream
172.12	174.25	176.38	snow20
182.75	182.75	184.88	rabbit
193.38	195.50	197.62	nlsv2
216.75	218.88	223.12	cryptmtv3
225.25	227.38	227.38	salsa20
286.88	289.00	293.25	dragon
393.12	397.38	399.50	sosemanuk
745.88	754.38	758.62	tpy6
1663.88	1672.38	1676.62	tpy
1751.00	1753.12	1763.75	tpypy
3797.38	3805.88	3816.50	hc128
10336.00	10340.20	10344.50	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
6.64	6.64	6.91	chacha8
7.97	9.03	9.30	chacha12
10.89	11.42	11.95	chacha20
15.94	16.20	16.20	salsa208
21.78	22.05	22.58	snow20
22.31	22.84	22.84	salsa2012
23.64	23.64	23.91	aes128estream
25.50	25.50	25.50	lexv2
26.03	26.30	26.56	trivium
30.28	30.28	30.28	rabbit
33.73	34.00	34.27	salsa20
34.00	34.00	34.00	cryptmtv3
34.53	35.06	35.33	nlsv2
38.25	39.05	39.84	aes256estream
42.77	44.09	45.42	sosemanuk
58.70	59.23	59.77	dragon
98.02	99.34	100.14	tpy6
215.95	216.22	216.75	tpy
225.78	228.97	229.77	tpypy
476.00	476.53	477.33	hc128
1292.53	1292.80	1293.06	hc256

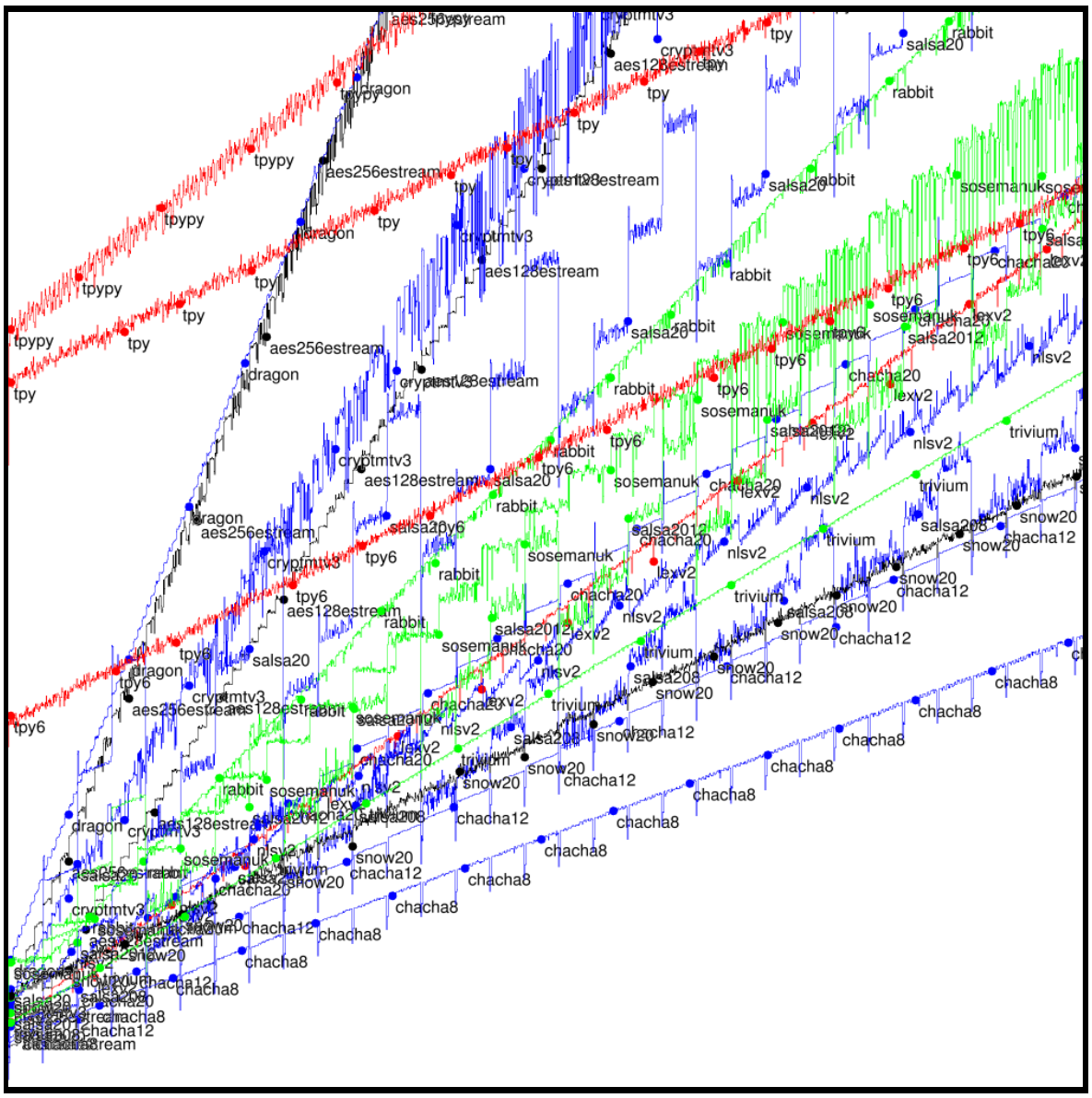
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
4.25	4.25	4.28	chacha8
5.70	5.73	5.73	chacha12
6.70	6.73	6.76	snow20
6.70	6.73	6.99	salsa208
8.38	8.38	8.41	trivium
8.44	8.47	8.47	chacha20
8.53	8.59	8.68	nlsv2
9.12	9.24	9.65	salsa2012
9.41	9.41	9.44	lexv2
11.57	11.92	12.57	salsa20
12.93	12.93	12.96	rabbit
13.96	13.99	14.02	cryptmtv3
15.97	16.14	16.38	tpy6
17.53	17.56	17.59	aes128estream
17.97	18.03	18.27	sosemanuk
26.00	26.24	26.27	aes256estream
28.33	28.36	28.42	dragon
28.86	29.01	29.16	tpy
31.93	32.23	32.52	tpypy
56.99	57.14	57.32	hc128
148.34	148.40	148.46	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
3.94	3.94	3.94	chacha8
5.30	5.30	5.31	chacha12
5.56	5.56	5.57	snow20
5.45	5.62	5.82	salsa208
6.86	6.87	6.90	nlsv2
6.95	6.96	6.98	trivium
7.23	7.47	7.49	salsa2012
8.12	8.13	8.13	chacha20
8.30	8.31	8.40	lexv2
9.63	9.68	9.73	tpy6
10.74	10.87	10.90	salsa20
11.18	11.18	11.49	rabbit
11.79	11.81	13.82	cryptmtv3
14.26	14.30	14.38	tpy
14.80	14.83	14.89	sosemanuk
17.01	17.01	17.17	aes128estream
16.93	17.13	17.15	tpypy
24.12	24.17	24.26	hc128
25.23	25.26	25.46	aes256estream
25.89	25.89	26.37	dragon
59.05	59.06	59.07	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
3.81	3.81	3.81	chacha8
5.14	5.14	5.17	snow20
5.21	5.23	5.23	chacha12
5.30	5.51	5.53	salsa208
6.04	6.07	6.11	nlsv2
6.42	6.42	6.42	trivium
6.94	7.26	7.27	salsa2012
7.31	7.33	7.38	tpy6
7.78	7.81	7.82	lexv2
8.00	8.00	8.00	chacha20
8.75	8.79	8.84	tpy
8.90	8.92	8.93	cryptmtv3
10.68	10.68	10.68	rabbit
10.31	10.79	10.80	salsa20
11.31	11.36	11.42	tpypy
11.82	11.84	11.86	hc128
13.43	13.48	13.53	sosemanuk
16.86	16.88	17.04	aes128estream
24.80	24.83	24.88	aes256estream
24.96	24.97	25.45	dragon
25.54	25.55	25.56	hc256

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
3.72	3.73	3.73	chacha8
4.32	4.43	4.48	hc128
4.86	4.88	4.94	snow20
5.13	5.15	5.19	chacha12
5.42	5.46	5.50	hc256
5.37	5.50	5.65	tpy
4.98	5.54	5.69	salsa208
5.59	5.67	5.78	nlsv2
5.89	5.94	6.08	tpy6
6.08	6.09	6.11	trivium
5.33	6.89	6.92	cryptmtv3
6.44	7.18	7.24	salsa2012
7.40	7.45	7.60	lexv2
7.91	7.93	7.93	chacha20
7.78	7.96	8.12	tpypy
10.08	10.09	10.40	rabbit
9.73	10.82	10.95	salsa20
12.57	12.91	13.05	sosemanuk
16.73	16.77	17.15	aes128estream
23.92	24.42	25.39	dragon
24.47	24.55	24.69	aes256estream

7.11 amd64, 3392MHz, Intel Pentium D (f64), `nmi0241`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
95.62	97.75	97.75	aes128estream
104.12	106.25	108.38	chacha8
114.75	116.88	119.00	chacha12
136.00	140.25	140.25	chacha20
142.38	142.38	146.62	salsa208
146.62	146.62	146.62	trivium
153.00	155.12	157.25	lexv2
172.12	172.12	174.25	salsa2012
189.12	189.12	195.50	nlsv2
187.00	197.62	201.88	aes256estream
195.50	199.75	206.12	cryptmtv3
206.12	208.25	218.88	snow20
210.38	212.50	214.62	rabbit
225.25	227.38	227.38	salsa20
291.12	291.12	299.62	sosemanuk
301.75	301.75	306.00	dragon
839.38	843.62	854.25	tpy6
1623.50	1625.62	1653.25	tpy
1731.88	1751.00	1761.62	tpypy
4252.12	4256.38	4258.50	hc128
12456.80	12471.60	12558.80	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
6.91	6.91	7.17	chacha8
8.23	8.50	9.03	chacha12
11.16	11.42	11.69	chacha20
16.20	16.20	16.20	salsa208
22.31	22.58	23.11	salsa2012
23.64	23.64	24.17	trivium
24.44	24.44	24.70	aes128estream
24.97	25.23	25.50	lexv2
27.62	27.89	28.42	snow20
33.20	33.47	33.47	rabbit
33.73	34.00	34.27	salsa20
34.00	34.00	34.27	nlsv2
35.59	36.12	37.45	sosemanuk
40.11	40.38	40.64	cryptmtv3
45.95	46.75	48.61	aes256estream
60.30	60.56	61.09	dragon
108.38	110.77	112.89	tpy6
207.98	207.98	210.64	tpy
223.92	224.72	224.98	tpypy
532.58	532.58	533.64	hc128
1555.23	1562.67	1565.06	hc256

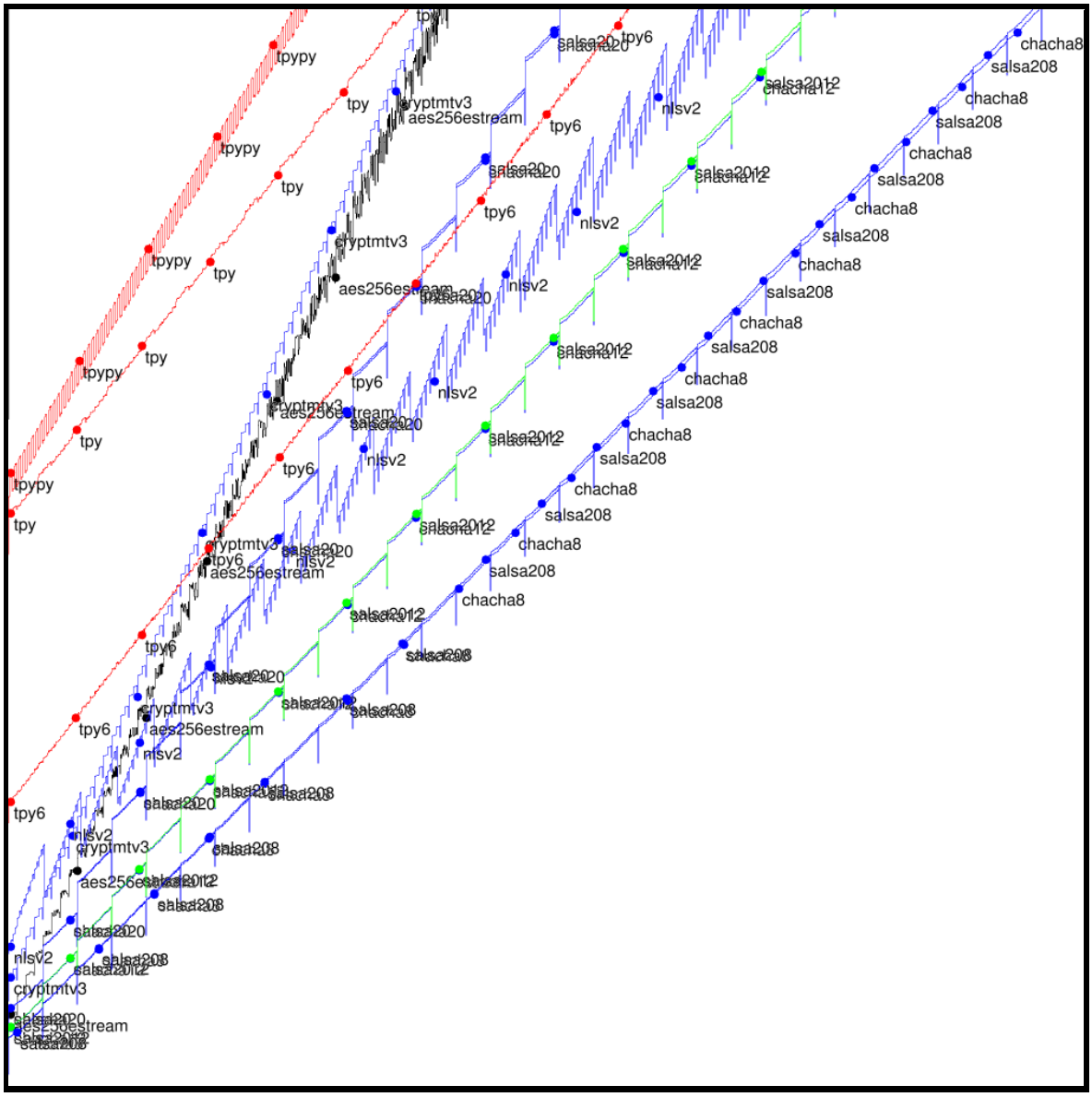
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
4.22	4.22	4.25	chacha8
5.64	5.64	5.64	chacha12
5.90	5.93	6.20	salsa208
7.23	7.35	7.70	snow20
7.59	7.88	8.09	salsa2012
8.12	8.15	8.15	trivium
9.06	9.18	9.24	nlsv2
8.44	9.33	9.33	chacha20
9.36	9.39	9.39	lexv2
11.81	11.95	12.25	salsa20
12.25	12.34	12.43	sosemanuk
13.10	13.10	13.13	rabbit
16.59	16.65	16.70	tpy6
17.56	17.56	17.59	aes128estream
20.01	20.31	20.75	cryptmtv3
27.54	27.65	28.01	tpy
28.39	28.54	28.92	aes256estream
29.45	29.54	30.10	dragon
31.40	31.52	32.41	tpypy
62.63	62.69	62.78	hc128
178.18	178.62	179.06	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
3.93	3.95	3.95	chacha8
5.29	5.32	5.33	salsa208
5.33	5.33	5.35	chacha12
5.79	5.84	5.89	snow20
6.81	6.82	6.83	trivium
6.94	7.07	7.17	salsa2012
7.43	7.46	7.51	nlsv2
8.08	8.11	9.03	chacha20
8.23	8.25	8.30	lexv2
9.35	9.40	9.42	tpy6
9.76	10.08	10.14	sosemanuk
10.68	10.78	10.79	salsa20
11.41	11.41	11.42	rabbit
13.14	13.26	13.29	tpy
14.95	15.00	15.07	cryptmtv3
16.75	16.83	16.93	tpypy
17.02	17.02	17.02	aes128estream
25.94	26.03	26.12	hc128
26.84	26.86	26.97	dragon
26.96	26.99	27.06	aes256estream
70.14	70.19	70.36	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
3.77	3.82	3.82	`chacha8`
5.22	5.23	5.23	`chacha12`
5.28	5.30	5.32	`snow20`
5.31	5.33	5.37	`salsa208`
6.33	6.33	6.33	`trivium`
6.63	6.65	6.72	`tpy6`
6.62	6.65	6.70	`nlsv2`
6.87	7.01	7.08	`salsa2012`
7.77	7.79	7.79	`lexv2`
7.99	7.99	7.99	`chacha20`
7.99	8.01	8.10	`tpy`
8.25	9.16	9.19	`sosemanuk`
10.54	10.54	10.64	`rabbit`
10.61	10.65	10.69	`salsa20`
11.26	11.28	11.32	`tpypy`
11.92	11.94	11.97	`cryptmtv3`
12.19	12.21	12.28	`hc128`
16.87	16.88	16.88	`aes128estream`
25.87	26.00	26.02	`dragon`
26.52	27.10	27.13	`aes256estream`
29.49	29.54	29.57	`hc256`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
3.65	3.75	3.79	`chacha8`
3.74	3.83	4.04	`hc128`
4.59	4.71	5.07	`tpy`
4.94	5.01	5.16	`tpy6`
4.94	5.04	5.12	`snow20`
5.15	5.15	5.16	`chacha12`
5.01	5.36	5.42	`hc256`
5.22	5.37	5.52	`salsa208`
6.02	6.03	6.04	`trivium`
6.20	6.28	6.39	`nlsv2`
6.50	6.78	7.07	`salsa2012`
7.45	7.50	7.55	`lexv2`
7.01	7.92	7.92	`chacha20`
7.89	7.96	8.12	`tpypy`
6.86	8.75	8.90	`sosemanuk`
9.91	9.92	10.12	`rabbit`
8.52	10.17	10.25	`cryptmtv3`
10.44	10.58	10.80	`salsa20`
16.78	16.81	16.82	`aes128estream`
25.18	25.44	25.62	`dragon`
26.20	27.38	27.45	`aes256estream`

7.12 ia64, 900MHz, HP Itanium II, nmi0025



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
118.25	118.25	118.25	chacha8
119.25	119.25	119.25	salsa208
140.50	140.50	140.50	chacha12
141.50	141.50	141.50	salsa2012
168.25	168.88	169.25	aes256estream
185.00	185.00	185.00	chacha20
186.00	186.00	186.00	salsa20
252.88	252.88	252.88	cryptmtv3
335.75	335.88	336.12	nlsv2
662.75	663.75	668.00	tpy6
1333.75	1334.38	1334.75	tpy
1380.00	1380.75	1381.50	tpypy
10943.60	10945.90	10951.60	aes128estream

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
13.70	13.70	13.70	chacha8
13.83	13.83	13.83	salsa208
16.48	16.48	16.48	chacha12
16.61	16.61	16.61	salsa2012
22.05	22.05	22.05	chacha20
22.17	22.17	22.17	salsa20
37.44	38.36	38.45	aes256estream
48.38	48.38	48.38	cryptmtv3
67.08	67.09	67.12	nlsv2
93.88	93.89	94.67	tpy6
177.77	177.81	178.23	tpy
186.41	186.50	186.59	tpypy
4883.64	4884.91	4909.81	aes128estream

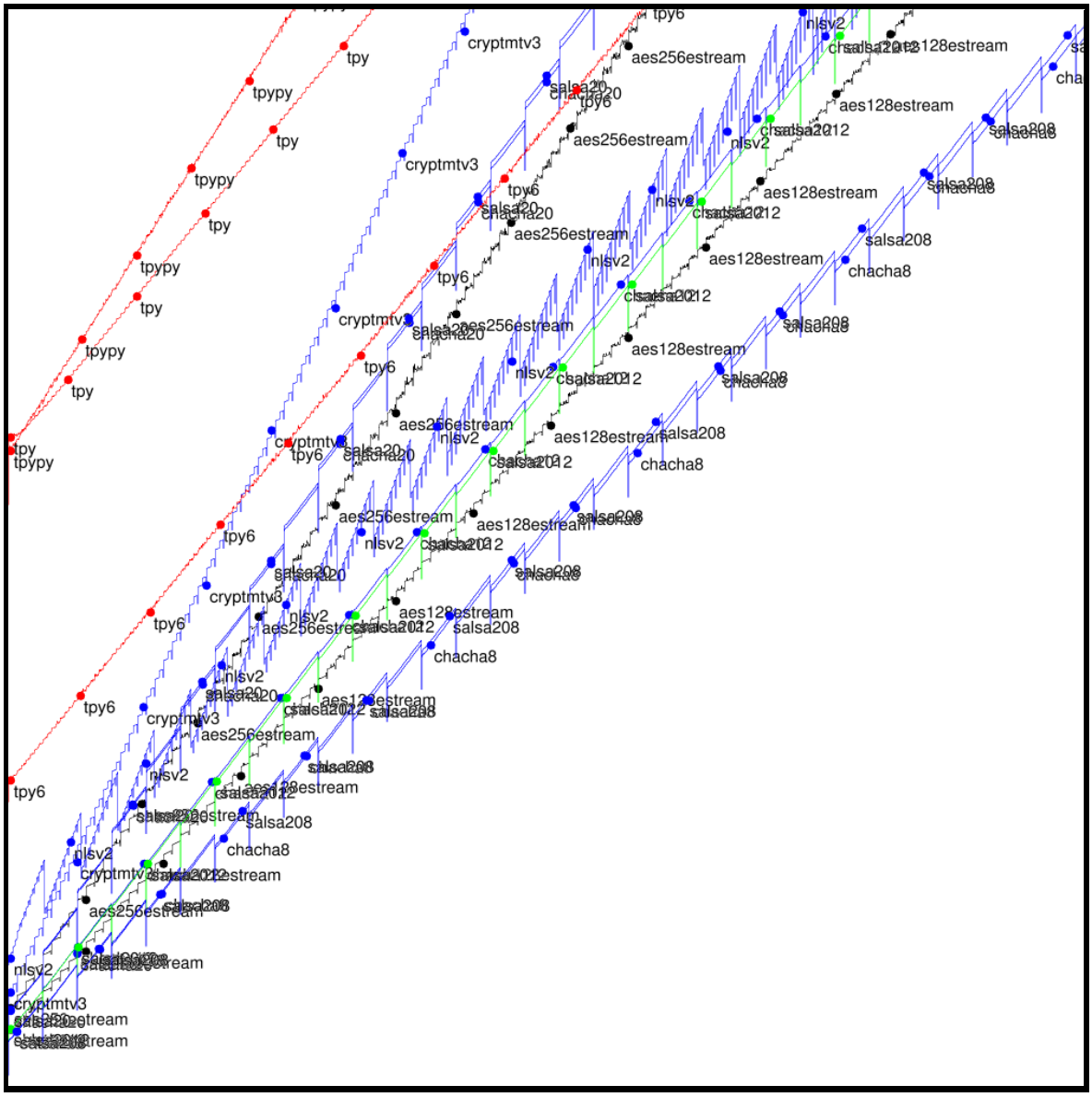
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
10.41	10.41	10.41	chacha8
10.48	10.48	10.48	salsa208
13.19	13.19	13.19	chacha12
13.26	13.26	13.26	salsa2012
17.71	17.72	17.73	nlsv2
18.75	18.75	18.75	chacha20
18.82	18.82	18.82	salsa20
21.86	21.88	21.97	tpy6
24.99	25.08	25.27	aes256estream
26.21	26.21	26.21	cryptmtv3
31.10	31.10	31.14	tpy
35.22	35.26	35.31	tpypy
4717.88	4718.61	4720.86	aes128estream

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
10.14	10.14	10.14	chacha8
10.21	10.21	10.21	salsa208
12.93	12.93	12.93	chacha12
12.99	12.99	12.99	salsa2012
14.48	14.48	14.49	nlsv2
16.21	16.22	16.23	tpy6
18.49	18.49	18.49	chacha20
18.55	18.55	18.55	salsa20
19.66	19.67	19.68	tpy
22.24	22.24	22.24	cryptmtv3
23.47	23.48	23.48	tpypy
24.16	24.40	24.41	aes256estream
4703.88	4704.48	4706.31	aes128estream

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
10.04	10.04	10.04	chacha8
10.11	10.11	10.11	salsa208
12.83	12.83	12.83	chacha12
12.89	12.89	12.89	salsa2012
13.11	13.11	13.11	nlsv2
14.08	14.10	14.10	tpy6
15.46	15.47	15.48	tpy
15.54	15.54	15.54	cryptmtv3
18.39	18.39	18.39	chacha20
18.45	18.45	18.45	salsa20
19.07	19.10	19.18	tpypy
23.77	23.78	23.79	aes256estream
4699.73	4701.47	4781.39	aes128estream

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
9.98	9.98	9.98	chacha8
10.05	10.05	10.05	salsa208
11.59	11.59	11.60	cryptmtv3
12.46	12.46	12.47	nlsv2
12.77	12.77	12.77	chacha12
12.77	12.82	12.83	tpy6
12.83	12.83	12.83	salsa2012
12.97	12.99	13.03	tpy
16.39	16.46	16.66	tpypy
18.33	18.33	18.33	chacha20
18.39	18.39	18.39	salsa20
23.55	23.94	24.03	aes256estream
4692.18	4700.20	4860.25	aes128estream

7.13 ia64, 997MHz, HP Itanium II, nmi0020



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
113.12	113.12	113.25	chacha8
114.88	114.88	115.00	salsa208
132.88	132.88	132.88	aes128estream
136.38	136.38	136.38	salsa2012
136.50	136.50	136.50	chacha12
178.75	178.75	178.88	chacha20
180.62	180.62	180.62	salsa20
182.88	182.88	183.50	aes256estream
219.00	219.00	219.38	cryptmtv3
308.00	308.25	308.75	nlsv2
713.62	715.25	717.50	tpy6
1484.38	1485.00	1485.62	tpypy
1509.25	1510.12	1510.38	tpy

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
12.58	12.58	12.58	chacha8
12.78	12.78	12.80	salsa208
15.50	15.50	15.50	salsa2012
15.53	15.53	15.53	chacha12
20.81	20.81	20.81	chacha20
21.00	21.00	21.00	salsa20
24.62	24.62	24.62	aes128estream
34.16	34.16	34.17	aes256estream
43.47	43.47	43.47	cryptmtv3
62.50	62.56	62.64	nlsv2
99.58	99.58	99.59	tpy6
195.98	196.16	196.52	tpy
197.95	197.95	198.48	tpypy

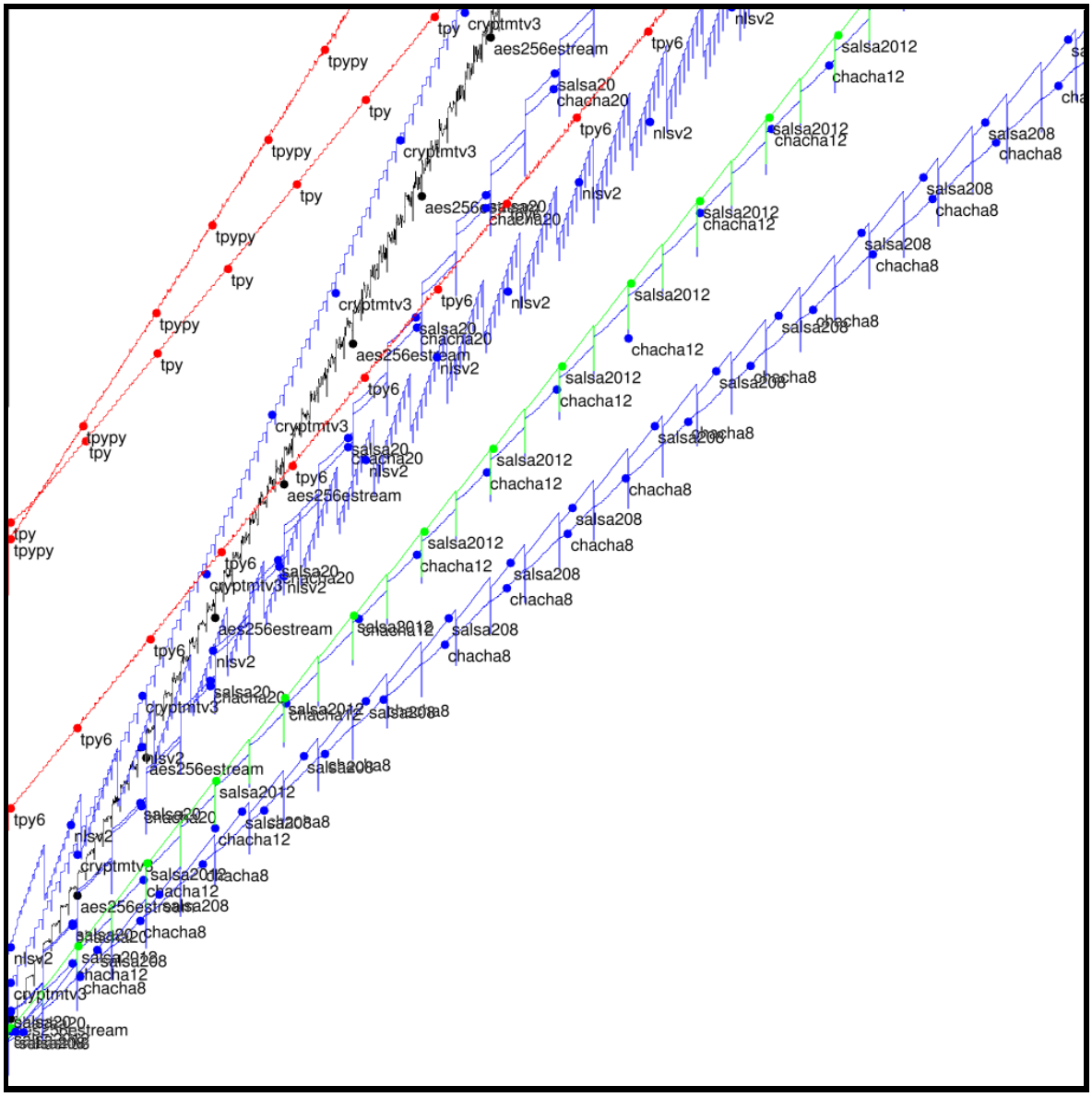
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
9.68	9.68	9.68	chacha8
9.79	9.79	9.79	salsa208
12.36	12.36	12.36	salsa2012
12.54	12.54	12.55	chacha12
12.81	12.81	12.81	aes128estream
15.96	15.96	15.97	nlsv2
17.78	17.85	17.86	aes256estream
17.87	17.87	17.87	chacha20
17.99	17.99	17.99	salsa20
21.89	21.94	21.97	tpy6
23.89	23.89	23.89	cryptmtv3
32.53	32.53	32.56	tpy
35.88	35.89	36.04	tpypy

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
9.44	9.44	9.44	chacha8
9.55	9.55	9.55	salsa208
11.87	11.87	11.88	aes128estream
12.12	12.12	12.12	salsa2012
12.30	12.30	12.30	chacha12
12.93	12.93	12.93	nlsv2
15.84	15.85	15.87	tpy6
16.52	16.52	16.53	aes256estream
17.63	17.63	17.63	chacha20
17.74	17.74	17.74	salsa20
19.64	19.65	19.67	cryptmtv3
19.79	19.79	19.82	tpy
23.04	23.04	23.04	tpypy

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
9.35	9.35	9.35	chacha8
9.46	9.46	9.46	salsa208
11.54	11.54	11.55	aes128estream
11.60	11.60	11.60	nlsv2
12.02	12.02	12.02	salsa2012
12.21	12.21	12.21	chacha12
13.30	13.31	13.32	cryptmtv3
13.56	13.58	13.58	tpy6
15.04	15.04	15.06	tpy
16.05	16.06	16.07	aes256estream
17.54	17.54	17.54	chacha20
17.65	17.65	17.65	salsa20
18.44	18.51	18.53	tpypy

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
9.30	9.30	9.30	chacha8
9.41	9.41	9.41	salsa208
9.49	9.52	9.54	cryptmtv3
11.02	11.02	11.02	nlsv2
11.31	11.34	11.37	aes128estream
11.97	11.97	11.97	salsa2012
12.15	12.16	12.16	chacha12
12.15	12.17	12.21	tpy
12.16	12.20	12.22	tpy6
15.55	15.71	15.77	tpypy
15.71	15.76	15.80	aes256estream
17.48	17.49	17.49	chacha20
17.59	17.59	17.59	salsa20

7.14 ia64, 997MHz, HP Itanium II, nmi0058



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
108.88	108.88	109.00	chacha8
118.25	118.25	118.25	salsa208
130.88	131.00	131.00	chacha12
138.38	138.38	138.50	salsa2012
155.88	157.12	157.12	aes256estream
174.88	174.88	174.88	chacha20
178.12	178.12	178.25	salsa20
240.25	240.38	240.50	cryptmtv3
335.50	335.62	335.75	nlsv2
649.75	650.12	651.38	tpy6
1280.75	1281.62	1284.00	tpypy
1308.62	1312.38	1313.75	tpy
10869.20	10871.50	10877.60	aes128estream

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
12.66	12.66	12.66	chacha8
13.23	13.23	13.23	salsa208
15.41	15.41	15.41	chacha12
15.78	15.78	15.78	salsa2012
20.91	20.91	20.91	chacha20
21.22	21.22	21.23	salsa20
34.20	34.30	34.36	aes256estream
45.31	45.34	45.52	cryptmtv3
67.05	67.06	67.06	nlsv2
91.41	91.47	91.50	tpy6
172.22	172.27	172.72	tpy
172.97	173.05	173.53	tpypy
4833.30	4837.91	4898.75	aes128estream

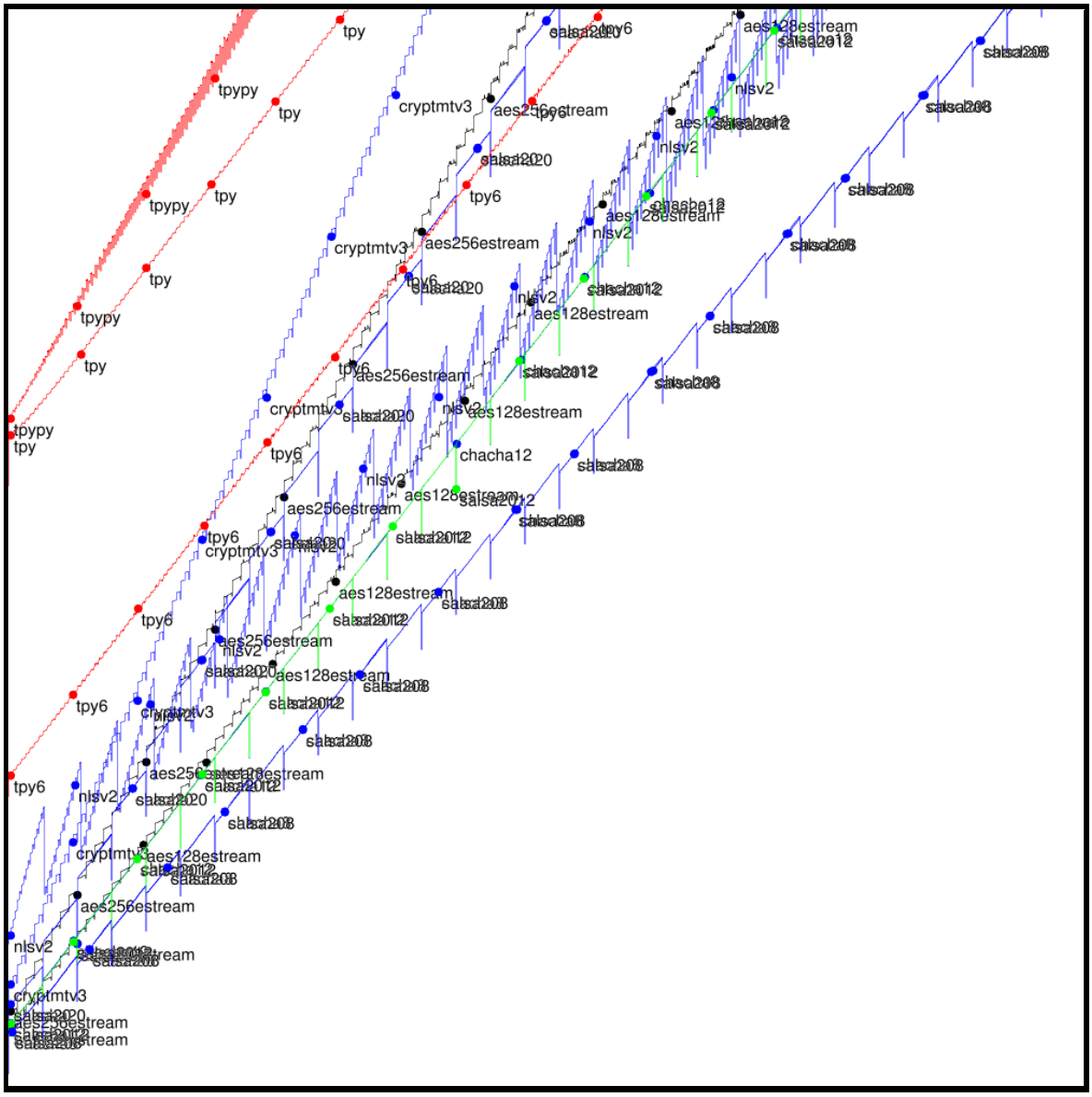
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
9.50	9.50	9.51	chacha8
9.78	9.78	9.78	salsa208
12.25	12.25	12.25	chacha12
12.41	12.41	12.42	salsa2012
17.66	17.67	17.69	nlsv2
17.75	17.75	17.75	chacha20
18.02	18.02	18.03	salsa20
20.99	21.04	21.06	tpy6
21.99	22.03	22.21	aes256estream
24.35	24.36	24.37	cryptmtv3
29.89	29.90	29.93	tpy
33.09	33.14	33.21	tpypy
4667.88	4669.09	4680.47	aes128estream

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
9.26	9.26	9.26	chacha8
9.51	9.51	9.51	salsa208
12.01	12.01	12.01	chacha12
12.15	12.15	12.16	salsa2012
14.47	14.47	14.48	nlsv2
15.51	15.52	15.53	tpy6
17.51	17.51	17.51	chacha20
17.76	17.77	17.77	salsa20
18.81	18.82	18.84	tpy
20.75	20.75	20.77	cryptmtv3
21.26	21.33	21.37	aes256estream
22.14	22.18	22.19	tpypy
4651.89	4651.99	4659.32	aes128estream

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
9.16	9.16	9.17	chacha8
9.41	9.41	9.42	salsa208
11.91	11.91	11.92	chacha12
12.05	12.05	12.06	salsa2012
13.09	13.09	13.10	nlsv2
13.45	13.46	13.46	tpy6
14.34	14.35	14.36	cryptmtv3
14.61	14.71	14.71	tpy
17.41	17.41	17.42	chacha20
17.68	17.68	17.68	salsa20
18.11	18.15	18.18	tpypy
20.72	20.74	20.74	aes256estream
4649.73	4661.59	4744.24	aes128estream

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
9.10	9.11	9.11	chacha8
9.34	9.35	9.37	salsa208
10.58	10.62	10.64	cryptmtv3
11.86	11.86	11.86	chacha12
11.98	12.00	12.01	salsa2012
11.89	12.22	12.24	tpy
12.19	12.22	12.23	tpy6
12.45	12.46	12.48	nlsv2
15.67	15.76	15.83	tpypy
17.36	17.36	17.38	chacha20
17.61	17.62	17.64	salsa20
20.37	20.47	20.67	aes256estream
4638.43	4666.08	4839.05	aes128estream

7.15 ia64, 1396MHz, HP Itanium II, nmi0065



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
126.75	127.12	127.12	salsa208
127.50	127.88	127.88	chacha8
135.88	135.88	135.88	aes128estream
149.00	149.38	149.38	salsa2012
149.75	150.12	150.12	chacha12
175.38	175.38	175.38	aes256estream
193.50	193.88	193.88	salsa20
193.88	193.88	193.88	chacha20
237.00	237.12	237.38	cryptmtv3
366.25	366.25	367.50	nlsv2
728.12	728.88	729.50	tpy6
1514.38	1515.00	1516.25	tpy
1562.12	1562.50	1562.88	tpypy

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
14.22	14.28	14.28	salsa208
14.25	14.31	14.31	chacha8
17.00	17.06	17.06	salsa2012
17.03	17.08	17.09	chacha12
22.55	22.55	22.55	chacha20
22.56	22.62	22.62	salsa20
27.14	27.14	27.14	aes128estream
36.02	36.02	36.02	aes256estream
47.36	47.38	47.41	cryptmtv3
77.64	77.64	77.77	nlsv2
101.89	101.91	101.98	tpy6
198.78	199.02	199.08	tpy
209.05	209.08	209.31	tpypy

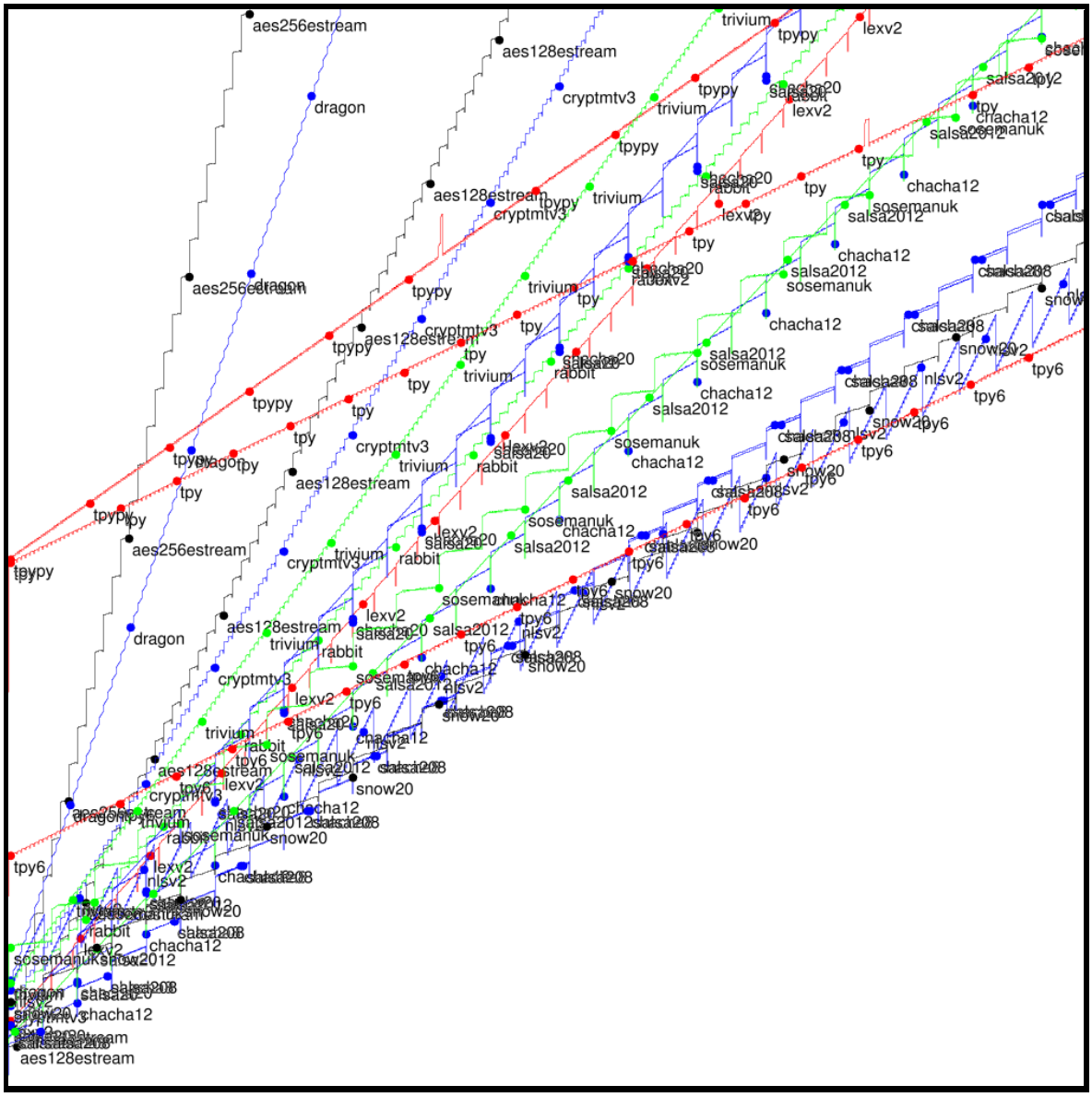
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
10.66	10.67	10.67	chacha8
10.67	10.68	10.68	salsa208
13.44	13.45	13.45	chacha12
13.45	13.46	13.46	salsa2012
15.48	15.48	15.48	aes128estream
17.04	17.05	17.07	nlsv2
19.00	19.00	19.00	chacha20
19.02	19.02	19.02	salsa20
21.13	21.13	21.14	aes256estream
22.82	22.87	22.88	tpy6
26.10	26.10	26.10	cryptmtv3
33.46	33.54	33.56	tpy
37.92	37.92	38.05	tpypy

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
10.38	10.38	10.38	chacha8
10.39	10.39	10.39	salsa208
13.16	13.16	13.16	chacha12
13.17	13.17	13.17	salsa2012
13.38	13.38	13.39	nlsv2
14.55	14.55	14.56	aes128estream
16.66	16.66	16.68	tpy6
18.72	18.72	18.72	chacha20
18.73	18.74	18.74	salsa20
19.96	19.96	20.00	aes256estream
20.63	20.63	20.63	tpy
22.01	22.01	22.02	cryptmtv3
24.60	24.62	24.63	tpypy

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
10.27	10.27	10.27	chacha8
10.28	10.28	10.28	salsa208
11.72	11.72	11.73	nlsv2
13.05	13.05	13.05	chacha12
13.06	13.06	13.06	salsa2012
14.22	14.22	14.24	aes128estream
14.33	14.34	14.36	tpy6
15.05	15.05	15.05	cryptmtv3
15.82	15.84	15.84	tpy
18.61	18.61	18.61	chacha20
18.63	18.63	18.63	salsa20
19.55	19.55	19.55	aes256estream
19.61	19.63	19.64	tpypy

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
10.20	10.20	10.21	chacha8
10.22	10.22	10.22	salsa208
10.83	10.84	10.84	cryptmtv3
11.05	11.05	11.07	nlsv2
12.91	12.95	12.98	tpy6
12.93	12.97	12.98	tpy
12.98	12.98	12.99	chacha12
13.00	13.00	13.00	salsa2012
14.00	14.03	14.07	aes128estream
16.63	16.67	16.69	tpypy
18.55	18.55	18.55	chacha20
18.56	18.56	18.56	salsa20
19.25	19.25	19.26	aes256estream

7.16 ppc32, 400MHz, Motorola PowerPC G4 7400, nmi0042



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
94.00	94.00	94.00	aes128estream
100.00	100.00	100.00	chacha8
100.00	100.00	100.00	salsa208
120.00	120.00	120.00	chacha12
120.00	120.00	120.00	salsa2012
138.00	138.00	140.00	aes256estream
144.00	144.00	146.00	chacha20
146.00	146.00	146.00	salsa20
156.00	156.00	158.00	lexv2
186.00	188.00	188.00	cryptmtv3
192.00	194.00	194.00	rabbit
194.00	194.00	196.00	snow20
234.00	234.00	234.00	nlsv2
236.00	236.00	238.00	trivium
250.00	250.00	252.00	dragon
322.00	322.00	324.00	sosemanuk
532.00	532.00	532.00	tpy6
1212.00	1212.00	1212.00	tpy
1226.00	1226.00	1226.00	tpypy

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
11.75	11.75	11.75	chacha8
11.75	11.75	11.75	salsa208
13.50	13.50	13.50	salsa2012
13.75	14.00	14.00	chacha12
16.50	16.75	16.75	salsa20
17.00	17.00	17.00	chacha20
25.50	25.75	25.75	snow20
26.75	26.75	27.00	aes128estream
29.50	29.75	29.75	lexv2
33.00	33.25	33.25	rabbit
36.75	36.75	37.00	cryptmtv3
41.50	41.50	41.75	sosemanuk
41.75	41.75	41.75	trivium
47.75	47.75	48.00	nlsv2
49.75	50.00	50.00	aes256estream
57.00	57.00	57.00	dragon
70.75	70.75	71.00	tpy6
155.75	155.75	155.75	tpy
159.25	159.50	159.50	tpypy

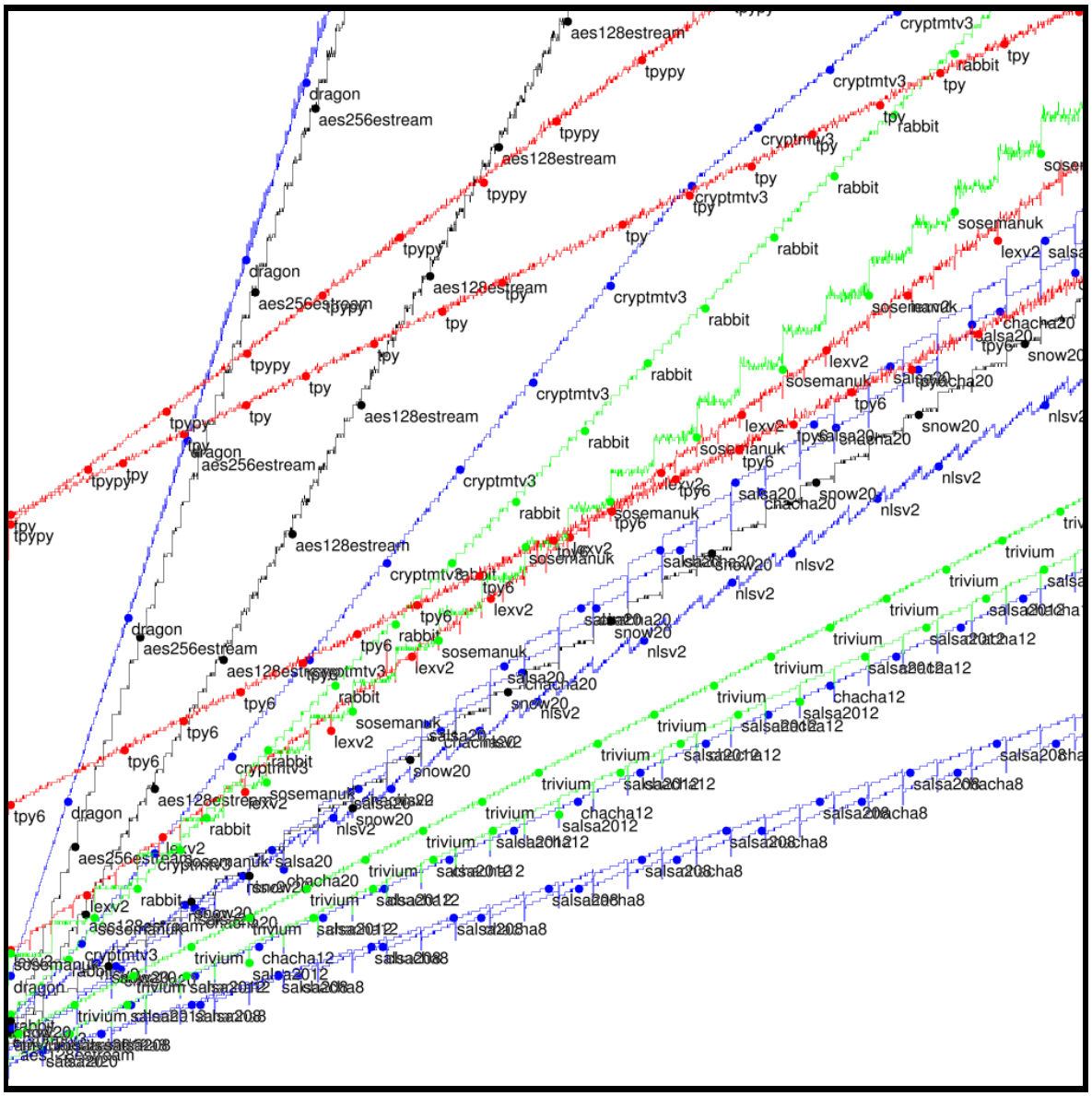
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
8.50	8.50	8.53	salsa208
8.53	8.53	8.56	chacha8
9.17	9.17	9.17	snow20
10.08	10.11	10.11	nlsv2
10.33	10.36	10.36	salsa2012
10.44	10.47	10.47	chacha12
12.22	12.22	12.25	tpy6
13.42	13.42	13.42	sosemanuk
13.47	13.50	13.50	salsa20
13.58	13.58	13.58	chacha20
13.83	13.83	13.86	lexv2
14.33	14.36	14.36	rabbit
16.92	16.92	16.92	trivium
19.08	19.08	19.11	cryptmtv3
21.53	21.53	21.56	aes128estream
21.64	21.64	21.64	tpy
23.94	23.94	23.94	tpypy
32.44	32.44	32.44	dragon
44.19	44.22	44.22	aes256estream

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
7.65	7.66	7.66	tpy6
7.80	7.80	7.80	nlsv2
7.88	7.88	7.89	snow20
8.24	8.25	8.25	salsa208
8.27	8.28	8.28	chacha8
10.10	10.10	10.10	salsa2012
10.18	10.18	10.19	chacha12
10.72	10.73	10.74	sosemanuk
11.17	11.17	11.18	tpy
12.57	12.58	12.58	lexv2
12.88	12.89	12.90	rabbit
13.24	13.24	13.25	salsa20
13.30	13.30	13.31	chacha20
13.36	13.36	13.38	tpypy
14.97	14.98	14.98	trivium
16.91	16.91	16.92	cryptmtv3
21.11	21.12	21.12	aes128estream
30.52	30.53	30.53	dragon
43.76	43.77	43.77	aes256estream

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.93	5.93	5.93	tpy6
6.77	6.77	6.78	nlsv2
7.24	7.24	7.24	tpy
7.39	7.39	7.39	snow20
8.15	8.15	8.15	salsa208
8.18	8.18	8.18	chacha8
9.39	9.39	9.40	tpypy
9.71	9.71	9.72	sosemanuk
10.01	10.01	10.01	salsa2012
10.08	10.08	10.08	chacha12
12.11	12.11	12.11	lexv2
12.32	12.32	12.33	rabbit
13.15	13.15	13.15	salsa20
13.20	13.20	13.20	chacha20
14.14	14.14	14.14	cryptmtv3
14.25	14.25	14.25	trivium
20.97	20.97	20.97	aes128estream
29.81	29.81	29.81	dragon
43.60	43.61	43.61	aes256estream

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
4.88	4.88	4.89	tpy
4.89	4.90	4.91	tpy6
6.35	6.35	6.36	nlsv2
7.00	7.01	7.02	tpypy
7.09	7.09	7.10	snow20
8.09	8.09	8.09	salsa208
8.12	8.12	8.13	chacha8
9.22	9.23	9.24	sosemanuk
9.95	9.95	9.96	salsa2012
10.02	10.02	10.02	chacha12
11.82	11.82	11.84	lexv2
11.98	11.98	12.01	rabbit
12.56	12.57	12.58	cryptmtv3
13.09	13.09	13.10	salsa20
13.14	13.14	13.14	chacha20
13.81	13.81	13.83	trivium
20.87	20.88	20.88	aes128estream
29.38	29.38	29.39	dragon
43.50	43.51	43.52	aes256estream

7.17 ppc32, 2000MHz, IBM PowerPC G5 970, geespaz



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
52.50	52.50	52.50	chacha8
52.50	52.50	52.50	salsa208
60.00	67.50	67.50	chacha12
60.00	67.50	67.50	salsa2012
82.50	90.00	90.00	chacha20
90.00	90.00	90.00	salsa20
97.50	97.50	105.00	aes128estream
112.50	112.50	112.50	trivium
120.00	127.50	127.50	aes256estream
135.00	135.00	135.00	cryptmtv3
150.00	157.50	157.50	snow20
157.50	157.50	157.50	nlsv2
165.00	172.50	172.50	rabbit
262.50	262.50	270.00	dragon
300.00	300.00	307.50	sosemanuk
322.50	322.50	322.50	lexv2
652.50	652.50	660.00	tpy6
1305.00	1312.50	1312.50	tpypy
1320.00	1320.00	1335.00	tpy

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
4.69	5.62	5.62	chacha8
5.62	5.62	5.62	salsa208
6.56	6.56	7.50	chacha12
6.56	7.50	7.50	salsa2012
10.31	10.31	10.31	salsa20
9.38	10.31	10.31	chacha20
17.81	18.75	18.75	trivium
19.69	19.69	20.62	snow20
25.31	26.25	26.25	aes128estream
26.25	26.25	27.19	cryptmtv3
28.12	28.12	29.06	nlsv2
28.12	29.06	29.06	rabbit
38.44	38.44	39.38	aes256estream
38.44	38.44	39.38	sosemanuk
45.94	46.88	46.88	lexv2
60.94	60.94	61.88	dragon
85.31	86.25	86.25	tpy6
168.75	169.69	170.62	tpypy
169.69	170.62	170.62	tpy

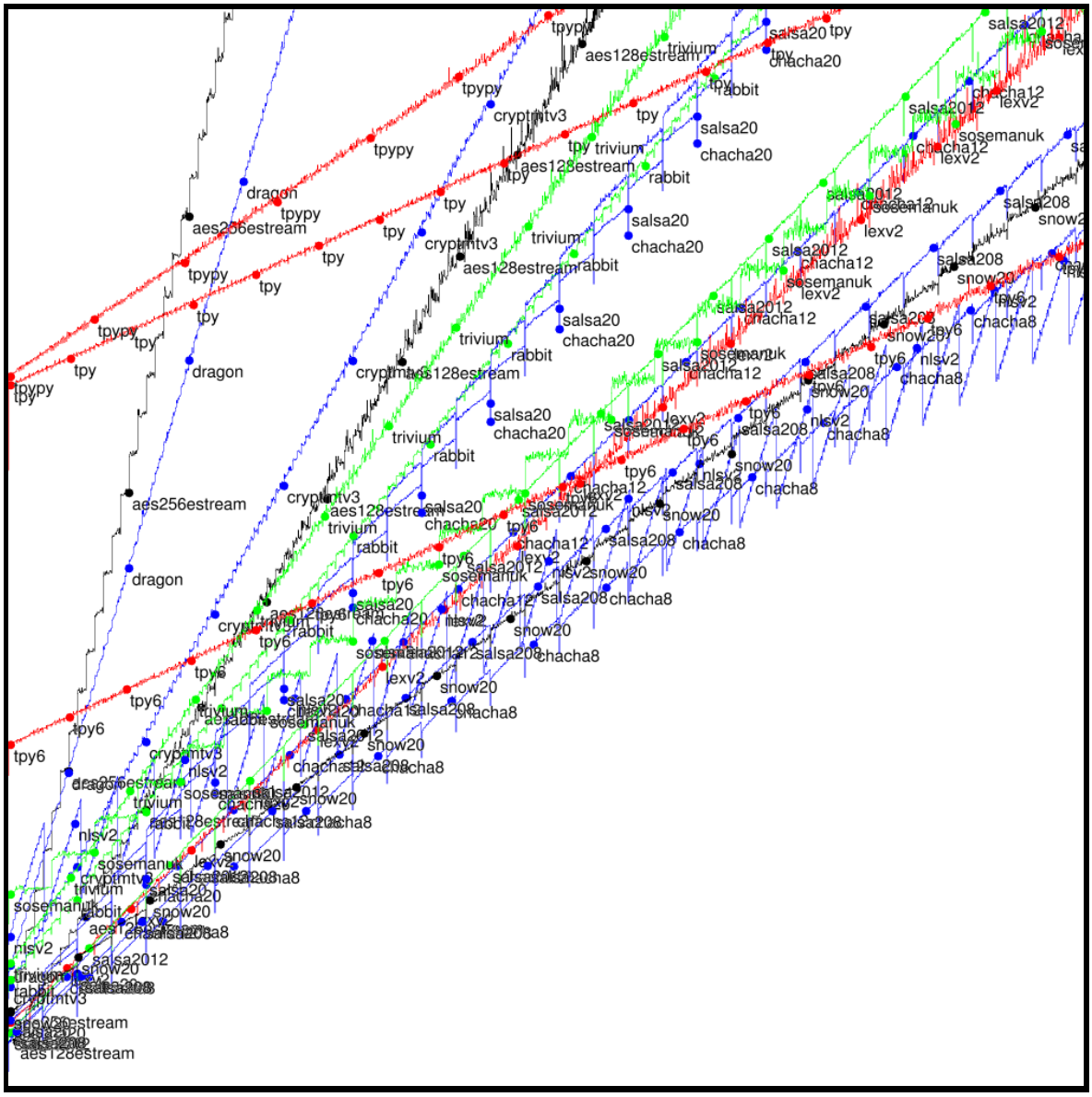
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
3.33	3.33	3.33	chacha8
3.44	3.54	3.54	salsa208
4.79	4.79	4.90	chacha12
5.00	5.00	5.00	salsa2012
6.46	6.46	6.56	trivium
7.81	7.81	7.81	chacha20
8.12	8.12	8.12	salsa20
8.12	8.23	8.23	nlsv2
8.23	8.23	8.33	snow20
11.77	11.88	12.08	sosemanuk
11.77	11.98	12.50	lexv2
12.19	12.29	12.40	rabbit
13.85	13.96	14.06	tpy6
14.06	14.06	14.17	cryptmtv3
19.27	19.38	19.48	aes128estream
22.92	23.02	23.12	tpy
25.21	25.31	25.52	tpypy
31.46	31.67	31.98	aes256estream
33.65	34.38	34.58	dragon

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
3.16	3.16	3.16	chacha8
3.32	3.32	3.36	salsa208
4.65	4.65	4.65	chacha12
4.84	4.84	4.84	salsa2012
5.55	5.55	5.59	trivium
6.76	6.80	6.84	nlsv2
7.27	7.30	7.34	snow20
7.62	7.66	7.66	chacha20
7.93	7.93	7.93	salsa20
8.24	8.28	8.36	tpy6
8.95	8.98	9.06	lexv2
9.53	9.61	9.65	sosemanuk
10.98	11.02	11.02	rabbit
11.60	11.68	11.72	tpy
12.30	12.38	12.38	cryptmtv3
14.06	14.10	14.18	tpypy
18.87	18.95	19.26	aes128estream
31.09	31.25	31.41	aes256estream
31.52	31.99	32.50	dragon

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
3.09	3.09	3.11	`chacha8`
3.27	3.27	3.28	`salsa208`
4.58	4.60	4.60	`chacha12`
4.78	4.78	4.78	`salsa2012`
5.21	5.21	5.23	`trivium`
6.11	6.15	6.20	`tpy6`
6.17	6.20	6.24	`nlsv2`
6.93	6.96	7.00	`snow20`
7.29	7.34	7.40	`tpy`
7.57	7.57	7.59	`chacha20`
7.85	7.87	7.87	`salsa20`
7.91	7.97	8.01	`lexv2`
8.86	8.88	8.91	`sosemanuk`
9.65	9.70	9.71	`cryptmtv3`
9.76	9.79	9.84	`tpypy`
10.49	10.52	10.55	`rabbit`
18.35	18.57	18.71	`aes128estream`
30.26	30.81	31.58	`dragon`
30.84	31.01	31.19	`aes256estream`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
3.05	3.05	3.08	`chacha8`
3.22	3.22	3.25	`salsa208`
4.54	4.57	4.57	`chacha12`
4.72	4.75	4.75	`salsa2012`
4.63	4.78	4.89	`tpy`
4.69	4.89	5.01	`tpy6`
4.98	5.01	5.04	`trivium`
5.74	5.89	6.01	`nlsv2`
6.65	6.77	6.88	`snow20`
7.09	7.18	7.35	`tpypy`
7.12	7.35	7.50	`lexv2`
7.53	7.53	7.56	`chacha20`
7.79	7.82	7.85	`salsa20`
7.79	7.97	8.03	`cryptmtv3`
8.50	8.55	8.64	`sosemanuk`
10.14	10.22	10.31	`rabbit`
17.81	18.34	18.81	`aes128estream`
28.68	30.32	32.93	`dragon`
30.41	30.88	31.38	`aes256estream`

7.18 ppc32, 2097MHz, IBM POWER5, nmi0154



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
104.00	106.00	108.00	aes128estream
110.00	111.50	113.00	chacha8
115.00	117.50	118.50	salsa208
129.00	130.50	133.00	chacha12
131.00	133.00	136.00	salsa2012
151.00	152.50	153.50	lexv2
153.00	154.00	157.50	chacha20
162.50	164.00	166.50	salsa20
173.50	175.50	178.50	snow20
175.00	177.00	178.50	aes256estream
231.00	234.00	237.50	cryptmtv3
248.00	251.50	258.50	rabbit
279.50	280.50	283.50	trivium
285.00	288.00	290.50	dragon
363.00	365.00	367.50	nlsv2
444.00	447.00	451.50	sosemanuk
787.00	792.00	796.00	tpy6
1621.50	1625.00	1630.50	tpy
1647.00	1650.50	1656.00	tpypy

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
12.06	12.25	12.44	chacha8
13.00	13.31	13.50	salsa208
14.62	14.69	14.94	chacha12
15.00	15.25	15.50	salsa2012
17.94	18.06	18.38	chacha20
18.44	18.69	19.00	salsa20
23.38	23.62	23.94	snow20
26.31	26.69	26.88	aes128estream
26.94	27.06	27.38	lexv2
40.06	40.56	41.38	rabbit
44.38	44.81	45.88	cryptmtv3
47.50	47.88	48.25	trivium
56.56	56.88	57.25	sosemanuk
56.44	56.94	57.25	aes256estream
65.12	65.62	66.00	dragon
73.94	74.38	74.75	nlsv2
102.12	102.62	103.00	tpy6
206.69	207.25	207.81	tpy
211.38	212.00	212.94	tpypy

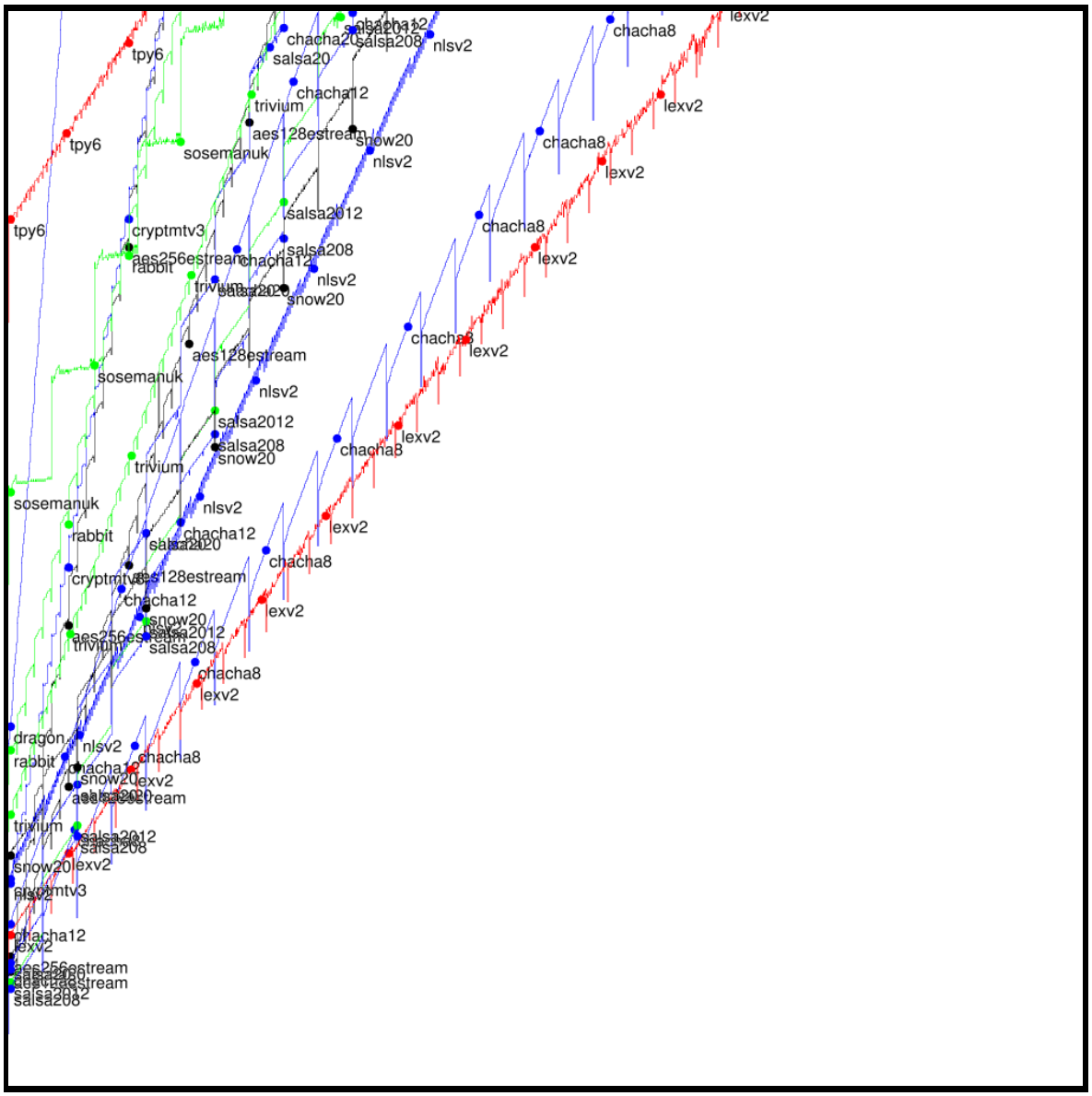
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
8.03	8.08	8.12	chacha8
8.99	9.07	9.14	salsa208
9.77	9.83	9.97	snow20
10.41	10.46	10.51	chacha12
10.94	10.99	11.05	salsa2012
11.51	11.60	12.26	lexv2
11.75	11.80	11.86	nlsv2
13.89	13.94	14.03	chacha20
14.24	14.32	14.40	sosemanuk
14.31	14.39	14.47	salsa20
15.49	15.56	15.68	tpy6
15.90	15.99	16.11	rabbit
17.82	17.89	18.00	trivium
18.43	18.70	18.83	aes128estream
21.26	21.43	21.55	cryptmtv3
26.95	27.01	27.08	tpy
29.35	29.44	29.59	tpypy
37.11	37.32	37.49	dragon
46.99	47.13	47.34	aes256estream

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
7.71	7.72	7.75	chacha8
8.05	8.08	8.10	nlsv2
8.58	8.61	8.68	snow20
8.68	8.71	8.74	salsa208
8.73	8.78	8.83	tpy6
10.06	10.11	10.14	chacha12
10.18	10.28	10.34	lexv2
10.62	10.64	10.70	salsa2012
10.68	10.80	10.85	sosemanuk
12.93	12.97	13.03	tpy
13.62	13.66	13.70	chacha20
14.00	14.04	14.09	salsa20
14.02	14.07	14.12	rabbit
15.12	15.17	15.38	tpypy
15.67	15.75	15.93	trivium
17.73	17.86	17.98	aes128estream
19.33	19.42	19.48	cryptmtv3
35.00	35.11	35.22	dragon
46.23	46.38	47.12	aes256estream

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
6.24	6.26	6.30	tpy6
6.37	6.40	6.44	nlsv2
7.57	7.59	7.63	chacha8
7.65	7.67	7.71	tpy
8.15	8.18	8.23	snow20
8.56	8.58	8.60	salsa208
9.71	9.72	9.75	sosemanuk
9.71	9.73	9.77	lexv2
9.96	9.99	10.02	chacha12
9.89	10.00	10.11	tpypy
10.50	10.53	10.57	salsa2012
13.10	13.15	13.18	cryptmtv3
13.29	13.34	13.37	rabbit
13.49	13.50	13.53	chacha20
13.86	13.87	13.91	salsa20
14.69	14.83	15.03	trivium
17.58	17.77	17.94	aes128estream
34.23	34.30	34.39	dragon
46.14	46.26	46.39	aes256estream

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
4.44	4.51	4.63	tpy
4.72	4.80	4.91	tpy6
5.66	5.74	5.83	nlsv2
6.31	6.69	6.99	tpypy
7.46	7.52	7.61	chacha8
7.85	7.94	8.07	snow20
8.43	8.49	8.56	salsa208
9.17	9.23	9.47	sosemanuk
9.15	9.30	9.41	cryptmtv3
9.29	9.49	9.61	lexv2
9.79	9.88	9.97	chacha12
10.35	10.43	10.55	salsa2012
12.74	12.87	13.01	rabbit
13.35	13.42	13.51	chacha20
13.74	13.80	13.89	salsa20
14.10	14.43	14.87	trivium
16.86	17.37	17.85	aes128estream
33.60	33.86	34.12	dragon
45.45	46.02	46.65	aes256estream

7.19 ppc32, 3192MHz, IBM Cell PPE, `nmips3`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
235.00	235.00	240.00	salsa208
245.00	250.00	250.00	salsa2012
280.00	280.00	285.00	aes128estream
285.00	290.00	290.00	chacha8
295.00	295.00	300.00	chacha20
295.00	295.00	300.00	salsa20
310.00	310.00	310.00	aes256estream
360.00	360.00	360.00	lexv2
395.00	395.00	400.00	chacha12
485.00	485.00	485.00	cryptmtv3
485.00	485.00	485.00	nlsv2
545.00	550.00	550.00	snow20
625.00	625.00	630.00	trivium
790.00	790.00	790.00	rabbit
890.00	895.00	895.00	dragon
1400.00	1400.00	1400.00	sosemanuk
2000.00	2005.00	2010.00	tpy6
4575.00	4580.00	4585.00	tpy
5005.00	5010.00	5010.00	tpypy

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
33.12	33.12	33.12	chacha8
42.50	42.50	43.12	salsa208
43.75	44.38	44.38	salsa2012
45.00	45.62	45.62	chacha12
50.00	50.62	50.62	chacha20
50.00	50.62	50.62	salsa20
57.50	57.50	58.12	lexv2
59.38	59.38	59.38	aes128estream
69.38	70.00	70.00	snow20
80.00	80.00	80.62	nlsv2
86.25	86.25	86.88	aes256estream
103.12	103.75	103.75	trivium
107.50	107.50	108.12	cryptmtv3
129.38	130.00	130.00	rabbit
175.62	175.62	175.62	sosemanuk
232.50	233.12	235.00	dragon
263.75	263.75	263.75	tpy6
585.00	585.62	586.88	tpy
644.38	645.00	645.62	tpypy

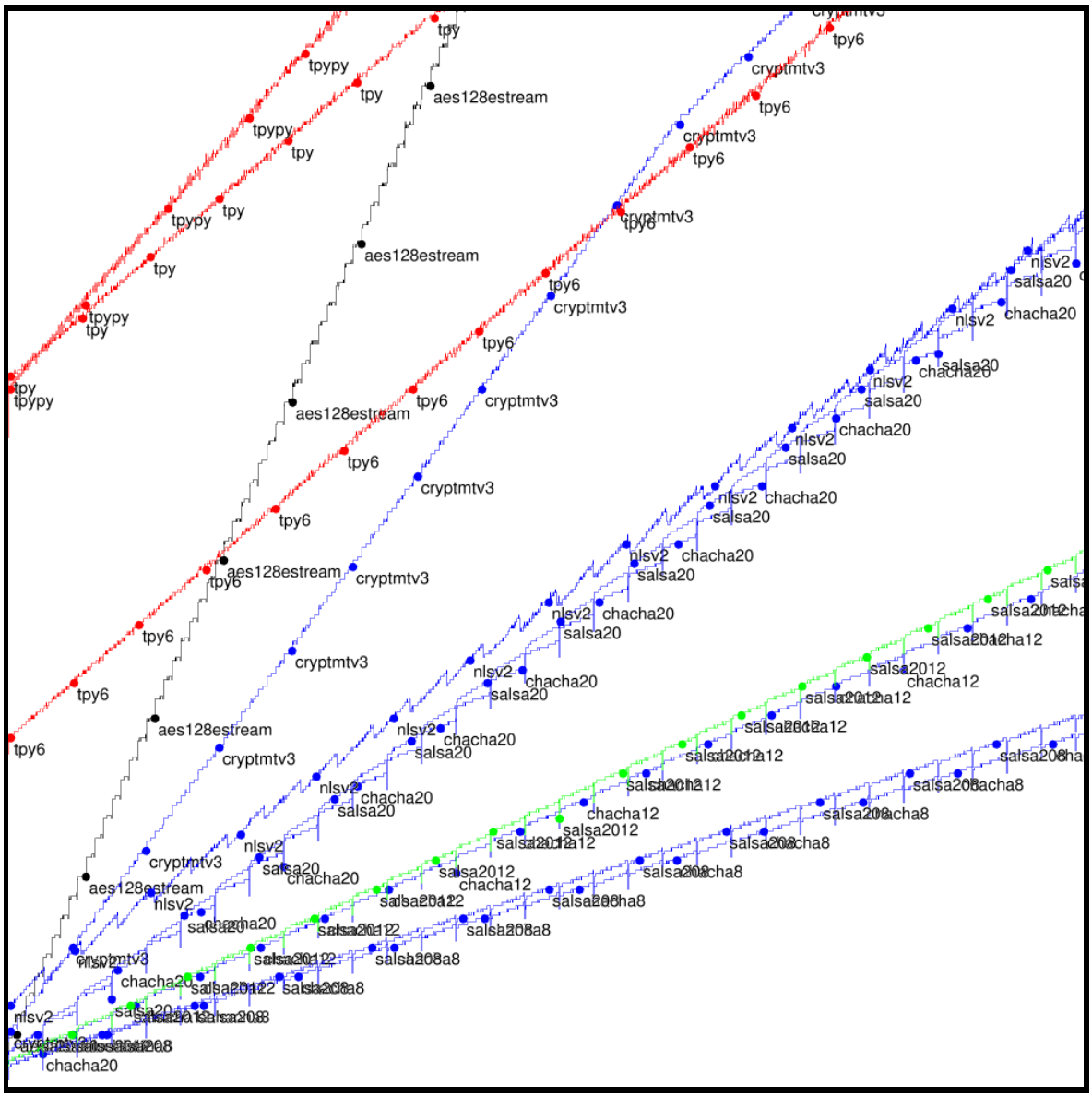
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
17.43	17.43	17.43	chacha8
18.06	18.06	18.12	lexv2
26.67	26.74	26.74	nlsv2
28.26	28.26	28.33	snow20
30.83	30.83	35.83	salsa208
31.32	31.32	31.39	chacha12
31.94	31.94	32.01	salsa2012
38.12	38.12	38.12	trivium
38.12	38.19	38.19	chacha20
38.19	38.19	38.40	salsa20
39.24	39.24	39.31	aes128estream
43.06	43.12	43.12	tpy6
44.93	45.14	52.99	sosemanuk
53.96	54.03	54.03	rabbit
63.06	63.19	63.26	cryptmtv3
65.56	65.69	65.69	aes256estream
78.40	78.54	78.54	tpy
90.90	90.97	91.11	tpypy
148.96	149.03	149.10	dragon

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
14.77	14.82	14.87	lexv2
16.20	16.20	16.20	chacha8
22.53	22.55	22.55	nlsv2
25.03	25.03	25.05	snow20
25.65	25.73	25.81	tpy6
29.82	29.90	29.90	salsa208
30.18	30.18	30.21	chacha12
30.83	30.94	30.96	salsa2012
33.12	33.12	33.12	trivium
33.54	33.67	33.83	sosemanuk
37.21	37.27	37.29	salsa20
37.29	37.34	37.34	chacha20
37.68	37.71	41.30	aes128estream
38.91	38.93	38.93	tpy
47.58	47.58	47.79	tpypy
48.05	48.07	48.07	rabbit
55.00	55.03	55.05	cryptmtv3
64.09	64.09	64.11	aes256estream
142.37	142.45	142.47	dragon

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
13.63	13.63	13.76	`lexv2`
15.84	15.84	15.85	`chacha8`
19.29	19.35	19.38	`tpy6`
21.00	21.00	21.01	`nlsv2`
23.80	23.83	23.86	`snow20`
24.04	24.07	24.09	`tpy`
29.31	29.32	35.68	`salsa208`
29.77	29.77	36.61	`chacha12`
29.72	29.79	29.79	`sosemanuk`
30.35	30.44	30.45	`salsa2012`
31.28	31.28	31.29	`trivium`
31.33	31.34	31.35	`tpypy`
36.80	36.81	36.88	`chacha20`
36.89	36.96	36.96	`salsa20`
37.17	37.18	37.18	`aes128estream`
40.45	40.46	40.47	`cryptmtv3`
45.85	45.86	46.09	`rabbit`
63.51	63.53	63.53	`aes256estream`
140.08	140.18	142.88	`dragon`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
12.85	12.89	13.26	`lexv2`
15.06	15.14	15.20	`tpy`
15.27	15.49	15.59	`tpy6`
15.66	15.66	15.70	`chacha8`
20.10	20.12	20.14	`nlsv2`
21.50	21.54	21.58	`tpypy`
23.05	23.11	23.18	`snow20`
27.77	28.07	28.16	`sosemanuk`
28.93	29.06	41.86	`salsa208`
29.51	29.51	43.20	`chacha12`
29.92	30.16	30.20	`salsa2012`
30.18	30.18	30.20	`trivium`
31.29	31.35	31.48	`cryptmtv3`
36.41	36.48	36.66	`chacha20`
36.60	36.76	36.88	`salsa20`
36.86	36.89	36.89	`aes128estream`
44.51	44.55	45.02	`rabbit`
63.12	63.20	63.20	`aes256estream`
138.44	138.67	144.40	`dragon`

7.20 ppc64, 2000MHz, IBM PowerPC G5 970, geespaz



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
52.50	52.50	52.50	chacha8
52.50	52.50	52.50	salsa208
60.00	60.00	67.50	chacha12
60.00	67.50	67.50	salsa2012
82.50	82.50	90.00	salsa20
82.50	90.00	90.00	chacha20
120.00	120.00	120.00	aes128estream
127.50	127.50	135.00	cryptmtv3
187.50	187.50	195.00	nlsv2
810.00	817.50	817.50	tpy6
1620.00	1620.00	1627.50	tpypy
1642.50	1650.00	1650.00	tpy

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
4.69	4.69	5.62	chacha8
4.69	5.62	5.62	salsa208
6.56	6.56	6.56	chacha12
6.56	6.56	7.50	salsa2012
9.38	9.38	10.31	chacha20
9.38	9.38	10.31	salsa20
27.19	27.19	28.12	cryptmtv3
31.88	31.88	32.81	aes128estream
32.81	33.75	33.75	nlsv2
108.75	108.75	109.69	tpy6
212.81	213.75	214.69	tpy
212.81	213.75	214.69	tpypy

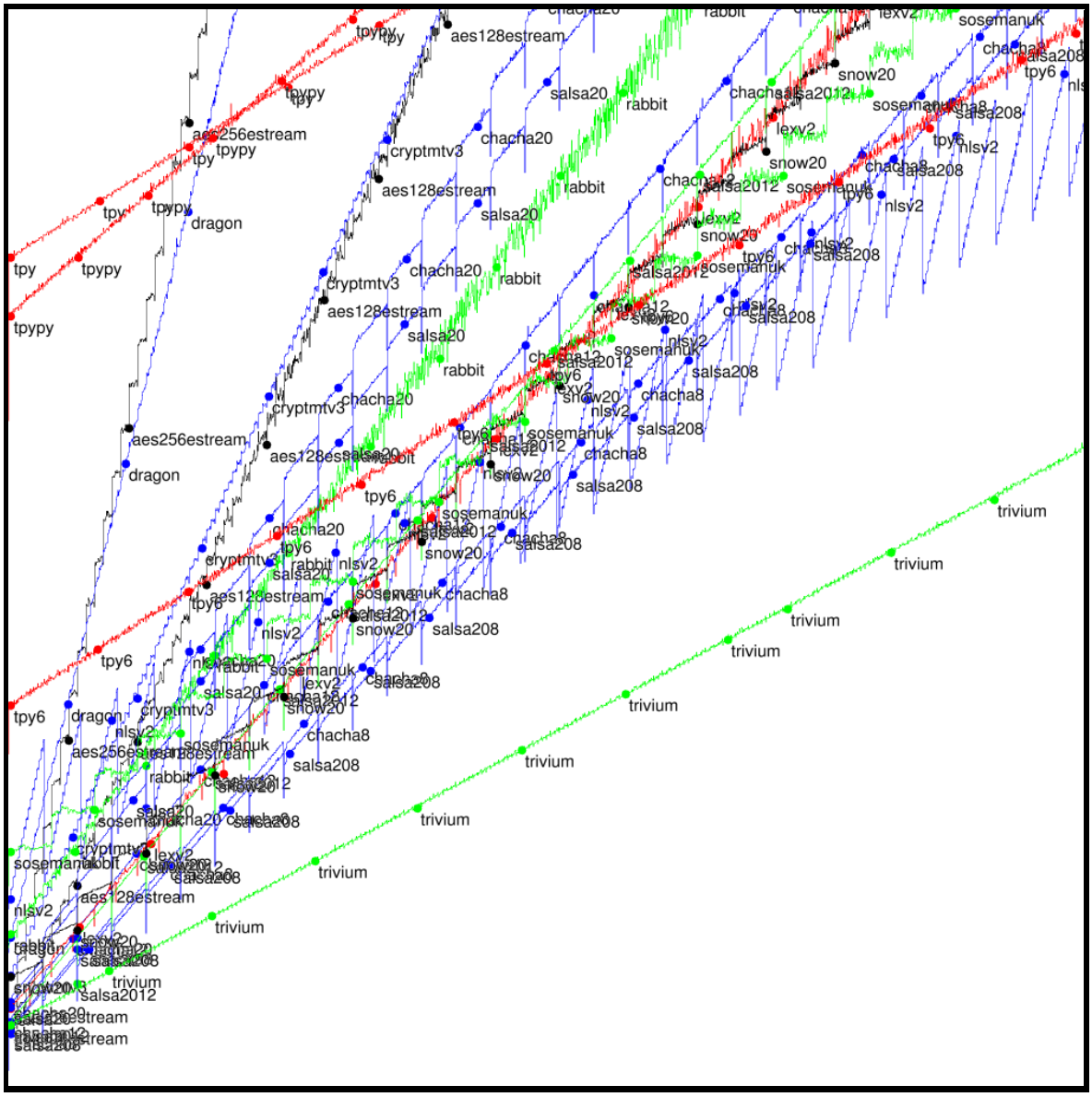
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
3.33	3.33	3.33	chacha8
3.44	3.44	3.54	salsa208
4.79	4.79	4.79	chacha12
5.00	5.00	5.00	salsa2012
7.92	7.92	7.92	chacha20
8.02	8.02	8.12	salsa20
10.00	10.10	10.10	nlsv2
15.21	15.21	15.31	cryptmtv3
19.79	19.90	20.00	tpy6
23.96	23.96	24.06	aes128estream
31.15	31.35	31.46	tpy
33.65	33.75	33.96	tpypy

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
3.16	3.16	3.16	chacha8
3.32	3.36	3.36	salsa208
4.65	4.65	4.65	chacha12
4.80	4.84	4.84	salsa2012
7.73	7.77	7.77	chacha20
7.89	7.89	7.93	salsa20
8.32	8.32	8.36	nlsv2
12.85	12.89	12.93	tpy6
13.48	13.52	13.55	cryptmtv3
17.15	17.19	17.27	tpy
19.61	19.69	19.73	tpypy
23.28	23.36	23.40	aes128estream

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
3.11	3.12	3.12	chacha8
3.28	3.28	3.30	salsa208
4.58	4.58	4.60	chacha12
4.76	4.78	4.78	salsa2012
7.59	7.59	7.71	chacha20
7.65	7.68	7.72	nlsv2
7.84	7.85	7.85	salsa20
10.12	10.20	10.27	tpy6
10.68	10.72	10.74	cryptmtv3
11.70	11.75	11.82	tpy
14.46	14.58	14.62	tpypy
23.13	23.14	23.50	aes128estream

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
3.05	3.11	3.11	chacha8
3.22	3.25	3.28	salsa208
4.54	4.54	4.57	chacha12
4.69	4.75	4.75	salsa2012
7.24	7.35	7.47	nlsv2
7.41	7.44	7.68	chacha20
7.79	7.82	7.82	salsa20
8.32	8.50	8.73	tpy
8.38	8.58	8.76	tpy6
8.91	9.05	9.11	cryptmtv3
11.25	11.54	11.72	tpypy
22.97	23.03	23.79	aes128estream

7.21 ppc64, 2097MHz, IBM POWER5, nmi0154



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
132.00	135.50	138.00	salsa208
136.50	139.50	141.50	trivium
139.50	141.50	144.00	chacha8
140.00	142.50	146.00	aes128estream
152.00	155.50	159.50	salsa2012
160.50	163.00	165.00	chacha12
186.00	188.50	191.50	lexv2
191.50	193.50	197.00	aes256estream
192.00	194.50	197.50	salsa20
208.00	210.00	213.00	chacha20
252.00	255.50	259.50	snow20
254.50	259.00	262.50	cryptmtv3
351.00	354.50	358.50	dragon
351.50	354.50	360.50	rabbit
456.00	461.00	465.00	nlsv2
545.00	547.50	550.50	sosemanuk
874.50	883.50	888.00	tpy6
1786.50	1794.50	1800.50	tpypy
1921.00	1927.00	1930.50	tpy

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
14.50	14.81	15.00	salsa208
14.88	15.00	15.38	chacha8
17.00	17.19	17.69	salsa2012
17.69	18.00	18.38	chacha12
22.06	22.31	22.56	trivium
22.00	22.31	22.69	salsa20
23.50	23.75	24.00	chacha20
32.50	32.94	33.25	snow20
32.94	33.31	33.75	lexv2
34.31	34.69	35.06	aes128estream
50.38	51.00	51.75	cryptmtv3
53.56	54.25	55.00	rabbit
61.31	61.69	62.06	aes256estream
68.81	69.25	69.50	sosemanuk
80.06	81.00	81.81	dragon
96.50	97.12	97.88	nlsv2
115.06	116.00	116.88	tpy6
230.56	231.19	232.38	tpypy
244.31	245.25	246.56	tpy

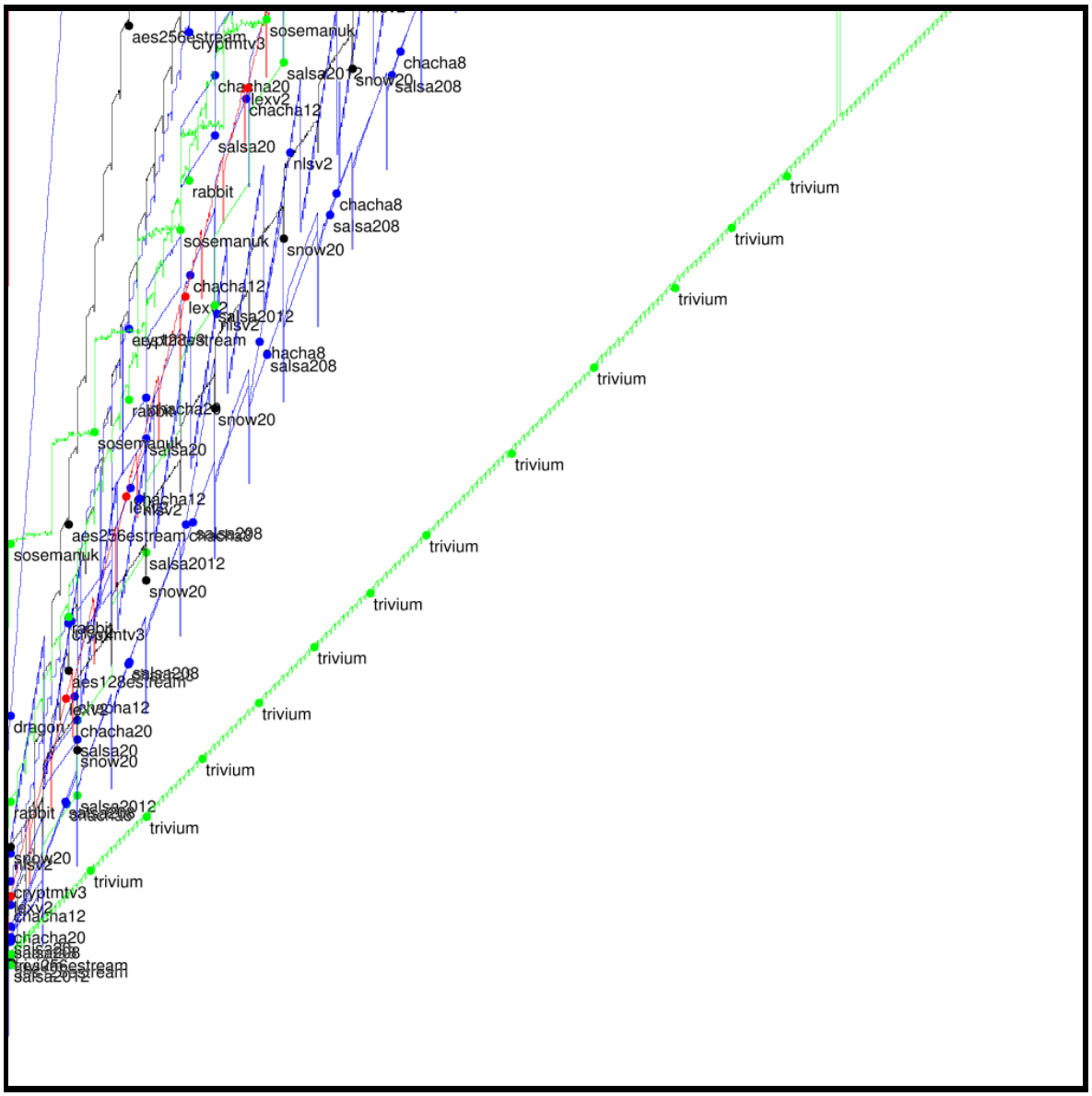
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
7.20	7.22	7.26	trivium
10.29	10.39	10.47	salsa208
10.74	10.78	10.84	chacha8
12.79	12.88	12.97	salsa2012
13.61	13.67	13.72	chacha12
13.83	13.90	14.08	snow20
14.05	14.11	14.17	lexv2
14.62	14.69	14.74	nlsv2
16.18	16.26	16.33	sosemanuk
17.83	17.89	17.99	salsa20
18.40	18.53	18.72	rabbit
18.42	18.56	18.68	tpy6
19.47	19.51	19.56	chacha20
24.67	24.94	25.25	aes128estream
25.49	25.62	25.78	cryptmtv3
32.83	32.91	33.00	tpy
33.31	33.40	33.63	tpypy
45.38	45.53	45.76	dragon
52.23	52.38	52.62	aes256estream

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
6.04	6.06	6.08	trivium
9.86	9.90	9.96	nlsv2
9.97	10.02	10.09	salsa208
10.38	10.40	10.43	chacha8
10.84	10.89	10.96	tpy6
11.80	11.92	12.03	sosemanuk
12.26	12.37	12.51	snow20
12.48	12.53	12.58	salsa2012
12.55	12.71	12.88	lexv2
13.28	13.31	13.36	chacha12
15.11	15.22	15.29	rabbit
16.17	16.24	16.32	tpy
17.53	17.57	17.64	salsa20
17.88	17.95	18.04	tpypy
19.13	19.18	19.22	chacha20
20.65	20.74	20.83	cryptmtv3
23.81	24.10	24.35	aes128estream
42.60	42.83	43.02	dragon
51.51	51.75	52.16	aes256estream

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.62	5.63	5.64	`trivium`
7.65	7.66	7.68	`nlsv2`
8.02	8.05	8.07	`tpy6`
9.85	9.87	9.90	`salsa208`
9.98	10.00	10.05	`tpy`
10.27	10.30	10.40	`chacha8`
10.72	10.75	10.77	`sosemanuk`
11.67	11.72	11.78	`snow20`
12.12	12.16	12.20	`tpypy`
12.06	12.19	12.29	`lexv2`
12.36	12.39	12.41	`salsa2012`
13.15	13.17	13.20	`chacha12`
14.00	14.03	14.07	`cryptmtv3`
14.15	14.30	14.61	`rabbit`
17.40	17.42	17.45	`salsa20`
19.00	19.03	19.09	`chacha20`
23.47	23.68	23.96	`aes128estream`
41.76	41.88	42.05	`dragon`
51.23	51.32	51.48	`aes256estream`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
5.34	5.37	5.40	`trivium`
6.15	6.27	6.38	`tpy`
6.19	6.34	6.44	`tpy6`
6.77	6.83	6.90	`nlsv2`
8.56	8.70	8.84	`tpypy`
9.71	9.79	9.88	`salsa208`
9.85	9.96	10.11	`cryptmtv3`
10.11	10.21	10.43	`chacha8`
10.12	10.27	10.43	`sosemanuk`
11.24	11.39	11.56	`snow20`
11.48	11.86	12.25	`lexv2`
12.18	12.31	12.40	`salsa2012`
13.00	13.09	13.16	`chacha12`
13.03	13.45	14.44	`rabbit`
17.25	17.33	17.42	`salsa20`
18.81	18.94	19.09	`chacha20`
22.86	23.51	24.20	`aes128estream`
41.05	41.40	41.89	`dragon`
49.90	51.00	51.55	`aes256estream`

7.22 ppc64, 3192MHz, IBM Cell PPE, `nmips3`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
290.00	290.00	290.00	salsa2012
300.00	300.00	305.00	aes128estream
300.00	305.00	305.00	trivium
310.00	315.00	315.00	aes256estream
350.00	350.00	350.00	chacha8
355.00	355.00	355.00	salsa20
355.00	360.00	360.00	salsa208
375.00	380.00	380.00	chacha20
440.00	440.00	440.00	chacha12
460.00	460.00	460.00	lexv2
475.00	480.00	575.00	cryptmtv3
565.00	565.00	570.00	snow20
575.00	575.00	575.00	nlsv2
670.00	675.00	675.00	rabbit
910.00	915.00	915.00	dragon
1260.00	1265.00	1265.00	sosemanuk
2570.00	2570.00	2575.00	tpy6
6185.00	6190.00	7310.00	tpypy
7770.00	7770.00	7780.00	tpy

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
40.62	40.62	41.25	chacha8
40.62	41.25	41.25	salsa208
46.88	46.88	46.88	trivium
48.75	48.75	49.38	salsa2012
51.88	52.50	52.50	chacha12
56.25	56.88	56.88	salsa20
59.38	60.00	60.00	chacha20
72.50	72.50	73.12	snow20
77.50	78.12	78.12	aes128estream
88.75	89.38	90.00	lexv2
98.75	99.38	100.00	cryptmtv3
100.00	100.00	100.00	aes256estream
108.75	108.75	108.75	rabbit
124.38	124.38	125.00	nlsv2
160.00	160.62	160.62	sosemanuk
234.38	234.38	235.62	dragon
336.88	338.12	338.12	tpy6
795.62	796.25	796.25	tpypy
986.88	986.88	987.50	tpy

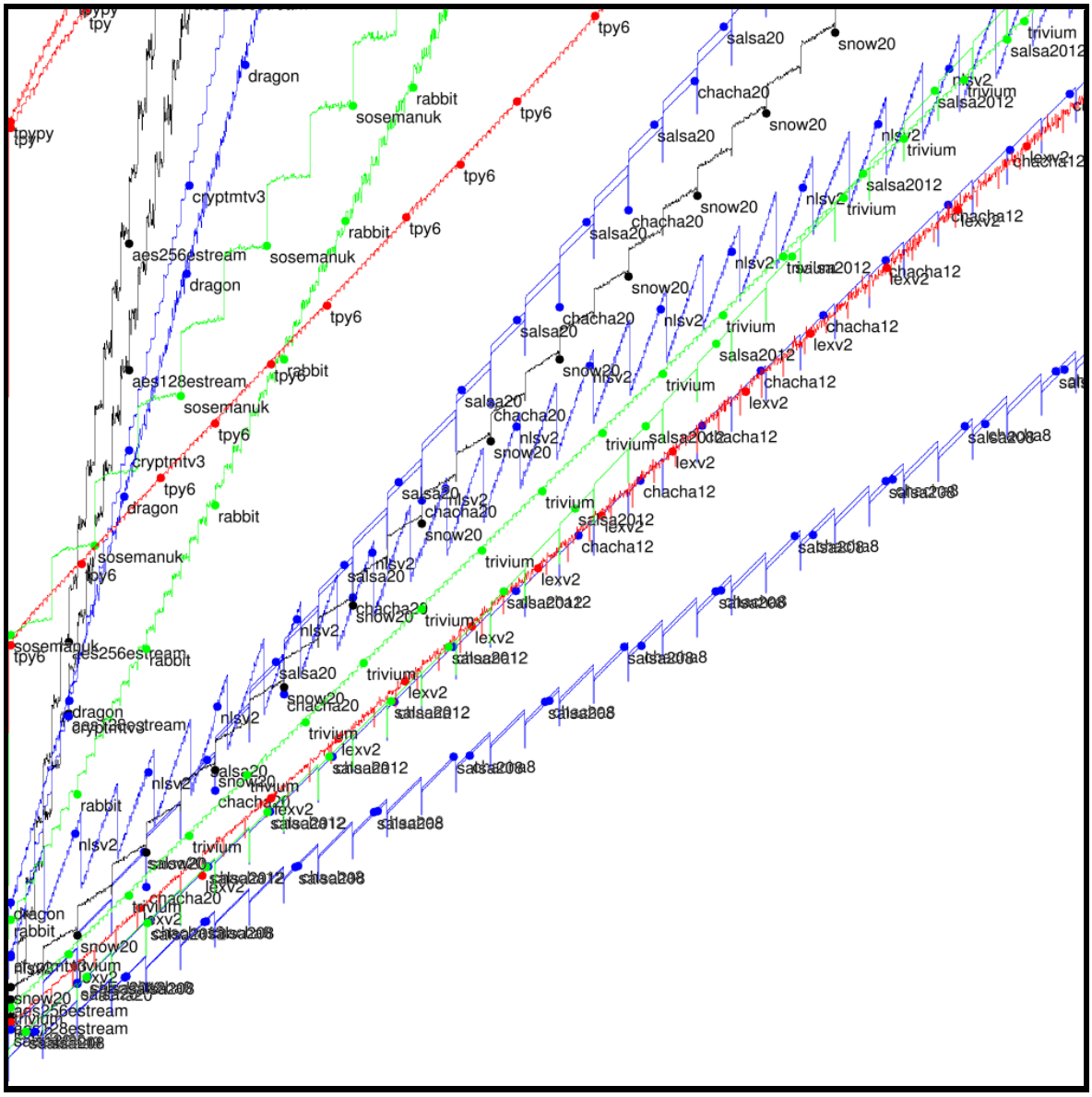
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
14.17	14.17	14.17	trivium
24.51	24.51	24.51	salsa208
24.58	24.58	24.65	chacha8
30.14	30.14	30.14	snow20
30.76	30.76	30.83	nlsv2
36.74	36.74	36.81	chacha12
36.74	36.88	36.94	salsa2012
40.14	40.14	40.35	lexv2
40.62	40.69	40.83	sosemanuk
44.24	44.72	53.26	rabbit
45.21	45.21	45.28	salsa20
47.78	48.12	48.12	chacha20
53.40	53.61	53.75	tpy6
54.17	54.24	54.31	cryptmtv3
59.17	59.24	59.24	aes128estream
84.72	84.79	84.79	aes256estream
111.04	111.04	111.04	tpypy
125.56	125.56	125.62	tpy
147.85	148.06	148.06	dragon

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
11.59	11.61	14.53	trivium
23.18	23.18	23.20	salsa208
23.44	23.46	31.41	chacha8
25.18	25.18	25.21	nlsv2
26.74	26.74	26.77	snow20
30.57	30.62	30.65	sosemanuk
31.35	31.43	31.59	tpy6
35.68	35.70	35.70	chacha12
36.02	36.04	36.07	salsa2012
36.33	36.43	36.46	lexv2
39.30	39.32	39.45	rabbit
44.27	44.30	44.35	salsa20
46.77	47.08	47.16	chacha20
47.06	47.08	47.11	cryptmtv3
57.27	57.29	57.45	tpypy
57.81	57.84	57.84	aes128estream
58.23	58.26	58.28	tpy
83.54	83.57	83.57	aes256estream
141.56	141.59	141.90	dragon

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
10.60	10.60	10.61	`trivium`
22.51	22.51	22.52	`salsa208`
22.63	22.63	22.65	`nlsv2`
22.87	22.87	22.88	`chacha8`
23.09	23.13	23.22	`tpy6`
25.45	25.45	25.46	`snow20`
27.29	27.35	41.53	`sosemanuk`
33.04	33.07	33.07	`tpy`
34.91	34.93	34.98	`lexv2`
35.15	35.18	35.18	`chacha12`
35.29	35.29	35.32	`cryptmtv3`
35.18	35.34	35.47	`salsa2012`
37.29	37.34	48.78	`tpypy`
37.25	37.40	37.49	`rabbit`
44.00	44.08	44.10	`salsa20`
46.81	46.89	46.92	`chacha20`
57.23	57.23	57.24	`aes128estream`
83.05	83.05	83.08	`aes256estream`
138.94	139.03	139.04	`dragon`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
9.98	10.00	10.02	`trivium`
17.89	17.99	18.01	`tpy`
17.89	18.14	18.34	`tpy6`
21.60	21.62	21.66	`nlsv2`
22.11	22.11	22.13	`salsa208`
22.52	22.54	22.56	`chacha8`
16.56	24.67	24.69	`snow20`
25.25	25.37	48.34	`tpypy`
22.54	25.84	54.28	`sosemanuk`
27.85	27.85	27.97	`cryptmtv3`
33.89	34.00	34.12	`lexv2`
34.34	34.77	35.02	`salsa2012`
34.82	34.88	34.90	`chacha12`
35.94	36.25	36.50	`rabbit`
43.75	43.91	44.00	`salsa20`
46.50	46.70	46.91	`chacha20`
56.84	56.86	56.89	`aes128estream`
82.73	82.73	82.81	`aes256estream`
136.99	137.28	137.31	`dragon`

7.23 sparcv9, 300MHz, Sun UltraSPARC IIi, nmi0096



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
74.00	74.25	75.00	chacha8
74.25	75.00	75.50	salsa208
94.25	94.50	95.00	chacha12
95.00	95.25	95.25	salsa2012
134.75	135.25	135.25	chacha20
136.00	136.25	136.25	salsa20
151.50	153.00	154.00	lexv2
160.75	162.75	165.00	aes128estream
180.12	180.50	180.88	trivium
193.75	201.75	204.50	aes256estream
227.50	232.25	234.25	snow20
307.00	307.50	308.25	cryptmtv3
313.12	314.25	315.75	nlsv2
386.50	387.00	387.50	rabbit
408.88	421.50	424.25	dragon
1024.25	1025.62	1026.50	tpy6
1047.75	1048.25	1050.75	sosemanuk
2218.75	2232.50	2252.00	tpy
2243.00	2252.00	2255.12	tpypy

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
7.78	7.81	7.84	salsa208
7.72	7.84	8.00	chacha8
10.31	10.34	10.39	chacha12
10.34	10.34	10.50	salsa2012
15.31	15.41	15.41	chacha20
15.47	15.47	15.50	salsa20
25.78	25.84	26.47	lexv2
30.81	30.89	31.17	trivium
31.06	32.06	32.34	snow20
63.72	63.81	64.09	rabbit
64.41	65.00	65.31	aes128estream
67.47	67.70	68.09	nlsv2
74.38	74.55	74.70	cryptmtv3
76.16	76.56	77.56	aes256estream
83.72	84.97	86.28	dragon
134.62	134.72	134.97	sosemanuk
139.16	139.28	139.69	tpy6
293.31	293.56	293.62	tpy
297.97	298.30	299.16	tpypy

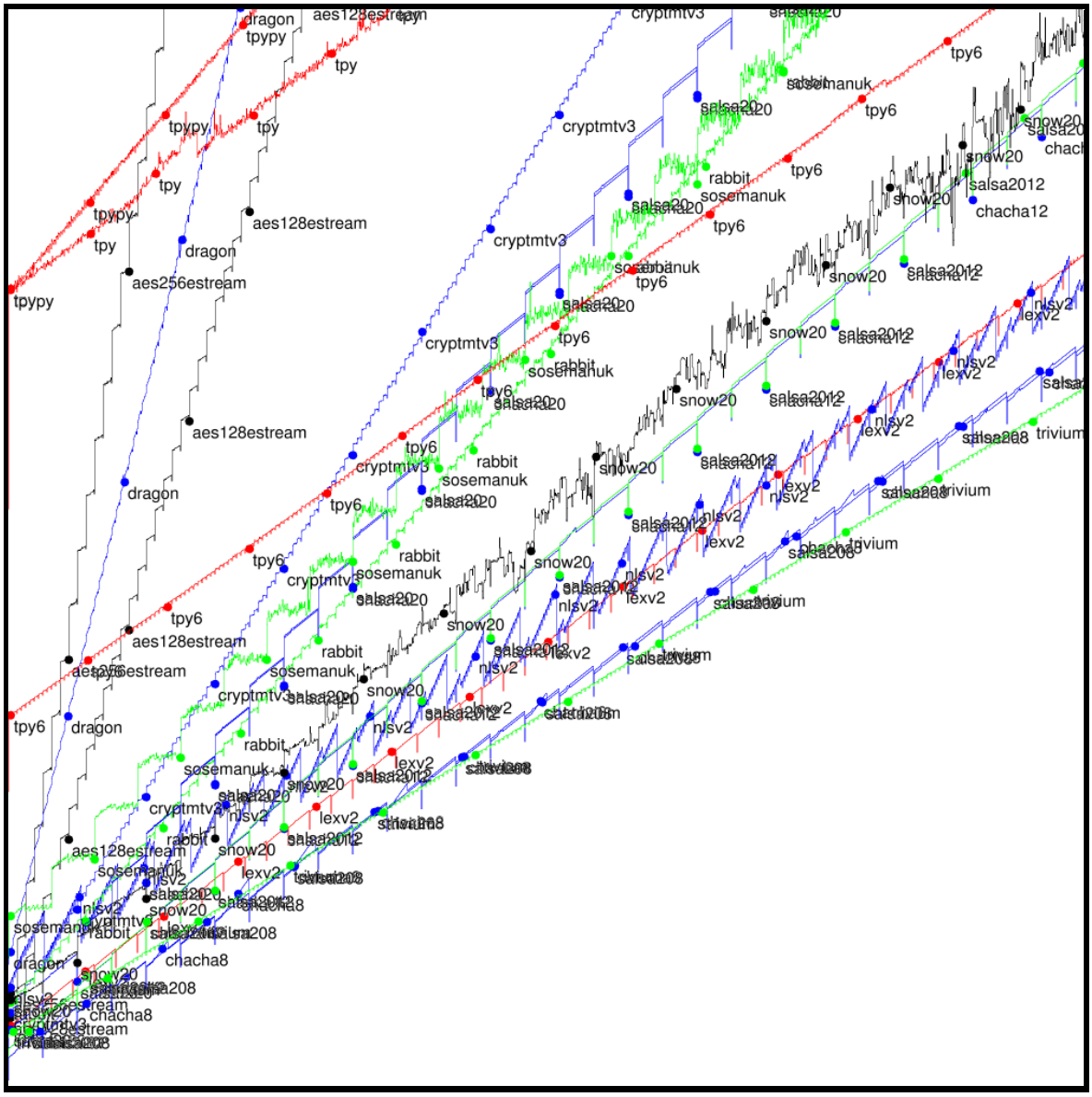
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.60	6.60	6.60	chacha8
6.66	6.66	6.67	salsa208
9.15	9.15	9.16	chacha12
9.22	9.22	9.23	salsa2012
10.47	10.60	10.65	lexv2
12.10	12.11	12.13	trivium
14.13	14.14	14.21	snow20
14.19	14.20	14.20	chacha20
14.35	14.35	14.36	salsa20
14.53	14.55	14.63	nlsv2
24.84	24.85	24.87	tpy6
25.75	25.81	25.90	rabbit
31.40	31.49	31.49	sosemanuk
41.90	41.97	42.01	dragon
42.94	42.97	42.99	tpy
47.32	47.41	47.44	cryptmtv3
48.14	48.20	48.32	tpypy
54.91	55.11	55.84	aes128estream
69.38	69.48	70.63	aes256estream

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
6.50	6.50	6.50	chacha8
6.56	6.56	6.56	salsa208
9.03	9.03	9.03	chacha12
9.25	9.29	9.32	lexv2
10.21	10.21	10.21	salsa2012
10.63	10.64	10.64	trivium
10.99	11.00	11.01	nlsv2
12.72	12.74	12.76	snow20
14.09	14.10	14.10	chacha20
14.25	14.25	14.25	salsa20
16.06	16.07	16.09	tpy6
21.95	22.10	22.12	sosemanuk
22.70	22.71	22.72	tpy
22.83	22.84	22.85	rabbit
28.40	28.51	28.60	tpypy
38.79	38.88	39.06	dragon
42.16	42.21	42.57	cryptmtv3
54.72	54.80	56.07	aes128estream
68.72	69.00	70.11	aes256estream

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
6.46	6.46	6.46	`chacha8`
6.52	6.52	6.52	`salsa208`
8.35	8.39	8.42	`lexv2`
8.99	8.99	9.00	`chacha12`
9.56	9.57	9.59	`nlsv2`
10.08	10.08	10.08	`trivium`
10.19	10.20	10.20	`salsa2012`
12.19	12.22	12.22	`snow20`
12.72	12.72	12.73	`tpy6`
14.06	14.06	14.06	`chacha20`
14.21	14.21	14.21	`salsa20`
15.17	15.17	15.18	`tpy`
18.78	18.92	18.99	`sosemanuk`
21.13	21.24	21.27	`tpypy`
21.58	21.61	21.82	`rabbit`
32.84	32.84	32.87	`cryptmtv3`
37.54	37.60	37.68	`dragon`
55.69	55.81	56.88	`aes128estream`
67.51	67.81	70.26	`aes256estream`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
6.43	6.44	6.44	`chacha8`
6.50	6.50	6.50	`salsa208`
7.52	7.61	7.67	`lexv2`
8.96	8.97	8.98	`chacha12`
8.98	9.00	9.06	`nlsv2`
9.29	9.30	9.32	`salsa2012`
9.74	9.75	9.75	`trivium`
10.52	10.55	10.57	`tpy`
10.54	10.56	10.58	`tpy6`
11.83	11.89	11.94	`snow20`
14.03	14.03	14.04	`chacha20`
14.19	14.19	14.19	`salsa20`
16.66	16.92	17.00	`tpypy`
16.90	17.33	17.63	`sosemanuk`
20.78	20.90	21.50	`rabbit`
26.62	26.92	27.11	`cryptmtv3`
36.35	36.63	37.07	`dragon`
54.79	55.79	57.97	`aes128estream`
65.29	65.98	71.81	`aes256estream`

7.24 sparcv9, 900MHz, Sun UltraSPARC III, `nmi0051`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
73.00	73.00	73.38	chacha8
73.38	73.38	73.38	salsa208
93.50	93.50	93.50	chacha12
93.88	93.88	93.88	salsa2012
117.50	118.38	120.00	trivium
134.50	134.50	134.50	chacha20
134.88	134.88	134.88	salsa20
142.50	142.50	142.50	lexv2
157.50	161.00	161.00	aes128estream
170.12	172.12	172.75	cryptmtv3
194.88	195.38	198.50	rabbit
200.75	206.38	211.12	snow20
216.12	216.12	216.88	aes256estream
237.38	238.88	239.88	nlsv2
324.88	325.88	328.00	dragon
394.88	397.75	403.38	sosemanuk
855.88	857.50	859.62	tpy6
1828.75	1842.88	1865.50	tpy
1840.50	1848.50	1858.12	tpypy

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
8.16	8.16	8.25	chacha8
8.20	8.20	8.22	salsa208
10.72	10.72	10.72	chacha12
10.77	10.77	10.77	salsa2012
15.84	15.84	15.84	chacha20
15.89	15.89	15.89	salsa20
19.88	19.91	19.95	trivium
24.45	24.45	24.45	lexv2
26.58	26.89	27.23	snow20
32.61	32.72	32.86	rabbit
34.42	34.61	34.72	cryptmtv3
45.36	45.48	45.48	aes128estream
47.44	47.58	47.69	nlsv2
50.80	50.97	52.41	sosemanuk
75.22	75.30	76.31	aes256estream
76.88	76.95	77.69	dragon
113.19	113.36	113.36	tpy6
236.45	237.22	260.92	tpy
239.77	240.73	241.41	tpypy

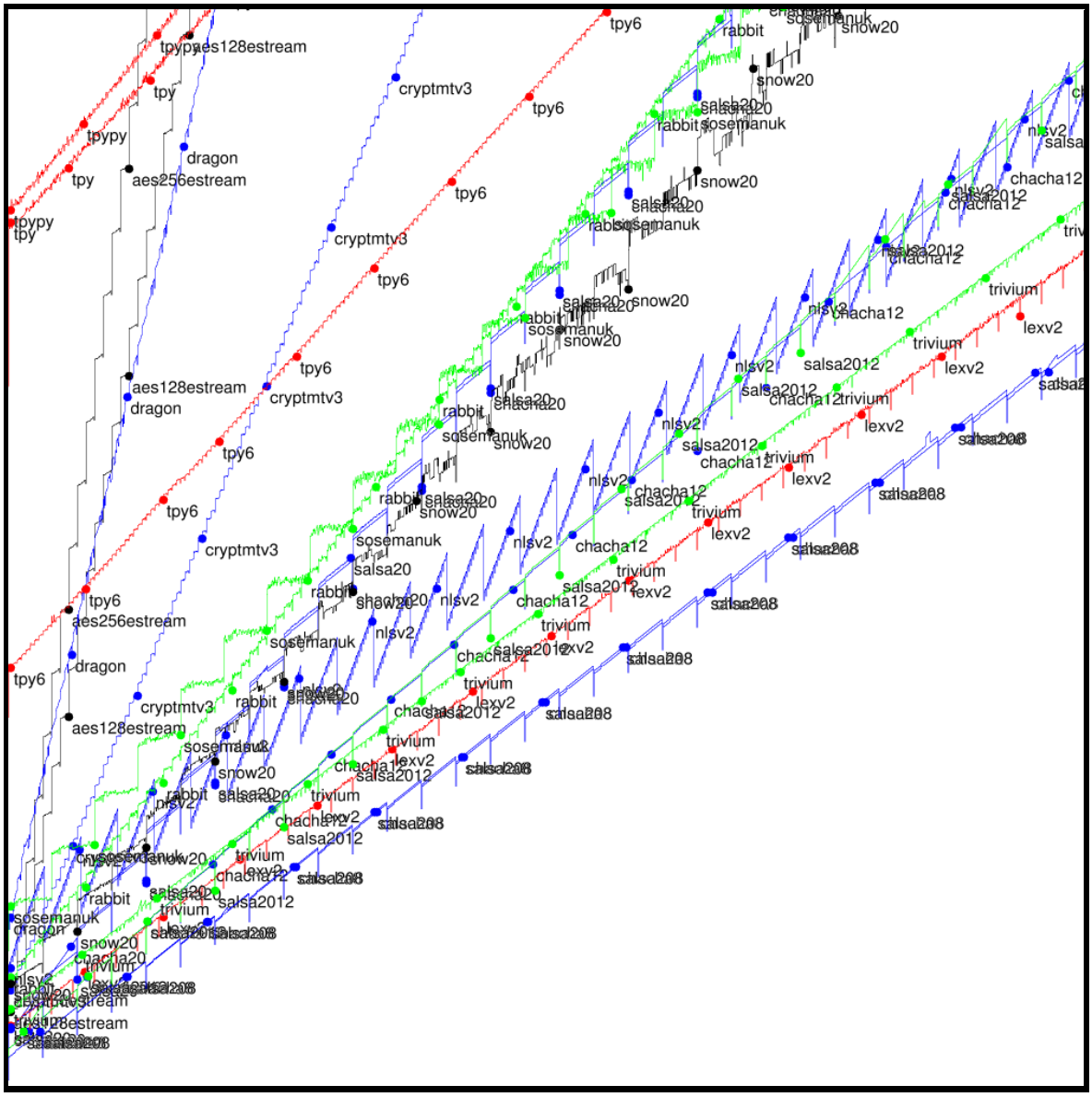
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.74	6.74	6.74	chacha8
6.79	6.79	6.79	salsa208
7.54	7.55	7.58	trivium
9.07	9.07	9.07	lexv2
9.31	9.31	9.31	chacha12
9.35	9.35	9.35	salsa2012
9.99	10.00	10.02	nlsv2
10.58	10.81	11.43	snow20
14.36	14.36	14.43	rabbit
14.44	14.44	14.44	chacha20
14.49	14.49	14.49	salsa20
16.77	16.98	17.19	sosemanuk
18.46	18.50	18.53	cryptmtv3
18.88	18.90	18.95	tpy6
32.85	32.96	33.09	tpy
35.87	35.89	35.89	aes128estream
36.86	36.99	37.10	tpypy
45.32	45.32	45.33	dragon
65.52	65.52	65.64	aes256estream

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
6.59	6.59	6.60	trivium
6.62	6.62	6.62	chacha8
6.67	6.67	6.67	salsa208
7.69	7.70	7.72	nlsv2
7.86	7.86	7.87	lexv2
9.18	9.18	9.19	chacha12
9.23	9.23	9.23	salsa2012
9.60	9.75	9.80	snow20
11.63	11.65	11.66	tpy6
13.00	13.08	13.09	rabbit
13.49	13.65	13.77	sosemanuk
14.31	14.31	14.32	chacha20
14.36	14.36	14.36	salsa20
16.66	16.68	16.71	cryptmtv3
16.93	16.97	17.15	tpy
21.03	21.07	21.11	tpypy
35.13	35.14	35.14	aes128estream
42.77	42.80	42.81	dragon
64.82	64.84	64.92	aes256estream

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
6.23	6.23	6.24	`trivium`
6.62	6.62	6.63	`chacha8`
6.67	6.67	6.67	`salsa208`
6.93	6.93	6.94	`nlsv2`
7.43	7.44	7.46	`lexv2`
8.82	8.83	8.84	`tpy6`
9.18	9.19	9.19	`chacha12`
9.18	9.21	9.96	`snow20`
9.23	9.23	9.24	`salsa2012`
10.99	11.00	11.01	`tpy`
12.06	12.36	12.47	`sosemanuk`
12.47	12.51	12.54	`rabbit`
14.31	14.31	14.31	`chacha20`
14.36	14.36	14.36	`salsa20`
14.46	14.47	14.49	`cryptmtv3`
15.13	15.14	15.15	`tpypy`
34.86	34.86	34.86	`aes128estream`
41.30	41.33	41.34	`dragon`
64.52	64.53	64.55	`aes256estream`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
6.00	6.01	6.03	`trivium`
6.62	6.63	6.64	`chacha8`
6.61	6.63	6.66	`nlsv2`
6.68	6.69	6.69	`salsa208`
7.12	7.15	7.18	`tpy6`
7.14	7.19	7.22	`lexv2`
7.35	7.41	7.47	`tpy`
8.32	8.72	10.48	`snow20`
9.19	9.20	9.20	`chacha12`
9.24	9.25	9.25	`salsa2012`
11.50	11.59	11.63	`tpypy`
10.81	11.71	12.07	`sosemanuk`
12.09	12.22	12.29	`rabbit`
13.07	13.10	13.15	`cryptmtv3`
14.31	14.32	14.33	`chacha20`
14.36	14.36	14.37	`salsa20`
34.68	34.69	34.69	`aes128estream`
40.30	40.39	40.46	`dragon`
64.32	64.37	64.41	`aes256estream`

7.25 sparcv9, 1200MHz, Sun UltraSPARC III, `nmisolaris10`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
73.00	73.00	74.00	chacha8
73.38	73.38	73.38	salsa208
93.50	93.50	94.50	chacha12
93.88	93.88	93.88	salsa2012
134.50	134.50	135.50	chacha20
139.62	139.62	141.25	salsa20
141.88	143.38	143.38	lexv2
176.25	176.25	176.88	aes128estream
176.88	177.38	178.00	trivium
224.88	225.00	225.00	cryptmtv3
226.75	226.75	227.50	aes256estream
238.00	241.12	242.75	snow20
254.12	257.38	259.12	rabbit
287.50	288.12	288.25	nlsv2
382.00	382.00	406.00	dragon
416.25	417.00	433.50	sosemanuk
967.25	971.12	973.25	tpy6
1983.25	1997.50	2020.00	tpy
2021.25	2035.00	2068.75	tpypy

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
8.16	8.16	8.16	chacha8
8.20	8.20	8.22	salsa208
10.72	10.72	10.72	chacha12
10.77	10.77	10.77	salsa2012
15.84	15.84	15.84	chacha20
16.48	16.48	16.48	salsa20
24.33	24.33	24.73	lexv2
28.88	28.95	29.09	trivium
32.77	32.80	32.94	snow20
40.00	40.50	40.66	rabbit
47.62	47.73	47.81	cryptmtv3
53.86	53.98	55.31	sosemanuk
60.06	60.14	61.56	nlsv2
64.58	64.72	64.78	aes128estream
83.39	83.42	83.42	aes256estream
86.88	89.88	89.88	dragon
130.53	130.81	132.19	tpy6
257.62	258.81	259.62	tpy
262.62	264.00	265.53	tpypy

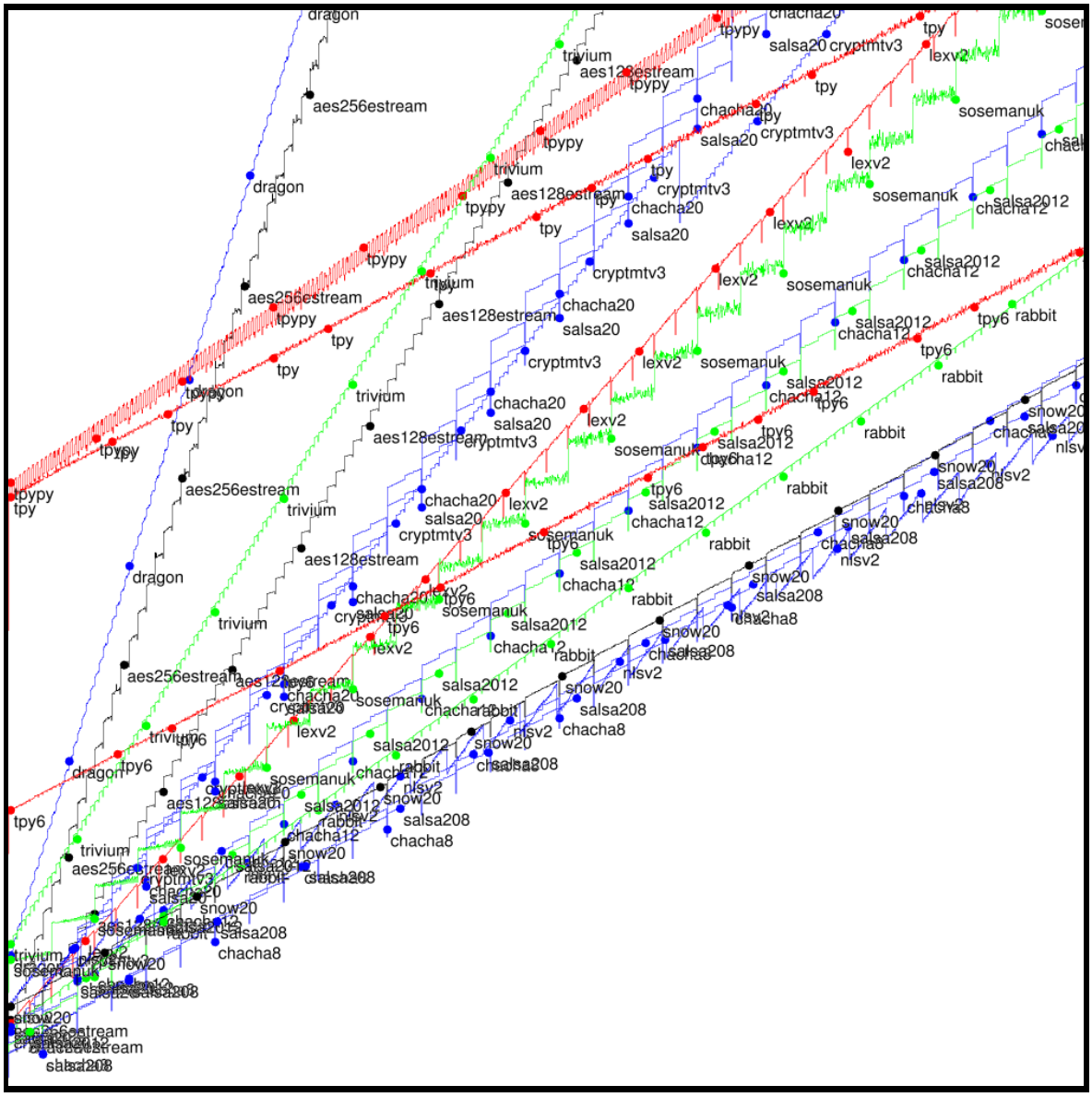
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.74	6.74	6.74	chacha8
6.79	6.79	6.79	salsa208
9.05	9.13	9.13	lexv2
9.31	9.31	9.31	chacha12
9.35	9.35	9.35	salsa2012
9.73	9.88	9.89	trivium
12.55	12.56	12.72	nlsv2
14.19	14.38	14.75	snow20
14.44	14.44	14.44	chacha20
14.55	14.55	14.58	salsa20
16.53	16.56	16.58	rabbit
17.73	17.77	17.93	sosemanuk
24.27	24.29	24.33	tpy6
26.50	26.53	26.56	cryptmtv3
38.34	38.55	38.60	tpy
40.00	40.17	40.28	tpypy
49.21	49.21	49.54	dragon
56.77	57.45	57.52	aes128estream
74.26	74.27	74.39	aes256estream

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
6.63	6.64	6.65	chacha8
6.68	6.68	6.69	salsa208
7.89	7.90	7.91	lexv2
8.34	8.34	8.39	trivium
9.20	9.20	9.20	chacha12
9.24	9.25	9.25	salsa2012
9.65	9.66	9.71	nlsv2
12.54	12.55	13.30	snow20
14.33	14.33	14.33	chacha20
14.19	14.35	14.44	sosemanuk
14.39	14.39	14.39	salsa20
14.64	14.74	14.77	rabbit
16.03	16.04	16.07	tpy6
21.27	21.32	21.36	tpy
22.57	22.65	22.70	tpypy
23.51	23.53	23.57	cryptmtv3
46.32	46.41	46.43	dragon
56.95	56.97	56.99	aes128estream
73.57	73.58	73.59	aes256estream

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
6.58	6.62	6.63	`chacha8`
6.67	6.67	6.67	`salsa208`
7.43	7.44	7.46	`lexv2`
7.81	7.82	7.83	`trivium`
8.52	8.53	8.97	`nlsv2`
9.19	9.19	9.19	`chacha12`
9.23	9.23	9.23	`salsa2012`
11.83	12.02	12.38	`snow20`
12.89	12.89	12.90	`tpy6`
13.30	13.31	13.33	`sosemanuk`
13.97	13.98	13.99	`rabbit`
14.31	14.31	14.32	`chacha20`
14.37	14.37	14.37	`salsa20`
14.88	14.93	14.94	`tpy`
16.05	16.08	16.12	`tpypy`
18.60	18.63	18.65	`cryptmtv3`
45.23	45.26	45.27	`dragon`
56.74	56.78	56.80	`aes128estream`
73.31	73.33	73.33	`aes256estream`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
6.52	6.62	6.63	`chacha8`
6.66	6.67	6.67	`salsa208`
7.11	7.14	7.19	`lexv2`
7.47	7.50	7.52	`trivium`
8.06	8.12	9.00	`nlsv2`
9.18	9.18	9.19	`chacha12`
9.22	9.23	9.23	`salsa2012`
10.97	11.00	11.04	`tpy6`
10.96	11.12	11.18	`tpy`
10.58	11.15	12.06	`snow20`
12.01	12.12	12.26	`tpypy`
12.99	13.04	13.11	`sosemanuk`
13.51	13.53	13.57	`rabbit`
14.30	14.31	14.32	`chacha20`
14.36	14.37	14.38	`salsa20`
15.52	15.59	15.65	`cryptmtv3`
44.48	44.55	44.67	`dragon`
56.56	56.66	56.71	`aes128estream`
73.03	73.17	73.20	`aes256estream`

7.26 x86, 1196MHz, Intel Celeron (6b1), `vieux`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
79.25	79.25	79.25	salsa208
80.62	80.62	81.00	chacha8
81.62	81.62	81.62	aes128estream
99.12	99.12	99.12	salsa2012
102.38	102.38	102.38	chacha12
127.38	127.38	127.38	cryptmtv3
139.12	139.12	139.12	salsa20
142.00	142.00	142.00	rabbit
143.50	143.50	143.50	chacha20
152.12	152.75	152.75	lexv2
158.62	158.62	158.75	aes256estream
186.62	187.38	187.50	snow20
191.88	192.00	192.00	nlsv2
292.00	292.50	294.38	sosemanuk
314.38	314.62	317.25	dragon
328.00	328.00	328.00	trivium
639.00	639.00	640.88	tpy6
1369.50	1369.75	1372.12	tpypy
1366.62	1372.00	1372.62	tpy
4417.75	4424.62	4427.12	hc128
11667.20	11667.20	11668.80	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
9.12	9.12	9.12	salsa208
9.30	9.30	9.34	chacha8
11.61	11.61	11.61	salsa2012
12.00	12.00	12.00	chacha12
16.59	16.59	16.59	salsa20
17.22	17.22	17.22	chacha20
22.16	22.16	22.16	rabbit
22.95	23.23	23.27	snow20
23.23	23.23	23.23	aes128estream
26.64	26.64	26.64	cryptmtv3
28.75	28.75	28.89	lexv2
35.86	35.86	35.86	nlsv2
37.27	37.42	37.59	sosemanuk
42.58	42.64	42.66	aes256estream
54.92	54.92	54.92	trivium
67.58	67.81	68.02	dragon
84.50	84.66	84.66	tpy6
175.62	176.06	176.22	tpy
175.55	177.09	177.12	tpypy
552.94	552.95	553.16	hc128
1455.34	1455.89	1456.09	hc256

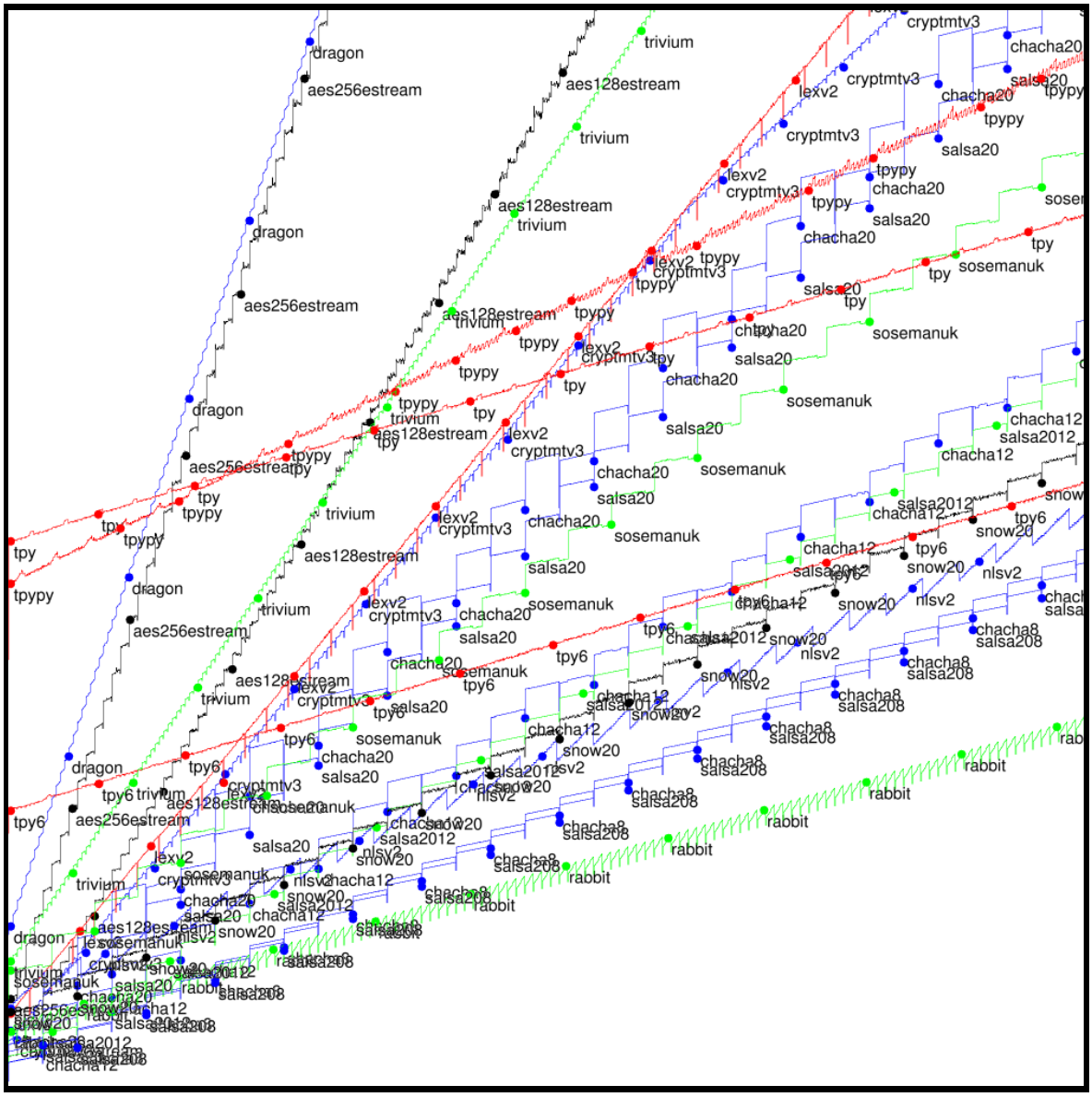
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.64	6.64	6.64	salsa208
6.79	6.79	6.79	chacha8
7.89	7.94	7.95	snow20
8.35	8.37	8.37	nlsv2
8.89	8.89	8.89	rabbit
9.12	9.12	9.12	salsa2012
9.46	9.46	9.46	chacha12
12.66	12.68	12.71	sosemanuk
12.69	12.70	12.73	lexv2
14.02	14.04	14.04	tpy6
14.09	14.09	14.09	salsa20
14.54	14.54	14.54	chacha20
14.82	14.82	14.82	cryptmtv3
18.34	18.34	18.34	aes128estream
20.79	20.79	20.79	trivium
24.25	24.31	24.38	tpy
25.40	25.56	25.62	tpypy
32.79	32.82	32.93	aes256estream
36.28	36.33	36.37	dragon
65.12	65.12	65.15	hc128
167.17	167.26	167.34	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
6.42	6.42	6.42	salsa208
6.48	6.48	6.48	nlsv2
6.60	6.60	6.60	chacha8
6.71	6.71	6.72	snow20
7.83	7.83	7.83	rabbit
8.56	8.59	8.59	tpy6
8.91	8.91	8.91	salsa2012
9.24	9.24	9.24	chacha12
10.88	10.96	10.96	sosemanuk
11.40	11.42	11.44	lexv2
12.34	12.38	12.41	tpy
12.86	12.86	12.86	cryptmtv3
13.67	13.67	13.76	tpypy
13.88	13.88	13.88	salsa20
14.31	14.31	14.31	chacha20
17.92	17.92	17.92	aes128estream
18.11	18.11	18.11	trivium
27.00	27.00	27.01	hc128
32.03	32.06	32.12	aes256estream
33.98	33.99	33.99	dragon
66.52	66.52	66.62	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.70	5.70	5.70	`nlsv2`
6.27	6.27	6.28	`snow20`
6.34	6.34	6.34	`salsa208`
6.51	6.51	6.51	`chacha8`
6.50	6.51	6.52	`tpy6`
7.44	7.44	7.44	`rabbit`
7.94	7.96	7.99	`tpy`
8.84	8.84	8.84	`salsa2012`
9.16	9.16	9.16	`chacha12`
9.29	9.29	9.31	`tpypy`
10.46	10.48	10.55	`sosemanuk`
11.00	11.01	11.03	`lexv2`
12.29	12.29	12.29	`cryptmtv3`
12.79	12.81	12.81	`hc128`
13.80	13.80	13.80	`salsa20`
14.22	14.22	14.22	`chacha20`
17.10	17.10	17.10	`trivium`
17.64	17.65	17.65	`aes128estream`
28.84	28.86	28.88	`hc256`
31.77	31.77	31.78	`aes256estream`
33.01	33.02	33.02	`dragon`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
4.28	4.31	4.34	`hc128`
5.26	5.31	5.38	`tpy`
5.28	5.31	5.35	`tpy6`
5.33	5.33	5.33	`nlsv2`
5.99	6.00	6.01	`snow20`
6.30	6.30	6.30	`salsa208`
6.19	6.30	6.34	`hc256`
6.45	6.45	6.45	`chacha8`
6.62	6.64	6.69	`tpypy`
7.21	7.21	7.21	`rabbit`
8.79	8.79	8.79	`salsa2012`
9.11	9.11	9.11	`chacha12`
10.31	10.44	10.60	`sosemanuk`
10.72	10.76	10.82	`lexv2`
12.03	12.03	12.03	`cryptmtv3`
13.75	13.75	13.75	`salsa20`
14.17	14.17	14.17	`chacha20`
16.50	16.50	16.50	`trivium`
17.48	17.48	17.48	`aes128estream`
31.53	31.57	31.62	`aes256estream`
32.39	32.42	32.44	`dragon`

7.27 x86, 1403MHz, AMD Opteron 240 (f58), nmisles8amd64



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
56.38	56.38	56.38	salsa208
57.25	57.25	57.25	chacha8
70.38	70.62	71.38	aes128estream
71.00	71.00	71.00	salsa2012
81.38	81.50	81.50	chacha12
98.75	98.75	98.75	salsa20
104.88	110.25	110.50	cryptmtv3
128.75	128.88	129.00	chacha20
130.38	131.50	131.62	rabbit
169.12	169.88	171.38	snow20
174.88	175.75	176.38	lexv2
185.62	187.25	189.00	nlsv2
206.00	206.50	208.00	aes256estream
268.88	269.12	271.12	sosemanuk
286.62	286.62	287.62	trivium
378.88	379.25	379.38	dragon
637.00	641.38	642.62	tpy6
1165.88	1168.75	1170.50	tpypy
1259.50	1263.38	1263.50	tpy
3114.12	3120.38	3122.12	hc128
7315.38	7316.00	7318.38	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
6.42	6.42	6.42	salsa208
6.59	6.59	6.59	chacha8
8.25	8.25	8.25	salsa2012
9.23	9.25	9.25	chacha12
11.78	11.78	11.78	salsa20
15.22	15.25	15.28	chacha20
15.39	15.44	15.44	rabbit
20.50	20.64	21.17	snow20
22.33	22.36	22.38	aes128estream
22.97	23.03	23.19	cryptmtv3
31.89	32.09	32.23	nlsv2
32.11	32.20	32.52	lexv2
34.42	34.53	34.73	sosemanuk
48.77	48.77	48.89	trivium
48.69	48.92	48.97	aes256estream
73.44	73.56	73.64	dragon
82.83	82.83	82.91	tpy6
149.61	150.42	151.14	tpypy
160.58	160.62	160.66	tpy
390.61	390.77	391.11	hc128
915.11	915.25	915.33	hc256

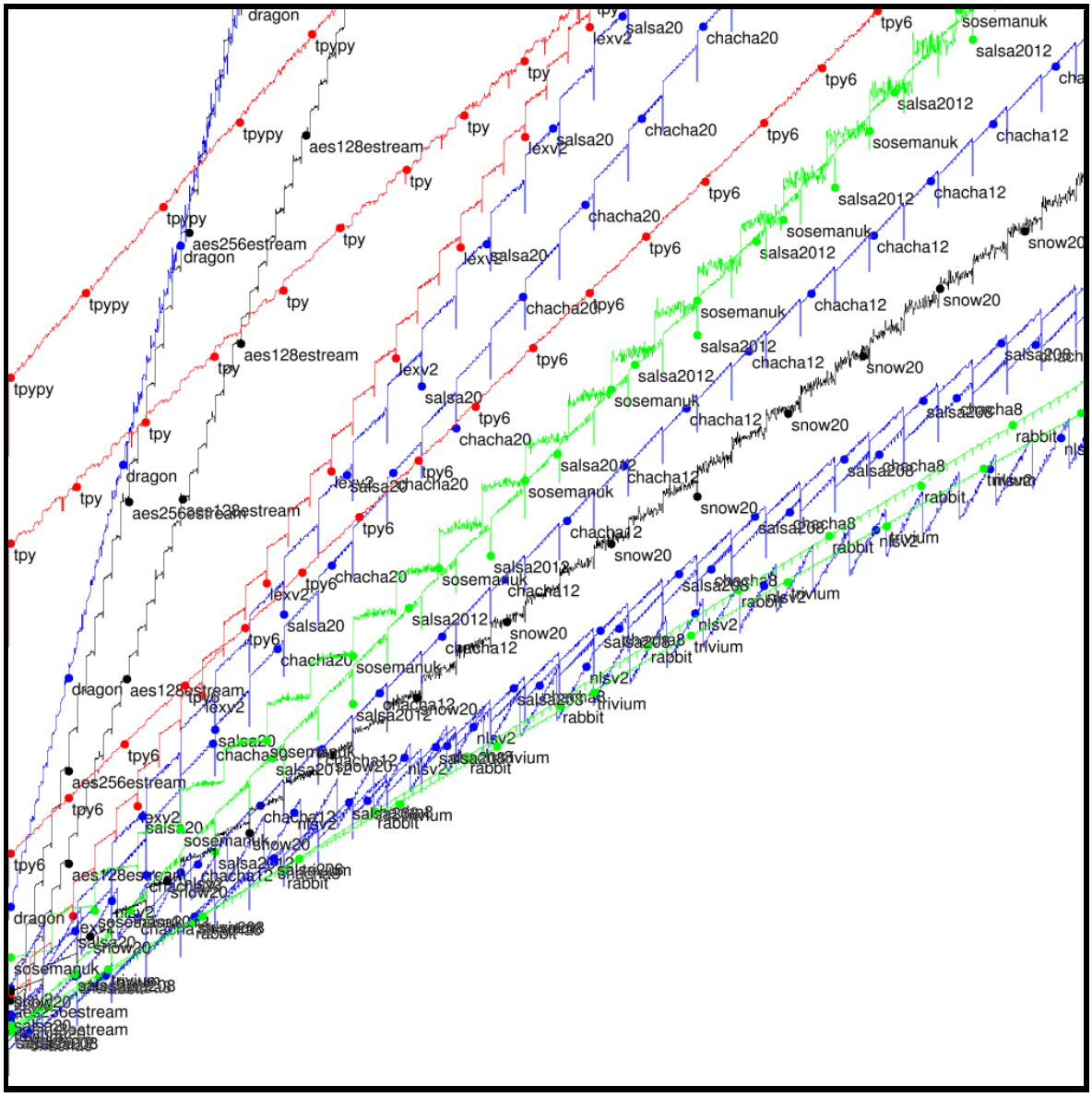
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
4.30	4.30	4.30	rabbit
4.88	4.88	4.88	salsa208
5.00	5.00	5.00	chacha8
6.70	6.70	6.70	salsa2012
7.00	7.01	7.02	chacha12
7.05	7.09	7.11	snow20
7.20	7.21	7.22	nlsv2
10.34	10.34	10.34	salsa20
10.98	10.99	10.99	chacha20
11.43	11.44	11.47	sosemanuk
11.91	11.91	11.94	tpy6
13.46	13.46	13.48	cryptmtv3
14.19	14.22	14.23	lexv2
18.35	18.39	18.64	aes128estream
18.61	18.61	18.63	trivium
20.55	20.57	20.58	tpy
21.21	21.21	21.22	tpypy
33.37	33.37	33.43	aes256estream
34.53	34.55	34.55	dragon
46.04	46.05	46.09	hc128
105.14	105.17	105.19	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
3.39	3.39	3.39	rabbit
4.74	4.74	4.74	salsa208
4.86	4.86	4.86	chacha8
5.56	5.56	5.57	nlsv2
5.96	5.96	5.97	snow20
6.36	6.37	6.38	tpy6
6.57	6.57	6.57	salsa2012
6.74	6.76	6.76	chacha12
9.19	9.20	9.21	sosemanuk
9.60	9.60	9.61	tpy
10.20	10.20	10.20	salsa20
10.43	10.43	10.43	chacha20
11.01	11.01	11.05	tpypy
12.19	12.23	12.23	cryptmtv3
12.73	12.76	12.77	lexv2
16.24	16.24	16.24	trivium
18.07	18.11	18.16	aes128estream
19.15	19.17	19.17	hc128
31.47	31.47	31.48	dragon
32.10	32.11	32.18	aes256estream
41.93	41.94	41.96	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
3.05	3.05	3.05	`rabbit`
4.42	4.42	4.43	`tpy6`
4.69	4.69	4.69	`salsa208`
4.82	4.82	4.82	`chacha8`
4.88	4.88	4.88	`nlsv2`
5.55	5.55	5.56	`snow20`
5.61	5.62	5.63	`tpy`
6.52	6.52	6.52	`salsa2012`
6.71	6.71	6.71	`chacha12`
7.33	7.33	7.35	`tpypy`
8.36	8.36	8.37	`sosemanuk`
9.03	9.04	9.05	`hc128`
10.15	10.15	10.15	`salsa20`
10.36	10.36	10.36	`chacha20`
11.84	11.84	11.84	`cryptmtv3`
12.20	12.21	12.22	`lexv2`
15.35	15.35	15.35	`trivium`
17.90	17.93	18.11	`aes128estream`
18.21	18.21	18.22	`hc256`
30.35	30.35	30.36	`dragon`
31.67	31.68	31.70	`aes256estream`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
2.84	2.84	2.84	`rabbit`
2.96	2.98	3.03	`hc128`
3.26	3.28	3.30	`tpy`
3.29	3.31	3.32	`tpy6`
3.94	3.97	3.98	`hc256`
4.53	4.53	4.54	`nlsv2`
4.66	4.66	4.66	`salsa208`
4.79	4.79	4.79	`chacha8`
5.16	5.17	5.21	`tpypy`
5.29	5.31	5.32	`snow20`
6.49	6.49	6.49	`salsa2012`
6.69	6.69	6.69	`chacha12`
7.96	7.97	7.98	`sosemanuk`
10.12	10.12	10.12	`salsa20`
10.32	10.32	10.32	`chacha20`
11.85	11.88	11.89	`lexv2`
12.16	12.17	12.17	`cryptmtv3`
14.81	14.81	14.82	`trivium`
17.78	17.85	18.22	`aes128estream`
29.65	29.68	29.69	`dragon`
31.35	31.36	31.49	`aes256estream`

7.28 x86, 1833MHz, Intel Core Duo, `nmi0068`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
92.12	92.12	93.50	salsa208
93.50	93.50	93.50	chacha8
114.12	114.12	115.50	chacha12
125.12	126.50	126.50	salsa2012
126.50	126.50	126.50	rabbit
137.50	137.50	138.88	trivium
151.25	151.25	152.62	chacha20
158.12	159.50	159.50	aes128estream
167.75	167.75	169.12	salsa20
199.38	199.38	200.75	aes256estream
218.62	218.62	224.12	lexv2
220.00	220.00	221.38	snow20
236.50	236.50	237.88	nlsv2
298.38	298.38	299.75	sosemanuk
422.12	423.50	424.88	dragon
539.00	539.00	540.38	tpy6
1255.38	1256.75	1258.12	tpy
1645.88	1645.88	1645.88	tpypy
4233.62	4246.00	4246.00	hc128
12100.00	12101.40	12109.60	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
10.31	10.31	10.31	chacha8
10.31	10.31	10.31	salsa208
12.89	12.89	12.89	chacha12
14.09	14.27	14.27	salsa2012
17.88	17.88	18.05	chacha20
19.59	19.59	19.77	rabbit
19.94	19.94	20.11	salsa20
22.17	22.17	22.34	trivium
28.02	28.02	28.02	snow20
39.02	39.19	39.19	sosemanuk
39.70	40.05	40.22	lexv2
41.77	41.94	41.94	aes128estream
45.38	45.55	45.55	nlsv2
57.92	58.09	58.27	aes256estream
76.14	76.48	76.48	tpy6
87.66	87.66	87.66	dragon
166.20	166.38	166.38	tpy
216.05	216.05	216.22	tpypy
529.89	530.06	530.75	hc128
1513.19	1514.05	1514.91	hc256

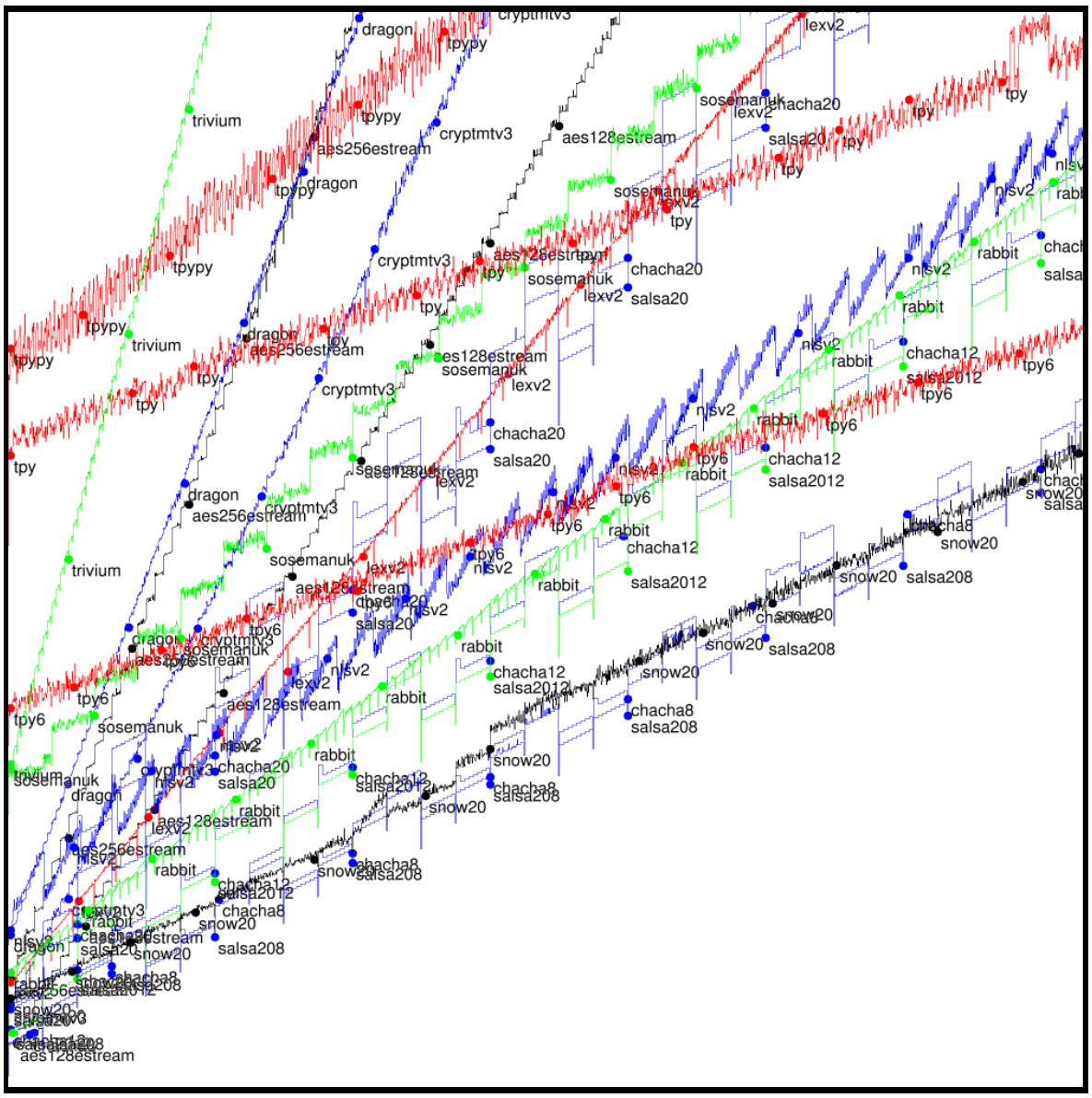
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
7.18	7.20	7.20	chacha8
7.39	7.39	7.41	salsa208
7.54	7.56	7.56	rabbit
7.60	7.60	7.60	trivium
8.71	8.71	8.73	nlsv2
9.72	9.72	9.72	chacha12
9.74	9.82	9.97	snow20
11.13	11.13	11.13	salsa2012
13.67	13.71	13.81	sosemanuk
14.78	14.78	14.80	chacha20
17.03	17.03	17.05	salsa20
17.07	17.09	17.11	tpy6
19.86	19.94	19.96	lexv2
26.97	26.98	26.98	tpy
31.47	31.47	31.72	aes128estream
34.07	34.11	34.16	tpypy
44.29	44.71	44.78	dragon
46.10	46.10	46.12	aes256estream
62.18	62.28	62.37	hc128
173.06	173.21	173.34	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
6.37	6.37	6.38	nlsv2
6.41	6.41	6.41	trivium
6.62	6.62	6.62	rabbit
6.94	6.94	6.95	chacha8
7.18	7.19	7.19	salsa208
8.42	8.48	8.55	snow20
9.45	9.45	9.46	chacha12
10.86	10.86	10.87	salsa2012
11.42	11.52	11.63	sosemanuk
12.49	12.49	12.50	tpy6
14.54	14.54	14.54	chacha20
16.18	16.19	16.22	tpy
16.78	16.78	16.79	salsa20
18.20	18.23	18.23	lexv2
19.81	19.87	19.91	tpypy
25.61	25.63	25.68	hc128
30.64	30.67	30.69	aes128estream
40.67	41.39	41.39	dragon
45.15	45.16	45.29	aes256estream
68.25	68.27	68.33	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.40	5.40	5.45	`nlsv2`
5.96	5.96	5.96	`trivium`
6.27	6.27	6.28	`rabbit`
6.87	6.87	6.87	`chacha8`
7.13	7.13	7.14	`salsa208`
7.96	7.99	8.01	`snow20`
9.38	9.39	9.39	`chacha12`
10.75	10.76	10.76	`tpy6`
10.81	10.81	10.81	`salsa2012`
10.84	10.92	10.98	`sosemanuk`
11.92	11.93	11.95	`hc128`
11.96	11.97	11.99	`tpy`
14.47	14.47	14.47	`chacha20`
14.52	14.52	14.54	`tpypy`
16.72	16.72	16.72	`salsa20`
17.61	17.64	17.66	`lexv2`
29.09	29.10	29.10	`hc256`
30.37	30.38	30.39	`aes128estream`
39.54	39.64	40.43	`dragon`
44.84	44.85	44.85	`aes256estream`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
3.70	3.72	3.79	`hc128`
4.98	4.98	5.12	`nlsv2`
5.53	5.54	5.61	`hc256`
5.70	5.70	5.70	`trivium`
6.06	6.06	6.10	`rabbit`
6.83	6.83	6.84	`chacha8`
7.10	7.10	7.12	`salsa208`
7.71	7.77	7.81	`snow20`
9.35	9.36	9.36	`chacha12`
9.39	9.43	9.47	`tpy`
9.70	9.72	9.74	`tpy6`
10.57	10.75	10.89	`sosemanuk`
10.79	10.79	10.79	`salsa2012`
11.28	11.32	11.41	`tpypy`
14.44	14.44	14.44	`chacha20`
16.67	16.67	16.67	`salsa20`
17.18	17.25	17.29	`lexv2`
30.19	30.23	30.27	`aes128estream`
38.17	38.52	40.16	`dragon`
44.58	44.62	44.68	`aes256estream`

7.29 x86, 2400MHz, Intel Pentium 4 (f24), nmitest4



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
100.00	100.00	100.00	salsa208
101.00	101.00	104.50	aes128estream
102.00	102.50	103.00	chacha8
126.00	126.00	126.00	salsa2012
132.50	133.00	135.50	chacha12
180.00	180.00	182.00	salsa20
186.00	189.50	193.00	cryptmtv3
190.50	190.50	190.50	chacha20
202.50	205.50	209.00	snow20
243.50	243.50	249.50	aes256estream
245.00	245.50	247.50	lexv2
269.50	275.50	283.50	rabbit
358.50	359.00	360.50	dragon
382.00	386.00	401.50	nlsv2
711.00	718.50	738.00	sosemanuk
741.00	742.50	744.50	trivium
870.50	896.50	904.00	tpy6
1483.50	1489.50	1494.00	tpy
1648.00	1674.00	1685.50	tpypy
5961.00	5994.00	6002.00	hc128
11389.50	11417.00	11433.50	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
11.12	11.31	13.12	salsa208
13.31	13.31	13.38	chacha8
14.38	14.94	17.44	salsa2012
18.06	18.06	18.06	chacha12
20.94	20.94	25.81	salsa20
25.06	25.12	25.12	aes128estream
25.31	25.69	25.88	snow20
22.44	27.31	27.56	chacha20
36.19	36.50	36.56	rabbit
39.25	39.69	40.06	cryptmtv3
40.62	40.88	41.69	lexv2
51.62	51.62	51.62	aes256estream
66.88	68.19	71.88	nlsv2
68.31	68.44	68.56	dragon
92.38	92.94	93.50	sosemanuk
111.19	112.25	114.12	tpy6
124.75	125.38	125.56	trivium
184.62	188.88	189.75	tpy
208.44	212.19	218.69	tpypy
743.88	745.69	747.50	hc128
1415.69	1423.56	1449.81	hc256

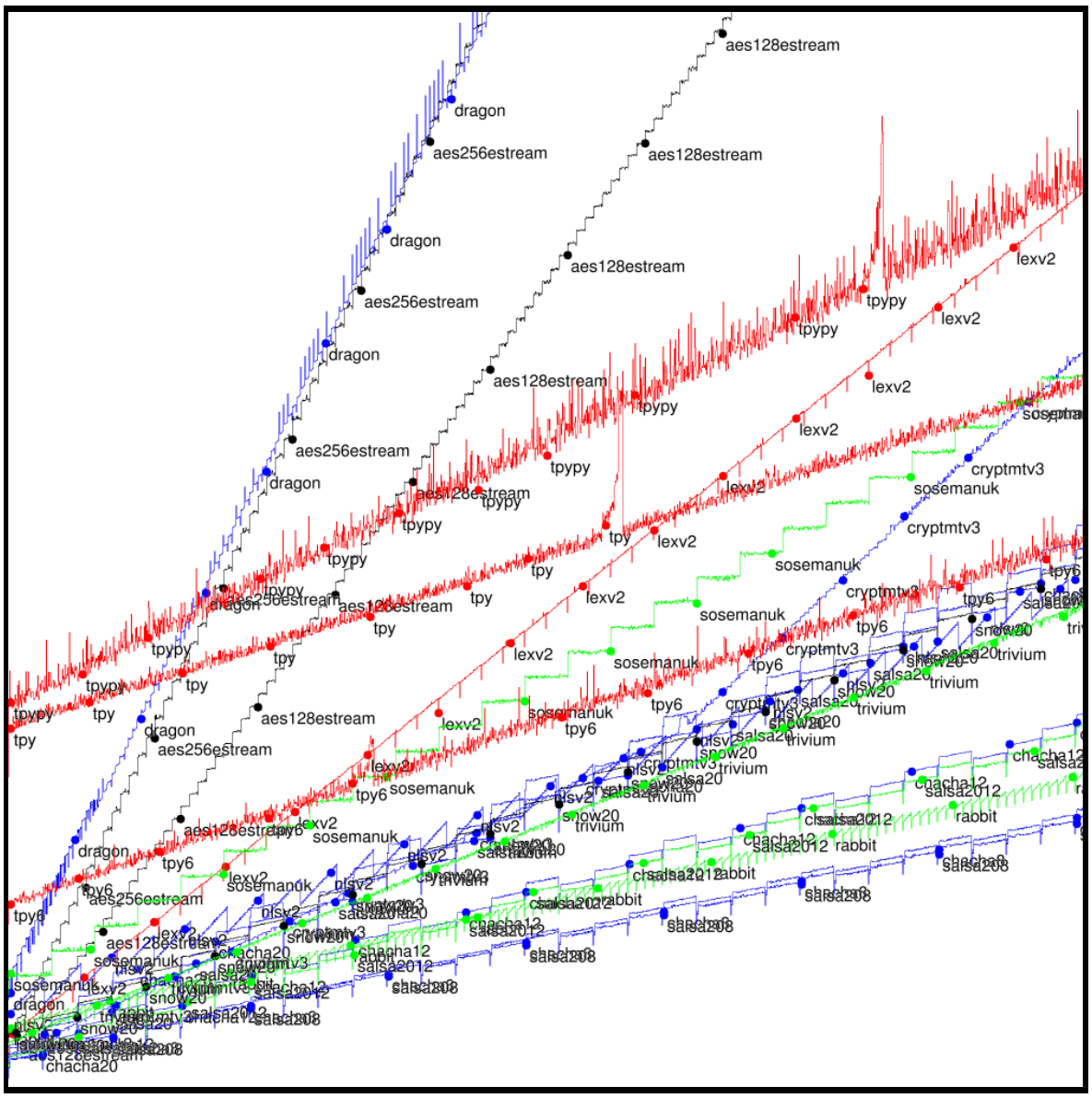
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.13	6.13	6.13	salsa208
6.31	6.31	6.33	chacha8
7.03	7.12	7.23	snow20
8.36	8.36	8.36	salsa2012
8.61	8.61	8.61	chacha12
10.87	10.90	11.09	rabbit
12.85	12.85	12.85	salsa20
13.26	13.27	13.27	chacha20
13.44	13.58	13.62	nlsv2
15.33	15.43	15.52	lexv2
15.55	15.72	15.77	tpy6
17.86	17.88	17.92	aes128estream
20.28	20.53	20.59	sosemanuk
22.58	22.67	22.88	cryptmtv3
23.99	24.21	24.38	tpy
29.40	29.48	30.79	tpypy
30.74	30.77	30.90	aes256estream
30.67	30.90	30.96	dragon
46.85	47.03	47.14	trivium
86.84	86.94	86.97	hc128
162.89	163.73	164.26	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
5.57	5.58	5.59	salsa208
5.78	5.78	5.78	chacha8
6.06	6.11	6.28	snow20
7.68	7.68	7.68	salsa2012
7.90	7.90	7.90	chacha12
7.97	8.09	8.16	tpy6
8.76	8.77	8.80	rabbit
9.52	9.54	9.61	nlsv2
11.24	11.30	11.44	tpy
11.91	11.91	11.91	salsa20
12.20	12.20	12.20	chacha20
13.50	13.54	13.56	lexv2
14.06	14.09	14.27	sosemanuk
15.97	16.03	16.30	tpypy
17.25	17.26	17.26	aes128estream
21.12	21.22	21.26	cryptmtv3
27.95	27.95	27.96	dragon
29.02	29.22	29.23	aes256estream
35.06	35.22	35.39	hc128
40.89	40.89	41.16	trivium
64.45	64.52	64.64	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.16	5.20	5.32	tpy6
5.29	5.38	5.47	snow20
5.47	5.47	5.47	salsa208
5.66	5.66	5.66	chacha8
6.52	6.53	6.70	tpy
7.58	7.58	7.58	salsa2012
7.80	7.80	7.80	chacha12
8.03	8.03	8.06	rabbit
8.06	8.07	8.10	nlsv2
10.91	10.91	10.96	tpypy
11.74	11.76	11.89	sosemanuk
11.79	11.79	11.80	salsa20
12.08	12.08	12.08	chacha20
12.63	12.65	12.76	lexv2
15.86	15.92	15.95	hc128
17.35	17.38	17.42	aes128estream
20.40	20.43	20.48	cryptmtv3
27.12	27.44	27.46	dragon
27.61	27.65	27.77	hc256
28.24	28.26	28.28	aes256estream
38.75	38.87	38.87	trivium

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
3.32	3.46	3.73	tpy6
3.53	3.59	4.03	tpy
3.95	4.18	4.31	hc128
4.78	5.02	5.25	snow20
5.40	5.41	5.41	salsa208
5.18	5.50	5.89	hc256
5.59	5.59	5.59	chacha8
7.24	7.29	7.40	nlsv2
7.51	7.52	7.52	salsa2012
7.50	7.54	7.60	rabbit
7.52	7.56	7.68	tpypy
7.74	7.74	7.74	chacha12
10.31	10.38	10.72	sosemanuk
11.74	11.74	11.75	salsa20
12.01	12.01	12.02	chacha20
12.03	12.13	12.38	lexv2
17.53	17.58	17.68	aes128estream
20.52	20.83	20.98	cryptmtv3
26.47	27.31	27.36	dragon
27.47	27.73	27.85	aes256estream
37.15	37.74	37.77	trivium

7.30 x86, 2400MHz, Intel Core 2 Duo (6fb), `utrecht`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
59.62	63.00	64.12	salsa208
65.25	66.38	68.62	chacha8
70.88	73.12	73.12	aes128estream
72.00	73.12	74.25	salsa2012
75.38	76.50	77.62	chacha12
76.50	77.62	78.75	cryptmtv3
90.00	91.12	92.25	salsa20
97.88	99.00	100.12	chacha20
101.25	101.25	102.38	trivium
120.38	120.38	120.38	aes256estream
121.50	122.62	123.75	lexv2
126.00	126.00	126.00	snow20
141.75	144.00	145.12	rabbit
173.25	174.38	175.50	nlsv2
253.12	254.25	257.62	sosemanuk
231.75	261.00	262.12	dragon
407.25	418.50	433.12	tpy6
831.38	838.12	857.25	tpy
868.50	880.88	883.12	tpypy
2976.75	2992.50	3011.62	hc128
7994.25	8042.62	8200.12	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
5.06	5.06	5.20	salsa208
5.20	5.34	5.48	chacha8
6.33	6.33	6.47	salsa2012
6.47	6.61	6.61	chacha12
8.72	8.72	8.86	salsa20
9.28	9.28	9.42	chacha20
12.80	12.94	13.08	cryptmtv3
15.61	15.61	15.75	snow20
16.17	16.31	16.45	trivium
16.45	17.02	17.30	rabbit
19.55	19.69	19.69	aes128estream
22.22	22.36	22.78	lexv2
30.52	30.66	30.66	nlsv2
30.80	30.80	30.94	aes256estream
31.64	31.92	32.48	sosemanuk
46.83	46.83	51.33	dragon
54.14	54.56	56.25	tpy6
106.31	107.02	109.83	tpy
114.05	116.44	126.56	tpypy
374.20	375.89	378.14	hc128
998.44	1000.55	1005.19	hc256

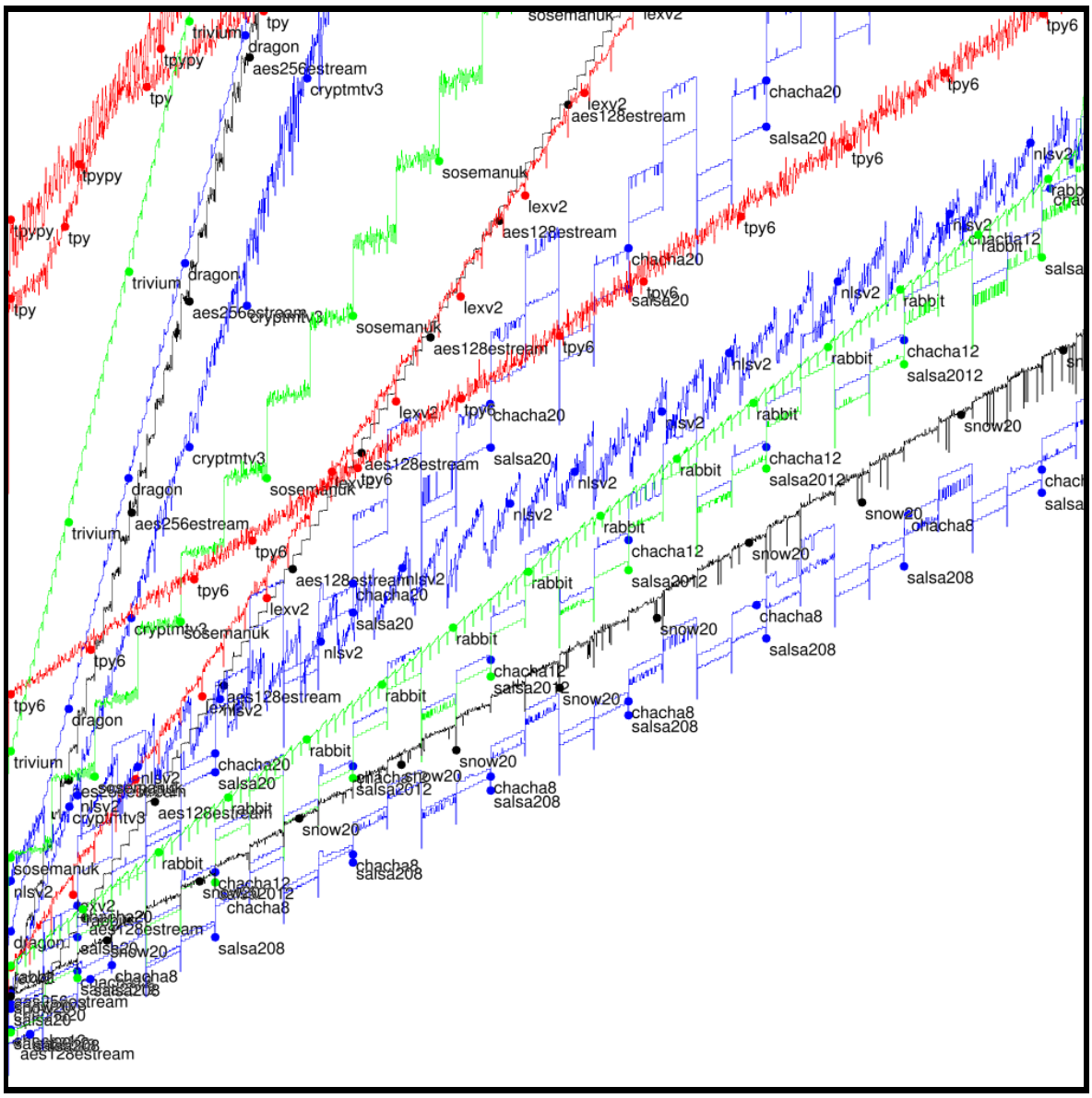
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
2.56	2.56	2.58	salsa208
2.56	2.58	2.61	chacha8
3.34	3.34	3.36	salsa2012
3.47	3.48	3.50	chacha12
3.91	3.91	3.92	rabbit
4.92	4.92	4.92	salsa20
5.19	5.20	5.22	chacha20
5.39	5.42	5.45	trivium
5.69	5.70	5.72	snow20
5.70	5.72	5.73	cryptmtv3
6.45	6.47	6.48	nlsv2
9.12	9.19	9.27	sosemanuk
9.16	9.31	9.36	tpy6
9.44	9.45	9.48	lexv2
14.64	14.67	14.73	tpy
15.08	15.11	15.12	aes128estream
16.75	17.12	17.16	tpypy
22.70	22.72	22.73	aes256estream
23.20	24.48	24.50	dragon
45.02	45.28	45.44	hc128
114.95	115.41	116.05	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
2.33	2.34	2.34	salsa208
2.38	2.38	2.38	chacha8
2.91	2.92	2.93	rabbit
3.08	3.09	3.10	salsa2012
3.16	3.17	3.18	chacha12
4.55	4.61	4.63	trivium
4.61	4.62	4.63	salsa20
4.75	4.75	4.76	chacha20
4.90	4.90	4.90	nlsv2
4.92	4.92	4.93	snow20
5.57	5.68	6.29	tpy6
6.02	6.03	6.08	cryptmtv3
7.03	7.06	7.09	sosemanuk
7.47	7.49	7.52	tpy
8.45	8.46	8.47	lexv2
9.53	9.55	9.76	tpypy
14.74	14.77	14.77	aes128estream
18.73	18.80	18.83	hc128
21.37	21.37	21.38	dragon
22.10	22.10	22.16	aes256estream
45.97	46.03	46.11	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
2.26	2.26	2.26	`salsa208`
2.30	2.30	2.32	`chacha8`
2.57	2.57	2.57	`rabbit`
3.04	3.04	3.05	`salsa2012`
3.11	3.11	3.12	`chacha12`
4.08	4.08	4.10	`cryptmtv3`
4.24	4.24	4.25	`nlsv2`
4.23	4.26	4.30	`tpy6`
4.21	4.29	4.31	`trivium`
4.53	4.53	4.54	`salsa20`
4.63	4.63	4.63	`snow20`
4.69	4.70	4.70	`chacha20`
4.85	4.87	4.89	`tpy`
6.27	6.29	6.30	`sosemanuk`
6.57	6.81	6.87	`tpypy`
8.09	8.09	8.09	`lexv2`
9.18	9.20	9.20	`hc128`
14.62	14.64	14.66	`aes128estream`
20.18	20.21	20.23	`hc256`
20.72	20.72	20.72	`dragon`
21.87	21.88	21.88	`aes256estream`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
1.23	1.25	1.33	`cryptmtv3`
2.21	2.21	2.22	`salsa208`
2.24	2.25	2.29	`chacha8`
2.34	2.39	2.40	`rabbit`
3.00	3.01	3.02	`salsa2012`
3.07	3.08	3.10	`chacha12`
3.06	3.13	3.32	`tpy`
3.26	3.39	3.52	`tpy6`
3.31	3.39	3.42	`hc128`
3.92	3.93	3.95	`nlsv2`
3.92	4.15	4.22	`trivium`
4.43	4.45	4.46	`snow20`
4.48	4.48	4.50	`salsa20`
4.65	4.67	4.68	`chacha20`
4.64	4.75	4.82	`hc256`
4.62	5.22	5.44	`tpypy`
5.84	5.91	5.96	`sosemanuk`
7.85	7.87	7.88	`lexv2`
14.51	14.62	14.71	`aes128estream`
20.35	20.36	20.36	`dragon`
21.70	21.70	21.77	`aes256estream`

7.31 x86, 2401MHz, Intel Pentium 4 (f24), nmi0086



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
101.50	102.00	102.50	salsa208
102.00	102.50	104.00	chacha8
103.00	104.00	104.00	aes128estream
126.00	126.50	126.50	salsa2012
132.00	132.50	132.50	chacha12
179.00	181.00	181.50	salsa20
192.50	193.00	193.00	chacha20
210.50	211.50	213.50	snow20
219.50	221.50	223.50	cryptmtv3
222.00	224.00	228.00	aes256estream
272.50	280.00	294.50	lexv2
281.50	286.50	288.00	rabbit
368.50	370.50	375.00	dragon
482.00	489.00	509.00	nlsv2
534.00	535.00	539.00	sosemanuk
768.50	772.50	773.50	trivium
898.50	906.50	909.50	tpy6
1791.50	1803.50	1811.50	tpy
1896.00	1943.00	1976.50	tpypy
6205.50	6220.00	6248.50	hc128
19317.50	19357.00	19405.50	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
10.62	10.62	13.00	salsa208
13.31	13.44	13.62	chacha8
14.19	14.25	17.25	salsa2012
18.06	18.12	18.12	chacha12
20.62	20.62	23.31	salsa20
26.62	26.62	26.69	aes128estream
27.25	27.44	28.38	snow20
22.62	27.56	27.62	chacha20
38.88	38.88	38.88	rabbit
48.62	49.31	50.31	lexv2
53.69	54.44	54.75	cryptmtv3
58.00	58.00	58.81	aes256estream
68.31	68.38	68.62	sosemanuk
75.19	78.75	79.94	nlsv2
80.62	81.12	81.19	dragon
117.69	118.44	118.94	tpy6
132.56	132.75	132.75	trivium
230.69	234.38	236.44	tpy
249.44	249.75	250.81	tpypy
777.50	779.69	784.12	hc128
2409.12	2421.88	2429.06	hc256

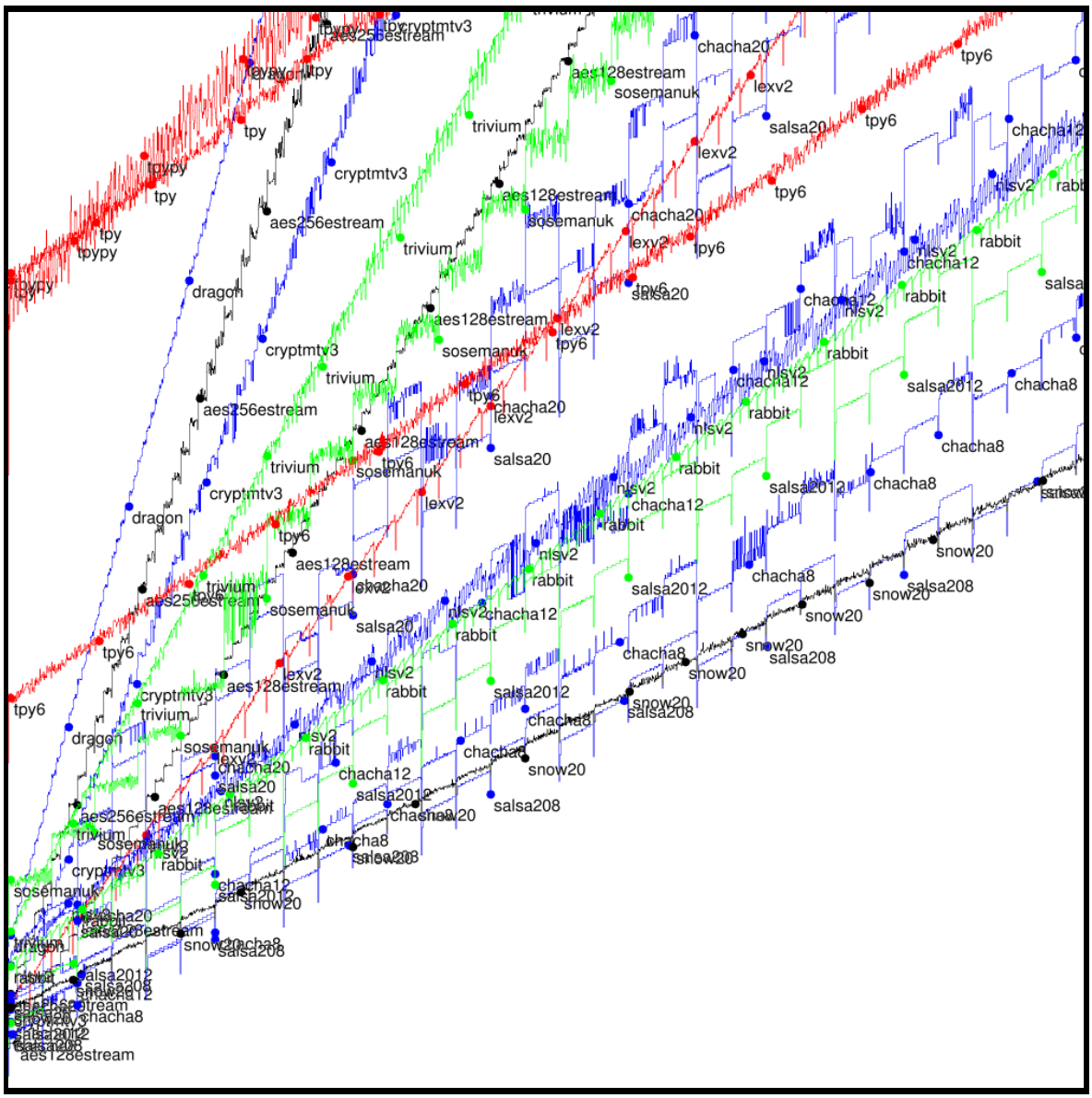
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.12	6.12	6.13	salsa208
6.31	6.31	6.32	chacha8
8.33	8.34	8.38	salsa2012
8.26	8.44	8.58	snow20
8.62	8.63	8.63	chacha12
11.09	11.09	11.12	rabbit
12.81	12.81	12.81	salsa20
13.22	13.22	13.22	chacha20
13.94	14.08	14.26	nlsv2
18.10	18.12	18.12	aes128estream
19.00	19.12	19.32	lexv2
19.11	19.17	19.31	tpy6
24.34	24.61	25.12	sosemanuk
33.81	34.15	34.44	cryptmtv3
35.87	35.96	36.83	tpy
40.94	40.98	41.76	tpypy
41.50	41.74	42.35	aes256estream
42.88	42.99	42.99	dragon
51.56	51.60	51.69	trivium
90.76	91.04	91.38	hc128
271.01	271.31	274.93	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
5.57	5.57	5.57	salsa208
5.76	5.76	5.76	chacha8
6.78	7.05	7.15	snow20
7.68	7.74	7.74	salsa2012
7.90	7.91	7.91	chacha12
8.88	8.88	8.90	rabbit
9.48	9.57	9.58	nlsv2
11.19	11.35	11.39	tpy6
11.92	11.92	11.92	salsa20
12.19	12.19	12.19	chacha20
16.76	16.78	16.84	lexv2
17.35	17.35	17.36	aes128estream
17.97	17.97	18.34	tpy
20.44	20.57	21.01	sosemanuk
25.21	25.34	25.40	tpypy
30.91	31.06	31.38	cryptmtv3
36.93	37.02	37.22	hc128
40.13	40.13	40.13	dragon
40.58	40.68	40.85	aes256estream
45.18	45.26	45.36	trivium
106.31	106.32	106.57	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.48	5.49	5.49	salsa208
5.63	5.64	5.64	chacha8
6.15	6.16	6.50	snow20
7.56	7.57	7.58	salsa2012
7.67	7.70	7.77	nlsv2
7.78	7.79	7.80	chacha12
8.09	8.11	8.15	rabbit
8.44	8.46	8.53	tpy6
11.14	11.19	11.25	tpy
11.82	11.82	11.82	salsa20
12.08	12.15	12.15	chacha20
15.74	15.90	15.92	lexv2
17.00	17.12	17.36	hc128
17.09	17.12	17.13	aes128estream
19.02	19.17	19.60	sosemanuk
19.32	19.34	19.42	tpypy
22.86	22.94	23.00	cryptmtv3
39.05	39.08	39.09	dragon
40.14	40.44	40.54	aes256estream
42.72	42.96	42.96	trivium
43.20	43.33	43.50	hc256

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
4.54	4.85	5.53	hc128
5.08	5.42	6.23	hc256
5.44	5.45	5.46	salsa208
5.42	5.47	6.16	snow20
5.54	5.57	5.58	chacha8
6.65	6.71	6.91	tpy6
6.62	6.73	7.06	nlsv2
7.14	7.28	7.43	tpy
7.30	7.47	7.50	salsa2012
7.54	7.64	7.74	rabbit
7.70	7.72	7.74	chacha12
11.77	11.77	11.77	salsa20
11.83	12.15	12.16	chacha20
14.91	15.24	15.30	lexv2
15.45	15.59	15.83	tpypy
16.13	16.37	16.92	cryptmtv3
16.95	17.01	17.03	aes128estream
18.04	18.64	19.62	sosemanuk
38.38	38.45	38.46	dragon
39.91	40.57	41.03	aes256estream
40.94	41.52	41.57	trivium

7.32 x86, 2658MHz, Intel Xeon (f25), `nmi0013`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
104.50	104.50	104.50	aes128estream
123.50	124.50	126.00	salsa208
123.50	126.50	127.50	chacha8
150.50	150.50	152.00	salsa2012
153.00	154.00	155.00	chacha12
178.50	183.00	187.00	cryptmtv3
188.00	191.00	193.00	snow20
198.50	199.50	200.00	lexv2
202.00	202.50	203.50	salsa20
215.50	216.00	216.00	chacha20
219.50	220.50	221.00	aes256estream
294.00	295.50	298.00	rabbit
305.50	308.00	315.50	nlsv2
353.50	355.00	359.50	dragon
356.00	356.00	356.50	trivium
462.50	468.50	470.00	sosemanuk
888.00	894.50	897.00	tpy6
1748.00	1835.00	2499.00	tpypy
1857.50	1893.50	1900.00	tpy
6264.50	6274.50	6310.50	hc128
11165.50	11303.50	11322.50	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
10.75	10.94	13.06	salsa208
11.25	11.25	11.25	chacha8
14.00	14.12	17.25	salsa2012
14.81	15.00	17.94	chacha12
20.69	20.69	20.81	salsa20
22.44	22.56	27.56	chacha20
22.81	23.00	23.19	snow20
26.19	26.19	26.19	aes128estream
37.38	37.50	39.12	lexv2
38.62	39.06	39.38	rabbit
46.12	46.81	46.88	cryptmtv3
49.00	49.31	53.69	nlsv2
50.44	50.62	50.62	aes256estream
59.62	59.88	60.38	sosemanuk
59.94	59.94	60.81	trivium
76.38	77.12	77.94	dragon
117.06	119.12	119.25	tpy6
231.25	232.06	235.19	tpypy
239.94	240.88	242.75	tpy
790.56	791.75	800.56	hc128
1376.94	1412.12	1420.62	hc256

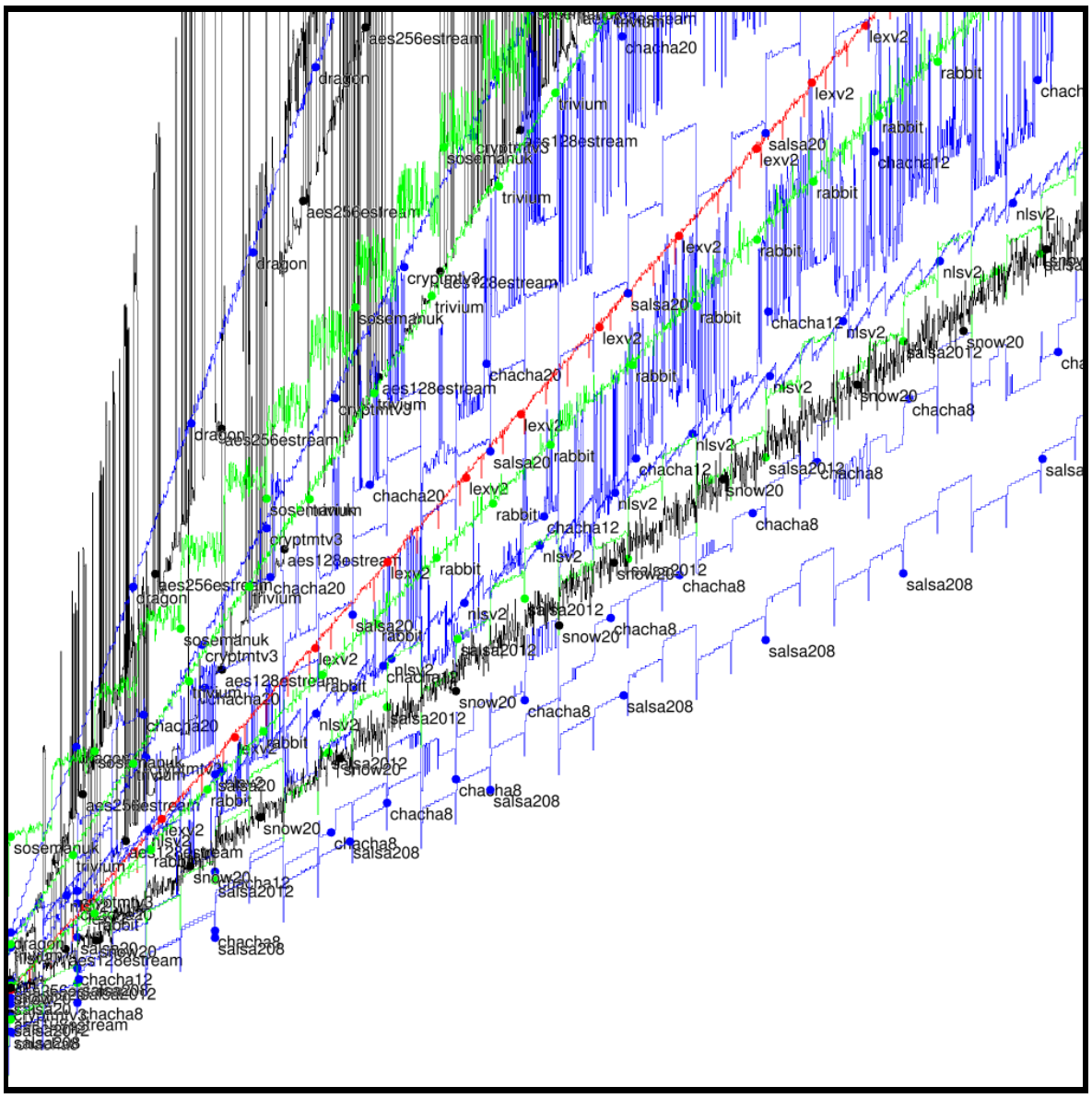
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
5.98	5.99	5.99	salsa208
6.98	6.98	6.98	chacha8
7.06	7.12	7.35	snow20
8.22	8.22	8.22	salsa2012
8.95	8.95	8.96	chacha12
11.10	11.17	11.19	rabbit
11.64	11.72	11.79	nlsv2
12.72	12.72	12.72	salsa20
13.73	13.73	14.27	chacha20
15.09	15.12	15.17	lexv2
18.75	18.81	18.85	aes128estream
18.85	19.20	19.54	tpy6
19.86	20.18	20.42	sosemanuk
22.94	22.94	22.94	trivium
28.81	29.41	29.42	cryptmtv3
33.07	33.26	33.36	tpy
33.60	33.71	34.10	aes256estream
33.88	35.49	35.59	tpypy
40.94	41.08	41.17	dragon
91.29	91.80	92.33	hc128
157.69	158.83	164.92	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
5.47	5.48	5.49	salsa208
5.86	5.88	5.93	snow20
6.61	6.61	6.62	chacha8
7.58	7.59	7.59	salsa2012
8.85	8.85	8.86	rabbit
9.03	9.03	9.03	chacha12
9.17	9.20	9.26	nlsv2
11.51	11.51	11.56	tpy6
11.99	12.03	12.03	salsa20
13.51	13.54	13.59	lexv2
13.45	13.69	13.69	chacha20
16.11	16.35	16.89	sosemanuk
16.88	16.92	16.98	tpy
18.12	18.18	18.22	aes128estream
19.10	19.35	19.81	tpypy
19.77	19.77	20.08	trivium
25.26	25.43	25.45	cryptmtv3
31.97	32.21	32.29	aes256estream
37.28	37.40	37.58	hc128
38.19	38.35	38.47	dragon
63.07	63.22	64.23	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.37	5.37	5.38	`salsa208`
5.42	5.43	5.46	`snow20`
6.56	6.56	6.56	`chacha8`
7.48	7.48	7.48	`salsa2012`
8.08	8.09	8.09	`rabbit`
8.30	8.30	8.33	`nlsv2`
8.72	8.75	8.75	`tpy6`
9.17	9.17	9.17	`chacha12`
10.77	10.79	10.80	`tpy`
11.78	11.78	11.78	`salsa20`
12.85	12.87	12.88	`lexv2`
13.36	13.50	13.50	`chacha20`
13.38	13.71	14.26	`sosemanuk`
13.70	13.72	13.74	`tpypy`
16.99	17.06	17.11	`hc128`
17.90	17.92	17.97	`aes128estream`
18.61	18.61	18.61	`trivium`
19.08	19.32	19.68	`cryptmtv3`
27.48	27.82	27.89	`hc256`
31.61	31.71	31.76	`aes256estream`
37.13	37.19	37.28	`dragon`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
4.54	4.95	5.15	`hc128`
5.05	5.18	5.23	`snow20`
5.30	5.30	5.33	`salsa208`
5.27	6.24	6.90	`hc256`
6.53	6.54	6.54	`chacha8`
6.96	7.13	7.24	`tpy`
7.02	7.16	7.20	`tpy6`
7.41	7.42	7.42	`salsa2012`
7.56	7.60	7.63	`rabbit`
7.83	7.84	7.92	`nlsv2`
9.28	9.28	9.28	`chacha12`
10.06	10.38	10.63	`tpypy`
11.63	11.63	11.63	`salsa20`
11.13	12.42	13.88	`sosemanuk`
12.46	12.51	12.57	`lexv2`
13.11	13.38	13.38	`chacha20`
14.06	15.02	15.83	`cryptmtv3`
17.62	17.71	17.83	`aes128estream`
17.82	17.83	17.92	`trivium`
31.18	31.44	31.63	`aes256estream`
36.22	36.49	36.73	`dragon`

7.33 x86, 2658MHz, Intel Xeon (f25), `nmibuild15`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
125.00	126.00	128.00	chacha8
125.50	127.00	129.00	salsa208
155.00	156.50	157.50	salsa2012
158.00	162.50	191.50	chacha12
110.00	166.00	180.00	aes128estream
192.50	198.00	203.00	cryptmtv3
206.00	206.50	206.50	salsa20
218.50	227.50	233.50	snow20
226.00	232.00	235.00	lexv2
230.50	235.00	241.00	rabbit
222.00	245.50	255.00	chacha20
250.00	254.50	260.00	aes256estream
330.50	331.00	332.00	trivium
337.50	342.50	345.00	nlsv2
364.00	364.50	365.00	dragon
573.00	575.00	584.00	sosemanuk
4363.00	4391.00	4409.00	hc128
12134.00	12515.00	19788.50	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
10.75	10.81	11.12	salsa208
11.38	13.25	13.38	chacha8
14.88	15.12	15.56	salsa2012
18.69	18.69	18.69	chacha12
20.62	20.62	20.94	salsa20
26.31	26.44	44.25	aes128estream
25.56	28.19	28.19	chacha20
28.81	29.69	31.31	snow20
35.19	36.25	36.75	rabbit
38.12	38.19	38.50	lexv2
38.06	38.25	39.00	cryptmtv3
50.56	51.25	53.56	nlsv2
53.75	53.81	54.25	trivium
51.06	55.12	82.81	aes256estream
70.06	70.31	71.00	dragon
71.56	71.69	72.50	sosemanuk
549.25	549.38	549.69	hc128
1474.38	1489.69	1535.44	hc256

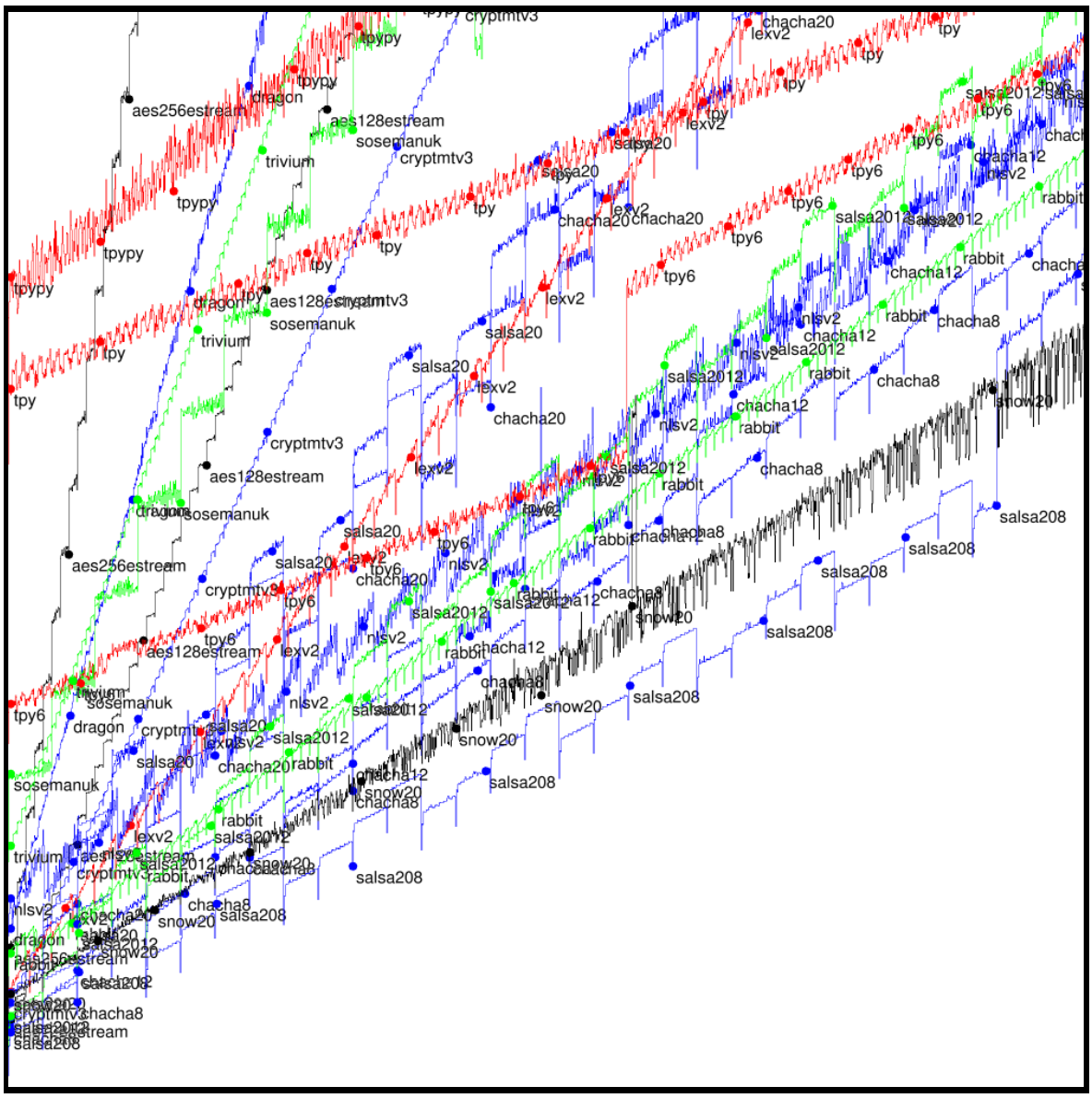
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.06	6.11	6.13	salsa208
7.08	7.08	7.09	chacha8
8.67	8.80	9.15	salsa2012
9.02	9.14	9.17	chacha12
9.21	9.55	9.81	snow20
11.88	11.89	11.99	nlsv2
12.70	12.76	12.80	salsa20
12.81	12.88	12.90	rabbit
14.35	14.38	14.46	lexv2
13.79	16.74	17.14	chacha20
19.40	19.41	19.41	trivium
21.12	21.18	21.24	cryptmtv3
23.26	23.56	23.99	sosemanuk
29.23	29.56	56.09	aes256estream
32.94	33.17	33.25	dragon
34.69	35.16	35.88	aes128estream
65.08	65.08	65.84	hc128
169.21	173.97	178.28	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
5.58	5.58	5.59	salsa208
7.17	7.18	7.18	chacha8
7.85	8.02	8.03	salsa2012
7.99	8.15	8.26	snow20
9.01	9.05	9.09	nlsv2
8.83	10.36	10.79	chacha12
11.10	11.21	11.58	rabbit
11.86	11.86	11.86	salsa20
12.46	12.48	12.51	lexv2
13.19	16.15	16.51	chacha20
17.02	17.05	17.14	trivium
19.49	19.56	19.61	cryptmtv3
18.45	19.84	20.20	sosemanuk
27.82	27.82	28.06	hc128
27.83	28.23	55.42	aes256estream
30.88	30.96	30.97	dragon
18.12	34.14	34.58	aes128estream
67.98	68.79	70.52	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.44	5.44	5.45	salsa208
6.91	6.99	7.03	chacha8
7.56	7.56	7.65	salsa2012
7.65	7.70	7.76	snow20
8.07	8.10	8.12	nlsv2
8.65	8.68	8.76	chacha12
10.54	10.82	10.83	rabbit
11.69	11.70	11.71	lexv2
11.86	11.88	11.92	salsa20
12.83	12.94	15.79	chacha20
14.04	14.16	14.17	hc128
15.83	15.87	15.90	trivium
16.46	16.50	16.58	cryptmtv3
17.03	17.04	17.59	sosemanuk
18.15	18.28	34.11	aes128estream
26.98	27.06	27.22	aes256estream
29.36	29.36	30.06	hc256
30.12	30.25	30.45	dragon

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
1.11	2.31	50.16	aes128estream
2.45	2.63	5.86	hc256
5.36	5.36	5.37	salsa208
5.84	6.07	6.10	hc128
6.42	7.08	8.69	chacha12
7.10	7.28	7.36	chacha8
7.34	7.42	7.59	salsa2012
7.02	7.54	7.74	snow20
7.55	7.62	7.67	nlsv2
8.77	10.19	18.42	chacha20
10.21	10.79	10.94	rabbit
11.19	11.26	11.31	lexv2
11.76	11.79	11.87	salsa20
14.41	14.49	14.76	cryptmtv3
15.06	15.16	15.31	trivium
15.19	16.03	17.15	sosemanuk
-0.62	17.44	27.02	aes256estream
28.02	28.37	28.84	dragon

7.34 x86, 2658MHz, Intel Xeon (f25), `nmibuild16`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
125.50	127.00	140.00	salsa208
127.00	140.00	140.00	chacha8
152.00	155.50	165.00	aes128estream
155.00	160.50	161.50	chacha12
150.50	166.50	168.00	salsa2012
199.50	200.50	202.00	cryptmtv3
213.00	218.00	290.50	snow20
216.50	219.00	219.00	chacha20
204.00	220.00	221.50	salsa20
237.50	243.00	244.50	lexv2
285.00	324.50	348.50	rabbit
279.00	336.00	347.50	aes256estream
373.50	378.50	470.50	nlsv2
381.00	388.50	519.50	dragon
318.50	555.50	557.50	trivium
708.00	723.50	733.00	sosemanuk
881.00	890.50	1120.50	tpy6
1658.50	1667.50	1683.50	tpy
1822.50	1850.00	2313.50	tpypy
6728.50	8065.50	8094.50	hc128
13601.50	13633.00	13667.50	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
10.88	10.88	12.88	salsa208
12.81	12.94	13.38	chacha8
14.00	16.19	16.31	salsa2012
18.06	18.06	18.12	chacha12
22.38	22.62	27.56	chacha20
20.88	22.75	22.88	salsa20
26.94	27.75	36.75	snow20
36.88	37.31	40.69	rabbit
40.75	41.38	44.19	aes128estream
42.56	42.75	43.12	cryptmtv3
41.94	42.94	44.38	lexv2
63.50	70.25	86.94	nlsv2
79.19	80.50	106.06	dragon
89.62	90.00	91.00	sosemanuk
53.81	93.81	94.50	trivium
70.75	97.81	98.75	aes256estream
112.06	113.25	139.69	tpy6
205.25	207.19	216.00	tpy
232.62	234.38	290.19	tpypy
840.56	1011.12	1014.38	hc128
1674.31	1682.81	1703.69	hc256

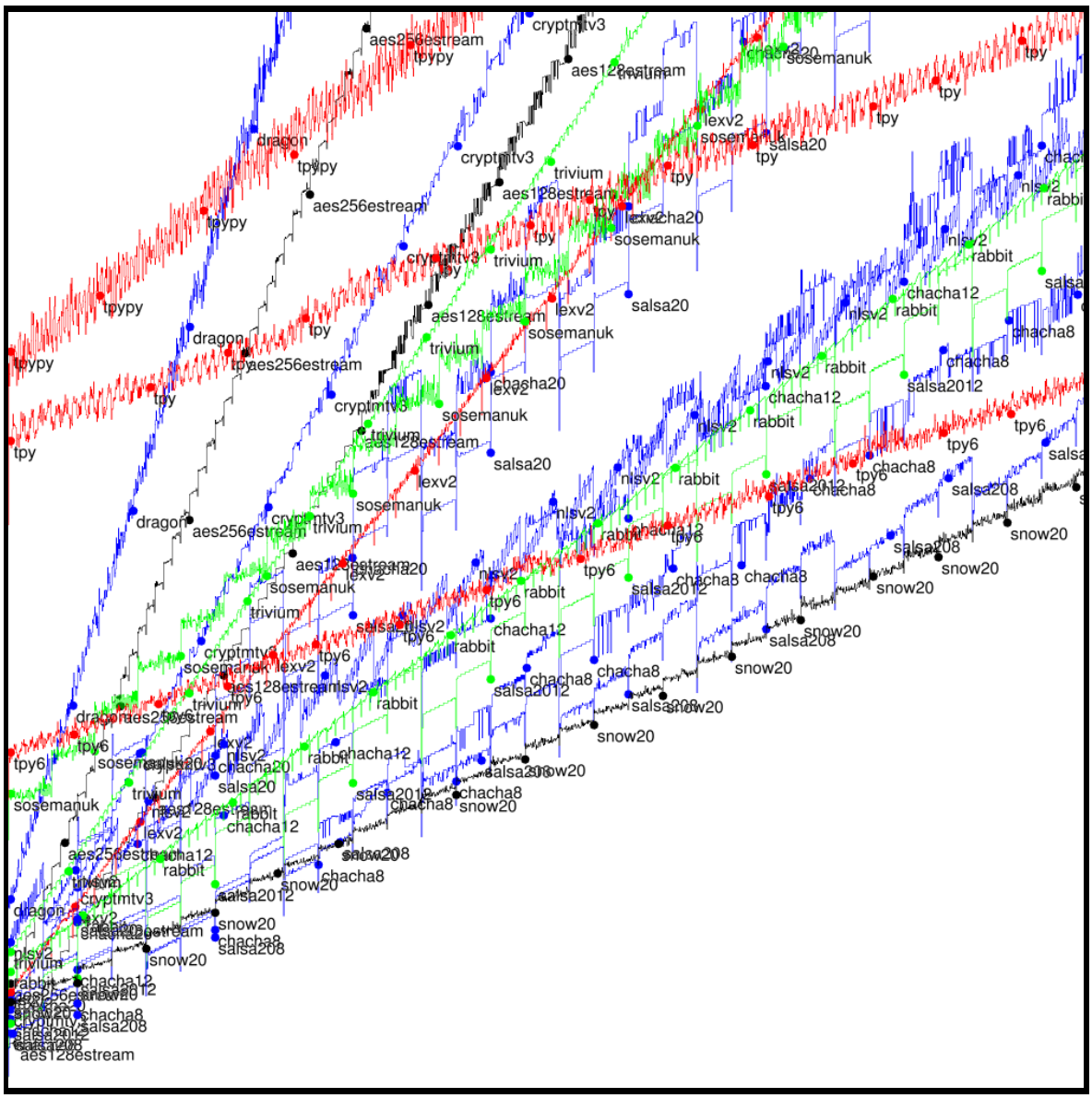
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.03	6.05	7.58	salsa208
7.62	8.31	8.38	chacha8
8.31	8.60	11.80	snow20
8.59	8.64	8.97	chacha12
8.29	10.14	10.17	salsa2012
10.85	10.94	11.81	rabbit
12.90	12.99	15.60	nlsv2
13.67	13.79	13.92	chacha20
12.75	15.36	15.46	salsa20
16.12	16.22	16.30	lexv2
16.27	16.52	20.39	tpy6
24.44	24.49	24.53	cryptmtv3
26.38	26.48	26.60	tpy
25.94	30.62	31.01	sosemanuk
30.64	30.70	33.23	aes128estream
32.73	33.13	39.88	tpypy
19.68	35.31	35.39	trivium
40.01	40.75	53.44	dragon
51.76	78.20	78.43	aes256estream
98.31	118.62	118.99	hc128
191.25	193.94	194.83	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
5.51	5.52	6.99	salsa208
6.90	7.18	9.89	snow20
6.79	7.84	7.91	chacha8
8.68	8.75	8.89	chacha12
8.78	8.83	9.55	rabbit
7.62	9.51	9.52	salsa2012
9.54	9.57	11.38	nlsv2
10.88	10.94	12.12	tpy6
12.33	12.40	12.47	tpy
13.14	13.29	13.40	chacha20
14.30	14.35	15.00	lexv2
14.62	14.65	15.32	salsa20
17.16	17.25	20.20	tpypy
19.45	20.20	25.00	sosemanuk
21.83	21.87	34.65	cryptmtv3
18.20	29.76	29.82	aes128estream
16.89	30.76	30.79	trivium
37.34	37.54	50.06	dragon
40.09	48.83	56.29	hc128
75.72	75.93	76.18	hc256
49.39	76.54	76.74	aes256estream

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.51	5.52	7.00	`salsa208`
6.00	6.03	7.49	`tpy6`
6.36	6.58	6.62	`snow20`
7.01	7.12	8.95	`tpy`
6.54	7.78	7.80	`chacha8`
8.03	8.05	8.67	`rabbit`
8.28	8.29	8.33	`nlsv2`
8.83	8.92	9.01	`chacha12`
9.41	9.48	9.49	`salsa2012`
11.17	12.78	15.18	`tpypy`
13.14	13.24	13.28	`chacha20`
13.42	13.49	19.83	`lexv2`
11.86	14.46	14.57	`salsa20`
19.93	19.97	19.98	`cryptmtv3`
18.42	22.50	22.57	`hc128`
17.43	23.05	23.31	`sosemanuk`
16.29	29.02	29.04	`trivium`
17.98	29.55	31.86	`aes128estream`
31.57	31.72	31.93	`hc256`
38.22	38.38	49.53	`dragon`
49.18	76.12	76.20	`aes256estream`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
2.42	2.53	7.43	`tpy6`
3.87	3.96	8.44	`salsa208`
3.70	3.97	7.74	`tpy`
4.71	5.65	6.32	`hc256`
2.92	6.27	6.96	`snow20`
6.13	7.55	7.79	`nlsv2`
6.87	7.61	8.86	`rabbit`
5.30	7.81	8.84	`chacha8`
8.67	9.02	9.25	`chacha12`
9.28	9.50	11.41	`salsa2012`
7.38	10.65	15.52	`tpypy`
12.85	13.03	25.78	`lexv2`
12.95	13.24	13.52	`chacha20`
-1.52	13.73	13.95	`hc128`
8.93	14.20	17.01	`salsa20`
9.17	19.79	19.86	`cryptmtv3`
10.54	26.94	27.86	`sosemanuk`
2.51	28.01	41.35	`trivium`
27.91	28.32	61.77	`dragon`
6.29	29.46	45.55	`aes128estream`
21.83	75.84	102.49	`aes256estream`

7.35 x86, 2658MHz, Intel Xeon (f25), nmibuild22



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
104.50	104.50	106.00	aes128estream
125.00	125.00	125.00	salsa208
126.00	126.50	130.00	chacha8
149.50	150.50	151.50	salsa2012
158.50	160.00	160.50	chacha12
179.50	181.50	184.50	cryptmtv3
194.50	200.00	201.00	snow20
203.00	203.00	203.00	salsa20
215.00	216.50	221.00	chacha20
225.00	227.50	233.50	lexv2
244.00	245.00	325.50	aes256estream
270.50	270.50	278.00	rabbit
310.50	312.50	314.00	trivium
340.00	370.00	381.50	nlsv2
421.50	444.50	453.00	dragon
671.50	679.00	682.50	sosemanuk
778.00	785.50	794.00	tpy6
1528.50	1530.50	1540.50	tpy
1650.00	1652.50	1661.00	tpypy
5872.50	5876.00	5886.00	hc128
11904.50	11978.50	12076.00	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
11.06	11.88	13.06	salsa208
13.12	13.38	13.38	chacha8
15.69	15.69	17.94	chacha12
17.44	17.44	17.44	salsa2012
22.44	22.44	22.44	chacha20
24.62	25.38	25.62	snow20
25.94	25.94	25.94	salsa20
26.12	26.12	26.44	aes128estream
37.06	37.19	37.25	rabbit
37.62	37.88	38.25	cryptmtv3
39.81	40.06	41.19	lexv2
49.81	49.81	49.88	aes256estream
51.62	52.06	52.31	trivium
59.88	64.94	65.00	nlsv2
80.38	82.06	89.69	dragon
82.56	85.00	85.50	sosemanuk
97.25	99.50	99.56	tpy6
190.50	192.38	193.56	tpy
212.44	214.25	220.69	tpypy
733.56	735.00	738.81	hc128
1492.50	1510.00	1524.81	hc256

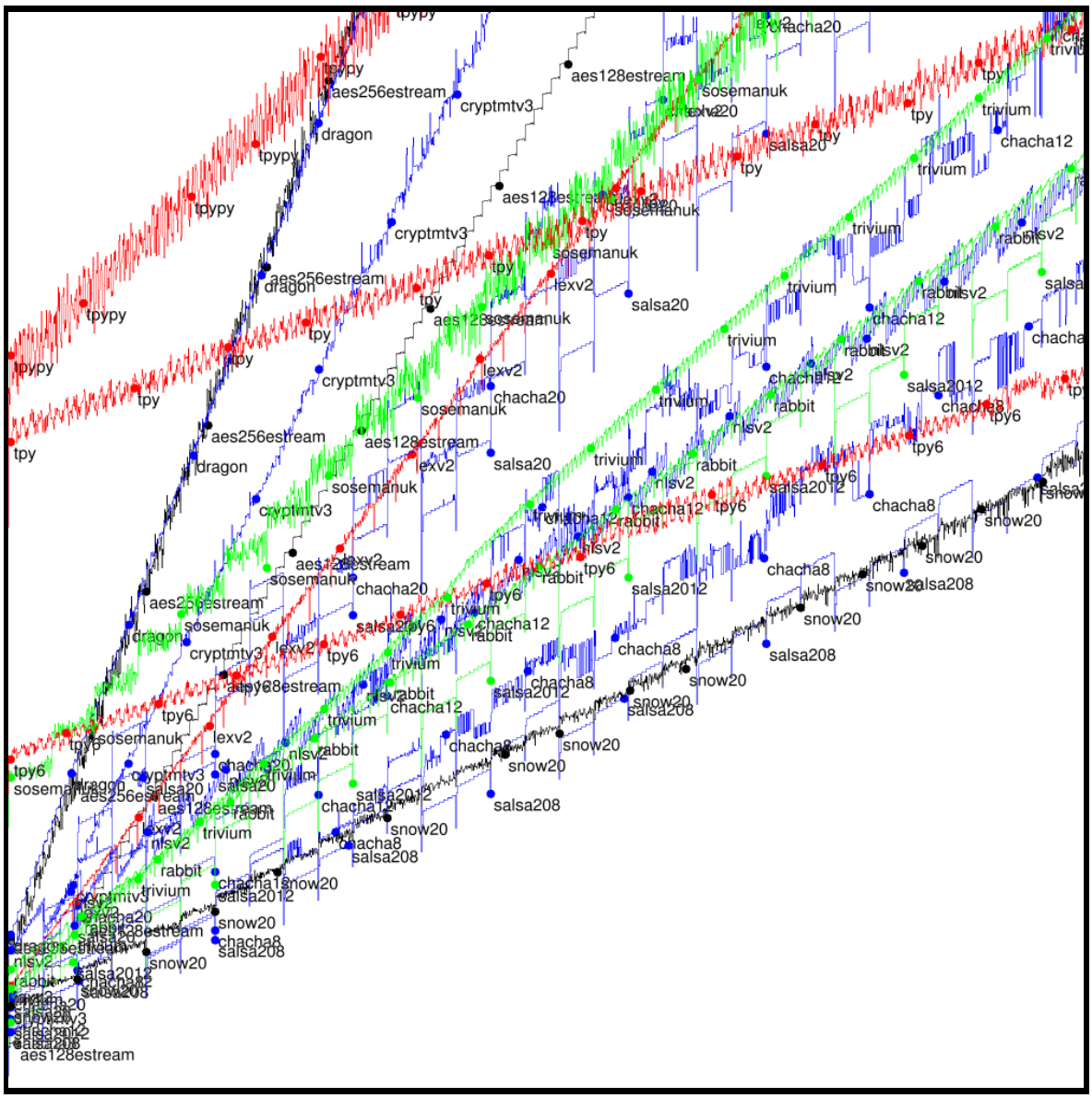
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.28	6.28	6.38	salsa208
7.12	7.18	7.19	snow20
7.19	7.19	7.20	chacha8
8.26	8.26	8.26	salsa2012
8.66	8.69	9.28	chacha12
10.85	10.90	10.92	rabbit
12.35	12.39	12.47	nlsv2
12.72	12.74	12.74	salsa20
13.75	13.75	13.75	chacha20
13.88	13.98	14.22	tpy6
15.94	16.20	16.44	lexv2
18.72	18.73	18.76	aes128estream
18.82	18.83	18.85	trivium
19.15	19.30	19.68	sosemanuk
21.81	21.81	21.81	cryptmtv3
24.69	25.02	25.04	tpy
29.55	29.58	29.59	aes256estream
30.81	31.14	31.52	tpypy
37.49	38.17	38.42	dragon
84.88	85.37	85.51	hc128
169.74	170.92	172.52	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
5.75	5.79	5.79	salsa208
5.83	5.86	5.97	snow20
7.16	7.16	7.20	chacha8
7.46	7.59	11.77	tpy6
7.61	7.62	7.62	salsa2012
8.78	8.79	8.80	rabbit
8.63	8.80	8.88	chacha12
9.17	9.19	9.21	nlsv2
11.65	11.67	11.75	tpy
11.82	11.82	11.82	salsa20
12.84	12.85	12.86	chacha20
13.31	13.35	13.91	sosemanuk
13.97	14.01	14.02	lexv2
16.26	16.27	16.28	trivium
16.12	16.29	16.48	tpypy
18.10	18.11	18.11	aes128estream
19.49	19.61	19.72	cryptmtv3
27.98	28.02	28.05	aes256estream
34.30	34.35	34.51	hc128
34.64	34.82	35.38	dragon
66.69	68.04	68.15	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
4.99	5.01	5.04	tpy6
5.28	5.30	5.30	snow20
5.48	5.49	5.55	salsa208
6.65	6.68	6.78	tpy
6.84	7.15	7.20	chacha8
7.48	7.48	7.48	salsa2012
8.00	8.02	8.04	nlsv2
8.01	8.02	8.03	rabbit
8.71	9.05	9.05	chacha12
10.95	11.04	11.05	tpypy
11.26	11.60	11.67	sosemanuk
11.70	11.70	11.70	salsa20
13.13	13.17	13.20	lexv2
13.27	13.27	13.27	chacha20
15.36	15.40	15.50	hc128
15.49	15.49	15.55	trivium
17.88	17.89	17.92	aes128estream
18.57	18.66	18.66	cryptmtv3
27.34	27.36	27.41	aes256estream
27.96	28.13	28.31	hc256
32.81	33.09	33.18	dragon

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
3.49	3.55	3.74	tpy6
3.42	3.63	3.87	tpy
3.93	4.04	4.25	hc128
4.13	4.99	5.51	hc256
4.92	5.02	5.04	snow20
5.23	5.27	5.44	salsa208
6.45	7.05	7.16	chacha8
7.40	7.40	7.41	salsa2012
7.42	7.47	7.52	nlsv2
7.53	7.55	7.56	rabbit
7.42	7.79	7.84	tpypy
8.77	9.45	9.63	chacha12
10.06	10.84	10.99	sosemanuk
11.62	11.62	11.63	salsa20
12.42	12.69	12.79	lexv2
13.34	13.34	13.55	chacha20
14.97	15.02	15.16	trivium
17.67	17.73	17.78	aes128estream
18.76	18.99	19.05	cryptmtv3
26.91	27.00	27.15	aes256estream
31.40	32.46	32.92	dragon

7.36 x86, 2659MHz, Intel Xeon (f25), `nmibuild21`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
105.50	105.50	105.50	aes128estream
128.50	129.50	129.50	chacha8
127.00	132.50	132.50	salsa208
151.00	151.50	152.00	salsa2012
159.50	159.50	159.50	chacha12
185.00	189.50	192.50	snow20
185.50	190.50	193.00	cryptmtv3
200.00	202.50	202.50	salsa20
208.50	208.50	209.00	trivium
219.50	221.00	221.00	chacha20
234.00	237.50	242.00	lexv2
272.00	273.50	281.50	rabbit
315.50	321.50	342.00	nlsv2
310.00	349.00	382.00	aes256estream
355.00	359.00	362.50	dragon
716.50	726.50	735.00	sosemanuk
783.50	785.50	791.00	tpy6
1522.00	1525.50	1527.00	tpy
1626.50	1633.00	1651.50	tpypy
5865.50	5879.50	5901.50	hc128
9940.50	10011.50	10013.00	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
13.19	13.31	13.38	salsa208
13.69	13.69	13.69	chacha8
14.00	14.00	14.00	salsa2012
18.31	18.31	18.38	chacha12
24.38	24.56	24.88	snow20
25.75	25.75	25.88	salsa20
26.25	26.25	26.56	aes128estream
27.81	27.81	27.94	chacha20
34.00	34.00	34.00	trivium
36.25	36.69	36.81	rabbit
40.19	40.75	40.88	cryptmtv3
41.19	41.56	42.94	lexv2
51.88	53.19	54.94	nlsv2
60.75	62.12	63.31	aes256estream
68.25	68.38	69.06	dragon
89.31	91.06	92.06	sosemanuk
98.00	98.94	99.50	tpy6
190.31	190.50	193.00	tpy
209.94	211.44	213.25	tpypy
733.94	735.88	738.75	hc128
1237.81	1244.38	1246.88	hc256

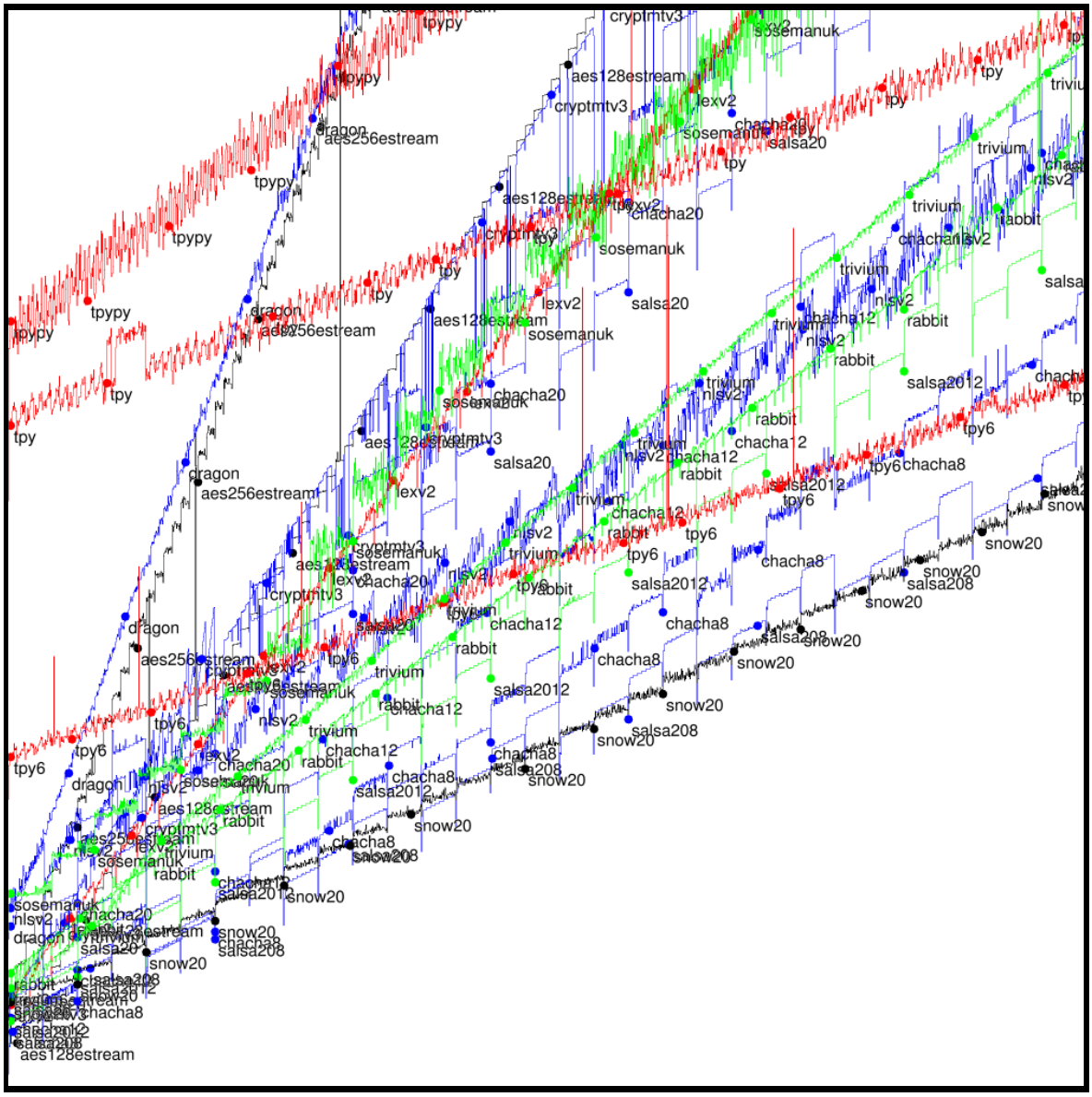
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.02	6.06	6.06	salsa208
6.80	6.80	6.82	chacha8
7.38	7.47	7.56	snow20
8.24	8.24	8.24	salsa2012
9.37	9.44	9.44	chacha12
10.82	10.83	10.85	rabbit
11.45	11.47	11.62	nlsv2
11.79	11.83	11.84	trivium
12.69	12.69	12.70	salsa20
13.66	13.66	14.03	chacha20
13.99	14.09	14.11	tpy6
16.53	16.62	16.70	lexv2
18.74	18.74	18.74	aes128estream
19.47	19.97	20.33	sosemanuk
22.77	22.92	23.76	cryptmtv3
24.24	24.75	24.76	tpy
30.97	30.98	31.47	aes256estream
30.73	31.13	31.25	dragon
31.79	31.97	32.35	tpypy
85.88	86.01	86.44	hc128
143.08	143.35	143.45	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
5.53	5.53	5.53	salsa208
5.79	5.95	5.99	snow20
7.05	7.05	7.05	chacha8
7.48	7.53	7.58	tpy6
7.59	7.59	7.59	salsa2012
8.79	8.81	8.84	nlsv2
8.81	8.81	8.81	rabbit
9.58	9.58	9.59	chacha12
10.27	10.27	10.30	trivium
11.61	11.70	11.78	tpy
11.81	11.81	11.82	salsa20
13.42	13.42	13.52	chacha20
13.57	14.02	14.17	sosemanuk
14.34	14.39	14.46	lexv2
18.12	18.12	18.13	aes128estream
18.21	18.31	18.41	tpypy
20.34	20.37	20.42	cryptmtv3
27.74	28.14	28.22	dragon
28.70	28.73	28.80	aes256estream
35.06	35.10	35.17	hc128
56.10	56.39	56.64	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
4.98	5.01	5.04	`tpy6`
5.22	5.38	5.41	`snow20`
5.39	5.40	5.40	`salsa208`
6.61	6.68	6.72	`tpy`
6.84	6.94	6.98	`chacha8`
7.48	7.48	7.48	`salsa2012`
7.70	7.70	7.71	`nlsv2`
8.02	8.03	8.04	`rabbit`
9.46	9.46	9.46	`chacha12`
9.48	9.49	9.49	`trivium`
11.70	11.70	11.70	`salsa20`
11.73	11.98	12.60	`sosemanuk`
13.05	13.16	13.47	`tpypy`
13.22	13.43	13.63	`chacha20`
13.61	13.66	13.89	`lexv2`
16.01	16.04	16.08	`hc128`
16.13	16.24	16.33	`cryptmtv3`
18.08	18.11	18.15	`aes128estream`
24.08	24.17	24.19	`hc256`
27.04	27.16	27.26	`dragon`
28.29	28.32	28.35	`aes256estream`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
3.39	3.50	3.59	`tpy6`
3.46	3.70	3.79	`tpy`
4.64	4.77	4.89	`hc128`
4.54	5.00	5.05	`hc256`
4.48	5.04	5.29	`snow20`
5.32	5.32	5.32	`salsa208`
6.44	6.87	7.09	`chacha8`
7.18	7.19	7.21	`nlsv2`
7.41	7.42	7.42	`salsa2012`
7.53	7.55	7.58	`rabbit`
8.99	9.01	9.02	`trivium`
9.38	9.38	9.86	`chacha12`
9.68	10.04	10.80	`tpypy`
10.31	11.11	12.36	`sosemanuk`
11.62	11.63	11.65	`salsa20`
13.05	13.25	13.75	`lexv2`
13.03	13.45	13.91	`chacha20`
13.07	13.71	13.97	`cryptmtv3`
3.31	18.19	18.27	`aes128estream`
25.99	26.57	26.89	`dragon`
27.56	27.73	27.84	`aes256estream`

7.37 x86, 2659MHz, Intel Xeon (f25), nmibuild26



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
100.00	100.00	100.00	aes128estream
124.00	125.00	125.00	salsa208
125.00	125.00	126.00	chacha8
149.00	150.50	151.00	salsa2012
155.50	157.50	158.00	chacha12
191.50	193.00	195.00	snow20
195.00	196.50	203.00	cryptmtv3
197.00	198.00	199.00	trivium
196.50	200.50	209.50	lexv2
200.00	202.00	203.00	salsa20
218.00	218.00	218.50	chacha20
225.00	228.50	231.00	aes256estream
264.50	267.50	270.50	rabbit
370.50	371.50	627.50	dragon
407.50	423.50	431.00	nlsv2
437.50	441.50	443.00	sosemanuk
757.00	760.50	774.00	tpy6
1567.00	1568.00	1574.50	tpy
1734.50	1737.00	1745.50	tpypy
5672.00	9708.00	9986.00	hc128
11878.00	11958.00	22565.50	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
10.81	12.69	13.06	salsa208
13.31	13.31	13.62	chacha8
13.94	16.06	17.38	salsa2012
15.88	18.19	18.31	chacha12
20.56	24.00	25.69	salsa20
24.12	24.44	25.31	snow20
25.69	25.69	25.69	aes128estream
28.00	28.00	28.06	chacha20
32.31	32.50	32.69	trivium
35.19	35.19	37.25	cryptmtv3
35.88	36.38	36.38	rabbit
37.31	38.00	38.50	lexv2
47.75	48.31	48.81	aes256estream
55.88	55.88	56.50	sosemanuk
68.06	68.38	70.12	nlsv2
69.06	69.81	70.75	dragon
97.69	98.44	138.00	tpy6
195.75	196.25	196.44	tpy
218.81	221.62	224.50	tpypy
708.50	1212.19	1240.25	hc128
1435.62	1448.38	1487.06	hc256

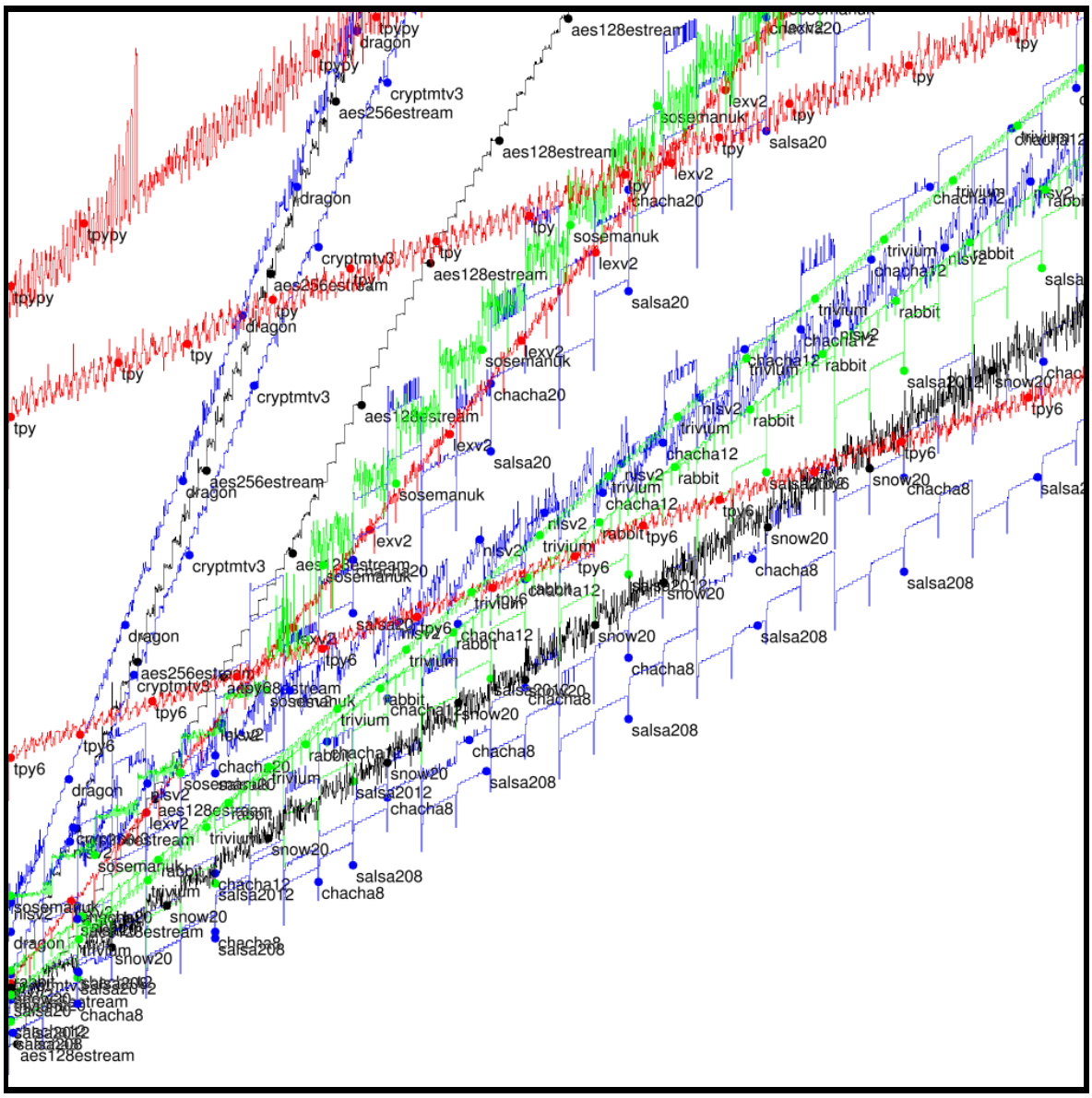
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.00	6.01	6.01	salsa208
6.68	6.70	6.96	chacha8
6.97	7.01	7.03	snow20
8.28	8.28	8.29	salsa2012
9.06	9.38	9.38	chacha12
10.73	10.78	10.86	rabbit
12.10	12.10	12.15	trivium
12.70	12.70	12.70	salsa20
13.40	13.47	13.70	nlsv2
13.67	13.92	13.99	tpy6
13.97	13.97	13.97	chacha20
16.15	16.24	16.26	lexv2
16.63	17.22	18.16	sosemanuk
18.66	18.66	18.67	aes128estream
18.06	19.03	19.05	cryptmtv3
25.03	25.05	25.10	tpy
29.85	29.90	30.03	aes256estream
31.39	31.72	31.96	tpypy
31.74	31.74	31.81	dragon
139.49	143.08	146.86	hc128
163.16	163.74	164.92	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
5.47	5.47	5.48	salsa208
5.75	5.78	5.88	snow20
6.96	6.97	6.97	chacha8
7.40	7.47	7.54	tpy6
7.61	7.61	7.61	salsa2012
8.77	8.78	8.79	rabbit
9.16	9.17	9.17	chacha12
9.22	9.23	9.24	nlsv2
9.97	9.97	9.97	trivium
11.62	11.66	11.73	tpy
11.80	11.81	11.81	salsa20
13.04	13.04	13.52	chacha20
13.34	13.71	14.39	sosemanuk
14.25	14.29	14.43	lexv2
16.54	16.74	16.76	tpypy
17.45	17.46	17.47	cryptmtv3
18.09	18.09	18.09	aes128estream
27.97	28.02	28.13	aes256estream
28.51	28.82	28.88	dragon
33.96	58.97	60.50	hc128
63.93	64.06	64.15	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
4.95	4.96	5.01	tpy6
5.21	5.23	5.24	snow20
5.36	5.36	5.36	salsa208
6.69	6.69	6.79	chacha8
6.64	6.70	6.73	tpy
7.48	7.48	7.48	salsa2012
7.77	7.79	7.83	nlsv2
8.11	8.12	8.14	rabbit
8.88	9.00	9.00	chacha12
9.18	9.18	9.18	trivium
11.04	11.08	11.24	tpypy
10.92	11.17	11.87	sosemanuk
11.70	11.71	11.71	salsa20
12.54	12.62	12.62	cryptmtv3
13.44	13.44	13.47	chacha20
13.58	13.76	13.78	lexv2
17.86	17.87	18.12	aes128estream
26.78	27.07	27.94	hc256
27.26	27.30	27.38	aes256estream
27.09	27.40	27.63	dragon
27.00	27.60	28.46	hc128

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
-1.56	3.31	3.54	tpy6
3.40	3.58	3.72	tpy
4.13	4.89	6.73	hc256
4.89	4.94	4.99	snow20
5.29	5.29	5.29	salsa208
5.62	5.94	7.59	rabbit
6.55	6.55	6.76	chacha8
7.26	7.34	7.40	nlsv2
7.41	7.42	7.42	salsa2012
7.53	7.81	8.21	tpypy
7.98	8.15	8.15	cryptmtv3
8.70	8.71	8.71	trivium
6.88	9.20	9.21	chacha12
7.12	9.49	30.98	hc128
8.31	9.60	11.75	sosemanuk
11.65	11.65	11.66	salsa20
13.49	13.49	13.92	chacha20
13.19	13.56	13.60	lexv2
17.72	17.73	18.25	aes128estream
25.93	26.71	27.60	dragon
26.77	26.91	27.07	aes256estream

7.38 x86, 2667MHz, Intel Xeon (f25), `nmi0036`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
100.00	100.00	100.50	aes128estream
124.50	126.00	126.00	chacha8
124.50	126.00	128.00	salsa208
150.00	150.50	151.00	salsa2012
155.00	156.00	156.00	chacha12
200.00	200.00	200.50	trivium
203.00	203.00	203.50	salsa20
215.00	215.50	215.50	chacha20
212.00	218.50	252.00	snow20
224.50	229.50	284.00	aes256estream
242.50	245.00	257.00	lexv2
264.00	264.50	264.50	cryptmtv3
275.50	276.50	283.50	rabbit
361.50	367.00	373.50	dragon
397.00	415.00	437.50	nlsv2
438.50	445.00	450.50	sosemanuk
776.00	783.00	792.50	tpy6
1592.00	1600.50	1607.50	tpy
1795.00	1818.50	1839.50	tpypy
5705.50	5723.00	6003.00	hc128
11532.00	11563.50	11612.50	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
10.94	11.00	13.25	chacha8
10.75	13.25	13.31	salsa208
16.81	17.44	17.44	salsa2012
14.75	18.00	18.19	chacha12
25.62	25.62	25.69	aes128estream
20.81	25.88	26.00	salsa20
26.69	27.19	27.56	snow20
23.12	27.50	27.69	chacha20
32.50	32.56	32.56	trivium
35.88	36.06	36.38	rabbit
40.88	41.06	41.38	lexv2
47.88	48.06	48.25	aes256estream
52.00	52.06	52.19	cryptmtv3
55.69	56.38	57.25	sosemanuk
69.12	69.69	72.81	dragon
69.25	69.75	69.88	nlsv2
99.38	99.62	100.00	tpy6
197.12	199.19	201.44	tpy
225.56	228.12	232.31	tpypy
710.81	716.12	720.94	hc128
1441.19	1444.31	1450.88	hc256

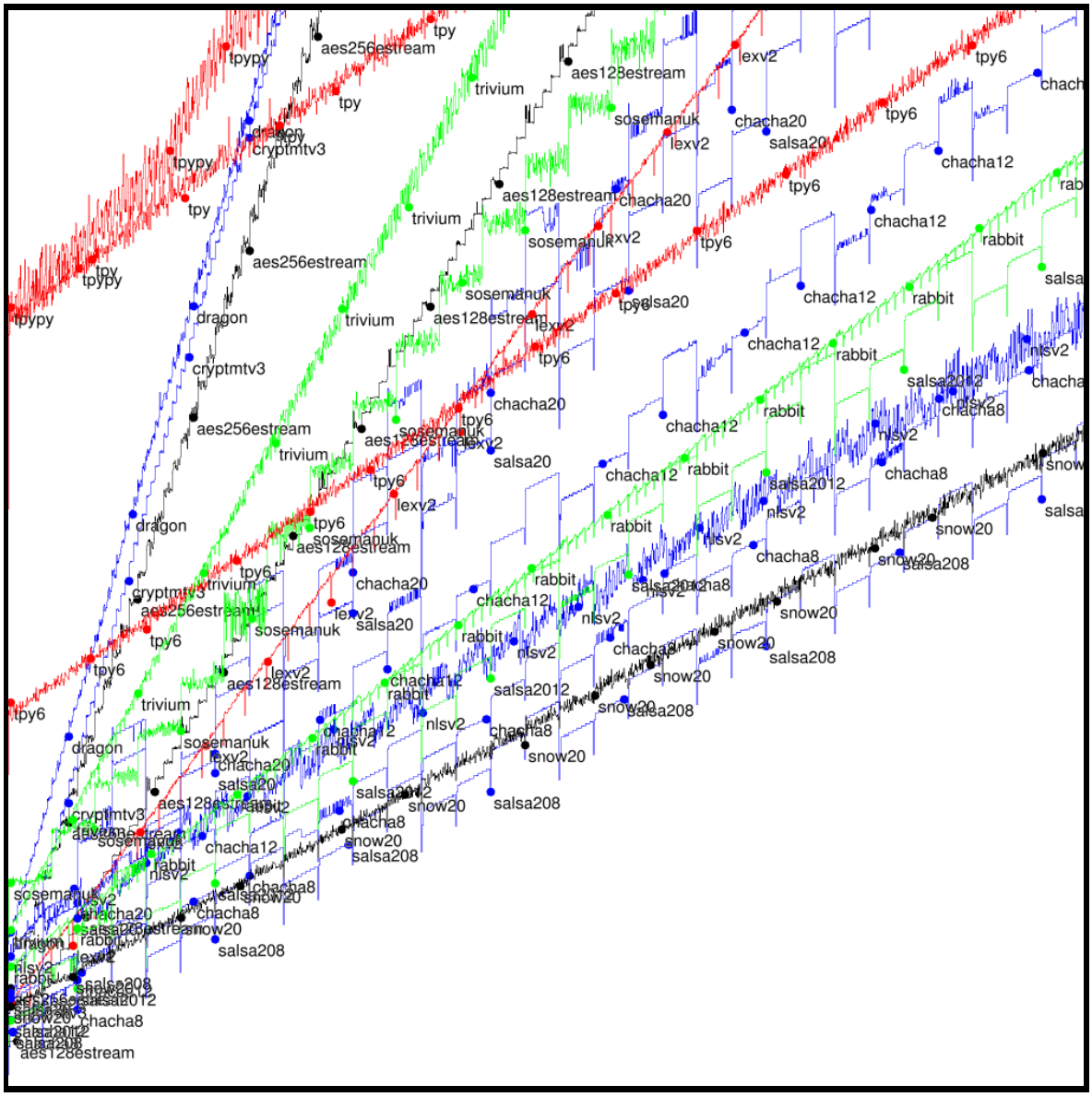
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.02	6.02	6.02	salsa208
6.62	6.62	6.62	chacha8
8.26	8.26	8.26	salsa2012
8.01	8.92	9.25	snow20
9.34	9.60	9.60	chacha12
10.74	10.83	10.87	rabbit
11.49	11.49	11.53	trivium
12.73	12.74	12.74	salsa20
13.05	13.05	13.54	nlsv2
13.97	14.02	14.15	tpy6
13.28	14.03	14.04	chacha20
15.66	15.81	16.05	lexv2
14.99	17.26	18.36	sosemanuk
18.97	18.97	18.98	aes128estream
25.38	25.47	25.56	tpy
27.12	27.13	27.22	cryptmtv3
30.01	30.07	30.12	aes256estream
31.46	31.52	32.06	dragon
32.45	32.69	32.83	tpypy
83.83	83.96	84.46	hc128
164.85	165.25	165.61	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
5.52	5.53	5.53	salsa208
6.51	6.51	6.51	chacha8
7.15	7.27	7.38	snow20
7.39	7.52	7.56	tpy6
7.64	7.64	7.65	salsa2012
8.79	8.81	8.84	rabbit
9.00	9.00	9.00	chacha12
9.49	9.49	9.49	nlsv2
9.68	9.69	9.69	trivium
11.85	11.86	11.86	salsa20
11.83	11.91	12.02	tpy
12.99	13.15	13.35	chacha20
12.67	13.49	14.46	sosemanuk
13.76	13.79	13.86	lexv2
17.29	17.49	17.59	tpypy
18.66	18.66	18.67	aes128estream
19.22	19.26	19.26	cryptmtv3
27.89	28.08	28.15	aes256estream
28.53	28.54	28.86	dragon
34.45	35.80	35.91	hc128
65.18	65.20	65.52	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
4.89	4.94	4.99	`tpy6`
5.40	5.40	5.40	`salsa208`
6.71	6.76	6.76	`chacha8`
6.49	6.81	6.92	`snow20`
6.79	6.81	6.88	`tpy`
7.50	7.51	7.51	`salsa2012`
7.86	7.87	7.91	`nlsv2`
8.04	8.05	8.05	`rabbit`
8.86	8.86	8.87	`chacha12`
9.00	9.00	9.01	`trivium`
10.89	11.29	11.95	`sosemanuk`
11.39	11.52	11.57	`tpypy`
11.72	11.72	11.73	`salsa20`
12.95	12.99	13.02	`lexv2`
13.01	13.01	13.03	`chacha20`
14.53	14.61	14.71	`cryptmtv3`
15.69	15.82	16.23	`hc128`
18.06	18.11	18.11	`aes128estream`
27.23	27.28	27.37	`aes256estream`
27.14	27.45	27.46	`dragon`
27.70	27.94	28.04	`hc256`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
3.21	3.36	3.54	`tpy6`
3.60	3.76	3.94	`tpy`
3.21	3.81	5.65	`hc128`
5.31	5.32	5.33	`salsa208`
4.76	5.43	5.84	`hc256`
5.81	6.62	6.98	`snow20`
6.89	6.99	6.99	`chacha8`
7.06	7.24	7.31	`nlsv2`
7.42	7.44	7.46	`salsa2012`
7.54	7.59	7.62	`rabbit`
7.59	8.02	8.34	`tpypy`
8.59	8.59	8.60	`trivium`
8.77	8.78	8.78	`chacha12`
7.72	9.82	11.64	`sosemanuk`
11.45	11.63	11.86	`cryptmtv3`
11.64	11.65	11.66	`salsa20`
12.28	12.44	12.69	`lexv2`
12.63	12.92	13.07	`chacha20`
17.61	17.71	17.85	`aes128estream`
25.93	26.79	26.84	`dragon`
26.69	26.83	27.16	`aes256estream`

7.39 x86, 2791MHz, Intel Xeon (f27), nmi0024



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
104.50	104.50	104.50	aes128estream
123.00	124.50	125.00	chacha8
122.50	125.50	127.00	salsa208
151.50	152.00	152.00	salsa2012
153.00	156.00	156.00	chacha12
182.50	183.00	186.50	snow20
195.50	197.00	206.00	lexv2
197.50	199.50	201.00	cryptmtv3
202.50	203.00	203.00	salsa20
213.50	213.50	215.50	chacha20
228.00	228.50	231.00	aes256estream
280.00	282.00	286.00	rabbit
298.00	304.00	333.50	nlsv2
351.00	353.50	355.50	trivium
354.00	356.00	369.00	dragon
470.50	474.50	479.00	sosemanuk
846.00	853.50	865.00	tpy6
1760.50	1779.00	1836.00	tpy
1755.00	1785.00	1796.00	tpypy
6210.00	6230.50	6315.00	hc128
11436.50	11437.00	11528.50	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
10.94	10.94	10.94	salsa208
11.19	11.19	13.31	chacha8
14.12	14.12	14.12	salsa2012
14.94	17.94	18.06	chacha12
22.44	22.44	22.56	chacha20
22.69	23.00	24.19	snow20
25.94	25.94	25.94	salsa20
26.19	26.19	26.19	aes128estream
36.94	37.50	37.62	lexv2
37.50	38.00	38.81	rabbit
51.50	51.94	54.69	aes256estream
49.69	54.81	54.81	nlsv2
54.75	55.12	55.12	cryptmtv3
58.69	59.25	60.19	sosemanuk
60.94	61.25	61.62	trivium
75.56	76.88	77.81	dragon
113.69	114.25	116.75	tpy6
220.50	225.38	227.94	tpypy
224.31	230.88	231.31	tpy
780.19	782.56	786.69	hc128
1432.50	1436.06	1441.81	hc256

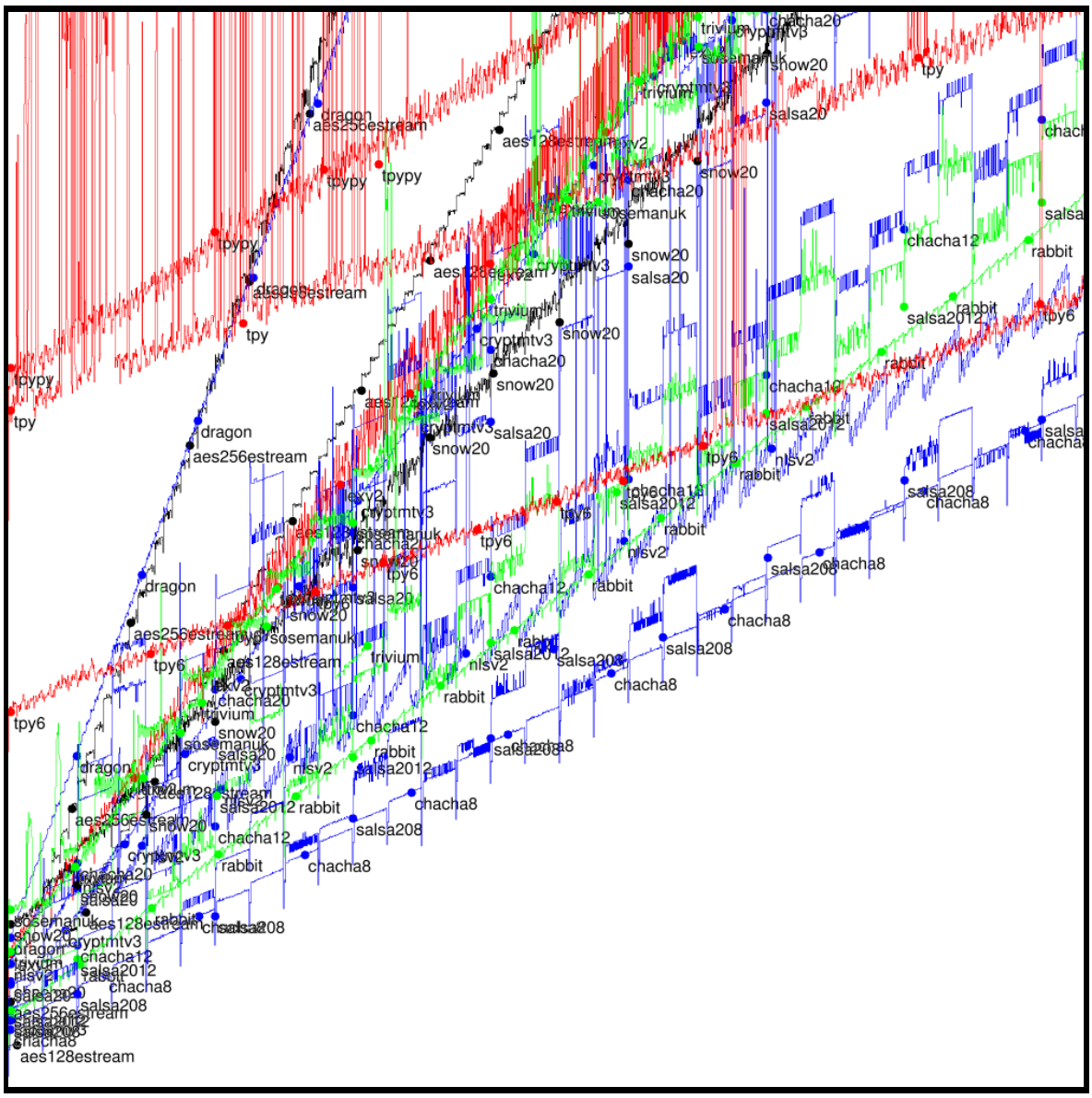
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
5.99	5.99	6.00	salsa208
7.22	7.23	7.23	chacha8
7.28	7.37	7.49	snow20
8.26	8.27	8.29	salsa2012
10.00	10.01	10.01	chacha12
10.15	10.42	10.59	nlsv2
10.95	10.97	11.02	rabbit
12.70	12.72	12.73	salsa20
13.79	14.31	14.31	chacha20
15.84	15.90	15.99	lexv2
18.61	18.73	18.83	tpy6
18.75	18.76	18.76	aes128estream
19.47	19.62	20.34	sosemanuk
23.02	23.43	23.57	trivium
31.17	31.81	31.87	tpy
33.69	34.28	34.60	aes256estream
36.31	37.05	37.33	tpypy
38.65	38.65	38.67	cryptmtv3
38.83	39.35	39.88	dragon
91.53	92.01	92.22	hc128
164.21	164.82	165.78	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
5.47	5.47	5.48	salsa208
6.03	6.06	6.17	snow20
6.64	6.66	6.66	chacha8
7.41	7.62	7.71	nlsv2
7.63	7.64	7.64	salsa2012
8.84	8.85	8.88	rabbit
9.45	9.45	9.45	chacha12
11.43	11.43	11.45	tpy6
11.83	11.84	11.84	salsa20
13.28	13.54	13.65	chacha20
14.09	14.16	14.20	lexv2
15.84	16.12	16.34	sosemanuk
16.31	16.33	16.36	tpy
18.12	18.12	18.12	aes128estream
20.57	20.57	20.59	trivium
20.93	21.86	21.92	tpypy
32.67	32.98	33.20	aes256estream
33.48	33.48	33.50	cryptmtv3
36.17	36.23	36.35	dragon
37.29	37.44	37.50	hc128
64.98	65.07	65.34	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.34	5.35	5.36	salsa208
5.62	5.66	5.71	snow20
6.36	6.36	6.36	nlsv2
6.51	6.53	6.54	chacha8
7.50	7.50	7.51	salsa2012
8.04	8.05	8.06	rabbit
8.60	8.70	8.75	tpy6
9.20	9.23	9.23	chacha12
10.45	10.57	10.59	tpy
11.81	11.82	11.83	salsa20
12.73	13.08	13.71	sosemanuk
12.91	13.12	13.47	chacha20
13.53	13.55	13.58	lexv2
14.56	14.61	14.75	tpypy
17.05	17.08	17.12	hc128
17.86	17.91	17.92	aes128estream
19.12	19.30	19.50	trivium
25.04	25.05	25.06	cryptmtv3
27.84	27.88	27.92	hc256
32.51	32.58	32.81	aes256estream
35.01	35.12	35.20	dragon

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
4.76	4.90	5.18	hc128
5.26	5.27	5.29	salsa208
5.28	5.40	5.53	snow20
5.21	5.58	5.70	hc256
5.65	5.80	5.80	nlsv2
6.43	6.47	6.50	chacha8
6.69	6.98	7.16	tpy6
6.77	7.04	7.21	tpy
7.41	7.42	7.43	salsa2012
7.52	7.55	7.57	rabbit
9.00	9.06	9.06	chacha12
10.20	10.43	10.80	tpypy
10.47	11.36	13.04	sosemanuk
11.84	11.84	11.88	salsa20
12.23	12.72	13.65	chacha20
13.07	13.16	13.27	lexv2
17.67	17.79	17.81	aes128estream
18.08	18.46	19.51	trivium
20.48	20.56	20.68	cryptmtv3
32.43	32.58	33.30	aes256estream
34.19	34.48	34.80	dragon

7.40 x86, 2800MHz, Intel Xeon (f41), `nmi0057`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
98.00	98.00	98.00	aes128estream
133.88	134.75	136.50	chacha8
154.88	154.88	155.75	salsa208
159.25	162.75	166.25	cryptmtv3
164.50	165.38	166.25	rabbit
177.62	178.50	179.38	salsa2012
181.12	181.12	182.00	chacha12
199.50	200.38	206.50	aes256estream
237.12	238.00	238.00	salsa20
245.00	245.00	246.75	chacha20
288.75	293.12	327.25	nlsv2
301.00	307.12	319.38	trivium
313.25	319.38	325.50	lexv2
357.00	358.75	360.50	dragon
371.00	382.38	400.75	snow20
412.12	415.62	422.62	sosemanuk
874.12	883.75	889.00	tpy6
1585.50	1591.62	2471.88	tpy
1617.88	1629.25	1666.00	tpypy
4123.88	4221.00	4242.00	hc128
18703.10	18992.80	19306.90	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
10.06	10.28	10.39	chacha8
12.91	13.02	13.02	salsa208
17.28	17.28	17.50	salsa2012
19.25	19.25	19.36	chacha12
25.05	25.16	25.38	rabbit
25.92	25.92	26.03	salsa20
26.14	26.25	26.25	aes128estream
29.86	29.97	30.08	chacha20
33.47	33.91	34.12	cryptmtv3
45.94	46.81	49.66	snow20
49.22	49.33	49.88	aes256estream
49.11	50.20	51.41	trivium
51.84	52.39	53.27	sosemanuk
50.09	52.83	55.89	lexv2
53.16	54.25	97.89	nlsv2
69.12	69.23	69.34	dragon
111.23	112.77	113.64	tpy6
197.64	198.52	309.75	tpy
206.06	206.72	213.83	tpypy
508.38	511.11	530.47	hc128
2340.08	2386.89	2398.48	hc256

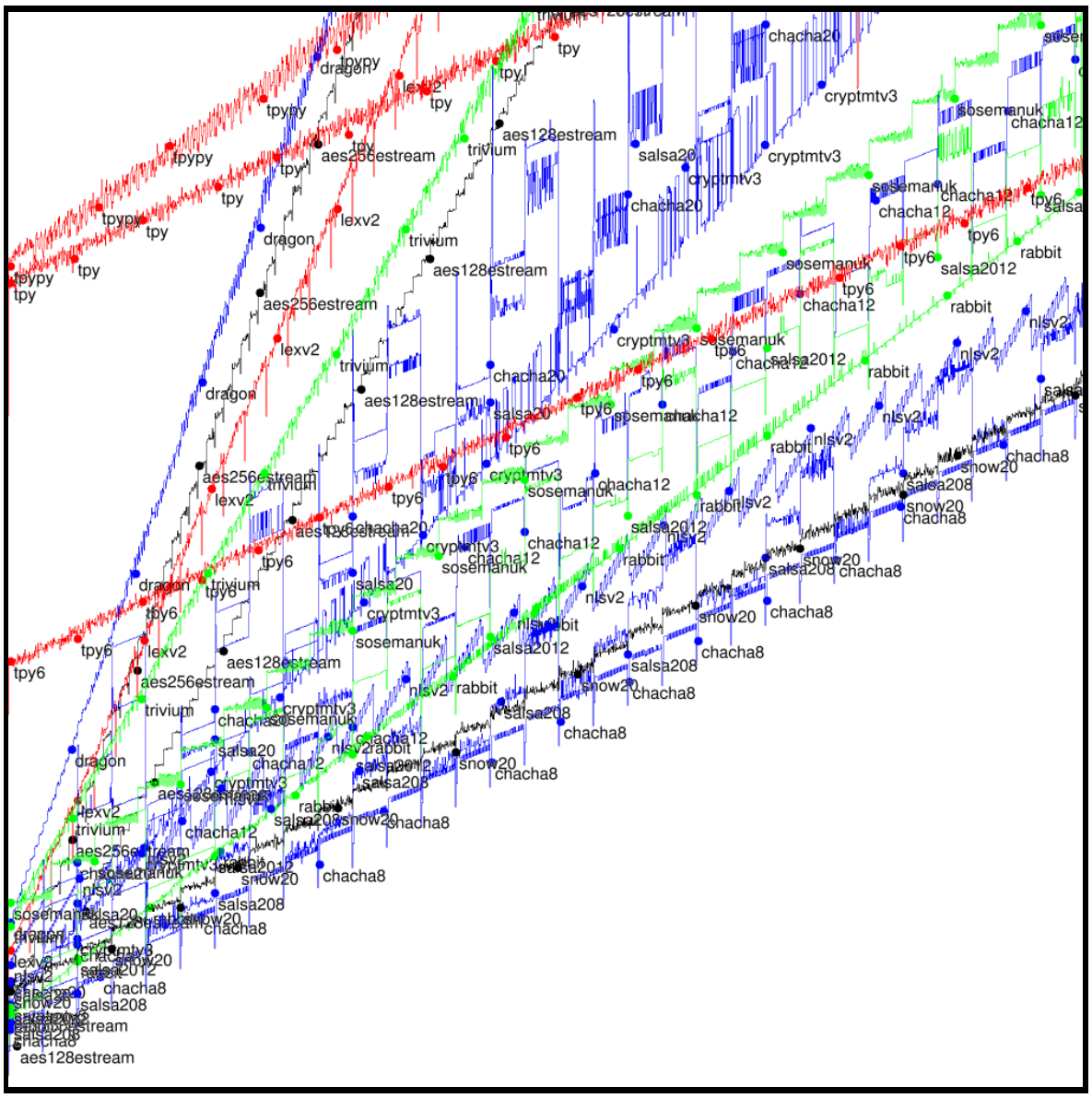
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.50	6.51	6.53	chacha8
6.27	7.04	7.04	salsa208
9.31	9.32	9.32	chacha12
8.90	9.44	9.44	salsa2012
9.65	9.66	9.67	rabbit
12.59	12.69	12.71	salsa20
14.05	14.06	14.07	chacha20
15.08	15.57	16.04	snow20
15.97	16.03	16.14	tpy6
16.70	16.76	16.88	cryptmtv3
12.65	17.79	18.03	trivium
18.05	18.17	26.69	sosemanuk
10.72	18.69	19.58	nlsv2
18.78	18.82	19.31	lexv2
19.77	19.78	19.89	aes128estream
25.70	25.93	37.09	tpy
28.61	28.89	29.52	tpypy
32.16	32.18	32.19	dragon
32.22	32.25	32.29	aes256estream
60.39	60.40	61.10	hc128
168.23	271.03	274.92	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
5.84	5.95	6.06	salsa208
6.11	6.12	6.12	chacha8
7.87	7.88	7.91	salsa2012
7.95	7.97	7.98	nlsv2
8.27	8.31	8.38	tpy6
8.37	8.37	8.38	rabbit
8.73	8.82	8.83	chacha12
11.80	11.83	11.89	tpy
11.75	11.87	11.88	salsa20
12.72	12.72	12.77	chacha20
12.96	13.29	13.54	snow20
14.19	14.21	14.26	sosemanuk
14.31	14.31	14.31	cryptmtv3
14.54	14.65	14.82	tpypy
10.72	15.02	15.40	trivium
15.21	15.69	16.71	lexv2
19.21	19.34	19.34	aes128estream
24.98	25.42	26.00	hc128
29.18	29.20	29.20	dragon
30.88	30.96	31.51	aes256estream
104.68	107.70	109.64	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.51	5.59	9.57	`tpy6`
5.73	5.81	5.84	`salsa208`
5.97	5.97	5.97	`chacha8`
6.65	6.66	6.68	`nlsv2`
7.89	7.89	7.89	`rabbit`
7.91	7.94	7.99	`salsa2012`
8.63	8.64	8.64	`chacha12`
9.50	9.58	9.68	`tpypy`
10.08	10.30	14.53	`trivium`
11.57	11.57	11.61	`cryptmtv3`
11.63	11.64	11.69	`salsa20`
7.05	11.81	12.48	`tpy`
11.69	11.97	12.16	`hc128`
11.91	12.16	12.43	`snow20`
12.54	12.55	12.58	`chacha20`
15.59	15.60	15.68	`lexv2`
19.08	19.13	19.16	`aes128estream`
12.85	20.04	26.16	`sosemanuk`
28.06	28.07	28.11	`dragon`
30.35	30.37	30.48	`aes256estream`
47.04	47.38	48.00	`hc256`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
2.67	3.50	4.42	`hc128`
0.03	3.87	11.90	`tpy6`
5.43	5.66	5.88	`salsa208`
5.88	5.89	5.89	`chacha8`
6.04	6.10	6.17	`nlsv2`
-0.42	6.41	6.76	`tpypy`
7.60	7.61	7.61	`rabbit`
7.63	7.98	8.09	`salsa2012`
8.52	8.60	8.61	`chacha12`
9.78	9.81	9.96	`cryptmtv3`
8.43	10.19	12.60	`hc256`
5.66	10.19	18.67	`trivium`
10.61	11.43	12.26	`snow20`
11.41	11.57	11.67	`salsa20`
12.38	12.39	12.53	`chacha20`
3.18	13.60	15.11	`tpy`
14.91	15.02	16.08	`lexv2`
18.91	19.00	19.19	`aes128estream`
12.09	26.60	38.92	`sosemanuk`
27.25	27.39	27.48	`dragon`
29.35	30.04	30.30	`aes256estream`

7.41 x86, 2800MHz, Intel Xeon (f41), nmi0063



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
96.25	97.12	98.00	aes128estream
131.25	132.12	141.75	chacha8
147.00	147.88	158.38	salsa208
168.88	169.75	169.75	rabbit
169.75	173.25	176.75	aes256estream
182.00	182.88	184.62	chacha12
181.12	183.75	184.62	salsa2012
191.62	196.00	205.62	cryptmtv3
226.62	231.88	235.38	snow20
238.00	238.88	238.88	salsa20
245.88	246.75	247.62	chacha20
292.25	293.12	295.75	nlsv2
317.62	330.75	344.75	lexv2
368.38	369.25	369.25	trivium
385.00	385.00	388.50	dragon
423.50	427.88	432.25	sosemanuk
973.00	980.88	986.12	tpy6
1859.38	1867.25	1873.38	tpy
1897.00	1932.00	1932.88	tpypy
4817.75	4834.38	4840.50	hc128
11272.60	11292.80	11527.20	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
9.95	10.06	10.17	chacha8
13.02	13.02	13.02	salsa208
17.50	17.50	17.83	salsa2012
19.47	19.58	19.69	chacha12
26.03	26.03	26.14	salsa20
26.25	26.25	26.36	aes128estream
26.14	26.47	27.34	rabbit
28.22	28.44	28.66	snow20
30.08	30.19	30.30	chacha20
30.19	31.28	31.94	cryptmtv3
40.91	41.23	41.89	aes256estream
52.83	52.94	53.05	nlsv2
53.81	54.47	55.45	sosemanuk
61.25	61.80	62.12	trivium
60.92	62.34	64.31	lexv2
73.94	74.16	74.27	dragon
124.58	126.88	128.08	tpy6
235.48	238.11	239.75	tpy
240.30	242.70	243.25	tpypy
601.78	603.75	604.95	hc128
1408.53	1412.91	1442.98	hc256

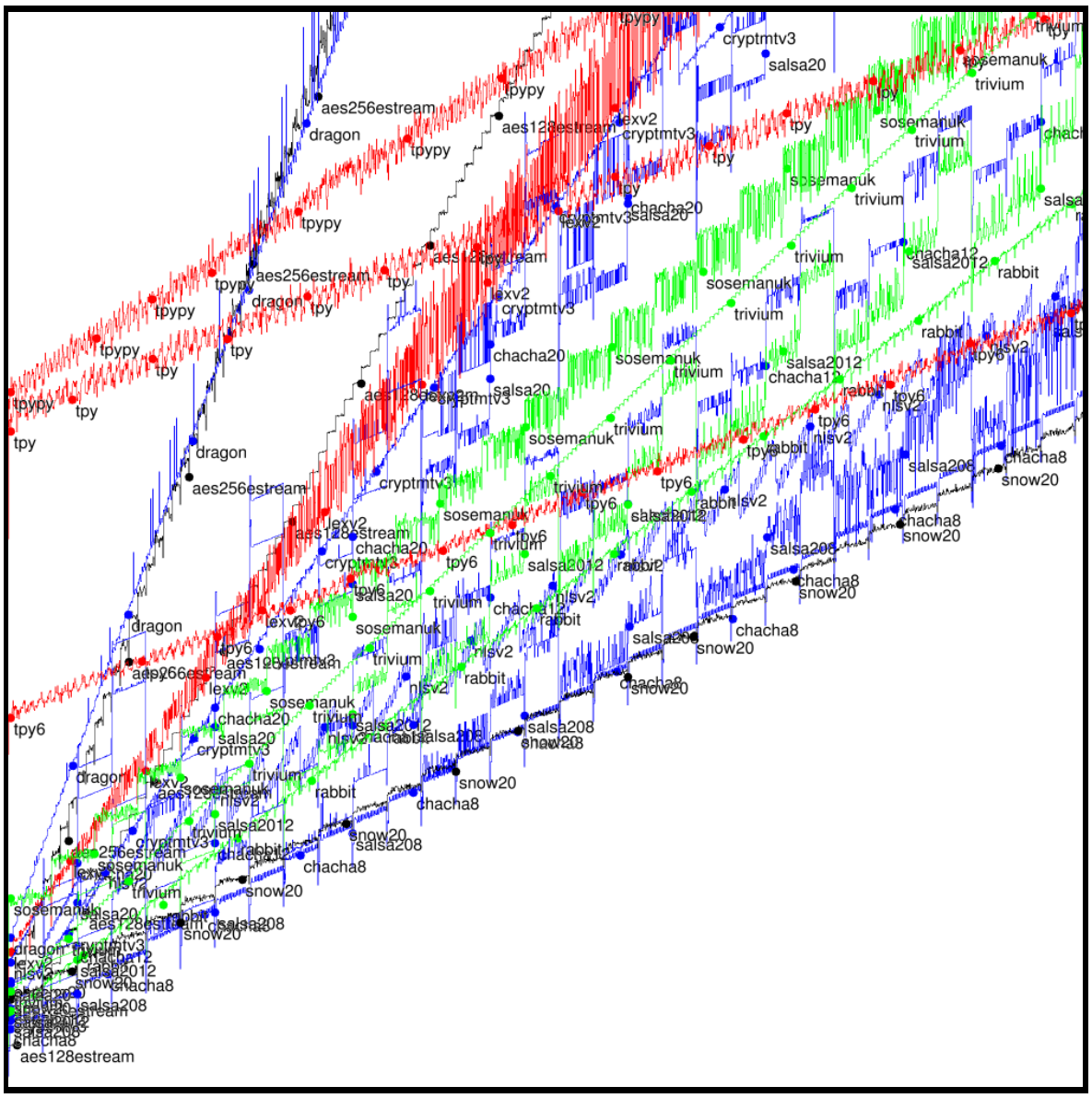
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.43	6.43	6.43	chacha8
6.40	6.44	6.95	salsa208
8.20	8.28	8.32	snow20
8.47	8.47	8.48	salsa2012
9.52	9.52	9.52	chacha12
9.81	9.94	10.00	rabbit
10.56	10.63	10.65	nlsv2
13.14	13.36	13.36	salsa20
13.43	13.64	13.65	cryptmtv3
13.81	13.81	13.81	chacha20
14.55	14.60	14.68	sosemanuk
18.12	18.33	18.33	tpy6
19.86	19.86	19.95	aes128estream
22.30	22.32	22.54	trivium
26.70	27.20	27.61	lexv2
30.35	30.44	30.49	aes256estream
30.69	30.89	30.98	tpy
32.82	32.93	32.97	tpypy
33.42	33.60	33.68	dragon
70.92	71.03	71.30	hc128
161.74	162.16	162.94	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
6.10	6.10	6.10	chacha8
6.64	6.67	6.74	snow20
6.47	6.75	7.36	salsa208
7.73	7.75	7.77	nlsv2
8.47	8.48	8.60	rabbit
8.57	8.58	8.58	salsa2012
8.69	8.69	8.87	chacha12
9.69	9.72	9.75	tpy6
10.92	10.96	11.00	sosemanuk
12.23	12.23	12.23	cryptmtv3
12.66	12.66	12.70	chacha20
12.77	12.77	12.77	salsa20
14.42	14.49	14.50	tpy
16.74	16.86	16.96	tpypy
19.22	19.22	19.26	trivium
19.30	19.30	19.30	aes128estream
11.73	23.94	24.68	lexv2
29.30	29.34	29.44	aes256estream
29.37	29.56	30.47	hc128
30.43	30.44	31.03	dragon
64.72	64.79	65.02	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.97	5.97	5.97	chacha8
6.14	6.16	6.16	snow20
6.34	6.44	7.48	salsa208
6.52	6.52	6.53	nlsv2
6.53	6.54	6.65	tpy6
7.96	7.97	7.97	salsa2012
8.04	8.04	8.04	rabbit
8.36	8.44	8.52	tpy
8.46	8.48	8.48	cryptmtv3
8.52	8.66	8.66	chacha12
9.66	9.68	9.73	sosemanuk
10.70	10.76	10.76	tpypy
12.40	12.40	12.40	salsa20
12.49	12.50	12.51	chacha20
13.80	13.85	14.03	hc128
18.07	18.07	18.07	trivium
19.13	19.13	19.17	aes128estream
22.80	23.05	23.39	lexv2
28.18	28.26	28.50	hc256
29.17	29.17	29.23	aes256estream
29.24	29.35	29.83	dragon

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
3.79	3.82	4.50	cryptmtv3
4.28	4.50	4.90	hc128
4.49	4.55	4.85	tpy6
4.79	5.04	5.21	tpy
5.79	5.87	5.96	snow20
5.87	5.87	5.88	chacha8
5.92	5.94	5.97	nlsv2
5.24	6.25	8.54	salsa208
5.36	6.32	6.85	hc256
7.05	7.27	7.30	tpypy
7.38	7.38	7.39	salsa2012
7.78	7.78	7.79	rabbit
8.26	8.53	8.69	chacha12
8.96	9.05	9.19	sosemanuk
12.17	12.17	12.18	salsa20
12.37	12.41	12.42	chacha20
17.38	17.38	17.44	trivium
19.04	19.06	19.13	aes128estream
21.63	22.41	23.43	lexv2
28.34	28.72	29.80	dragon
29.00	29.05	29.19	aes256estream

7.42 x86, 2801MHz, Intel Xeon (f41), `nmi0060`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
97.12	97.12	98.00	aes128estream
130.38	136.50	141.75	chacha8
154.00	154.00	154.88	salsa208
171.50	172.38	174.12	cryptmtv3
168.88	173.25	179.38	rabbit
175.88	176.75	184.62	salsa2012
182.00	182.00	182.88	chacha12
199.50	203.88	206.50	aes256estream
206.50	210.00	213.50	snow20
214.38	217.00	217.88	trivium
238.88	239.75	239.75	salsa20
244.12	245.00	245.88	chacha20
294.88	300.12	302.75	nlsv2
314.12	321.12	329.88	lexv2
350.88	352.62	357.88	dragon
415.62	421.75	433.12	sosemanuk
875.88	880.25	886.38	tpy6
1554.00	1557.50	1561.88	tpy
1592.50	1617.88	1632.75	tpypy
4187.75	4351.38	4361.88	hc128
12104.80	12147.60	12182.60	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
9.84	10.06	10.17	chacha8
12.91	12.91	13.02	salsa208
17.50	17.61	17.61	salsa2012
19.14	19.25	19.25	chacha12
25.81	25.92	25.92	salsa20
25.70	26.03	26.36	snow20
26.25	26.25	26.36	aes128estream
26.47	26.80	27.12	rabbit
29.75	29.86	29.97	chacha20
32.81	32.92	32.92	cryptmtv3
35.77	35.88	35.88	trivium
48.02	50.20	52.06	aes256estream
52.06	53.27	53.59	lexv2
53.05	53.38	53.92	nlsv2
53.27	54.14	55.67	sosemanuk
69.02	69.45	69.56	dragon
111.12	112.00	112.88	tpy6
195.56	197.31	197.42	tpy
203.55	203.77	206.17	tpypy
544.47	545.02	546.44	hc128
1512.55	1512.77	1519.77	hc256

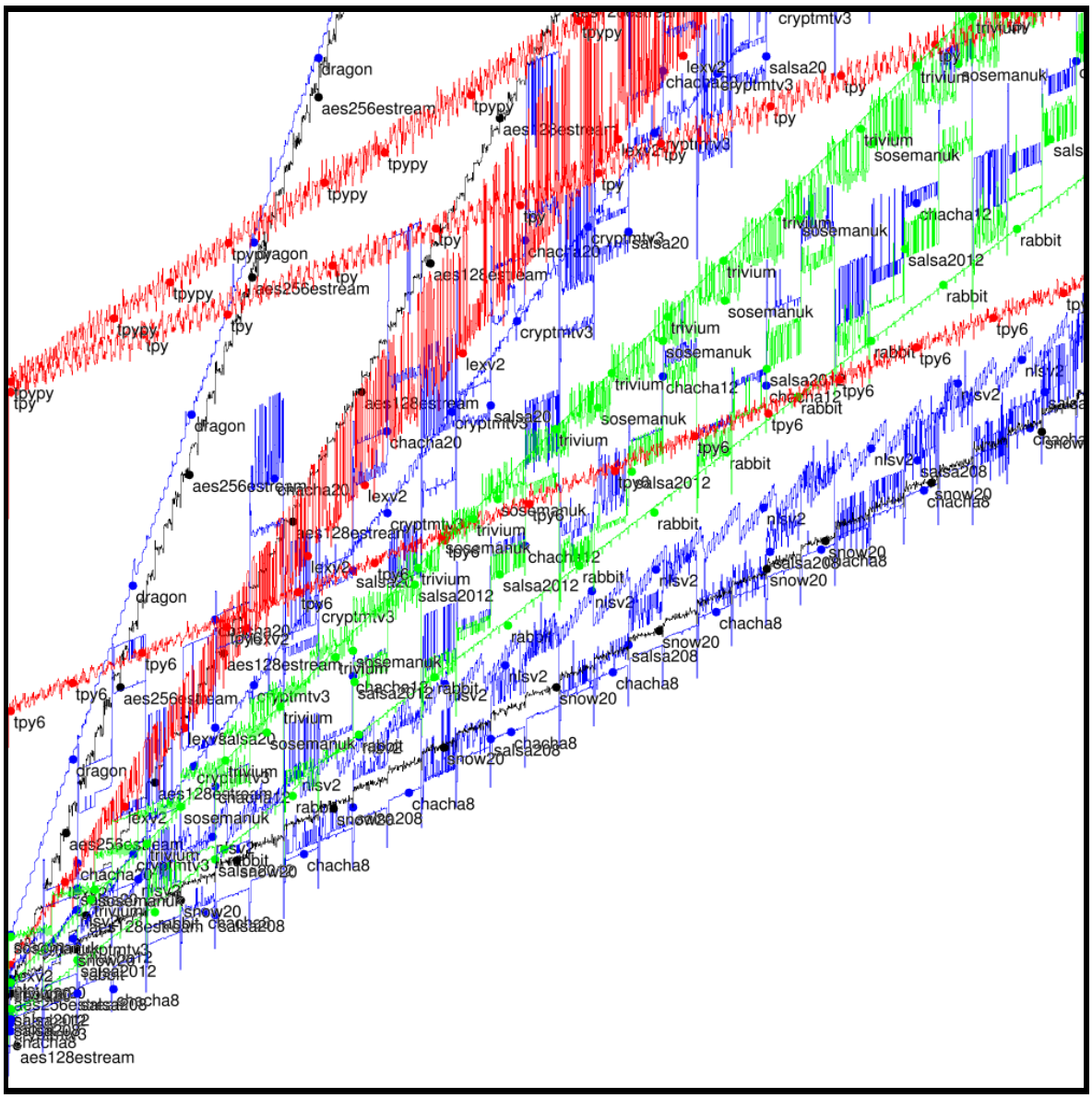
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.48	6.53	6.56	chacha8
6.55	6.56	7.68	salsa208
7.68	7.70	7.72	snow20
8.99	9.02	9.05	chacha12
8.68	9.84	9.86	salsa2012
9.76	9.86	9.88	rabbit
10.69	10.74	10.89	nlsv2
12.57	12.58	12.58	trivium
13.36	13.67	13.68	salsa20
13.79	13.81	13.81	chacha20
15.11	15.39	15.58	sosemanuk
15.66	15.79	15.85	tpy6
16.87	16.89	17.04	cryptmtv3
18.44	19.41	19.48	lexv2
19.83	19.85	19.86	aes128estream
25.45	25.56	25.70	tpy
28.24	28.33	28.79	tpypy
31.86	31.99	32.79	aes256estream
32.20	32.22	32.23	dragon
61.63	61.72	64.07	hc128
172.85	173.71	173.88	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
5.90	6.04	6.33	salsa208
6.10	6.10	6.12	chacha8
6.29	6.34	6.35	snow20
7.88	7.89	7.93	nlsv2
8.07	8.10	8.21	salsa2012
8.24	8.28	8.37	tpy6
8.43	8.45	8.46	rabbit
8.61	8.76	8.84	chacha12
10.69	10.69	10.70	trivium
11.82	11.84	11.87	sosemanuk
11.73	11.87	11.89	tpy
12.28	12.29	12.31	salsa20
12.82	13.06	13.06	chacha20
14.29	14.31	14.32	cryptmtv3
14.63	14.68	14.79	tpypy
15.35	15.43	15.48	lexv2
19.39	19.40	19.48	aes128estream
26.48	26.48	26.53	hc128
29.21	29.21	29.22	dragon
30.61	31.12	31.56	aes256estream
68.27	68.30	68.48	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.45	5.48	5.51	`tpy6`
5.79	5.80	5.81	`snow20`
5.96	5.96	5.96	`chacha8`
6.63	6.65	6.66	`nlsv2`
6.46	6.83	6.89	`salsa208`
6.91	6.95	7.00	`tpy`
7.91	7.91	7.92	`rabbit`
8.02	8.04	8.44	`salsa2012`
8.56	8.67	8.69	`chacha12`
9.55	9.56	9.61	`tpypy`
9.98	9.99	9.99	`trivium`
10.35	10.51	10.65	`sosemanuk`
11.59	11.60	11.62	`cryptmtv3`
12.06	12.10	12.11	`hc128`
12.20	12.20	12.45	`salsa20`
12.59	12.76	12.82	`chacha20`
14.26	14.29	16.14	`lexv2`
19.17	19.18	19.22	`aes128estream`
28.07	28.07	28.07	`dragon`
29.05	29.12	29.20	`hc256`
30.30	30.33	30.61	`aes256estream`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
3.25	3.40	3.60	`hc128`
3.75	3.83	3.91	`tpy6`
3.77	3.98	4.15	`tpy`
5.50	5.52	5.56	`snow20`
5.24	5.53	5.77	`hc256`
5.87	5.88	5.89	`chacha8`
6.03	6.14	6.19	`nlsv2`
6.30	6.45	6.60	`tpypy`
6.12	6.86	7.65	`salsa208`
7.62	7.63	7.64	`rabbit`
7.83	8.04	8.84	`salsa2012`
7.88	8.59	8.71	`chacha12`
9.56	9.56	9.57	`trivium`
9.44	9.80	10.13	`sosemanuk`
9.81	9.84	9.92	`cryptmtv3`
11.77	12.10	12.61	`salsa20`
12.41	12.75	12.87	`chacha20`
12.29	13.48	17.32	`lexv2`
18.99	19.03	19.14	`aes128estream`
27.40	27.41	27.42	`dragon`
29.88	30.14	30.75	`aes256estream`

7.43 x86, 2801MHz, Intel Xeon (f41), nmi0061



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
98.00	98.88	98.88	aes128estream
128.62	133.00	136.50	chacha8
154.00	158.38	161.00	cryptmtv3
160.12	161.00	163.62	salsa208
165.38	172.38	174.12	rabbit
181.12	181.12	182.00	chacha12
182.88	183.75	183.75	salsa2012
209.12	223.12	228.38	aes256estream
230.12	230.12	231.00	trivium
236.25	238.00	238.88	salsa20
245.00	245.00	247.62	chacha20
253.75	253.75	259.88	snow20
254.62	274.75	282.62	nlsv2
291.38	293.12	296.62	lexv2
350.88	352.62	353.50	sosemanuk
358.75	360.50	362.25	dragon
889.00	896.88	897.75	tpy6
1606.50	1627.50	1639.75	tpypy
1629.25	1636.25	1638.00	tpy
4455.50	4489.62	4489.62	hc128
21759.50	21973.00	22134.00	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
10.06	10.17	10.39	chacha8
13.12	13.23	13.23	salsa208
17.28	17.39	17.50	salsa2012
19.25	19.25	19.25	chacha12
25.81	25.92	27.23	rabbit
25.92	25.92	26.03	salsa20
26.25	26.36	26.47	aes128estream
29.86	29.86	29.97	chacha20
30.08	30.30	30.41	cryptmtv3
32.05	32.59	33.25	snow20
38.61	38.61	38.61	trivium
44.08	44.30	46.16	nlsv2
44.08	45.06	46.16	sosemanuk
50.09	51.19	51.52	aes256estream
51.08	51.73	52.61	lexv2
70.77	70.88	71.97	dragon
111.34	113.31	114.62	tpy6
204.97	205.41	207.05	tpy
207.27	208.47	208.91	tpypy
554.75	561.20	561.20	hc128
2703.97	2728.91	2754.94	hc256

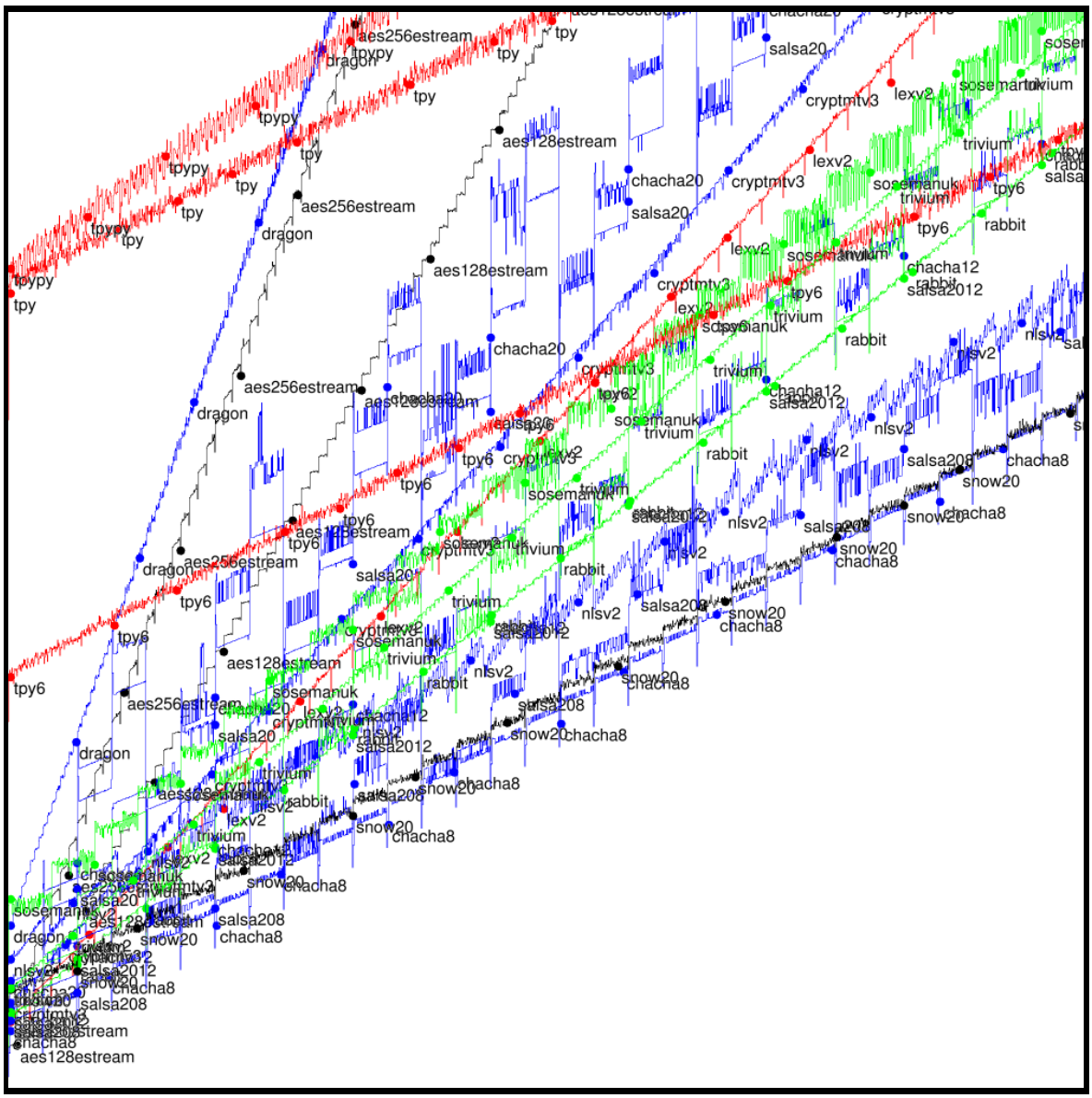
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.42	6.43	6.44	chacha8
6.74	6.76	6.76	salsa208
8.54	8.63	8.68	snow20
8.75	8.96	8.96	salsa2012
9.02	9.13	9.19	chacha12
9.94	10.03	10.07	nlsv2
10.17	10.23	10.24	rabbit
12.95	13.27	13.31	salsa20
13.33	13.33	13.34	trivium
13.77	13.79	13.90	chacha20
13.89	14.39	14.46	sosemanuk
15.49	15.57	15.65	cryptmtv3
16.07	16.10	16.41	tpy6
17.34	17.77	20.55	lexv2
19.89	19.89	19.91	aes128estream
25.98	26.34	26.38	tpy
28.07	28.43	29.25	tpypy
31.88	31.97	32.11	aes256estream
33.21	33.24	34.53	dragon
64.46	64.75	65.31	hc128
311.88	313.95	318.18	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
6.08	6.08	6.08	chacha8
5.92	6.37	6.42	salsa208
6.59	6.66	6.68	snow20
7.42	7.45	7.53	nlsv2
7.60	8.37	8.37	salsa2012
8.43	8.53	8.59	tpy6
8.48	8.61	8.61	chacha12
8.64	8.65	8.65	rabbit
11.29	11.29	11.29	trivium
10.85	11.44	11.47	sosemanuk
12.07	12.09	12.11	tpy
12.13	12.14	12.84	salsa20
12.63	12.63	12.65	chacha20
13.80	13.82	13.86	cryptmtv3
14.70	14.72	14.79	tpypy
15.81	17.93	18.01	lexv2
19.33	19.37	19.40	aes128estream
26.77	26.85	27.19	hc128
30.28	30.29	30.53	dragon
30.51	30.52	30.60	aes256estream
123.58	124.64	125.88	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.66	5.69	5.72	tpy6
5.81	5.81	6.18	salsa208
5.95	5.96	5.96	chacha8
5.90	5.96	5.98	snow20
6.34	6.34	6.35	nlsv2
6.90	6.93	6.94	tpy
7.98	7.98	7.98	salsa2012
8.04	8.04	8.05	rabbit
8.49	8.52	8.52	chacha12
9.44	9.55	9.58	tpypy
9.77	9.78	10.34	sosemanuk
10.52	10.52	10.53	trivium
11.70	11.71	11.76	cryptmtv3
11.80	11.82	11.83	salsa20
12.47	12.47	12.47	chacha20
12.59	12.65	12.70	hc128
14.56	14.59	14.61	lexv2
19.10	19.13	19.15	aes128estream
29.17	29.18	29.29	dragon
30.10	30.12	30.15	aes256estream
53.80	54.00	54.27	hc256

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
3.76	3.84	3.91	tpy
3.82	3.94	4.06	tpy6
3.95	4.17	4.31	hc128
5.24	5.25	5.98	salsa208
5.40	5.58	5.66	snow20
5.72	5.78	5.82	nlsv2
5.87	5.88	5.88	chacha8
6.04	6.50	6.63	tpypy
7.66	7.68	7.72	rabbit
7.56	7.89	7.90	salsa2012
8.37	8.48	8.70	chacha12
9.09	9.15	10.29	sosemanuk
10.06	10.07	10.08	trivium
10.06	10.13	10.25	cryptmtv3
10.48	11.35	12.98	hc256
11.50	11.57	11.63	salsa20
12.36	12.37	12.39	chacha20
12.83	14.52	14.68	lexv2
18.88	19.04	19.17	aes128estream
28.25	28.44	28.74	dragon
29.85	29.91	30.13	aes256estream

7.44 x86, 2801MHz, Intel Xeon (f41), `nmi0062`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
98.88	100.62	173.25	aes128estream
132.12	132.12	132.12	chacha8
154.88	154.88	155.75	salsa208
156.62	160.12	161.88	lexv2
162.75	163.62	165.38	aes256estream
168.00	168.00	168.88	rabbit
174.12	175.00	175.88	salsa2012
182.88	183.75	183.75	chacha12
186.38	200.38	204.75	cryptmtv3
226.62	227.50	229.25	trivium
217.00	228.38	240.62	snow20
231.00	231.00	232.75	salsa20
246.75	246.75	247.62	chacha20
298.38	300.12	302.75	nlsv2
378.00	378.88	383.25	dragon
398.12	402.50	409.50	sosemanuk
947.62	954.62	959.88	tpy6
1866.38	1880.38	1890.00	tpy
1876.88	1888.25	1906.62	tpypy
4697.88	4733.75	4811.62	hc128
12114.40	12130.10	12188.80	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
9.95	10.06	10.17	chacha8
13.02	13.02	13.12	salsa208
17.28	17.28	17.39	salsa2012
19.47	19.47	19.69	chacha12
26.14	26.14	26.36	salsa20
26.25	26.25	47.14	aes128estream
27.12	27.23	28.22	rabbit
26.69	27.56	28.66	snow20
29.42	29.86	30.08	lexv2
30.08	30.19	30.19	chacha20
28.88	30.73	30.95	cryptmtv3
35.98	36.20	36.31	trivium
39.59	40.14	40.25	aes256estream
49.22	49.44	49.55	nlsv2
54.25	55.02	56.00	sosemanuk
72.62	73.28	73.61	dragon
124.80	125.45	126.44	tpy6
236.69	237.02	240.52	tpy
237.56	240.30	240.41	tpypy
590.95	591.72	608.56	hc128
1490.89	1515.06	1537.59	hc256

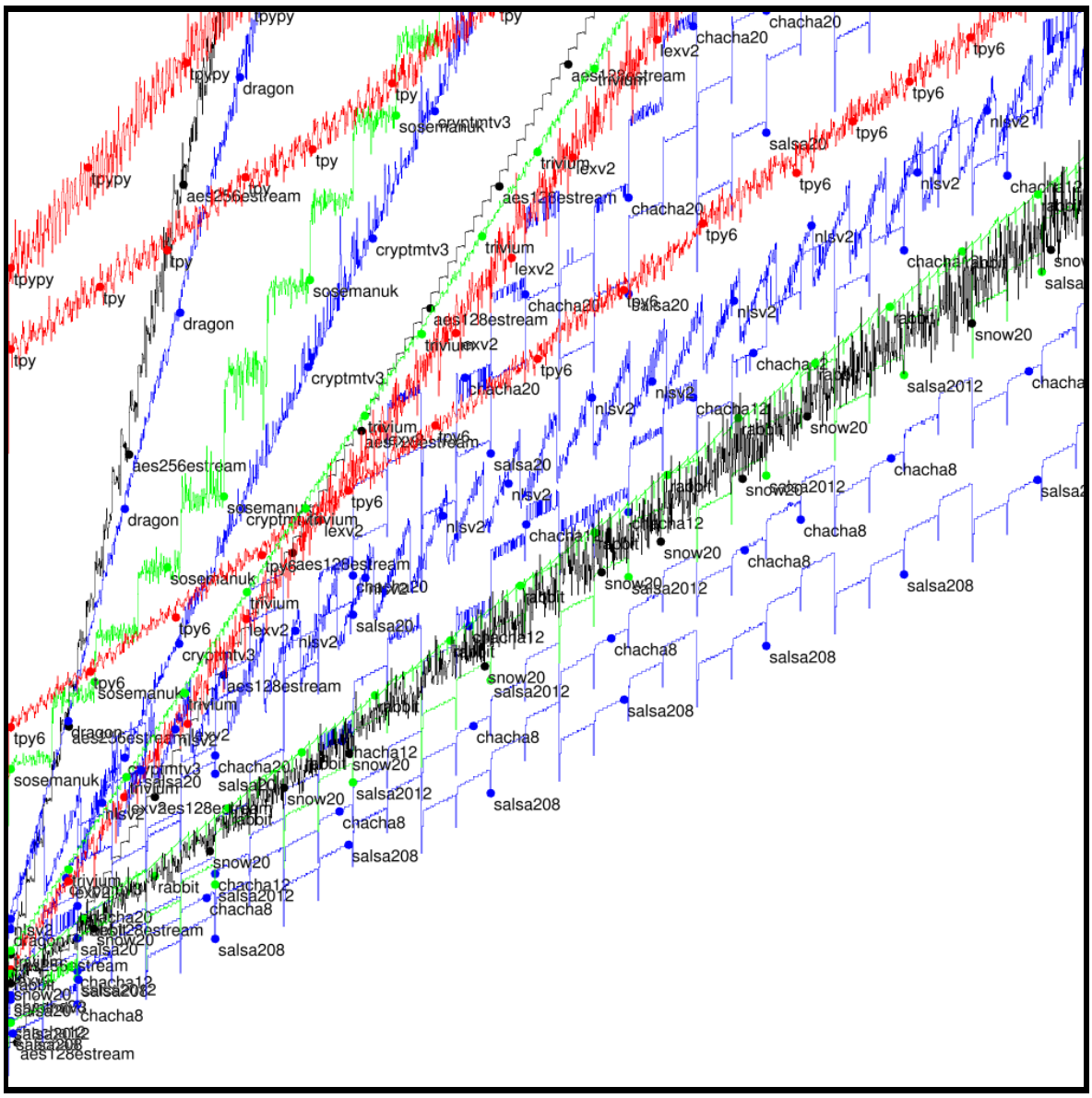
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.43	6.45	6.47	chacha8
6.64	7.32	8.03	salsa208
7.89	7.94	8.58	snow20
9.24	9.25	9.25	salsa2012
9.48	9.49	9.60	chacha12
10.27	10.35	10.40	nlsv2
10.48	10.50	10.50	rabbit
12.13	12.14	12.15	trivium
13.14	13.22	13.26	lexv2
13.02	13.62	13.79	salsa20
13.65	13.66	13.94	cryptmtv3
14.10	14.50	14.51	chacha20
14.34	14.55	14.68	sosemanuk
18.38	18.44	18.84	tpy6
19.86	19.86	19.89	aes128estream
30.09	30.13	30.18	aes256estream
30.72	30.93	31.33	tpy
32.41	33.07	33.12	tpypy
33.04	33.07	33.15	dragon
70.45	70.89	72.02	hc128
174.61	175.19	175.85	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
6.09	6.09	6.09	chacha8
6.43	6.43	7.00	salsa208
6.51	6.55	6.61	snow20
7.86	7.87	7.90	nlsv2
8.86	8.87	8.90	chacha12
8.89	8.89	9.05	salsa2012
9.09	9.12	15.07	rabbit
9.96	10.09	10.20	tpy6
10.18	10.19	10.19	trivium
10.60	10.64	10.68	sosemanuk
11.70	11.71	11.77	lexv2
12.46	12.50	12.56	cryptmtv3
12.71	12.74	12.74	chacha20
12.91	13.01	13.01	salsa20
14.61	14.67	15.00	tpy
16.57	16.62	16.78	tpypy
19.28	19.28	19.30	aes128estream
29.26	29.29	29.38	aes256estream
28.98	29.57	29.81	hc128
29.89	29.91	29.91	dragon
69.74	70.28	70.84	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.96	5.96	5.97	`chacha8`
5.97	6.01	6.01	`snow20`
6.33	6.41	6.58	`salsa208`
6.67	6.69	6.70	`nlsv2`
6.89	6.92	6.97	`tpy6`
8.57	8.57	8.57	`rabbit`
8.60	8.66	8.66	`chacha12`
8.63	8.66	8.82	`tpy`
8.68	8.72	8.73	`salsa2012`
8.89	8.90	9.43	`cryptmtv3`
9.25	9.27	9.29	`sosemanuk`
9.45	9.45	9.46	`trivium`
10.60	10.62	10.64	`tpypy`
11.29	11.30	11.30	`lexv2`
11.99	12.00	12.49	`salsa20`
12.51	12.54	12.65	`chacha20`
13.61	13.94	13.96	`hc128`
19.10	19.15	19.19	`aes128estream`
28.58	28.68	28.70	`dragon`
29.09	29.15	29.16	`aes256estream`
30.52	30.64	30.71	`hc256`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
3.76	4.82	5.10	`hc128`
4.88	4.98	5.15	`tpy6`
4.98	5.08	5.43	`tpy`
5.19	5.27	6.34	`cryptmtv3`
5.62	5.73	5.74	`snow20`
5.88	5.89	5.91	`chacha8`
5.99	6.09	6.12	`nlsv2`
5.96	6.42	6.76	`salsa208`
6.46	6.93	7.92	`hc256`
6.88	7.05	7.22	`tpypy`
8.09	8.15	8.61	`sosemanuk`
8.22	8.25	8.25	`rabbit`
8.40	8.69	8.80	`chacha12`
8.57	8.72	8.72	`salsa2012`
8.99	9.00	9.02	`trivium`
11.09	11.12	11.14	`lexv2`
11.18	11.19	12.17	`salsa20`
12.35	12.41	12.68	`chacha20`
18.87	19.07	19.17	`aes128estream`
27.73	27.98	28.10	`dragon`
28.97	29.09	29.17	`aes256estream`

7.45 x86, 2802MHz, Intel Xeon (f29), `nmibuild40`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
104.50	104.50	106.00	aes128estream
123.00	124.00	128.50	chacha8
123.50	124.50	126.50	salsa208
148.00	149.00	151.00	salsa2012
153.50	153.50	154.00	chacha12
202.50	202.50	203.00	salsa20
209.00	210.50	213.50	cryptmtv3
213.50	214.00	215.00	chacha20
232.00	259.00	271.00	snow20
268.00	268.00	268.00	rabbit
268.00	273.50	277.00	lexv2
298.50	309.00	340.00	aes256estream
306.50	309.00	314.50	trivium
371.50	375.00	376.50	dragon
412.50	420.00	445.00	nlsv2
748.50	755.00	757.50	sosemanuk
852.50	862.50	872.50	tpy6
1739.00	1752.50	1755.00	tpy
1860.50	1868.50	1930.50	tpypy
6692.00	6795.50	6797.00	hc128
11871.00	11955.50	12055.00	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
13.06	13.06	13.06	salsa208
13.25	13.31	13.50	chacha8
14.25	17.31	17.44	salsa2012
18.25	18.25	18.25	chacha12
25.75	25.75	25.75	salsa20
26.25	26.31	26.31	aes128estream
27.75	27.75	27.75	chacha20
27.94	31.06	36.56	snow20
36.19	36.19	36.50	rabbit
44.12	44.25	44.38	cryptmtv3
47.88	48.19	49.69	lexv2
51.25	52.00	52.00	trivium
69.81	69.81	69.81	aes256estream
73.00	73.38	82.06	nlsv2
80.25	81.62	82.19	dragon
96.62	97.44	97.88	sosemanuk
108.50	111.88	112.81	tpy6
214.38	215.75	217.69	tpy
236.12	238.31	239.06	tpypy
827.06	828.44	828.50	hc128
1496.19	1514.31	1536.56	hc256

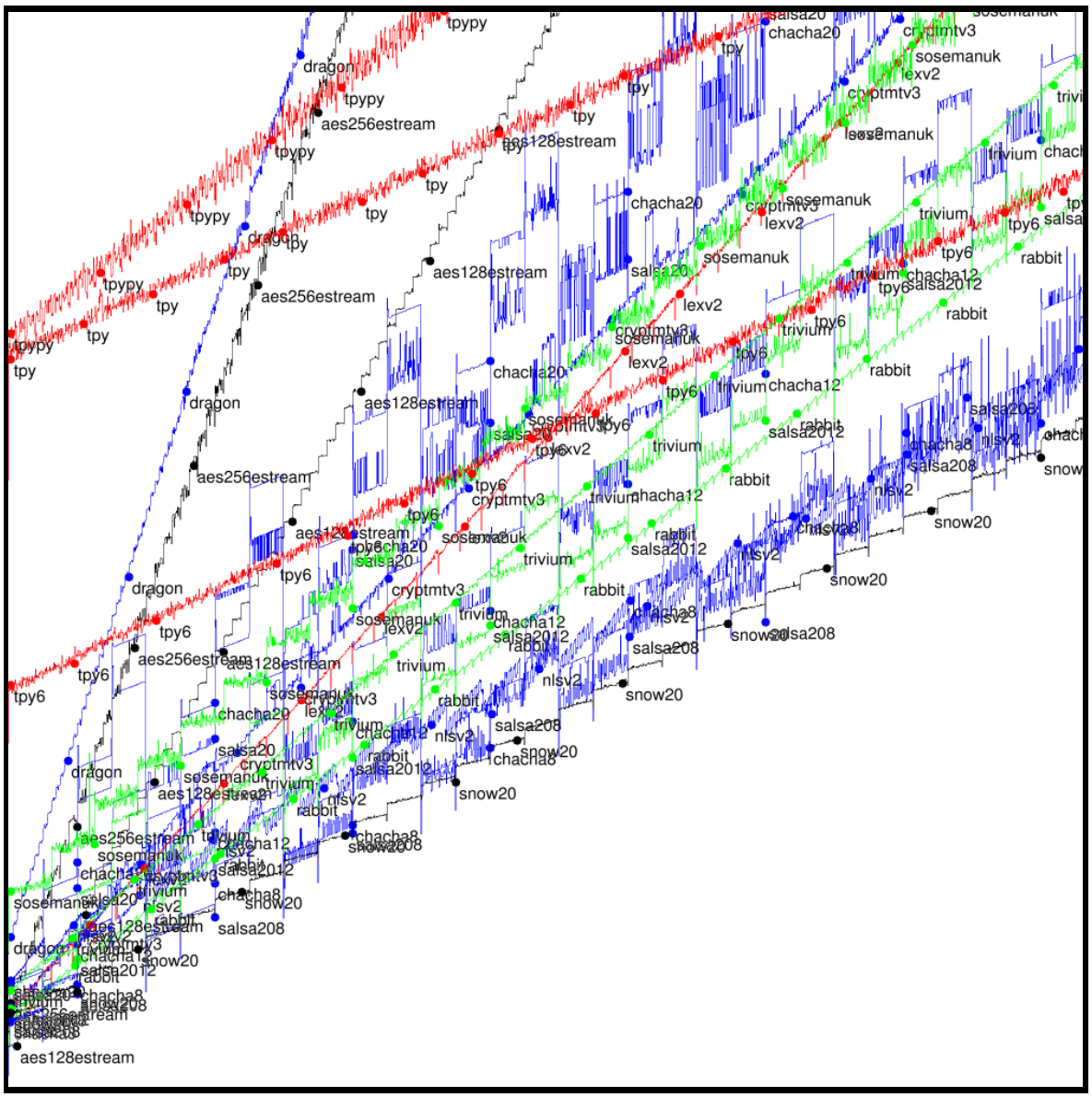
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.01	6.01	6.01	salsa208
7.22	7.22	7.24	chacha8
8.22	8.24	8.25	salsa2012
9.06	9.06	9.60	chacha12
10.14	10.41	10.45	snow20
10.81	10.82	10.82	rabbit
12.67	12.67	12.72	salsa20
13.71	13.81	14.03	chacha20
14.81	14.85	14.90	nlsv2
17.86	18.33	18.36	lexv2
18.03	18.34	18.56	tpy6
18.72	18.73	18.73	aes128estream
19.28	19.30	19.39	trivium
23.77	24.22	26.15	cryptmtv3
28.26	28.56	29.01	sosemanuk
29.98	30.28	30.85	tpy
37.06	37.71	38.33	tpypy
41.83	42.24	42.39	dragon
48.58	49.12	49.36	aes256estream
95.62	96.76	97.26	hc128
168.17	168.84	171.45	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
5.48	5.48	5.49	salsa208
6.67	6.67	6.67	chacha8
7.58	7.59	7.59	salsa2012
8.11	8.28	8.68	snow20
8.79	8.79	8.79	rabbit
8.91	9.09	9.09	chacha12
10.16	10.30	10.49	nlsv2
11.45	11.53	11.62	tpy6
11.81	11.82	11.82	salsa20
13.15	13.17	13.26	chacha20
15.44	15.88	15.98	lexv2
15.84	15.89	16.14	tpy
16.73	16.73	16.73	trivium
18.11	18.16	18.20	aes128estream
20.88	20.91	21.46	cryptmtv3
20.96	20.98	21.18	tpypy
21.47	21.72	22.10	sosemanuk
38.71	39.02	39.12	hc128
38.64	39.04	39.45	dragon
45.99	47.05	47.28	aes256estream
67.00	67.60	68.28	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.41	5.41	5.45	salsa208
6.54	6.54	6.54	chacha8
7.56	7.57	7.58	salsa2012
7.49	7.72	8.33	snow20
8.03	8.03	8.03	rabbit
8.62	8.68	8.73	nlsv2
8.59	8.81	8.84	tpy6
9.25	9.25	9.25	chacha12
11.21	11.28	11.49	tpy
11.74	11.75	11.79	salsa20
13.47	13.47	13.47	chacha20
14.89	14.95	15.00	lexv2
16.01	16.04	16.05	trivium
15.91	16.05	16.32	tpypy
16.44	16.60	16.75	cryptmtv3
16.86	16.91	16.94	hc128
17.07	17.59	17.93	sosemanuk
17.90	17.90	17.95	aes128estream
28.61	28.92	29.20	hc256
38.14	38.59	38.99	dragon
45.74	47.38	47.53	aes256estream

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
3.63	3.92	4.05	hc128
5.38	5.39	5.47	salsa208
4.55	5.58	6.71	hc256
6.47	6.48	6.48	chacha8
6.73	7.21	7.34	tpy6
6.85	7.53	8.96	snow20
7.56	7.56	7.56	rabbit
7.59	7.60	7.62	salsa2012
7.64	7.87	8.01	nlsv2
8.82	8.98	9.50	tpy
9.40	9.40	9.55	chacha12
11.71	11.74	11.82	salsa20
12.92	13.23	14.20	tpypy
13.62	13.62	13.75	chacha20
13.65	14.11	14.43	cryptmtv3
14.11	14.45	14.75	lexv2
13.49	14.78	15.64	sosemanuk
15.57	15.63	15.71	trivium
17.66	17.72	17.85	aes128estream
37.36	38.44	40.14	dragon
44.09	48.05	48.46	aes256estream

7.46 x86, 2995MHz, Intel Xeon (f41), `nmi0079`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
95.62	96.50	96.62	aes128estream
150.00	150.00	150.88	chacha8
146.25	153.75	155.62	salsa208
163.12	163.12	165.00	rabbit
170.62	170.62	173.38	snow20
175.25	176.25	183.75	salsa2012
178.12	180.88	181.88	lexv2
182.75	182.88	182.88	chacha12
176.25	183.75	191.25	cryptmtv3
196.00	198.75	208.12	aes256estream
216.62	218.50	221.25	trivium
237.25	238.12	239.12	salsa20
245.62	245.62	245.62	chacha20
244.75	247.50	247.50	nlsv2
351.62	353.50	355.25	dragon
451.00	461.25	475.38	sosemanuk
906.50	923.38	933.75	tpy6
1676.25	1711.00	2665.38	tpy
1733.50	1741.00	1741.88	tpypy
4367.75	4402.50	4435.38	hc128
10074.40	10096.90	10268.50	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
13.00	13.02	13.02	salsa208
13.95	14.06	14.19	chacha8
17.34	17.34	17.34	salsa2012
19.45	19.45	19.58	chacha12
21.33	21.45	21.56	snow20
25.55	25.67	26.14	rabbit
25.91	25.91	26.12	salsa20
26.02	26.12	26.14	aes128estream
28.12	29.53	30.47	cryptmtv3
30.00	30.00	30.12	chacha20
32.34	32.92	33.17	lexv2
35.39	35.86	36.20	trivium
41.59	41.84	41.95	nlsv2
44.06	45.94	47.69	aes256estream
56.83	58.12	60.11	sosemanuk
71.48	71.83	72.06	dragon
117.89	118.59	121.88	tpy6
215.98	217.27	218.33	tpy
218.80	219.50	220.55	tpypy
544.69	547.62	550.08	hc128
1261.30	1262.69	1287.66	hc256

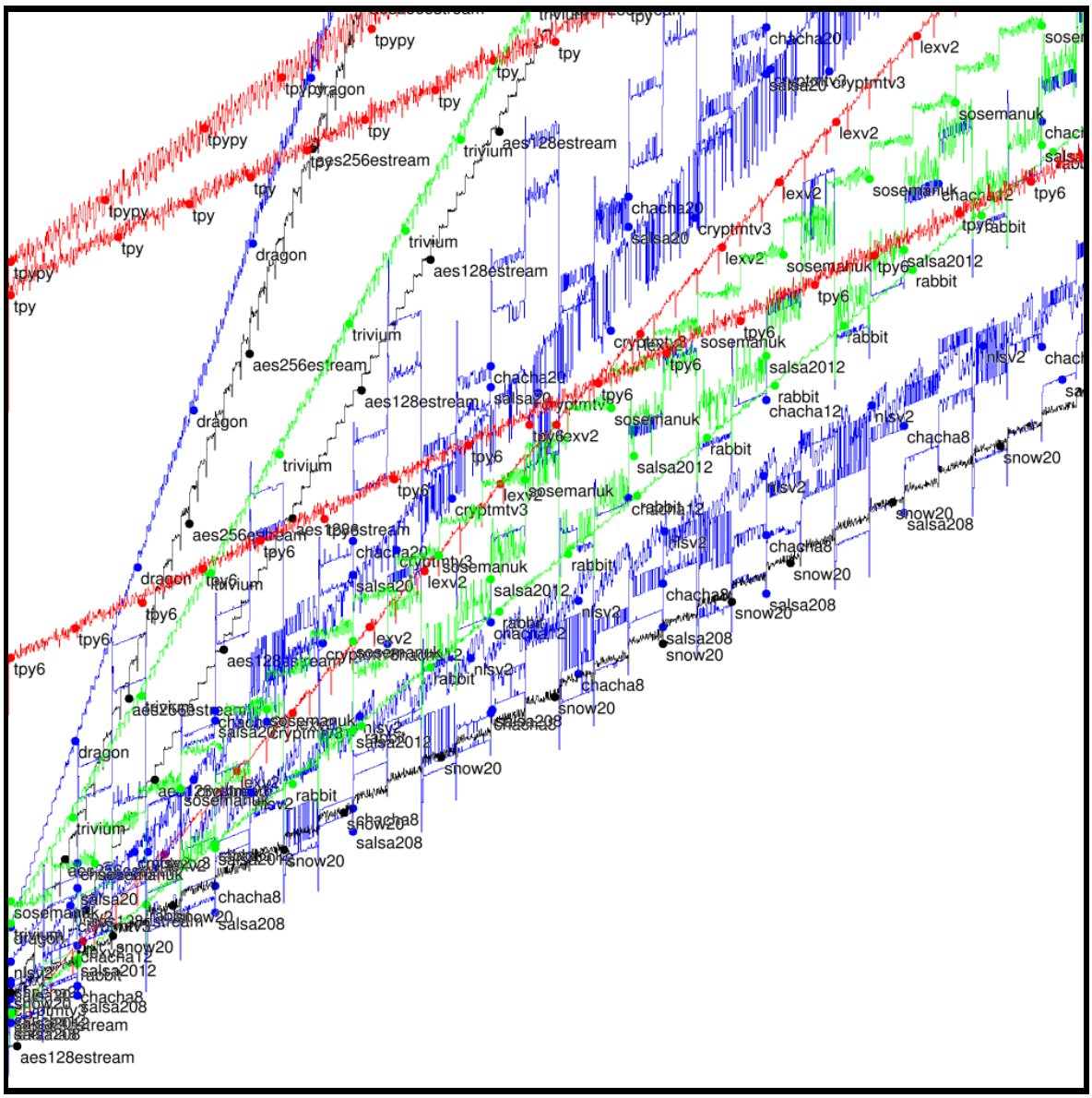
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.58	6.59	6.59	salsa208
6.60	7.29	7.57	chacha8
7.33	7.37	7.45	snow20
8.78	9.02	9.05	salsa2012
9.32	9.38	9.39	nlsv2
9.38	9.38	9.38	chacha12
9.70	9.73	9.74	rabbit
11.74	11.76	11.82	trivium
12.72	12.72	12.73	salsa20
13.01	13.06	13.11	lexv2
13.52	13.67	13.79	cryptmtv3
14.71	14.73	14.73	chacha20
15.47	15.57	15.85	sosemanuk
17.47	17.67	17.73	tpy6
19.78	19.82	19.84	aes128estream
28.10	28.24	28.32	tpy
31.07	31.46	31.70	aes256estream
31.22	31.68	31.68	tpypy
35.05	35.45	35.56	dragon
63.58	64.18	65.10	hc128
145.25	145.56	148.23	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
6.12	6.12	6.26	chacha8
6.24	6.24	6.26	snow20
6.01	6.63	7.29	salsa208
6.99	7.00	7.00	nlsv2
7.99	8.08	8.36	salsa2012
8.40	8.41	8.42	rabbit
8.54	8.72	8.88	chacha12
9.49	9.54	9.60	tpy6
9.83	9.85	9.86	trivium
11.53	11.61	11.65	sosemanuk
11.60	11.62	11.64	lexv2
11.73	11.89	12.74	salsa20
11.99	12.07	12.59	cryptmtv3
12.71	12.74	16.83	chacha20
13.37	13.41	13.44	tpy
16.24	16.59	16.70	tpypy
19.23	19.28	19.30	aes128estream
27.21	27.42	27.63	hc128
30.22	30.35	30.59	aes256estream
32.10	32.21	32.69	dragon
58.29	59.08	59.38	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.84	5.85	5.87	`snow20`
5.93	5.94	5.99	`chacha8`
6.03	6.03	6.04	`nlsv2`
5.75	6.08	6.13	`salsa208`
6.54	6.56	6.64	`tpy6`
7.92	7.92	7.92	`rabbit`
7.87	7.94	13.67	`tpy`
7.90	7.99	8.13	`salsa2012`
8.25	8.52	8.52	`cryptmtv3`
8.59	8.60	8.64	`chacha12`
9.12	9.13	9.13	`trivium`
10.91	10.91	19.25	`sosemanuk`
11.04	11.05	11.08	`lexv2`
11.09	11.21	11.31	`tpypy`
11.80	11.91	11.98	`salsa20`
12.49	12.54	12.54	`chacha20`
13.05	13.15	13.27	`hc128`
19.08	19.16	19.16	`aes128estream`
25.59	25.63	26.01	`hc256`
29.60	29.88	29.92	`aes256estream`
30.49	30.77	30.99	`dragon`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
4.34	4.59	4.98	`hc128`
4.60	4.73	4.90	`tpy6`
4.55	4.75	16.23	`tpy`
3.98	5.21	5.32	`cryptmtv3`
5.53	5.54	5.58	`nlsv2`
5.59	5.62	5.68	`snow20`
4.91	5.75	6.69	`salsa208`
5.72	5.82	5.93	`chacha8`
5.18	6.00	6.83	`hc256`
7.62	7.63	7.64	`rabbit`
7.59	7.92	8.24	`salsa2012`
7.61	8.02	8.32	`tpypy`
8.47	8.55	8.75	`chacha12`
8.67	8.68	8.69	`trivium`
10.36	10.66	27.52	`sosemanuk`
10.70	10.74	10.85	`lexv2`
10.73	11.95	12.24	`salsa20`
12.36	12.45	12.46	`chacha20`
18.91	19.12	19.14	`aes128estream`
28.78	29.46	30.31	`dragon`
29.13	29.78	29.95	`aes256estream`

7.47 x86, 2996MHz, Intel Xeon (f41), nmi0076


tpypy
tpy
dragon
tpypy
tpy
tpypy
tpy
tpypy
tpy

Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
96.62	97.50	101.25	aes128estream
147.25	148.12	149.12	salsa208
150.88	151.00	151.88	chacha8
156.50	156.62	159.38	lexv2
168.75	169.75	170.62	rabbit
171.50	172.50	175.38	aes256estream
174.38	176.25	183.75	salsa2012
181.88	182.88	183.75	chacha12
203.38	207.25	211.00	cryptmtv3
220.25	224.12	235.38	snow20
231.62	232.50	240.00	salsa20
246.62	247.50	248.38	chacha20
290.62	299.00	303.75	nlsv2
374.12	376.88	378.75	trivium
375.00	377.75	380.62	dragon
416.25	424.75	433.12	sosemanuk
982.50	991.88	992.88	tpy6
1845.88	1846.88	1851.62	tpy
1911.62	1932.12	1945.25	tpypy
4780.25	4870.25	4898.50	hc128
11936.20	11964.40	11997.10	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
13.23	13.23	13.25	salsa208
14.06	14.17	14.19	chacha8
17.23	17.34	17.34	salsa2012
19.45	19.45	19.58	chacha12
26.12	26.25	26.36	salsa20
26.25	26.72	27.06	aes128estream
27.55	28.23	28.36	rabbit
28.12	28.95	30.23	snow20
30.00	30.11	30.12	chacha20
30.11	30.47	31.41	lexv2
30.47	32.34	32.70	cryptmtv3
40.55	41.02	41.95	aes256estream
48.62	49.33	51.45	nlsv2
52.39	53.44	56.14	sosemanuk
62.11	62.69	62.92	trivium
72.08	72.42	72.89	dragon
127.86	130.66	130.78	tpy6
235.44	237.89	239.06	tpy
238.94	239.89	240.47	tpypy
598.02	613.12	614.88	hc128
1494.84	1496.14	1544.42	hc256

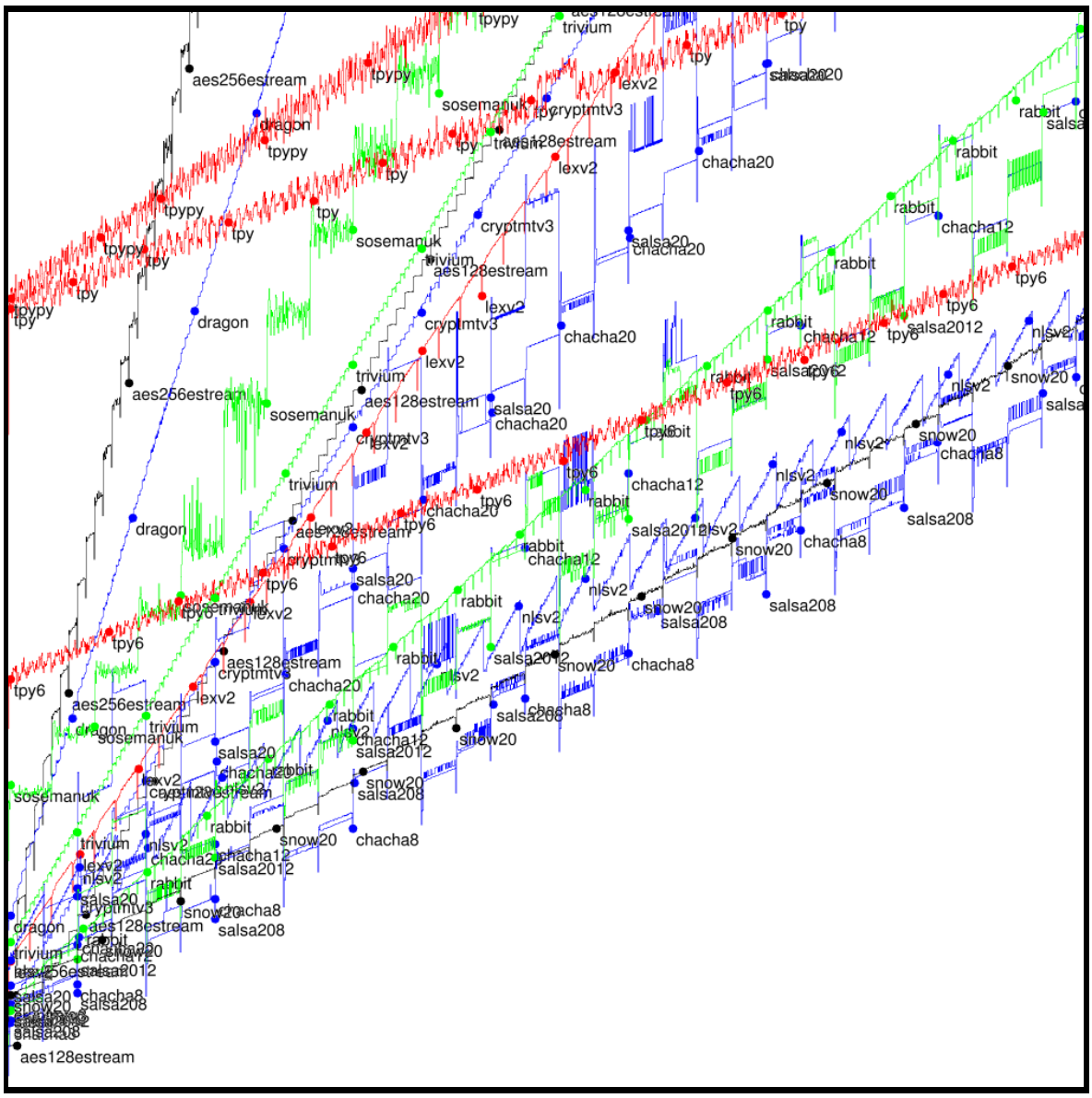
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.33	6.34	7.02	salsa208
7.08	7.10	7.11	chacha8
8.02	8.10	8.20	snow20
8.85	9.02	9.04	salsa2012
9.02	9.19	9.39	chacha12
10.47	10.55	10.60	nlsv2
10.48	10.60	10.61	rabbit
12.98	13.01	13.03	lexv2
12.66	13.07	13.67	salsa20
13.74	13.75	13.89	chacha20
14.44	14.57	14.69	sosemanuk
14.77	14.78	14.78	cryptmtv3
18.28	18.50	18.56	tpy6
19.84	19.95	20.01	aes128estream
22.50	22.67	22.71	trivium
30.05	30.16	30.26	aes256estream
30.68	30.76	31.04	tpy
32.67	32.89	32.98	tpypy
33.09	33.19	33.70	dragon
70.31	70.72	72.16	hc128
168.83	171.19	171.65	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
6.03	6.03	6.04	salsa208
6.52	6.57	6.64	snow20
6.71	6.88	6.88	chacha8
7.80	7.86	7.88	nlsv2
8.29	8.45	8.54	chacha12
8.38	8.57	8.72	salsa2012
9.13	9.13	9.17	rabbit
9.67	9.89	9.92	tpy6
10.88	10.97	11.03	sosemanuk
11.65	11.70	11.75	lexv2
12.30	12.30	12.33	cryptmtv3
12.63	12.64	12.64	chacha20
12.73	12.74	12.82	salsa20
14.26	14.28	14.30	tpy
16.58	16.67	16.85	tpypy
19.14	19.30	19.34	aes128estream
19.21	19.32	19.49	trivium
29.31	29.35	29.50	aes256estream
29.15	29.75	29.91	hc128
29.82	29.96	30.08	dragon
68.19	68.30	70.33	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.76	5.79	5.80	salsa208
6.00	6.01	6.02	snow20
6.64	6.67	6.71	tpy6
6.67	6.70	6.72	nlsv2
6.44	6.82	6.82	chacha8
8.17	8.17	8.18	chacha12
8.36	8.37	8.70	cryptmtv3
8.34	8.38	8.44	tpy
8.57	8.58	8.58	rabbit
8.33	8.60	8.67	salsa2012
9.62	9.64	9.72	sosemanuk
10.71	10.72	10.74	tpypy
11.22	11.23	11.25	lexv2
12.45	12.45	12.45	chacha20
12.46	12.47	12.48	salsa20
13.66	13.88	13.95	hc128
18.06	18.07	18.19	trivium
19.07	19.15	19.22	aes128estream
28.81	28.83	28.84	aes256estream
28.74	28.86	28.99	dragon
29.52	29.80	30.30	hc256

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
3.54	3.54	4.21	cryptmtv3
3.71	4.27	4.60	hc128
4.57	4.74	4.93	tpy
4.72	4.84	4.94	tpy6
4.37	5.64	5.67	salsa208
5.67	5.71	5.75	snow20
6.06	6.17	6.22	nlsv2
6.05	6.69	7.90	hc256
6.00	6.76	6.89	chacha8
7.07	7.18	7.33	tpypy
7.98	7.98	8.01	chacha12
8.23	8.27	8.28	rabbit
7.96	8.62	8.82	salsa2012
8.91	9.03	9.23	sosemanuk
10.98	11.01	11.06	lexv2
12.16	12.19	12.37	salsa20
12.32	12.32	12.32	chacha20
17.14	17.26	17.52	trivium
18.86	19.05	19.19	aes128estream
27.20	28.09	28.41	dragon
28.32	28.40	28.71	aes256estream

7.48 x86, 3000MHz, Intel Xeon (f4a), `nmi0090`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
96.50	96.62	97.50	aes128estream
149.00	149.12	150.88	chacha8
152.88	153.75	153.75	salsa208
178.12	178.12	179.00	salsa2012
180.88	181.88	181.88	chacha12
182.75	182.88	183.75	rabbit
195.00	195.88	196.88	cryptmtv3
188.38	197.75	198.75	chacha20
213.75	214.62	216.50	snow20
234.38	235.25	236.25	salsa20
296.25	297.12	298.12	nlsv2
298.12	299.00	299.12	aes256estream
300.00	300.00	300.88	lexv2
335.62	336.50	336.62	trivium
399.38	402.12	416.25	dragon
682.50	682.50	696.62	sosemanuk
941.25	945.00	972.25	tpy6
1817.88	1822.50	1831.88	tpypy
1830.00	1831.00	1843.12	tpy
4812.25	4816.00	4825.25	hc128
11528.40	11555.60	11618.50	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
13.12	13.12	13.23	salsa208
13.94	13.95	14.06	chacha8
16.75	16.77	16.88	chacha20
17.34	17.45	17.81	salsa2012
19.22	19.33	19.45	chacha12
26.02	26.02	26.14	salsa20
26.02	26.12	26.25	aes128estream
27.06	27.19	27.77	snow20
30.81	31.05	31.30	rabbit
38.20	38.56	39.03	cryptmtv3
51.80	51.80	51.80	lexv2
54.95	54.97	55.55	nlsv2
56.84	56.95	56.95	trivium
75.94	76.17	77.11	aes256estream
78.98	79.11	79.56	dragon
85.44	86.83	87.55	sosemanuk
119.88	121.64	124.81	tpy6
227.34	229.33	229.69	tpy
229.45	234.61	234.73	tpypy
596.48	599.64	602.11	hc128
1443.75	1446.33	1452.42	hc256

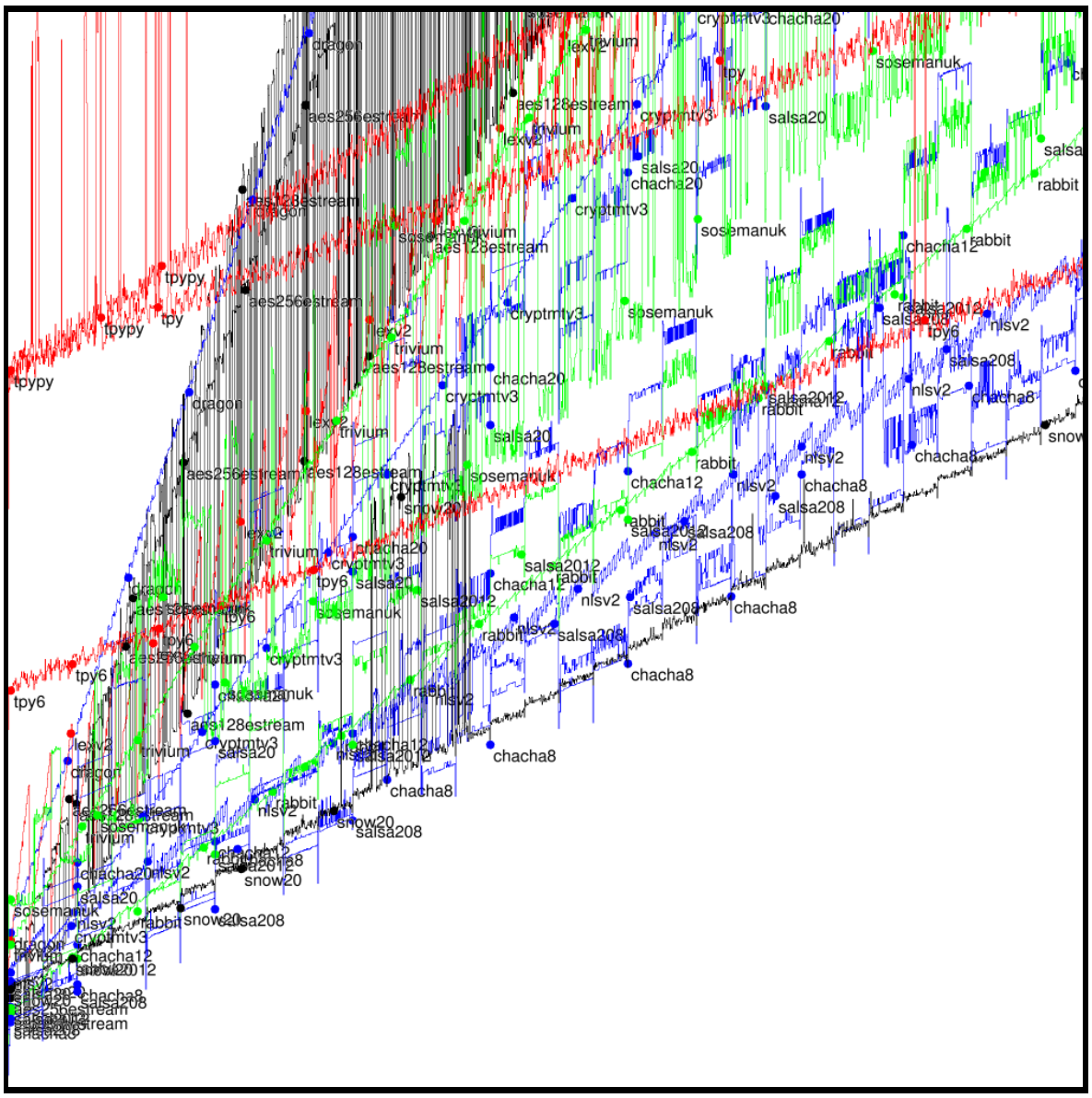
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.93	6.93	6.94	chacha8
6.97	6.97	6.98	salsa208
8.78	8.79	8.80	snow20
9.00	9.01	9.01	chacha12
8.54	9.54	9.55	salsa2012
11.07	11.12	11.12	nlsv2
11.54	11.55	11.56	rabbit
13.26	13.26	13.27	chacha20
13.40	13.41	13.45	salsa20
17.02	17.21	17.30	tpy6
18.87	18.89	18.91	lexv2
19.26	19.32	19.34	cryptmtv3
19.86	19.87	19.88	aes128estream
21.42	21.42	21.43	trivium
27.15	27.59	28.50	sosemanuk
28.44	28.49	28.50	tpy
30.82	30.93	31.34	tpypy
38.02	38.07	38.07	dragon
52.75	54.35	54.44	aes256estream
70.35	70.51	70.60	hc128
165.96	166.04	166.04	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
5.96	5.96	5.96	salsa208
6.13	6.30	6.30	chacha8
7.22	7.23	7.34	snow20
7.73	7.75	7.75	nlsv2
8.10	8.10	8.10	salsa2012
8.23	8.24	8.24	chacha12
8.94	9.06	9.12	tpy6
9.97	9.97	9.97	rabbit
12.75	12.78	12.78	salsa20
12.90	12.90	12.90	chacha20
12.95	13.07	13.23	tpy
16.04	16.04	16.13	tpypy
16.23	16.24	16.24	lexv2
17.15	17.16	17.16	cryptmtv3
18.62	18.62	18.62	trivium
19.29	19.29	19.29	aes128estream
19.17	19.57	20.15	sosemanuk
29.09	29.10	29.11	hc128
34.69	34.71	34.71	dragon
52.23	52.57	52.65	aes256estream
65.50	65.55	65.57	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.73	5.73	5.76	`salsa208`
5.85	5.92	5.93	`tpy6`
5.94	6.00	6.00	`chacha8`
6.36	6.36	6.38	`nlsv2`
6.78	6.79	6.80	`snow20`
7.37	7.40	7.43	`tpy`
8.01	8.01	8.01	`salsa2012`
8.08	8.08	8.08	`chacha12`
9.37	9.38	9.38	`rabbit`
10.02	10.07	10.11	`tpypy`
12.19	12.41	12.41	`salsa20`
12.77	12.77	12.77	`chacha20`
13.53	13.60	13.62	`hc128`
15.26	15.27	15.28	`lexv2`
15.25	15.42	15.92	`sosemanuk`
15.51	15.51	15.52	`cryptmtv3`
17.57	17.57	17.58	`trivium`
19.11	19.12	19.12	`aes128estream`
27.99	27.99	28.00	`hc256`
33.46	33.46	33.46	`dragon`
51.24	51.50	51.87	`aes256estream`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
3.86	3.93	4.00	`tpy`
3.91	4.07	4.11	`tpy6`
4.12	4.31	4.36	`hc128`
5.48	5.49	5.54	`hc256`
5.63	5.63	5.68	`salsa208`
5.68	5.71	5.77	`nlsv2`
5.69	5.82	5.83	`chacha8`
6.25	6.53	6.68	`tpypy`
6.56	6.60	6.62	`snow20`
7.96	7.96	7.97	`salsa2012`
7.98	7.99	8.00	`chacha12`
9.01	9.02	9.03	`rabbit`
11.59	12.30	12.61	`salsa20`
12.69	12.69	12.69	`chacha20`
12.26	12.91	14.25	`sosemanuk`
14.70	14.71	14.74	`lexv2`
15.07	15.08	15.09	`cryptmtv3`
16.93	16.94	16.96	`trivium`
19.01	19.03	19.04	`aes128estream`
32.63	32.71	32.73	`dragon`
50.10	50.80	52.61	`aes256estream`

7.49 x86, 3000MHz, Intel Xeon (f4a), nmi0102



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
149.00	150.00	150.88	chacha8
155.62	157.50	178.12	salsa208
103.12	173.50	180.88	aes128estream
175.38	175.38	176.25	cryptmtv3
179.12	181.88	184.75	rabbit
183.75	183.75	185.62	salsa2012
181.88	185.62	185.62	chacha12
209.00	211.88	214.75	aes256estream
230.62	241.00	243.75	snow20
240.00	241.88	242.88	salsa20
244.62	244.75	245.62	chacha20
271.00	272.88	285.00	nlsv2
330.00	332.88	619.75	trivium
363.75	364.62	365.62	dragon
363.75	370.25	375.00	lexv2
416.25	421.88	608.50	sosemanuk
915.88	924.38	933.75	tpy6
1661.25	1663.12	2880.00	tpypy
1671.62	1687.50	1698.75	tpy
4340.62	4349.12	4367.88	hc128
9228.75	9268.12	9287.75	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
13.12	13.36	14.53	salsa208
14.06	14.06	14.30	chacha8
17.45	17.58	17.58	salsa2012
19.33	19.34	19.34	chacha12
26.12	26.25	26.25	salsa20
26.48	27.19	47.92	aes128estream
28.59	28.59	28.59	rabbit
29.88	29.89	30.00	chacha20
30.11	30.47	31.17	snow20
31.64	31.77	32.69	cryptmtv3
44.88	45.00	45.47	nlsv2
52.03	52.50	52.86	aes256estream
55.31	55.44	111.20	trivium
72.55	72.78	73.12	dragon
76.30	76.88	77.47	lexv2
53.44	78.17	82.73	sosemanuk
117.30	118.12	119.19	tpy6
209.53	212.00	315.94	tpy
211.53	212.23	311.61	tpypy
543.64	545.16	546.09	hc128
1149.27	1156.05	1161.92	hc256

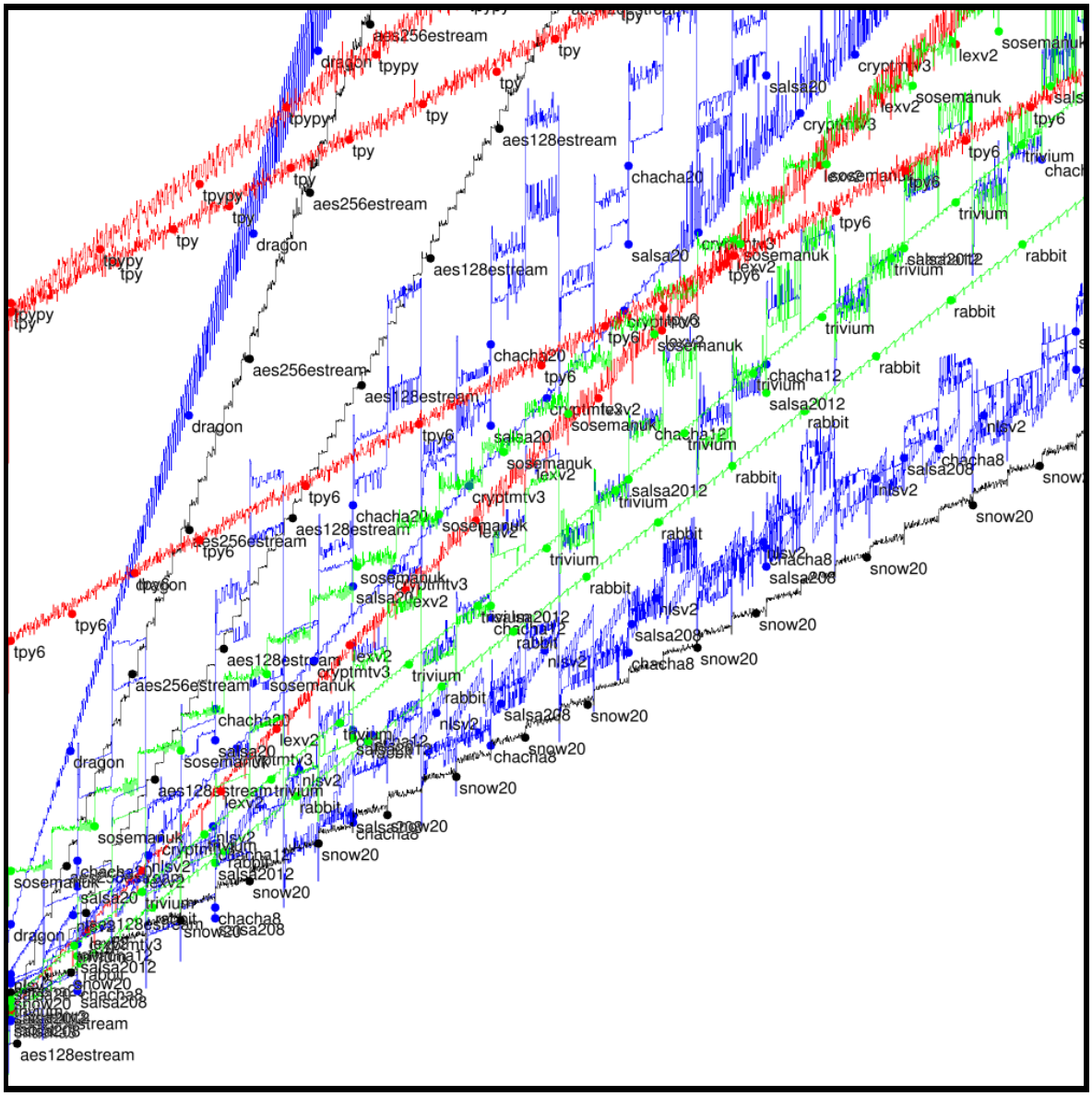
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.57	6.58	6.60	chacha8
6.95	7.21	8.71	salsa208
8.23	8.31	14.70	snow20
8.83	9.27	9.39	salsa2012
9.06	9.36	9.57	chacha12
10.21	10.30	10.33	nlsv2
10.48	10.48	10.49	rabbit
12.63	12.75	13.53	salsa20
14.18	14.20	14.32	chacha20
14.95	15.12	26.08	sosemanuk
16.52	16.61	16.77	cryptmtv3
16.47	16.65	16.80	tpy6
19.95	20.05	37.27	aes128estream
19.57	20.17	20.29	lexv2
20.26	20.27	20.47	trivium
26.59	26.94	27.14	tpy
28.88	28.91	29.18	tpypy
31.89	31.95	32.03	aes256estream
35.10	35.16	35.27	dragon
63.80	63.89	64.19	hc128
132.45	132.54	132.67	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
6.31	6.31	6.32	chacha8
6.45	6.47	11.79	snow20
7.95	7.97	7.99	nlsv2
7.00	8.22	8.37	salsa208
8.73	8.84	13.31	tpy6
8.43	8.90	9.08	salsa2012
8.80	8.94	9.06	chacha12
9.01	9.01	9.04	rabbit
11.80	11.90	11.98	salsa20
11.46	11.99	20.71	sosemanuk
12.35	12.39	20.06	tpy
12.76	12.77	12.77	chacha20
14.81	14.83	15.06	cryptmtv3
14.88	15.00	24.01	tpypy
16.48	17.24	17.63	lexv2
17.62	17.64	17.67	trivium
19.49	19.73	36.60	aes128estream
26.56	26.60	26.64	hc128
30.38	30.40	30.56	aes256estream
31.82	31.87	32.32	dragon
52.72	52.98	52.99	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.76	5.79	5.81	tpy6
5.91	5.94	5.96	snow20
5.94	6.01	6.01	chacha8
6.95	6.98	7.01	nlsv2
6.98	7.00	7.04	tpy
6.41	7.99	8.22	salsa208
8.46	8.46	8.46	rabbit
8.51	8.83	8.87	salsa2012
8.85	9.05	9.22	chacha12
9.75	10.01	16.52	tpypy
10.11	10.14	18.29	sosemanuk
11.67	11.73	11.74	salsa20
12.47	12.51	12.52	hc128
12.51	12.51	12.61	chacha20
14.25	14.26	14.29	cryptmtv3
15.35	15.36	15.84	lexv2
16.54	16.61	16.64	trivium
19.17	19.29	21.21	aes128estream
23.07	23.12	23.18	hc256
30.00	30.02	30.04	aes256estream
30.75	30.80	31.26	dragon

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
3.76	3.85	3.97	tpy
3.92	4.11	4.26	tpy6
3.97	4.12	4.18	hc128
5.22	5.45	5.64	hc256
5.59	5.68	5.73	snow20
5.69	5.82	5.96	chacha8
6.36	6.43	6.51	nlsv2
6.42	7.08	20.21	tpypy
8.10	8.13	8.13	rabbit
8.07	8.84	9.18	salsa2012
8.53	8.97	9.31	chacha12
5.86	9.11	9.68	salsa208
0.93	9.66	26.04	sosemanuk
11.38	11.52	11.61	salsa20
11.65	12.35	12.55	chacha20
14.34	14.38	16.00	lexv2
14.39	14.60	14.66	cryptmtv3
15.84	16.14	16.23	trivium
1.93	17.74	23.21	aes128estream
29.47	29.66	29.78	aes256estream
30.01	30.15	31.08	dragon

7.50 x86, 3391MHz, Intel Pentium D (f64), `nmi0099`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
97.75	99.88	99.88	aes128estream
148.75	150.88	159.38	salsa208
150.88	150.88	150.88	chacha8
161.50	163.62	165.75	rabbit
174.25	174.25	180.62	lexv2
180.62	180.62	182.75	salsa2012
180.62	182.75	182.75	chacha12
182.75	182.75	184.88	aes256estream
189.12	193.38	197.62	cryptmtv3
195.50	195.50	197.62	trivium
212.50	214.62	214.62	snow20
231.62	233.75	240.12	salsa20
244.38	246.50	246.50	chacha20
265.62	267.75	269.88	nlsv2
378.25	384.62	386.75	dragon
497.25	499.38	505.75	sosemanuk
1037.00	1043.38	1054.00	tpy6
1778.62	1789.25	1819.00	tpy
1785.00	1795.62	1812.62	tpypy
4488.00	4522.00	4615.50	hc128
12556.60	12558.80	12571.50	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
13.28	13.28	13.55	salsa208
14.08	14.08	14.34	chacha8
17.27	17.53	17.53	salsa2012
19.39	19.39	19.66	chacha12
25.50	25.50	26.56	snow20
25.50	25.77	26.30	rabbit
26.03	26.30	26.30	salsa20
26.56	26.56	26.56	aes128estream
29.48	30.02	30.55	cryptmtv3
30.02	30.02	30.28	chacha20
31.88	31.88	32.14	trivium
32.67	33.20	33.47	lexv2
41.44	41.97	42.23	aes256estream
46.75	47.02	47.55	nlsv2
62.42	62.69	63.75	sosemanuk
74.91	75.17	75.44	dragon
132.81	134.14	135.73	tpy6
226.31	227.91	228.97	tpy
227.91	229.77	231.09	tpypy
560.20	564.19	566.58	hc128
1562.67	1566.66	1571.17	hc256

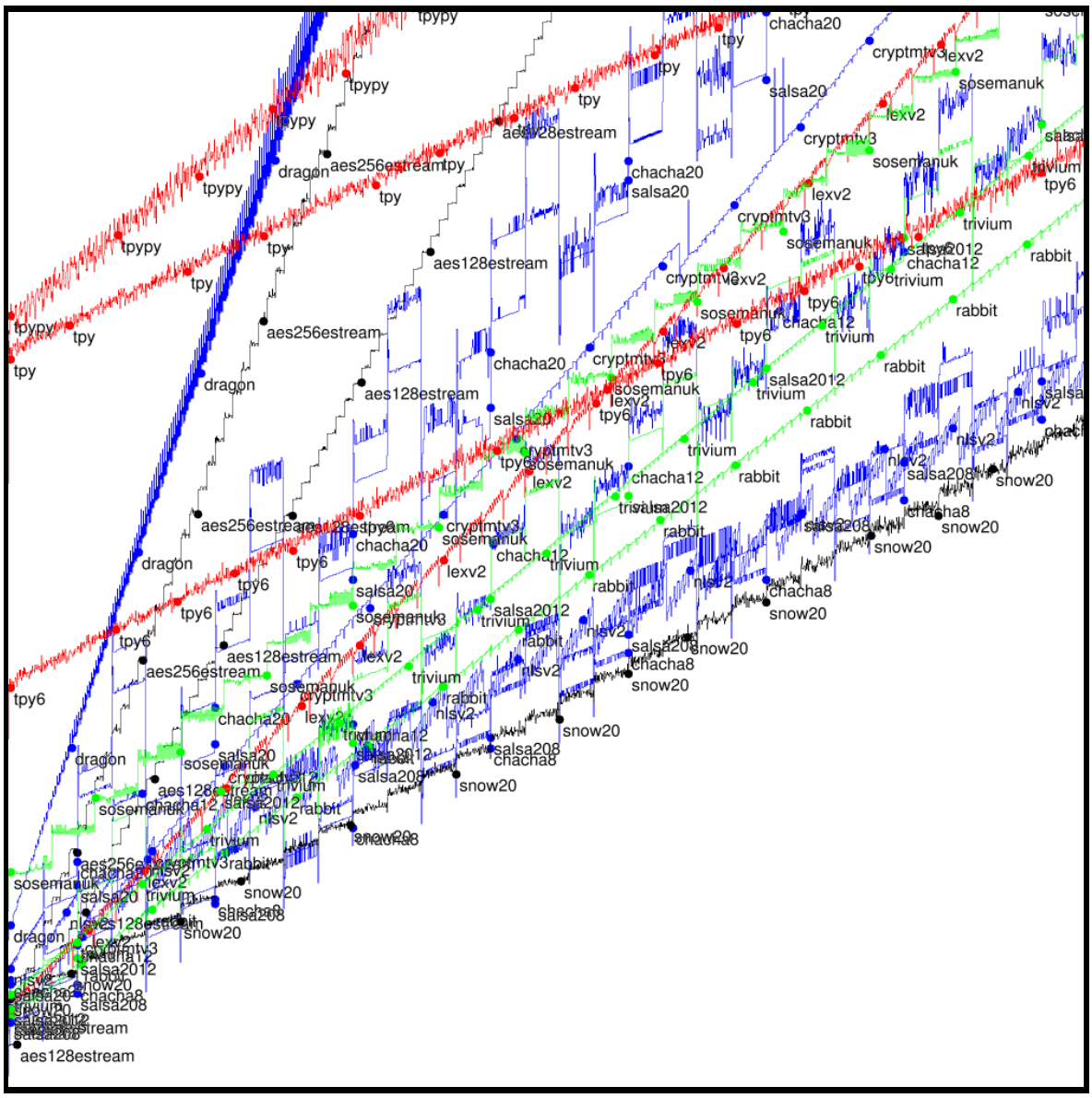
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.61	6.61	6.61	chacha8
6.97	7.17	7.47	salsa208
7.82	7.82	7.85	snow20
8.50	8.53	8.53	salsa2012
9.03	9.06	9.56	chacha12
9.56	9.59	9.65	nlsv2
9.68	9.68	9.71	rabbit
11.13	11.16	11.16	trivium
12.93	13.13	13.16	lexv2
13.64	13.69	14.02	cryptmtv3
13.72	13.75	13.75	chacha20
13.78	13.81	13.81	salsa20
15.61	15.67	15.73	sosemanuk
19.45	19.72	20.01	tpy6
19.86	19.89	19.92	aes128estream
29.60	29.69	29.72	aes256estream
30.10	30.22	30.37	tpy
31.52	31.73	31.79	tpypy
35.12	35.21	35.24	dragon
67.47	67.76	68.27	hc128
179.33	179.86	180.48	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
6.11	6.14	6.15	chacha8
6.09	6.16	6.20	snow20
6.40	6.40	6.40	salsa208
6.96	6.98	6.98	nlsv2
8.38	8.38	8.38	rabbit
8.27	8.48	8.49	chacha12
8.82	8.82	8.83	salsa2012
9.44	9.45	9.45	trivium
10.47	10.58	10.67	tpy6
11.33	11.38	11.68	lexv2
11.34	11.57	11.91	sosemanuk
12.15	12.16	12.99	cryptmtv3
12.34	12.42	12.52	salsa20
12.64	12.88	13.05	chacha20
14.26	14.34	14.43	tpy
16.41	16.50	16.63	tpypy
19.28	19.40	19.41	aes128estream
28.57	28.62	28.63	aes256estream
28.46	28.69	28.91	hc128
31.96	31.97	31.99	dragon
71.33	71.46	71.66	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.62	5.64	5.67	`snow20`
5.89	5.89	5.89	`nlsv2`
5.95	5.97	6.00	`chacha8`
6.36	6.40	6.40	`salsa208`
7.21	7.29	7.34	`tpy6`
7.94	7.94	7.95	`rabbit`
8.13	8.18	8.21	`chacha12`
8.61	8.65	8.67	`tpy`
8.80	8.80	8.80	`salsa2012`
8.82	8.82	8.82	`trivium`
9.20	9.29	9.35	`cryptmtv3`
9.91	9.93	9.96	`sosemanuk`
10.60	10.63	10.66	`tpypy`
10.72	10.82	10.96	`lexv2`
12.28	12.35	12.42	`salsa20`
12.68	12.89	12.96	`chacha20`
13.57	13.64	13.70	`hc128`
19.09	19.09	19.13	`aes128estream`
28.21	28.27	28.38	`aes256estream`
30.63	30.72	30.87	`hc256`
30.78	30.79	30.80	`dragon`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
4.27	4.57	4.86	`hc128`
5.11	5.20	5.29	`tpy`
5.03	5.32	5.50	`tpy6`
5.35	5.38	5.45	`snow20`
5.38	5.39	5.39	`nlsv2`
5.77	5.83	5.88	`chacha8`
5.95	6.28	6.72	`hc256`
6.33	6.40	6.41	`salsa208`
6.29	6.50	6.63	`cryptmtv3`
7.11	7.18	7.30	`tpypy`
7.41	7.69	7.72	`rabbit`
7.89	7.99	8.19	`chacha12`
8.42	8.43	8.43	`trivium`
8.67	8.94	8.95	`salsa2012`
9.01	9.08	9.16	`sosemanuk`
10.03	10.30	10.84	`lexv2`
12.14	12.30	12.45	`salsa20`
12.46	13.15	13.34	`chacha20`
18.85	18.93	19.03	`aes128estream`
27.92	28.06	28.41	`aes256estream`
30.07	30.12	31.01	`dragon`

7.51 x86, 3392MHz, Intel Pentium D (f64), nmi0104



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
97.75	99.88	104.12	aes128estream
148.75	150.88	150.88	salsa208
150.88	150.88	150.88	chacha8
157.25	163.62	165.75	aes256estream
163.62	165.75	167.88	rabbit
165.75	167.88	170.00	cryptmtv3
180.62	180.62	182.75	salsa2012
182.75	184.88	184.88	chacha12
182.75	184.88	184.88	lexv2
204.00	206.12	206.12	snow20
210.38	210.38	212.50	trivium
235.88	238.00	238.00	salsa20
246.50	248.62	248.62	chacha20
280.50	280.50	282.62	nlsv2
384.62	384.62	386.75	dragon
499.38	501.50	516.38	sosemanuk
932.88	939.25	949.88	tpy6
1689.38	1714.88	1719.12	tpy
1785.00	1793.50	1795.62	tpypy
4517.75	4683.50	4694.12	hc128
11477.10	11485.60	11500.50	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
13.28	13.28	13.28	salsa208
11.95	14.34	14.61	chacha8
17.53	17.80	17.80	salsa2012
19.39	19.39	19.66	chacha12
25.50	25.50	25.77	snow20
25.50	25.77	26.03	rabbit
26.03	26.03	26.30	salsa20
26.30	26.56	27.09	aes128estream
27.36	27.36	27.36	cryptmtv3
30.02	30.02	30.28	chacha20
33.20	33.20	33.47	lexv2
33.47	33.73	34.00	trivium
40.11	40.38	40.38	aes256estream
49.14	49.67	49.67	nlsv2
65.08	65.08	65.08	sosemanuk
74.38	74.64	74.64	dragon
120.33	122.45	123.52	tpy6
217.28	217.81	218.08	tpy
224.98	225.52	227.11	tpypy
561.53	569.23	584.64	hc128
1433.84	1436.23	1438.09	hc256

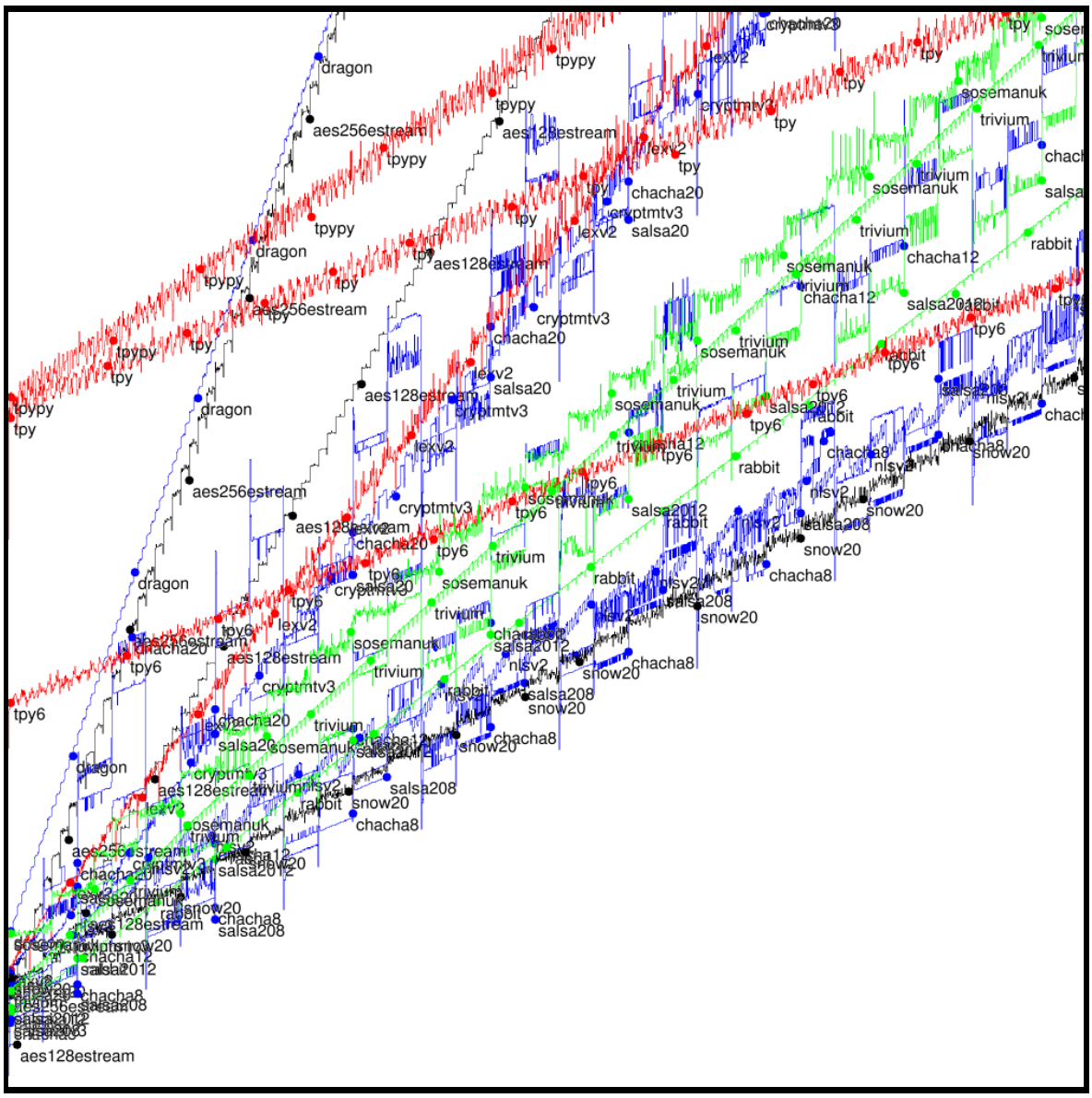
Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
6.58	6.58	6.61	chacha8
6.91	7.17	7.17	salsa208
7.61	7.70	7.79	snow20
8.71	8.71	8.71	salsa2012
9.00	9.33	10.06	chacha12
9.65	9.71	9.77	nlsv2
9.68	9.71	9.71	rabbit
11.19	11.22	11.22	trivium
12.96	12.99	12.99	lexv2
13.46	13.49	13.49	salsa20
13.66	13.69	13.72	cryptmtv3
13.78	14.67	14.85	chacha20
15.38	15.41	15.41	sosemanuk
17.62	17.77	18.03	tpy6
20.04	20.04	20.04	aes128estream
28.27	28.63	28.66	tpy
29.34	29.37	29.37	aes256estream
31.93	31.99	32.14	tpypy
33.76	34.27	34.35	dragon
67.20	67.73	68.03	hc128
164.75	164.89	165.22	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
6.07	6.13	6.14	chacha8
6.34	6.41	6.42	snow20
6.55	6.56	6.71	salsa208
7.01	7.02	7.03	nlsv2
8.37	8.38	8.38	rabbit
8.29	8.56	8.90	chacha12
7.97	8.62	9.11	salsa2012
9.35	9.36	9.36	trivium
9.81	9.85	9.89	tpy6
11.30	11.34	11.34	sosemanuk
11.34	11.34	11.37	lexv2
12.12	12.12	12.12	cryptmtv3
13.61	13.61	13.62	salsa20
13.58	13.62	13.83	tpy
13.04	13.69	13.71	chacha20
17.11	17.20	17.29	tpypy
19.47	19.47	19.47	aes128estream
27.98	28.41	28.91	hc128
28.44	28.44	28.57	aes256estream
30.65	30.70	30.71	dragon
65.71	65.78	65.88	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.69	5.76	5.84	snow20
5.89	5.90	5.91	nlsv2
5.94	5.94	5.94	chacha8
6.44	6.50	6.57	salsa208
6.74	6.80	6.84	tpy6
7.89	7.89	7.89	rabbit
7.99	8.02	8.08	tpy
8.15	8.35	8.68	chacha12
8.45	8.45	8.45	salsa2012
8.67	8.67	8.67	trivium
9.03	9.24	9.26	cryptmtv3
9.72	9.75	9.77	sosemanuk
10.80	10.80	10.81	lexv2
11.44	11.54	11.60	tpypy
12.76	12.99	13.13	chacha20
13.28	13.28	13.28	salsa20
13.51	13.61	13.70	hc128
19.28	19.28	19.29	aes128estream
28.17	28.18	28.19	aes256estream
28.48	28.55	28.60	hc256
29.46	29.50	29.98	dragon

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
4.62	4.67	4.84	tpy
4.67	4.91	5.10	hc128
4.68	4.94	5.10	tpy6
5.37	5.40	5.42	nlsv2
5.30	5.48	5.64	snow20
5.82	5.83	5.89	chacha8
5.98	6.18	6.36	hc256
5.90	6.36	6.38	cryptmtv3
6.13	6.47	6.62	salsa208
7.59	7.60	7.60	rabbit
7.23	8.05	8.94	chacha12
7.90	8.18	8.41	tpypy
8.25	8.25	8.25	trivium
8.58	8.58	8.60	salsa2012
8.92	8.98	9.04	sosemanuk
10.50	10.53	10.55	lexv2
12.73	12.73	12.74	salsa20
12.29	12.77	13.36	chacha20
19.17	19.18	19.20	aes128estream
27.94	27.98	28.07	aes256estream
28.17	28.35	29.89	dragon

7.52 x86, 3392MHz, Intel Pentium D (f64), `nmi0241`



Cycles/byte to encrypt 8 bytes			
quartile	median	quartile	cipher
99.88	99.88	99.88	aes128estream
146.62	146.62	148.75	chacha8
155.12	157.25	157.25	salsa208
161.50	165.75	165.75	cryptmtv3
172.12	178.50	180.62	rabbit
182.75	182.75	182.75	chacha12
182.75	184.88	187.00	salsa2012
208.25	208.25	208.25	trivium
225.25	229.50	229.50	aes256estream
235.88	238.00	240.12	salsa20
244.38	246.50	246.50	chacha20
246.50	250.75	257.12	snow20
274.12	278.38	282.62	nlsv2
282.62	286.88	291.12	lexv2
346.38	354.88	359.12	sosemanuk
367.62	367.62	369.75	dragon
892.50	896.75	905.25	tpy6
1568.25	1574.62	1585.25	tpypy
1574.62	1585.25	1587.38	tpy
4279.75	4288.25	4313.75	hc128
11749.10	11844.80	12146.50	hc256

Cycles/byte to encrypt 64 bytes			
quartile	median	quartile	cipher
13.02	13.02	13.28	salsa208
13.81	14.08	14.08	chacha8
17.53	17.53	17.80	salsa2012
19.12	19.39	19.39	chacha12
26.03	26.03	26.30	salsa20
26.03	26.30	27.09	rabbit
26.30	26.56	26.56	aes128estream
29.75	30.02	30.02	chacha20
30.28	30.55	31.34	cryptmtv3
32.41	32.67	33.20	snow20
34.00	34.27	34.27	trivium
44.09	44.62	45.95	sosemanuk
46.22	46.48	47.28	nlsv2
48.88	49.41	50.20	lexv2
49.14	49.94	50.47	aes256estream
71.19	71.72	71.72	dragon
114.48	115.02	115.81	tpy6
197.36	197.62	199.48	tpy
202.67	203.73	204.27	tpypy
516.38	532.58	534.17	hc128
1461.20	1476.34	1512.73	hc256

Cycles/byte to encrypt 576 bytes			
quartile	median	quartile	cipher
7.11	7.11	7.29	chacha8
6.94	7.17	8.00	salsa208
8.65	8.74	8.85	snow20
8.71	9.00	9.09	salsa2012
9.15	9.18	9.44	chacha12
9.83	9.86	9.92	rabbit
9.92	9.98	10.01	nlsv2
12.04	12.07	12.07	trivium
13.34	13.37	13.37	salsa20
13.75	13.90	13.99	sosemanuk
14.82	14.85	14.85	chacha20
15.52	15.61	15.61	cryptmtv3
16.11	16.23	16.41	tpy6
17.21	17.24	17.30	lexv2
20.04	20.04	20.07	aes128estream
25.62	25.82	25.94	tpy
28.39	28.57	28.75	tpypy
31.99	32.05	32.08	aes256estream
33.26	33.29	33.32	dragon
60.56	60.62	61.36	hc128
169.14	172.57	175.61	hc256

Cycles/byte to encrypt 1536 bytes			
quartile	median	quartile	cipher
6.07	6.13	6.14	chacha8
6.77	6.80	6.96	snow20
6.87	6.87	6.87	salsa208
7.42	7.44	7.46	nlsv2
8.49	8.50	8.52	rabbit
8.54	8.59	8.64	tpy6
8.69	8.72	8.79	chacha12
8.29	9.57	9.61	salsa2012
10.27	10.27	10.28	trivium
10.93	10.96	10.99	sosemanuk
12.07	12.10	12.38	tpy
12.54	12.55	12.61	salsa20
12.77	12.78	12.78	chacha20
13.91	13.93	13.98	cryptmtv3
14.80	14.81	14.89	tpypy
14.68	15.06	16.04	lexv2
19.47	19.47	19.48	aes128estream
25.06	25.71	26.06	hc128
30.34	30.36	30.45	dragon
30.59	30.69	30.82	aes256estream
66.93	67.34	67.75	hc256

Cycles/byte to encrypt 4096 bytes			
quartile	median	quartile	cipher
5.72	5.74	5.77	`tpy6`
5.91	5.94	5.94	`chacha8`
6.13	6.16	6.23	`snow20`
6.36	6.36	6.39	`nlsv2`
6.49	6.49	6.49	`salsa208`
7.11	7.15	7.18	`tpy`
7.99	7.99	7.99	`rabbit`
8.50	8.50	8.52	`chacha12`
8.19	8.84	9.83	`salsa2012`
9.59	9.60	9.60	`trivium`
9.67	9.69	10.46	`sosemanuk`
9.67	9.74	9.85	`tpypy`
11.77	11.77	11.77	`cryptmtv3`
11.77	12.01	12.14	`hc128`
12.32	12.33	12.36	`salsa20`
12.65	12.65	12.65	`chacha20`
13.75	14.28	14.54	`lexv2`
19.27	19.27	19.28	`aes128estream`
28.77	28.93	29.39	`hc256`
29.19	29.24	29.29	`dragon`
30.16	30.24	30.26	`aes256estream`

Cycles/byte to encrypt long messages			
quartile	median	quartile	cipher
2.95	3.64	4.28	`hc128`
3.98	4.09	4.27	`tpy6`
4.08	4.22	4.34	`tpy`
5.77	5.78	5.87	`nlsv2`
5.73	5.80	5.98	`snow20`
5.76	5.81	5.88	`chacha8`
4.88	6.02	7.28	`hc256`
6.25	6.25	6.27	`salsa208`
6.61	6.81	7.13	`tpypy`
7.67	7.69	7.70	`rabbit`
6.70	8.02	11.29	`salsa2012`
8.46	8.47	8.77	`chacha12`
8.40	8.92	10.75	`sosemanuk`
9.18	9.20	9.21	`trivium`
10.11	10.19	10.22	`cryptmtv3`
12.14	12.21	12.29	`salsa20`
12.63	12.63	12.63	`chacha20`
12.41	14.24	14.94	`lexv2`
19.15	19.17	19.36	`aes128estream`
28.31	28.55	28.70	`dragon`
29.82	30.08	30.15	`aes256estream`

Chapter 8

Measurements of public-key secret-sharing systems

8.1 Introduction

This chapter presents a series of graphs, one for each computer. There are five horizontal positions on each graph:

- Time to compute a shared secret, given one user's secret key and another user's public key.
- Time to compute a key pair.
- Space for a secret key.
- Space for a public key.
- Space for a shared secret.

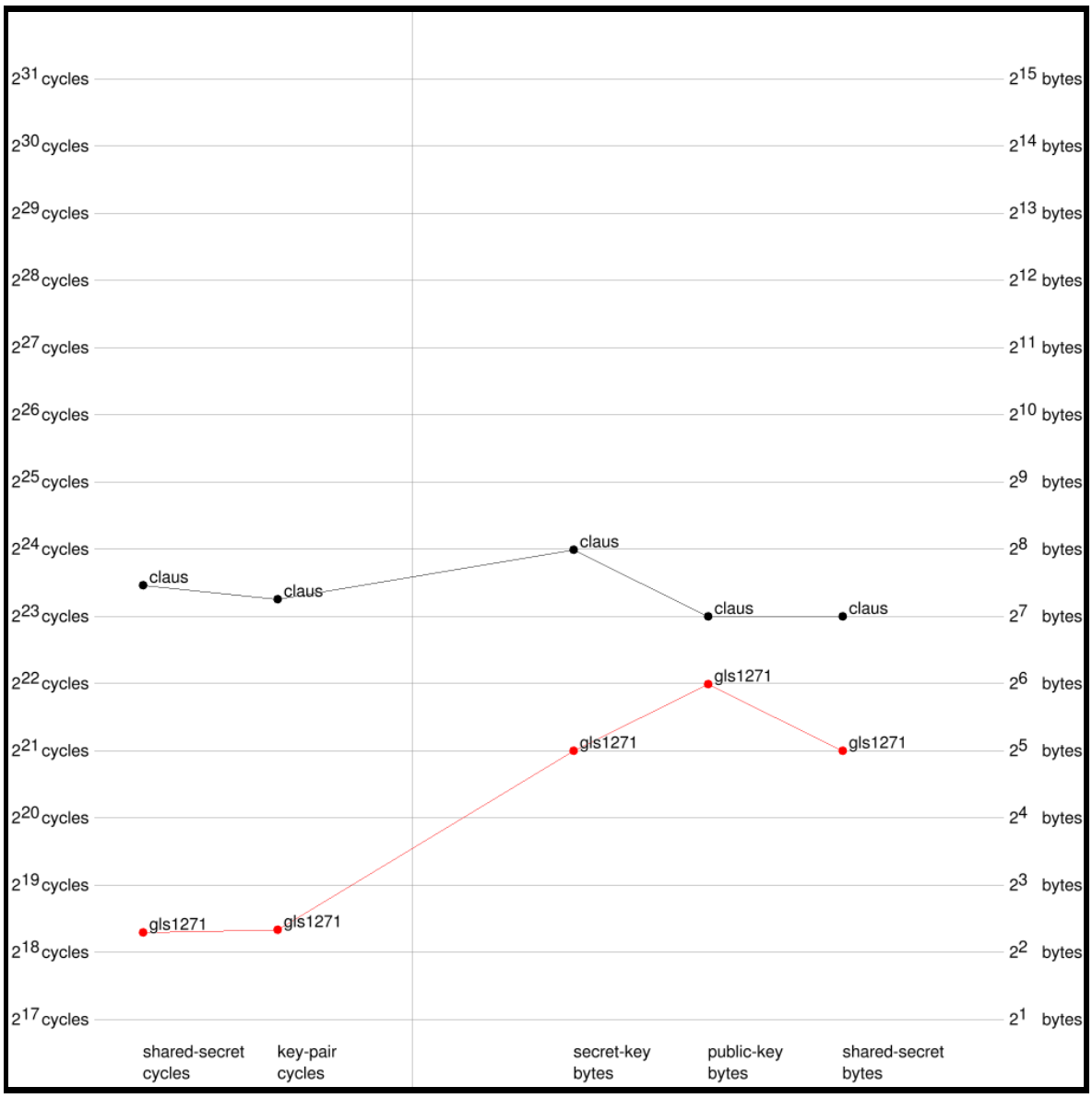
Each graph is a superimposition of several curves, one curve for each secret-sharing system.

This chapter also presents a series of tables, five for each computer. The first table shows the time, in cycles, to generate a key pair. Each row of the table lists

- the first quartile of many time measurements,
- the median of many time measurements,
- the third quartile of many time measurements, and
- the name of the secret-sharing system.

The second table shows the length of a secret key. The third table shows the length of a public key. The fourth table shows the time to compute a shared secret. The fifth table shows the length of the shared secret.

8.2 amd64, 1403MHz, AMD Opteron 240 (f58), `nmisles8amd64`



Cycles to generate a key pair			
quartile	median	quartile	system
326814	331602	335978	`gls1271`
10054797	10060916	10068180	`claus`

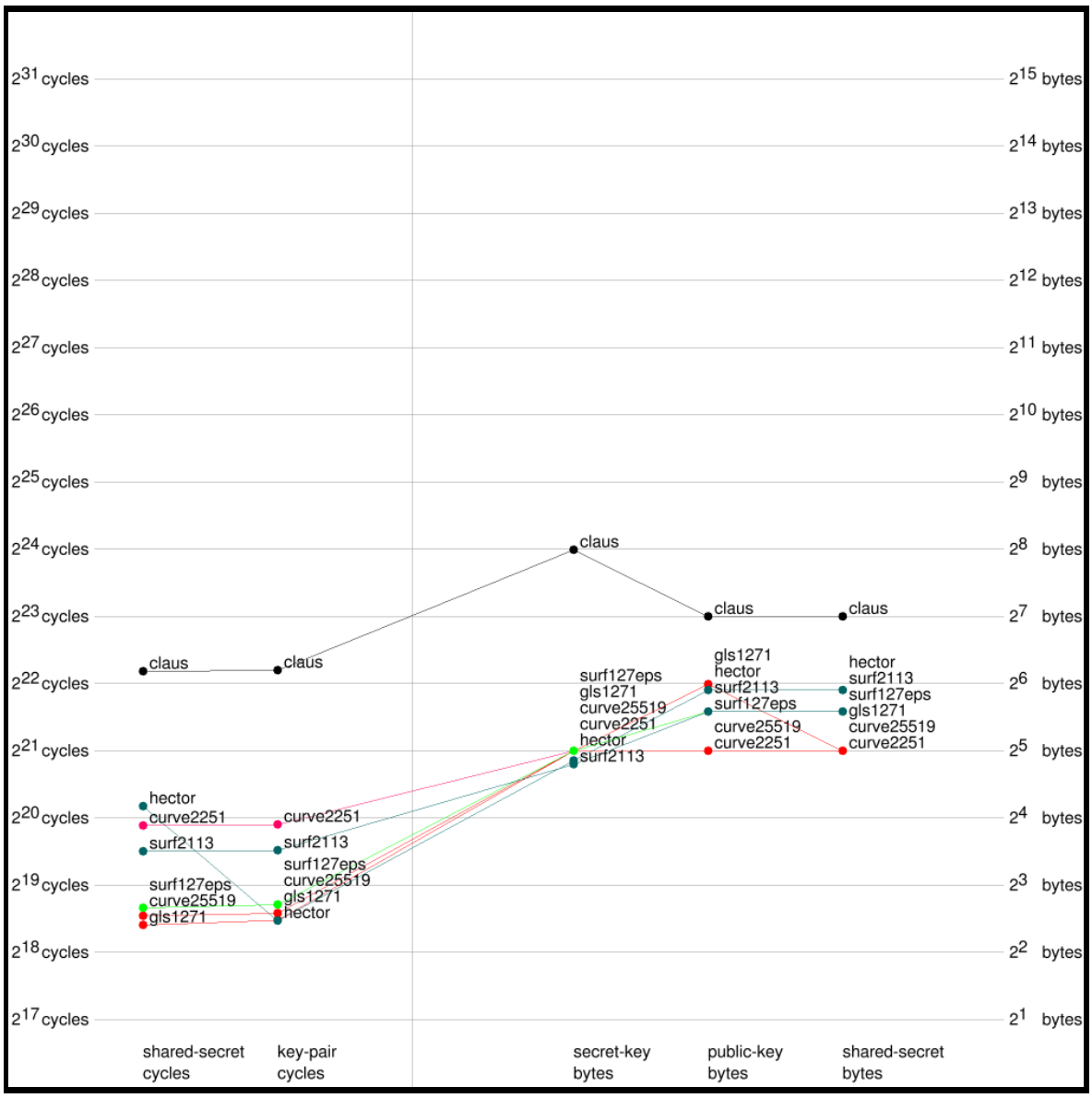
Secret key	
bytes	system
32	`gls1271`
256	`claus`

Public key	
bytes	system
64	`gls1271`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
322904	323621	326875	`gls1271`
11531129	11586938	11634926	`claus`

Shared secret	
bytes	system
32	`gls1271`
128	`claus`

8.3 amd64, 2400MHz, Intel Core 2 Duo (6fb), `utrecht`



Cycles to generate a key pair			
quartile	median	quartile	system
361512	365436	405873	`hector`
361962	366111	369936	`gls1271`
393003	394623	395757	`curve25519`
428607	430344	431973	`surf127eps`
750501	753813	756306	`surf2113`
980343	984159	985626	`curve2251`
4809492	4819482	4830561	`claus`

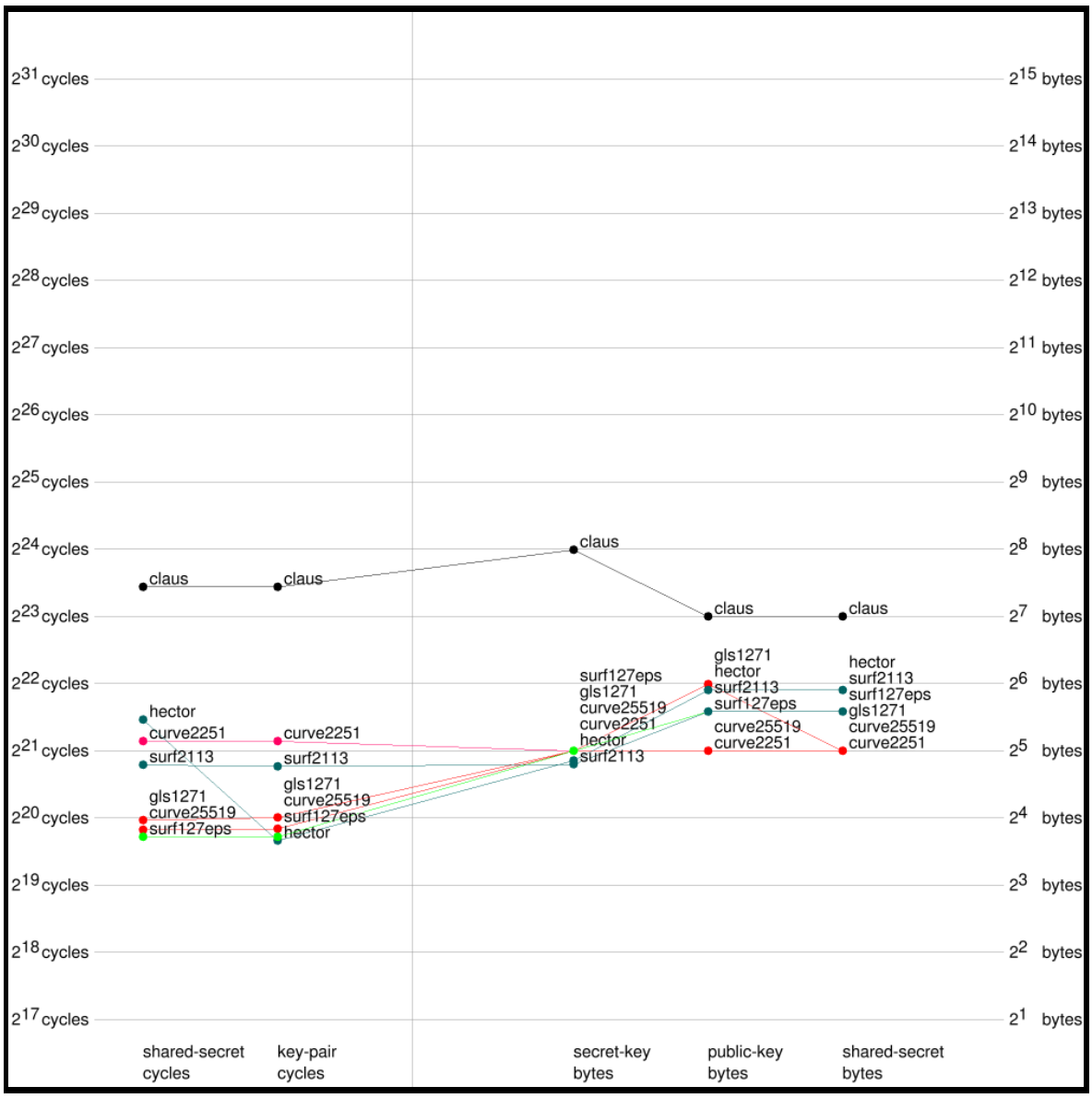
Secret key	
bytes	system
28	`surf2113`
29	`hector`
32	`curve2251`
32	`curve25519`
32	`gls1271`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve2251`
32	`curve25519`
48	`surf127eps`
48	`surf2113`
60	`hector`
64	`gls1271`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
342180	348516	353106	`gls1271`
382617	383202	383715	`curve25519`
416241	417024	418041	`surf127eps`
743904	744075	744615	`surf2113`
971883	974601	974925	`curve2251`
1176957	1184706	1189881	`hector`
4782609	4786704	4787424	`claus`

Shared secret	
bytes	system
32	`curve2251`
32	`curve25519`
32	`gls1271`
48	`surf127eps`
48	`surf2113`
60	`hector`
128	`claus`

8.4 amd64, 2800MHz, Intel Xeon (f41), nmi0056



Cycles to generate a key pair			
quartile	median	quartile	system
807317	835121	869806	`hector`
849723	864976	873565	`surf127eps`
938609	943537	950439	`curve25519`
1045772	1056965	1072127	`gls1271`
1782872	1790915	1800561	`surf2113`
2303910	2319604	2330678	`curve2251`
11415383	11438021	11468940	`claus`

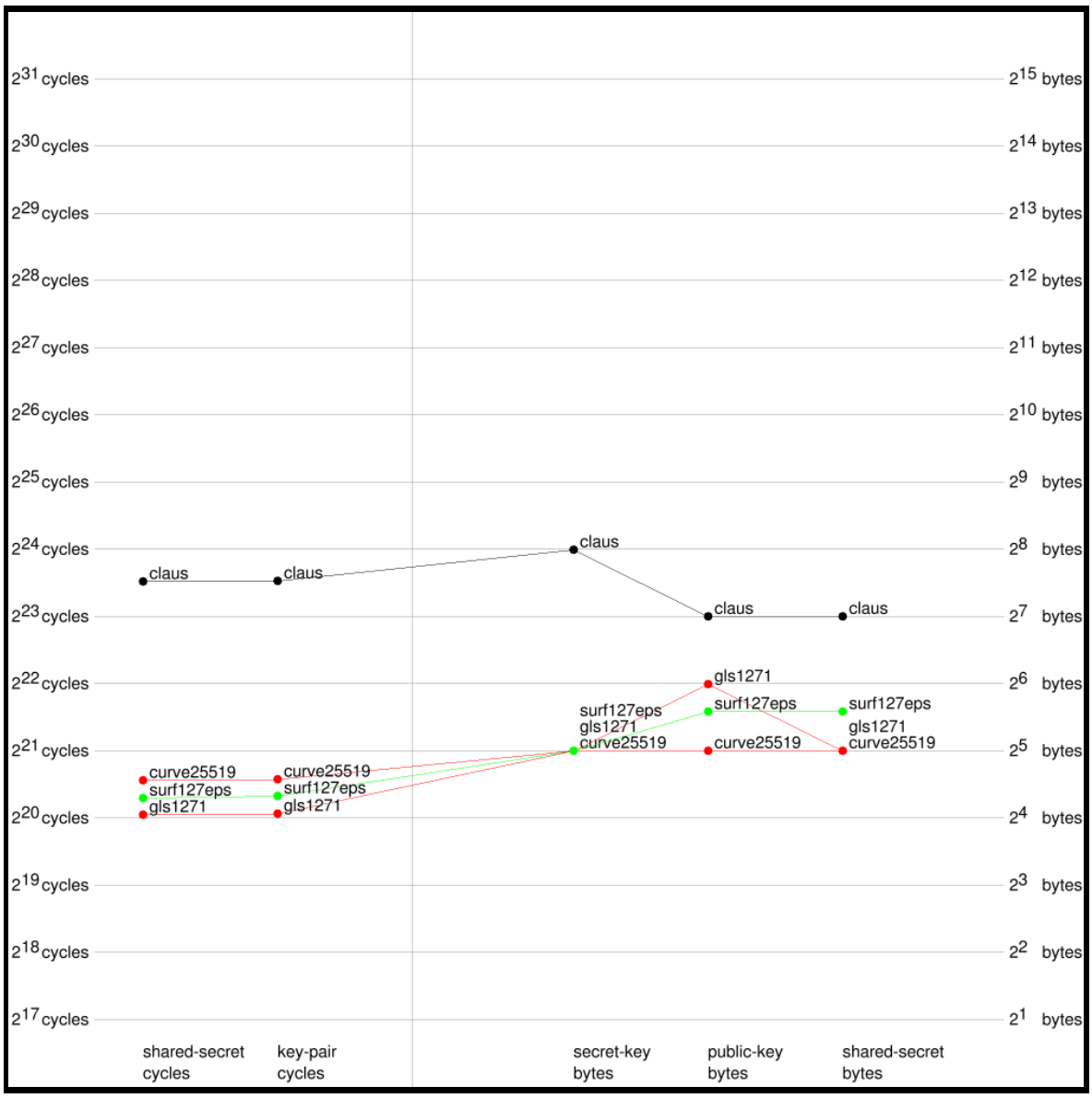
Secret key	
bytes	system
28	`surf2113`
29	`hector`
32	`curve2251`
32	`curve25519`
32	`gls1271`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve2251`
32	`curve25519`
48	`surf127eps`
48	`surf2113`
60	`hector`
64	`gls1271`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
843976	864409	879977	`surf127eps`
925918	930566	939015	`curve25519`
1015231	1030708	1042587	`gls1271`
1816514	1819237	1831508	`surf2113`
2307452	2317560	2325148	`curve2251`
2882432	2893009	2904209	`hector`
11386949	11419163	11447891	`claus`

Shared secret	
bytes	system
32	`curve2251`
32	`curve25519`
32	`gls1271`
48	`surf127eps`
48	`surf2113`
60	`hector`
128	`claus`

8.5 amd64, 2800MHz, Intel Xeon (f41), nmi0057



Cycles to generate a key pair			
quartile	median	quartile	system
1076901	1098111	1437828	`gls1271`
1302378	1320704	1333906	`surf127eps`
1547882	1567279	1598562	`curve25519`
12052572	12159896	15260308	`claus`

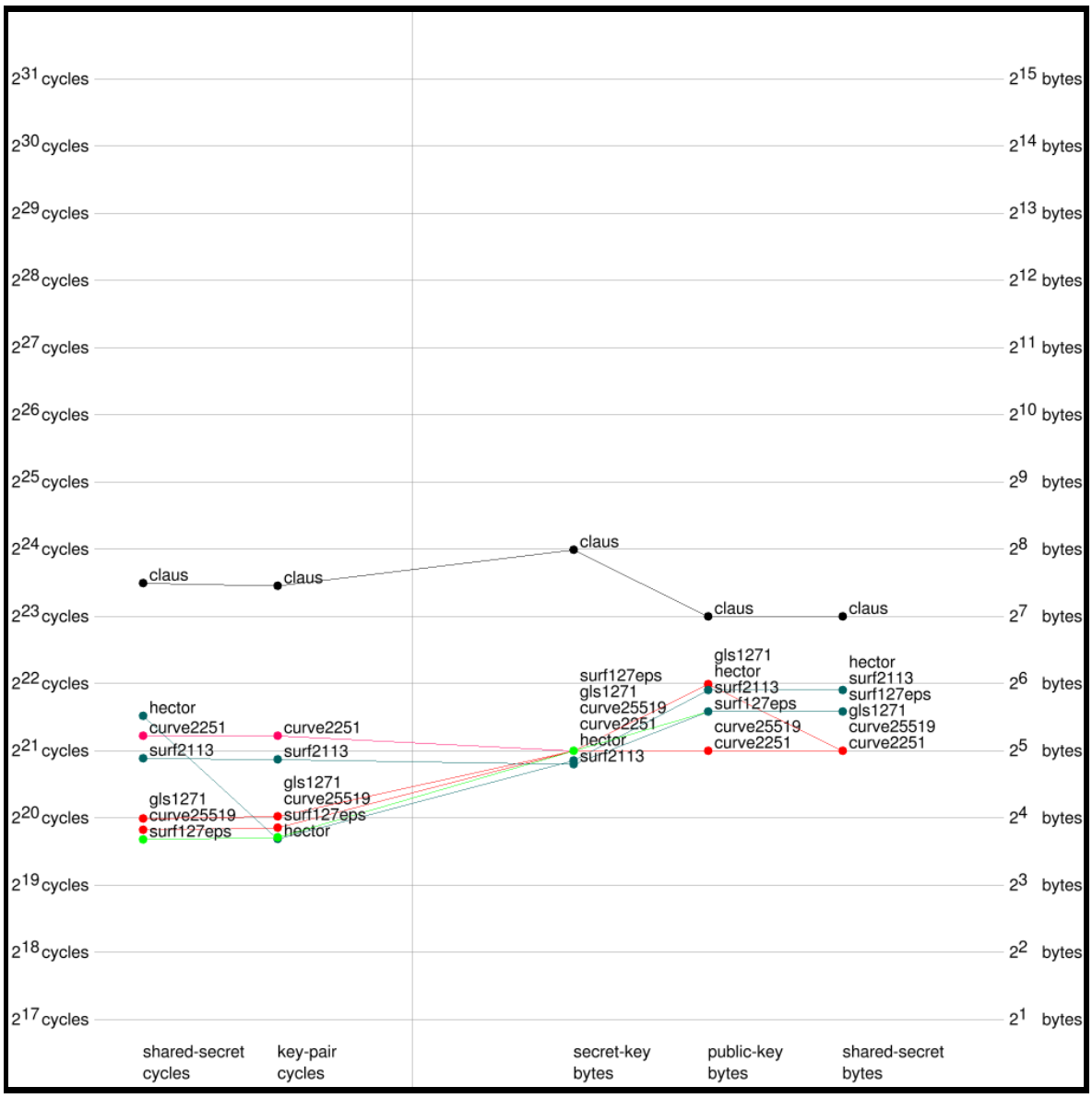
Secret key	
bytes	system
32	`curve25519`
32	`gls1271`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve25519`
48	`surf127eps`
64	`gls1271`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
1066618	1085329	1617035	`gls1271`
1277892	1294314	1302406	`surf127eps`
1524929	1547147	1620199	`curve25519`
12004559	12081412	14066206	`claus`

Shared secret	
bytes	system
32	`curve25519`
32	`gls1271`
48	`surf127eps`
128	`claus`

8.6 amd64, 2800MHz, Intel Xeon (f41), nmi0063



Cycles to generate a key pair			
quartile	median	quartile	system
835786	847588	901138	`hector`
854210	862561	876148	`surf127eps`
941129	951538	963172	`curve25519`
1057028	1068753	1083397	`gls1271`
1911658	1927534	1937068	`surf2113`
2448768	2459401	2472568	`curve2251`
10759210	11552226	11921063	`claus`

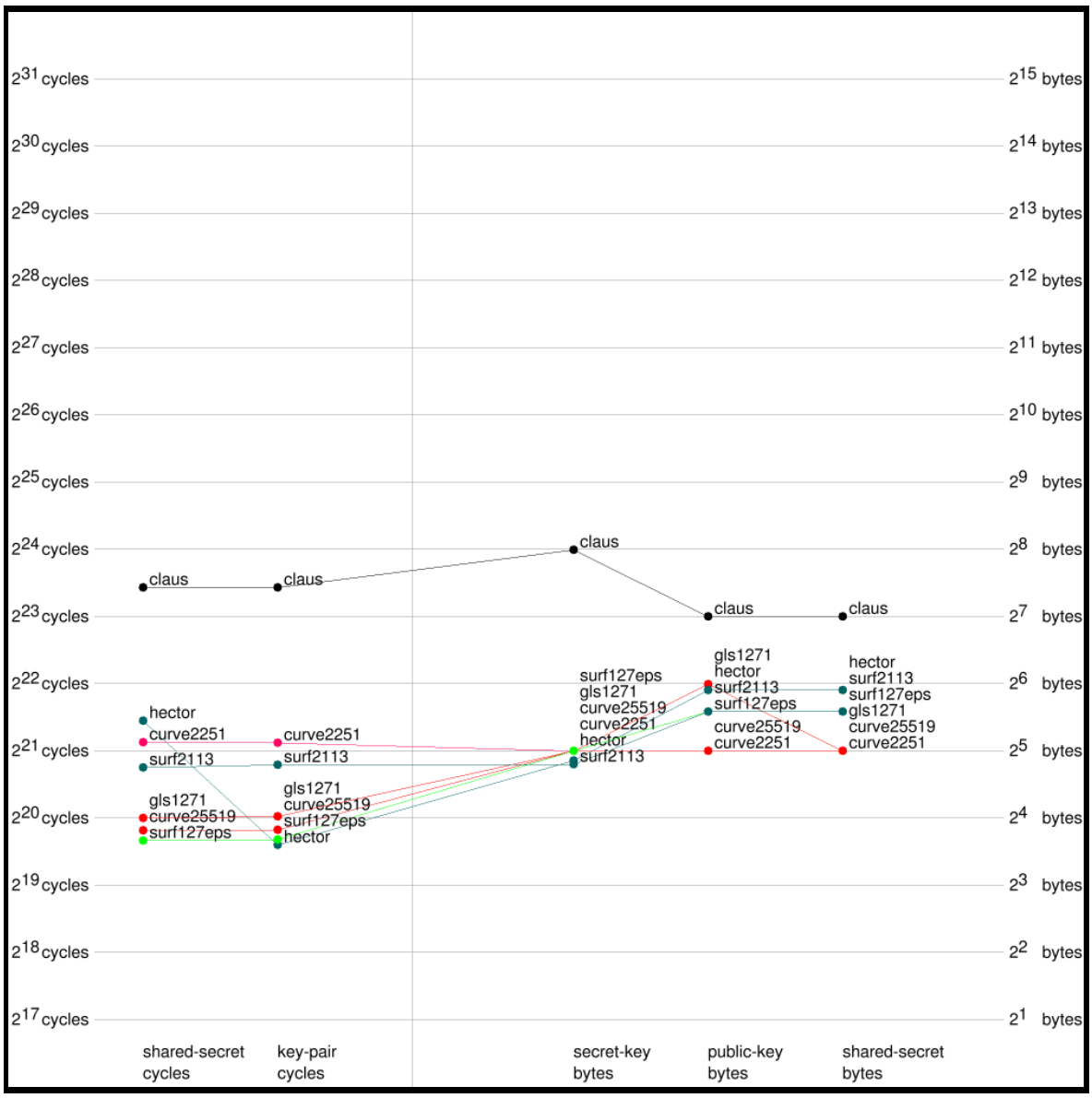
Secret key	
bytes	system
28	`surf2113`
29	`hector`
32	`curve2251`
32	`curve25519`
32	`gls1271`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve2251`
32	`curve25519`
48	`surf127eps`
48	`surf2113`
60	`hector`
64	`gls1271`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
827309	840525	859474	`surf127eps`
922488	931455	938721	`curve25519`
1033991	1046157	1058904	`gls1271`
1925105	1941597	1944957	`surf2113`
2447620	2457434	2465799	`curve2251`
2988132	3008838	3022957	`hector`
11870446	11883711	11901260	`claus`

Shared secret	
bytes	system
32	`curve2251`
32	`curve25519`
32	`gls1271`
48	`surf127eps`
48	`surf2113`
60	`hector`
128	`claus`

8.7 amd64, 3000MHz, Intel Pentium D (f64), speed



Cycles to generate a key pair			
quartile	median	quartile	system
787140	798330	849690	`hector`
833745	842940	863355	`surf127eps`
927915	932730	939480	`curve25519`
1055490	1066860	1079130	`gls1271`
1816710	1825500	1829475	`surf2113`
2282325	2291130	2299515	`curve2251`
11196765	11333445	11407575	`claus`

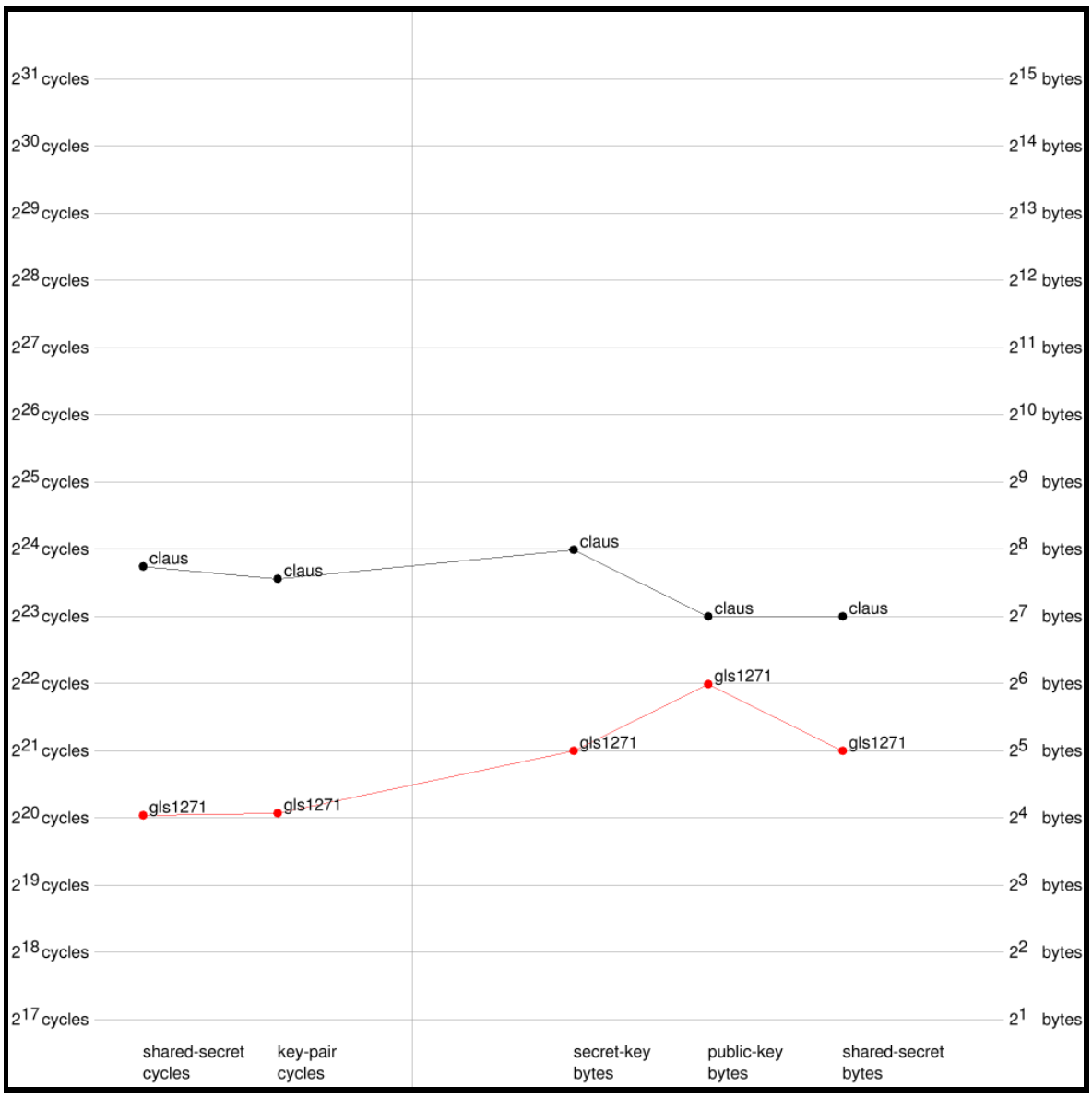
Secret key	
bytes	system
28	`surf2113`
29	`hector`
32	`curve2251`
32	`curve25519`
32	`gls1271`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve2251`
32	`curve25519`
48	`surf127eps`
48	`surf2113`
60	`hector`
64	`gls1271`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
824175	835200	859380	`surf127eps`
913545	927555	936180	`curve25519`
1035975	1052340	1056540	`gls1271`
1767105	1768560	1770300	`surf2113`
2295750	2300850	2304660	`curve2251`
2857095	2873760	2885235	`hector`
11153430	11370525	11375685	`claus`

Shared secret	
bytes	system
32	`curve2251`
32	`curve25519`
32	`gls1271`
48	`surf127eps`
48	`surf2113`
60	`hector`
128	`claus`

8.8 amd64, 3000MHz, Intel Xeon (f4a), `nmi0090`



Cycles to generate a key pair			
quartile	median	quartile	system
1091655	1104300	1118325	`gls1271`
12377527	12389093	12399705	`claus`

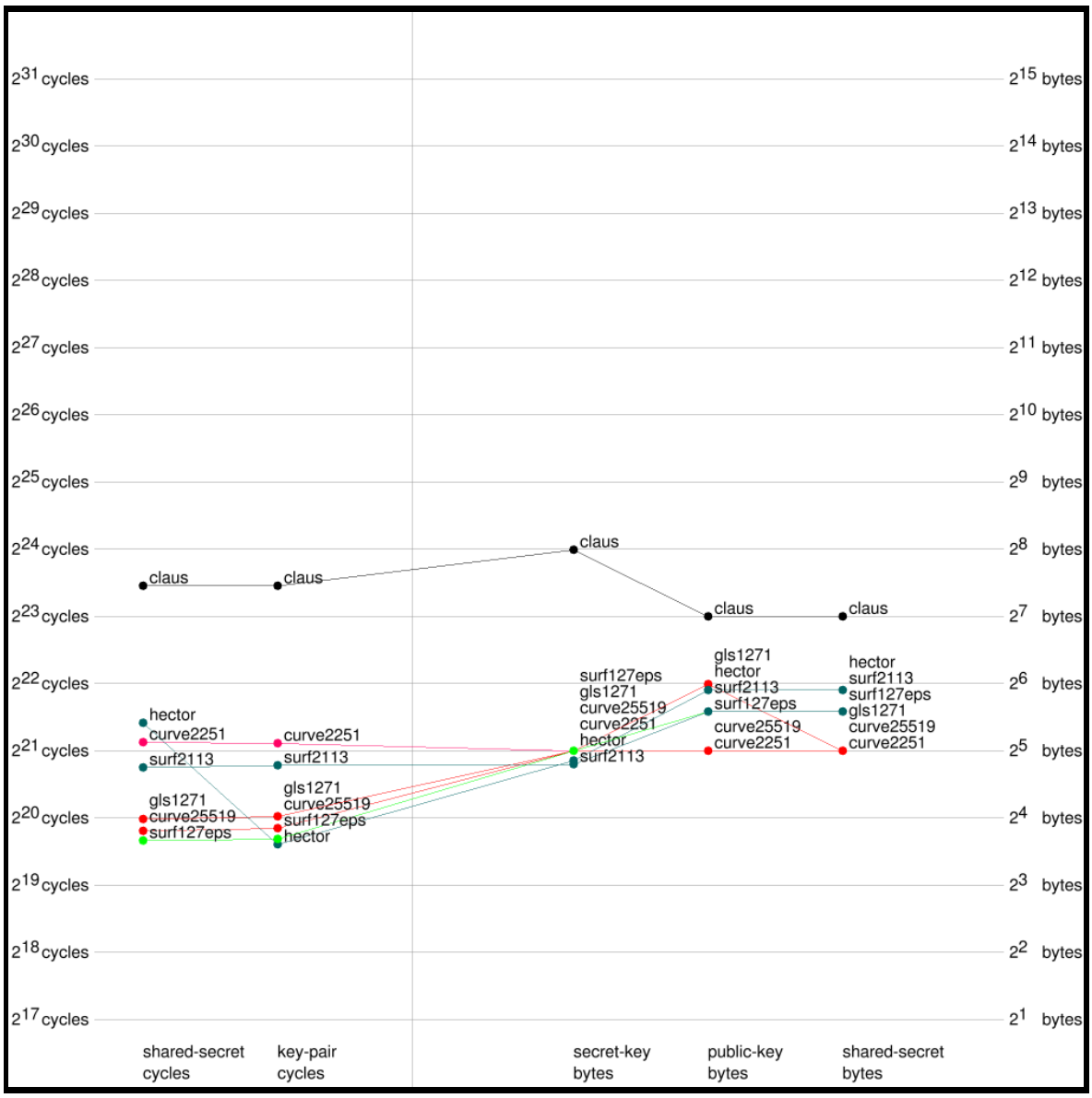
Secret key	
bytes	system
32	`gls1271`
256	`claus`

Public key	
bytes	system
64	`gls1271`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
1050667	1080458	1091790	`gls1271`
14066355	14081617	14098987	`claus`

Shared secret	
bytes	system
32	`gls1271`
128	`claus`

8.9 amd64, 3392MHz, Intel Pentium D (f64), nmi0104



Cycles to generate a key pair			
quartile	median	quartile	system
793339	803080	855321	`hector`
833425	848045	875109	`surf127eps`
938655	946458	952714	`curve25519`
1057791	1072071	1084209	`gls1271`
1802578	1811588	1815736	`surf2113`
2266593	2273342	2278510	`curve2251`
11507300	11535639	11568687	`claus`

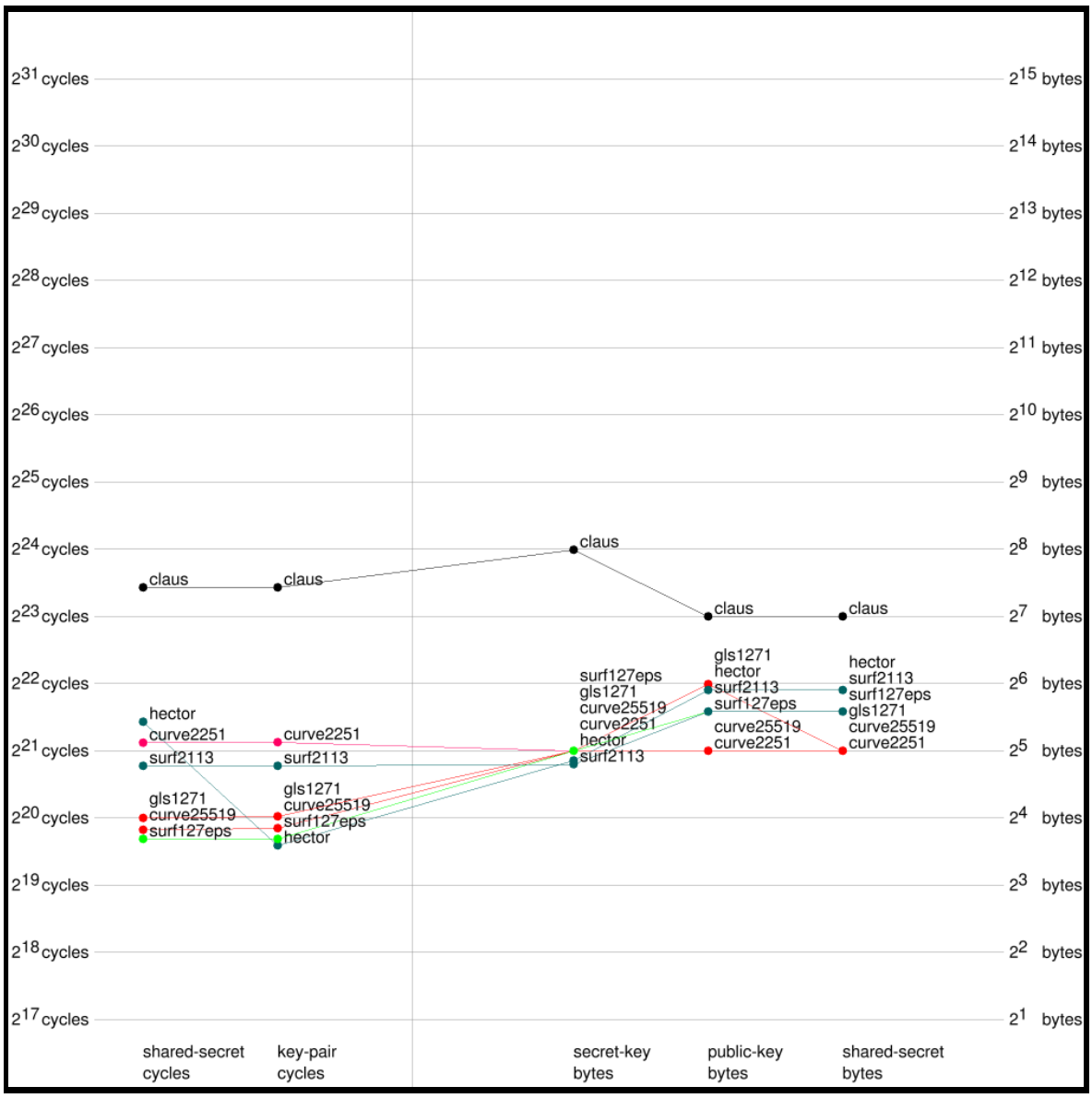
Secret key	
bytes	system
28	`surf2113`
29	`hector`
32	`curve2251`
32	`curve25519`
32	`gls1271`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve2251`
32	`curve25519`
48	`surf127eps`
48	`surf2113`
60	`hector`
64	`gls1271`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
818159	835074	841942	`surf127eps`
913750	920686	936156	`curve25519`
1022431	1041624	1055615	`gls1271`
1763631	1765960	1769394	`surf2113`
2285769	2292314	2295119	`curve2251`
2783801	2802110	2814639	`hector`
11506875	11525779	11552809	`claus`

Shared secret	
bytes	system
32	`curve2251`
32	`curve25519`
32	`gls1271`
48	`surf127eps`
48	`surf2113`
60	`hector`
128	`claus`

8.10 amd64, 3392MHz, Intel Pentium D (f64), nmi0161



Cycles to generate a key pair			
quartile	median	quartile	system
782816	794155	845308	`hector`
832490	846107	870621	`surf127eps`
937431	947155	952493	`curve25519`
1058964	1071646	1082611	`gls1271`
1788043	1796305	1800266	`surf2113`
2281638	2293368	2304333	`curve2251`
11349863	11368342	11390272	`claus`

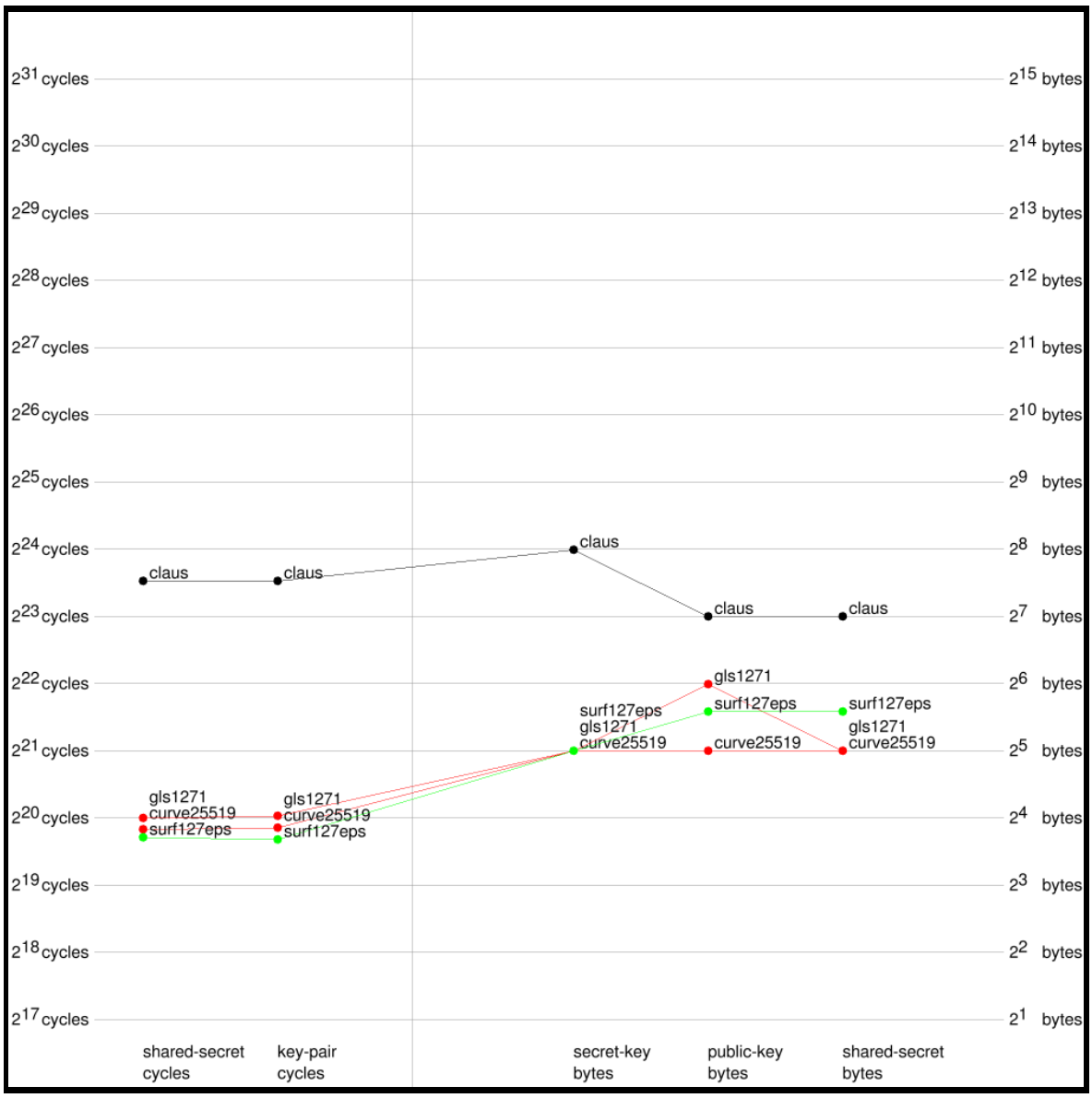
Secret key	
bytes	system
28	`surf2113`
29	`hector`
32	`curve2251`
32	`curve25519`
32	`gls1271`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve2251`
32	`curve25519`
48	`surf127eps`
48	`surf2113`
60	`hector`
64	`gls1271`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
845597	849031	853944	`surf127eps`
920771	928608	933895	`curve25519`
1032138	1051535	1063775	`gls1271`
1797784	1798991	1801201	`surf2113`
2273104	2279904	2285735	`curve2251`
2822340	2840581	2850696	`hector`
10264498	11355218	11396562	`claus`

Shared secret	
bytes	system
32	`curve2251`
32	`curve25519`
32	`gls1271`
48	`surf127eps`
48	`surf2113`
60	`hector`
128	`claus`

8.11 amd64, 3392MHz, Intel Pentium D (f64), nmi0241



Cycles to generate a key pair			
quartile	median	quartile	system
837250	843880	869550	`surf127eps`
948328	953462	959242	`curve25519`
1063282	1075267	1086572	`gls1271`
12108658	12137388	12163194	`claus`

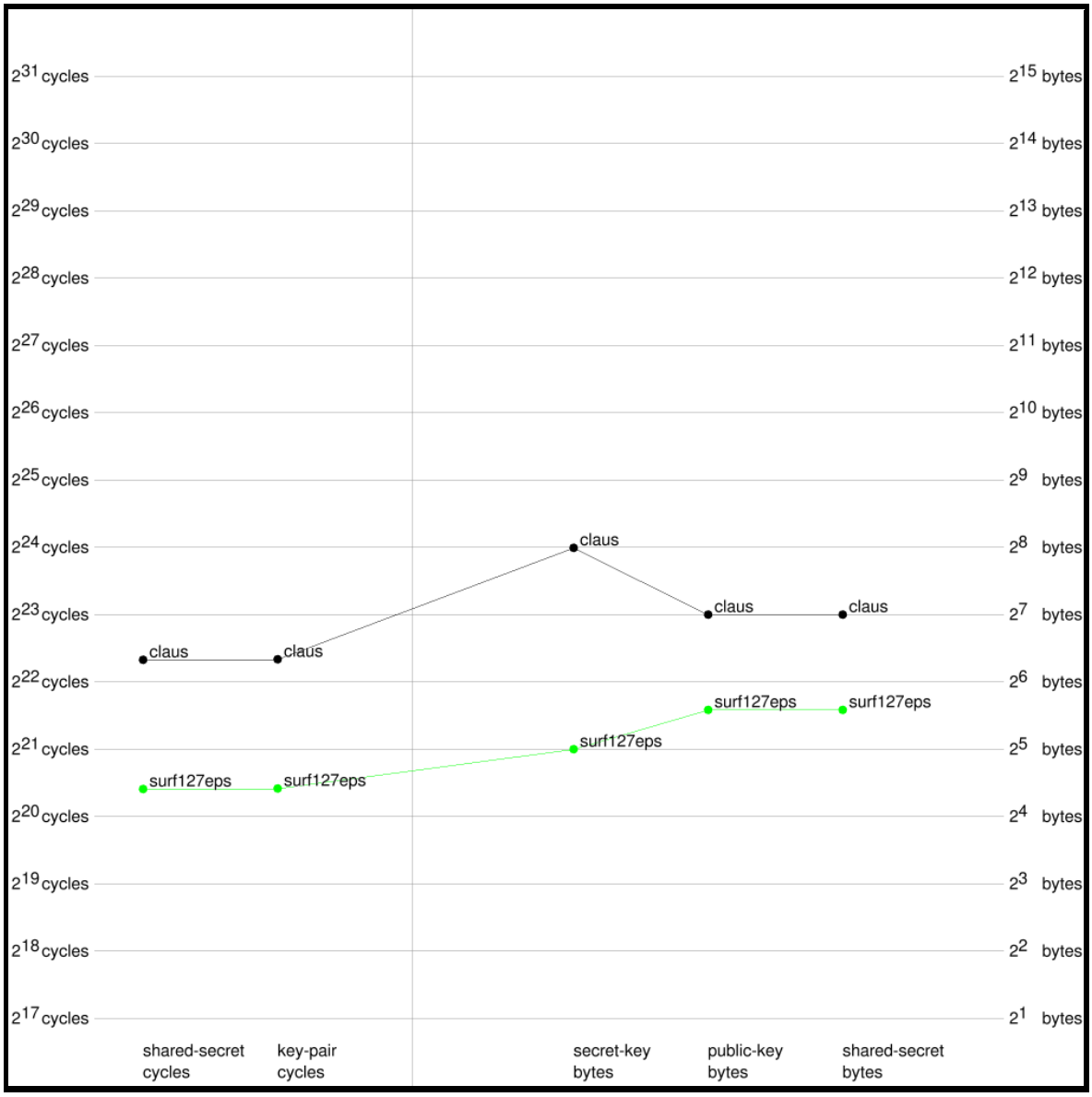
Secret key	
bytes	system
32	`curve25519`
32	`gls1271`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve25519`
48	`surf127eps`
64	`gls1271`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
851071	862920	884289	`surf127eps`
935221	937567	941851	`curve25519`
1035912	1053949	1061701	`gls1271`
12097234	12124706	12161562	`claus`

Shared secret	
bytes	system
32	`curve25519`
32	`gls1271`
48	`surf127eps`
128	`claus`

8.12 ia64, 900MHz, HP Itanium II, nmi0025



Cycles to generate a key pair			
quartile	median	quartile	system
1398889	1403511	1406192	`surf127eps`
5311891	5320472	5332705	`claus`

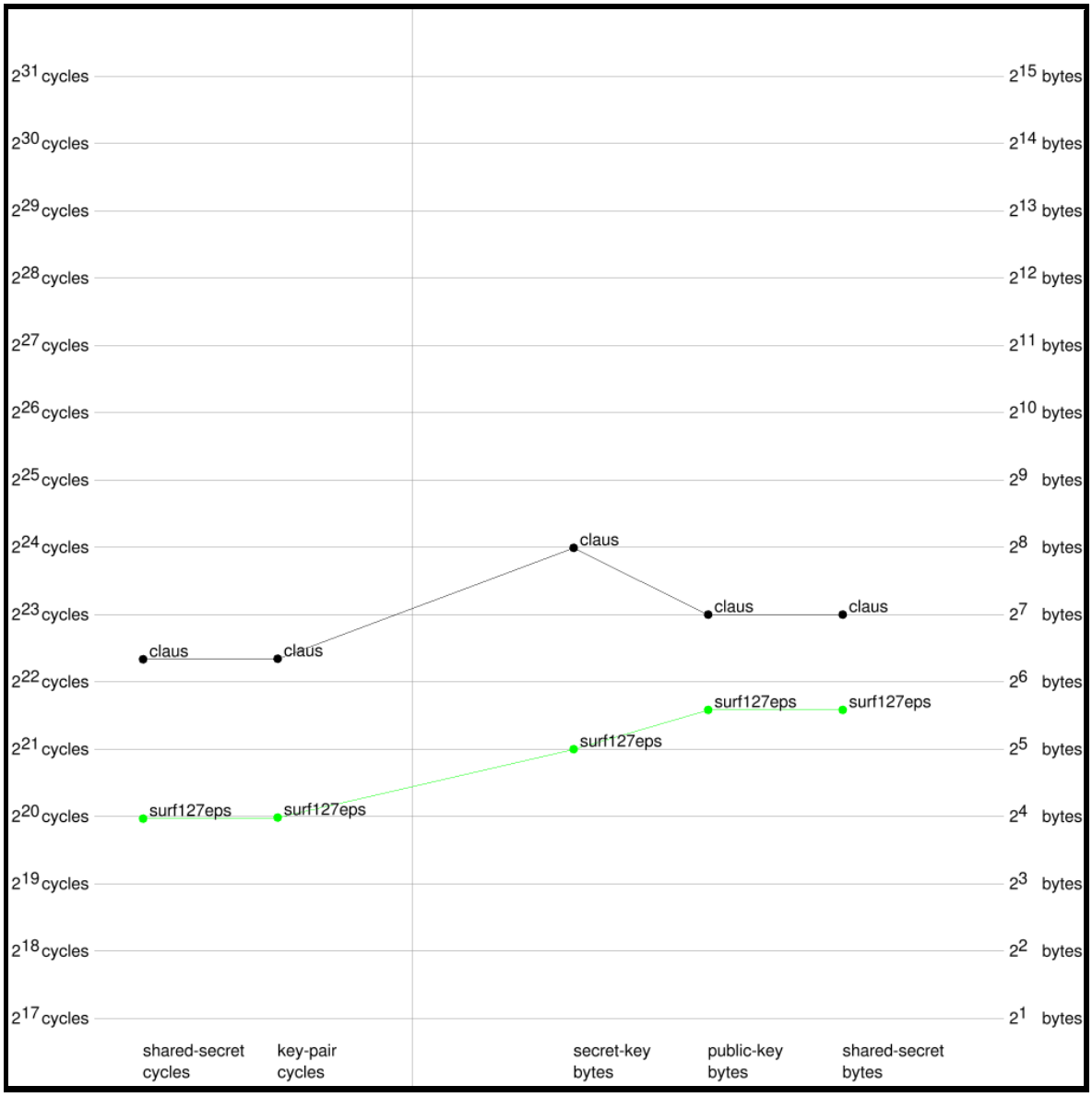
Secret key	
bytes	system
32	`surf127eps`
256	`claus`

Public key	
bytes	system
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
1388826	1393118	1394730	`surf127eps`
5276549	5278778	5298061	`claus`

Shared secret	
bytes	system
48	`surf127eps`
128	`claus`

8.13 ia64, 997MHz, HP Itanium II, `nmi0020`



Cycles to generate a key pair			
quartile	median	quartile	system
1035604	1037979	1040320	`surf127eps`
5335922	5342763	5352623	`claus`

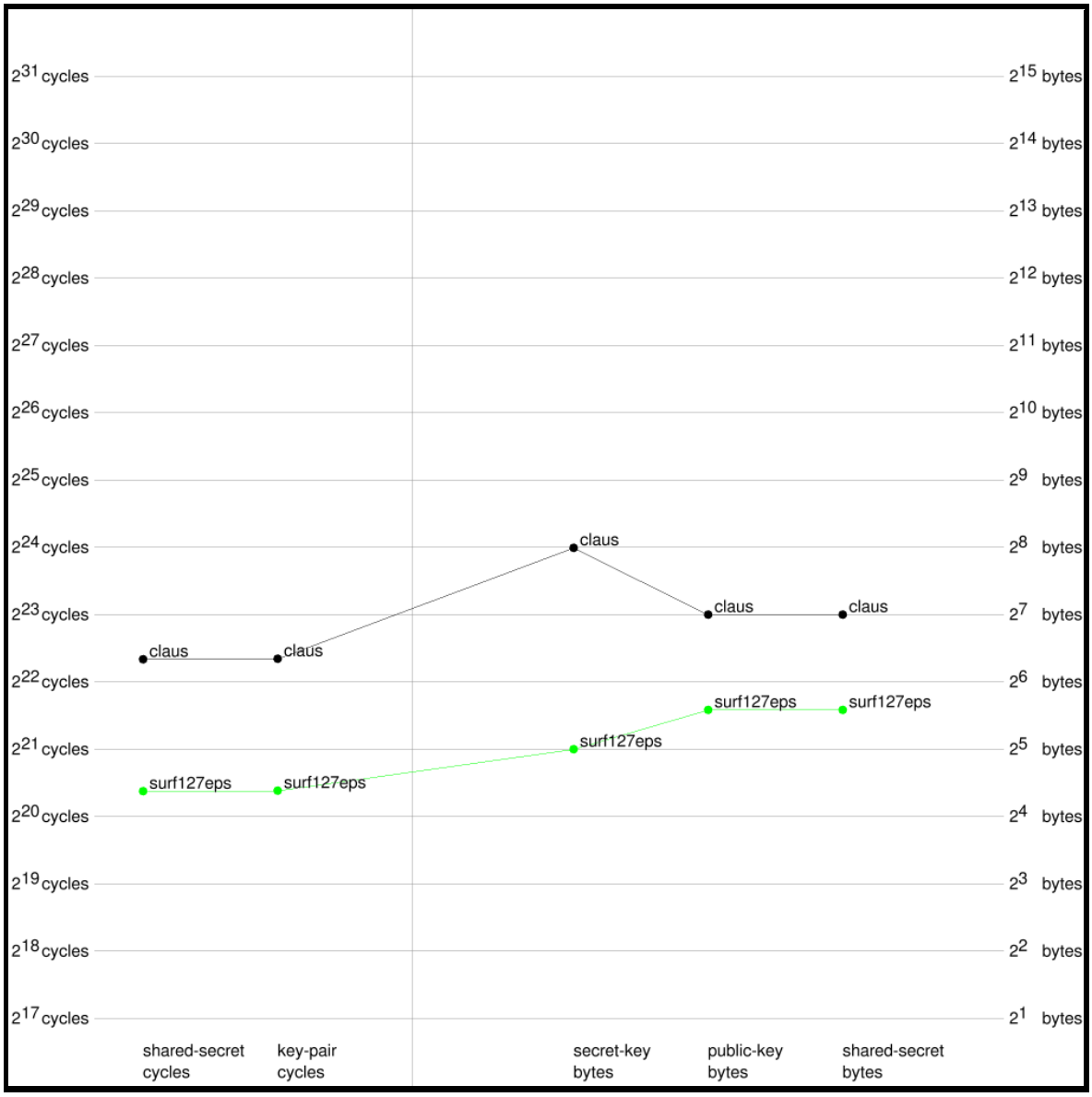
Secret key	
bytes	system
32	`surf127eps`
256	`claus`

Public key	
bytes	system
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
1026352	1029479	1029650	`surf127eps`
5314548	5316971	5331968	`claus`

Shared secret	
bytes	system
48	`surf127eps`
128	`claus`

8.14 ia64, 997MHz, HP Itanium II, nmi0058



Cycles to generate a key pair			
quartile	median	quartile	system
1370854	1375853	1378048	`surf127eps`
5327626	5335609	5347581	`claus`

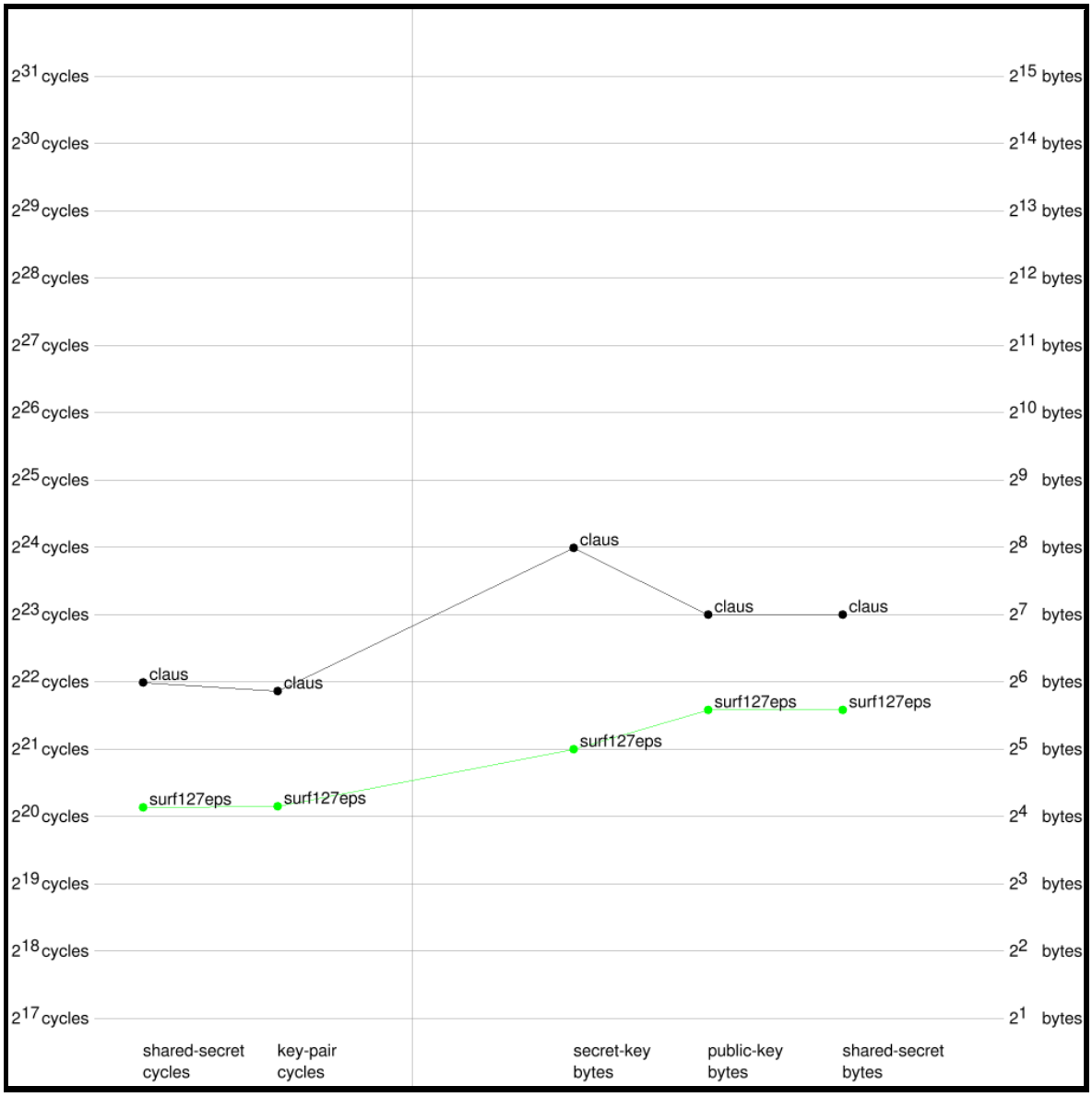
Secret key	
bytes	system
32	`surf127eps`
256	`claus`

Public key	
bytes	system
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
1363871	1365241	1366513	`surf127eps`
5294488	5295913	5314777	`claus`

Shared secret	
bytes	system
48	`surf127eps`
128	`claus`

8.15 ia64, 1396MHz, HP Itanium II, nmi0065



Cycles to generate a key pair			
quartile	median	quartile	system
1162893	1166353	1169735	`surf127eps`
3821371	3824635	3827840	`claus`

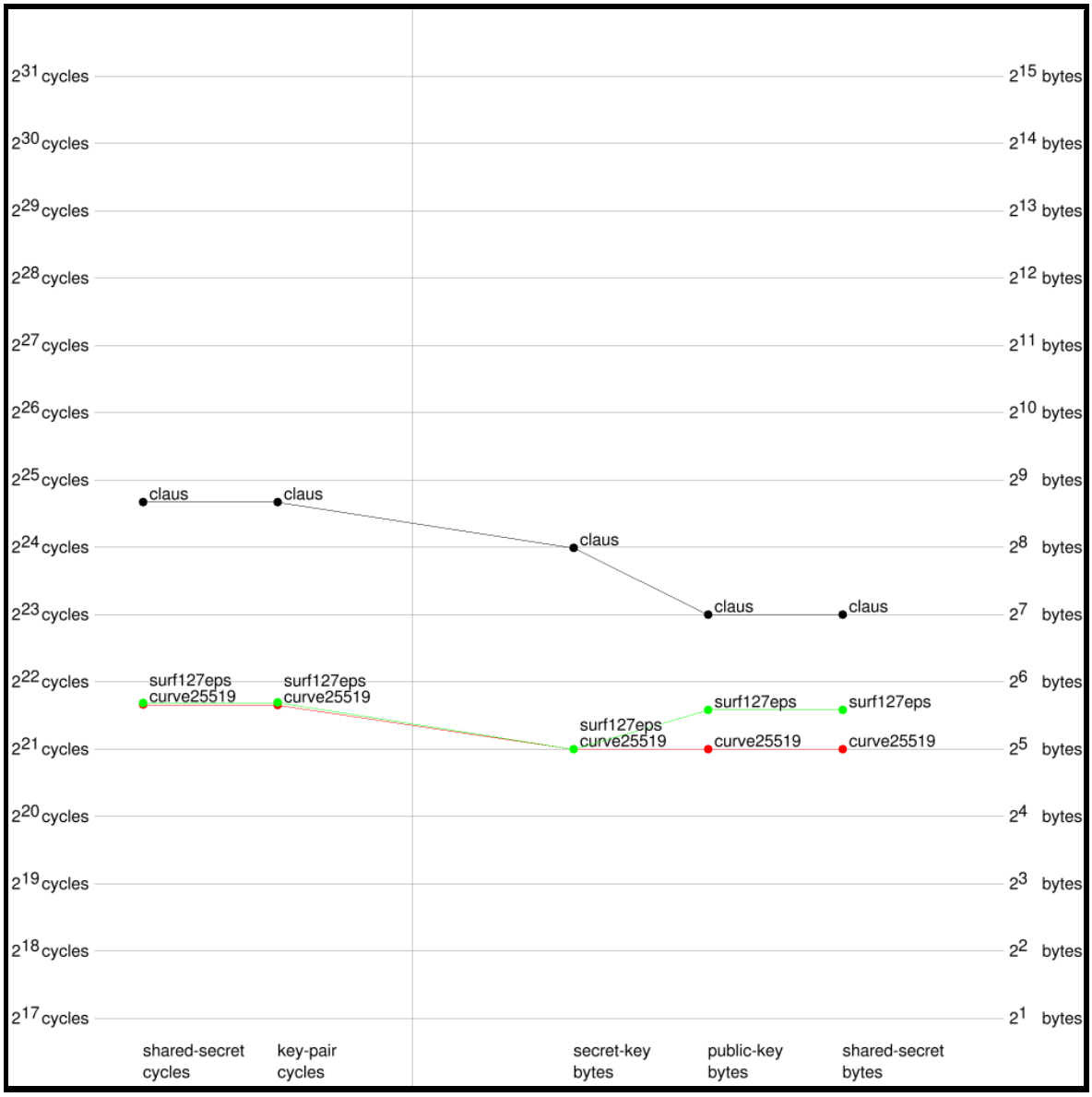
Secret key	
bytes	system
32	`surf127eps`
256	`claus`

Public key	
bytes	system
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
1155601	1158581	1159178	`surf127eps`
4167030	4174607	4184196	`claus`

Shared secret	
bytes	system
48	`surf127eps`
128	`claus`

8.16 ppc32, 400MHz, Motorola PowerPC G4 7400, `nmi0042`



Cycles to generate a key pair			
quartile	median	quartile	system
3308704	3320960	3327056	`curve25519`
3386848	3398752	3403440	`surf127eps`
26777104	26829472	26894912	`claus`

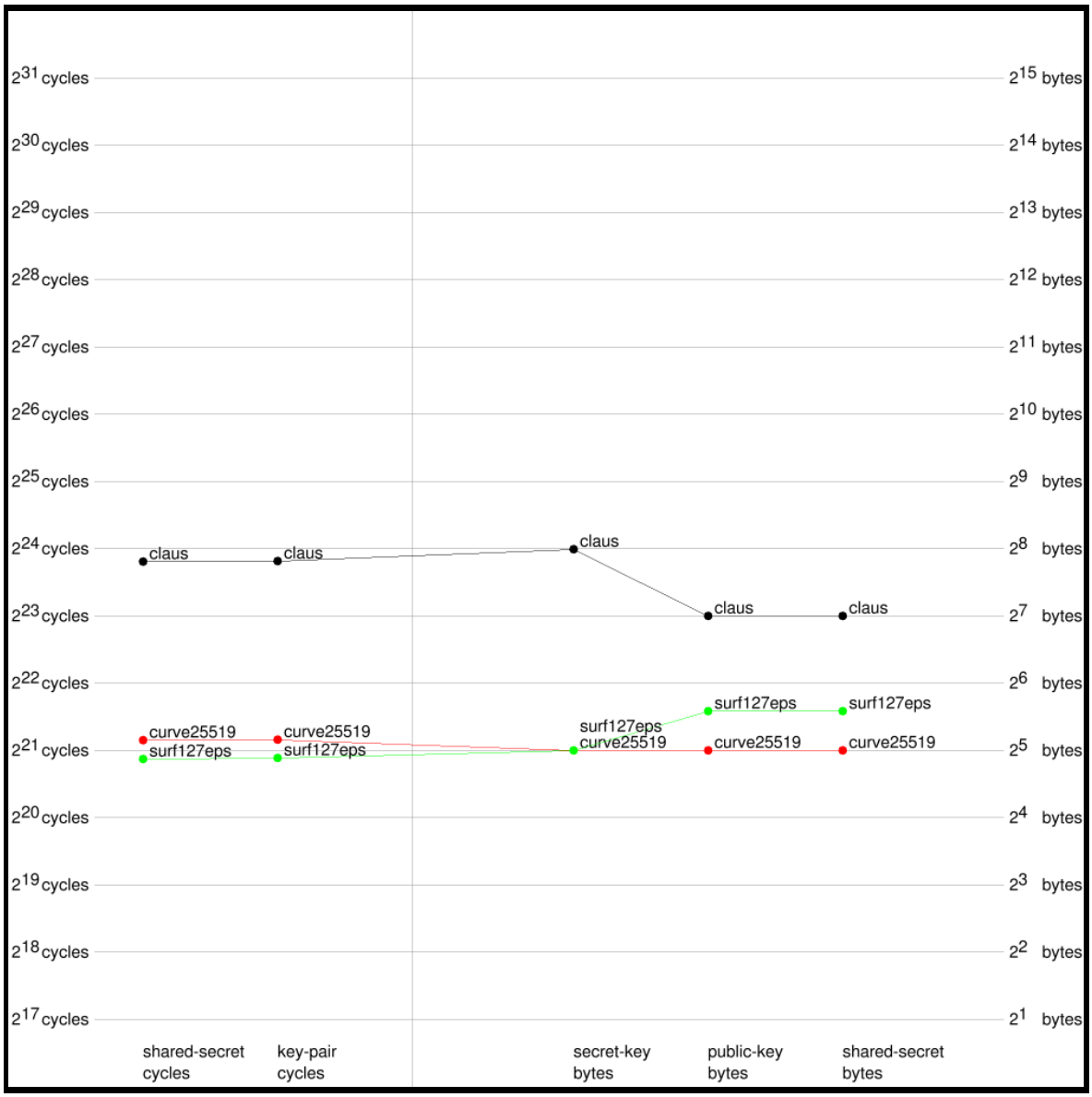
Secret key	
bytes	system
32	`curve25519`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
3327216	3333136	3335856	`curve25519`
3386448	3395680	3398576	`surf127eps`
26809376	26818160	26911680	`claus`

Shared secret	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

8.17 ppc32, 2000MHz, IBM PowerPC G5 970, geespaz



Cycles to generate a key pair			
quartile	median	quartile	system
1939380	1945620	1950480	`surf127eps`
2345040	2353920	2359140	`curve25519`
14763240	14787780	14820720	`claus`

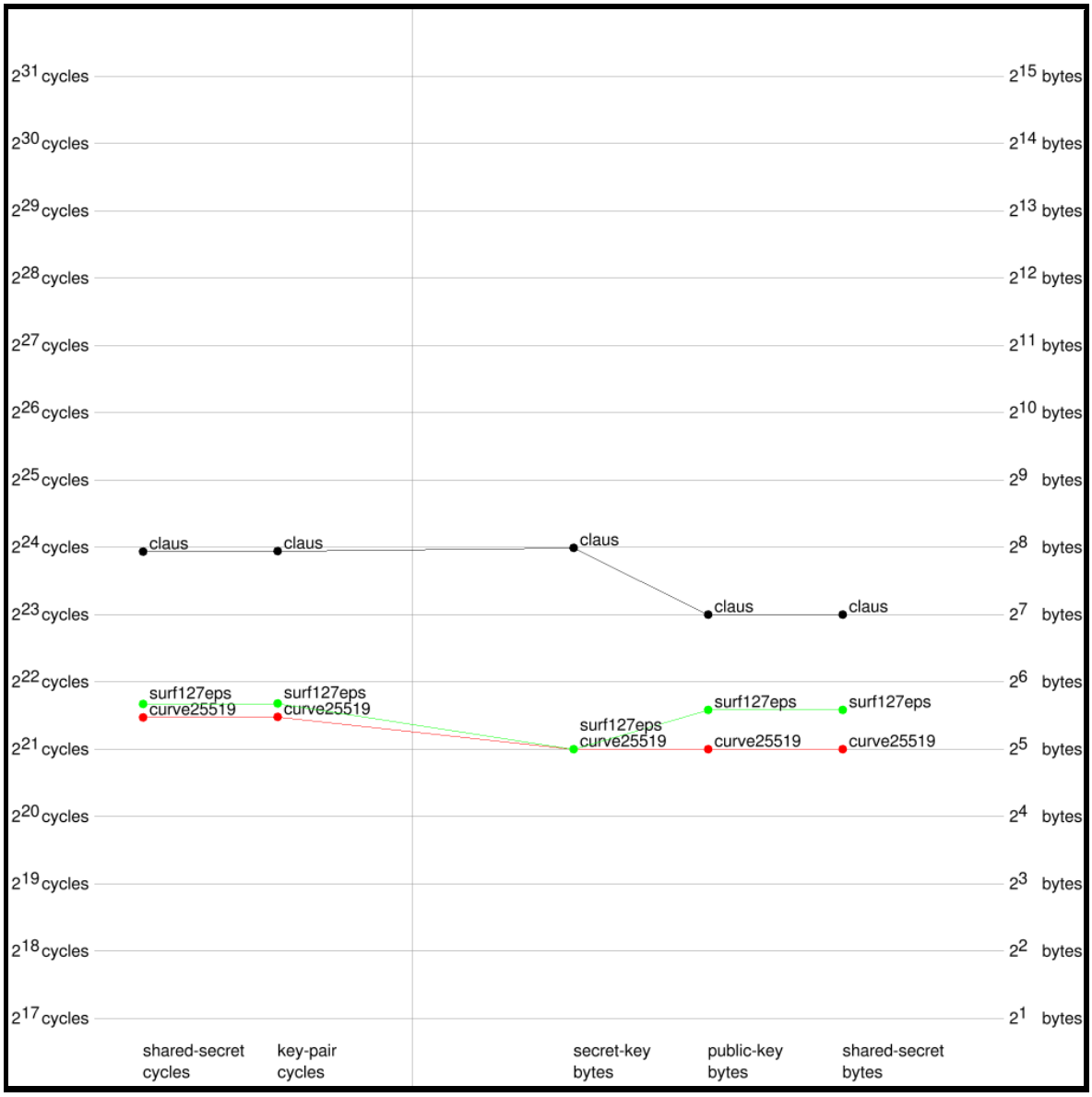
Secret key	
bytes	system
32	`curve25519`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
1923240	1927320	1931700	`surf127eps`
2335740	2340120	2341920	`curve25519`
14742960	14756220	14796300	`claus`

Shared secret	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

8.18 ppc32, 2097MHz, IBM POWER5, `nmi0154`



Cycles to generate a key pair			
quartile	median	quartile	system
2927124	2936176	2940860	`curve25519`
3361616	3372000	3382420	`surf127eps`
16149156	16188024	16220772	`claus`

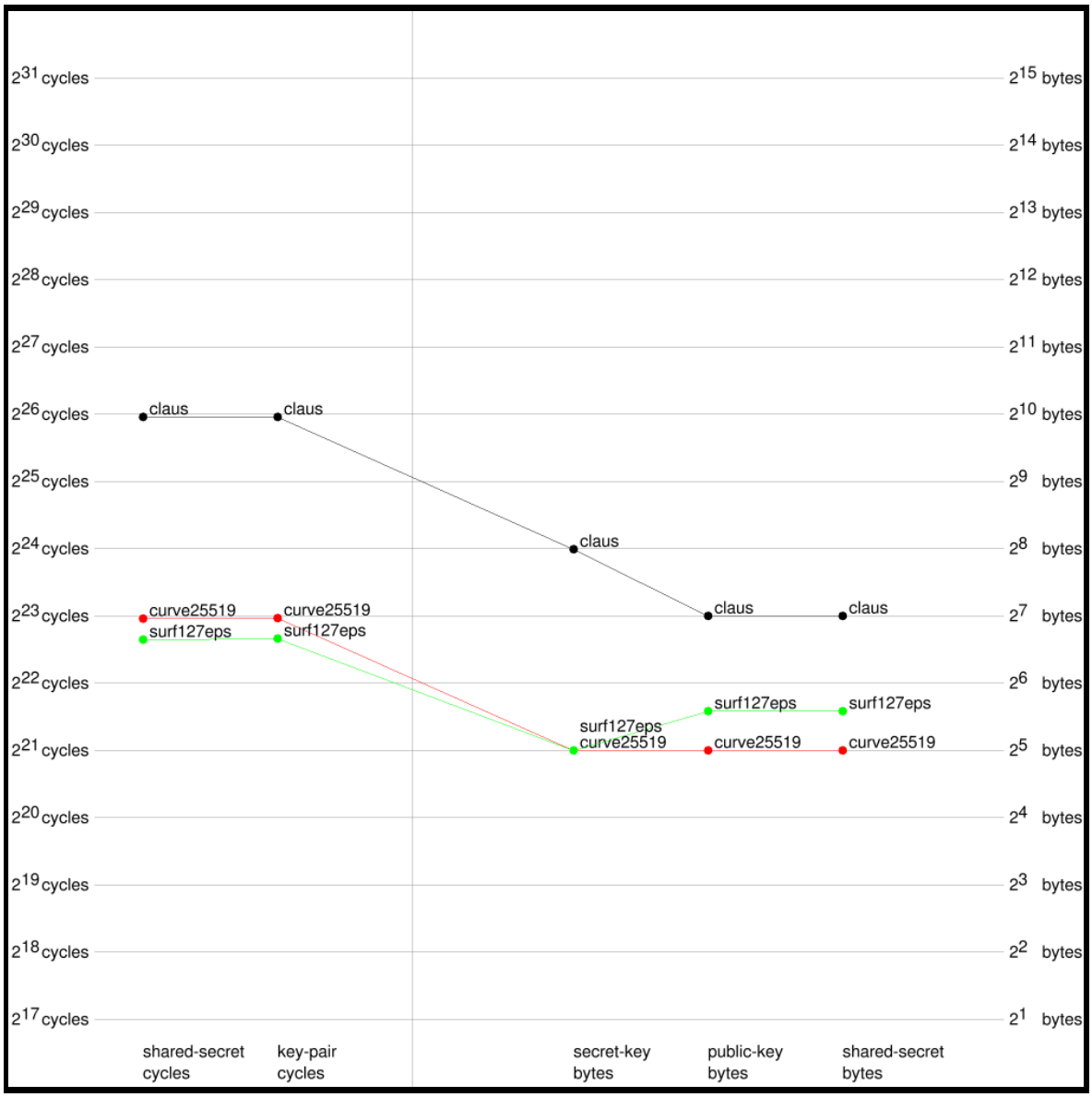
Secret key	
bytes	system
32	`curve25519`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
2907968	2911672	2914544	`curve25519`
3249492	3357300	3362800	`surf127eps`
16093332	16112376	16139656	`claus`

Shared secret	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

8.19 ppc32, 3192MHz, IBM Cell PPE, `nmips3`



Cycles to generate a key pair			
quartile	median	quartile	system
6643080	6666960	6680480	`surf127eps`
8209040	8240120	8312160	`curve25519`
65332920	65616840	65846040	`claus`

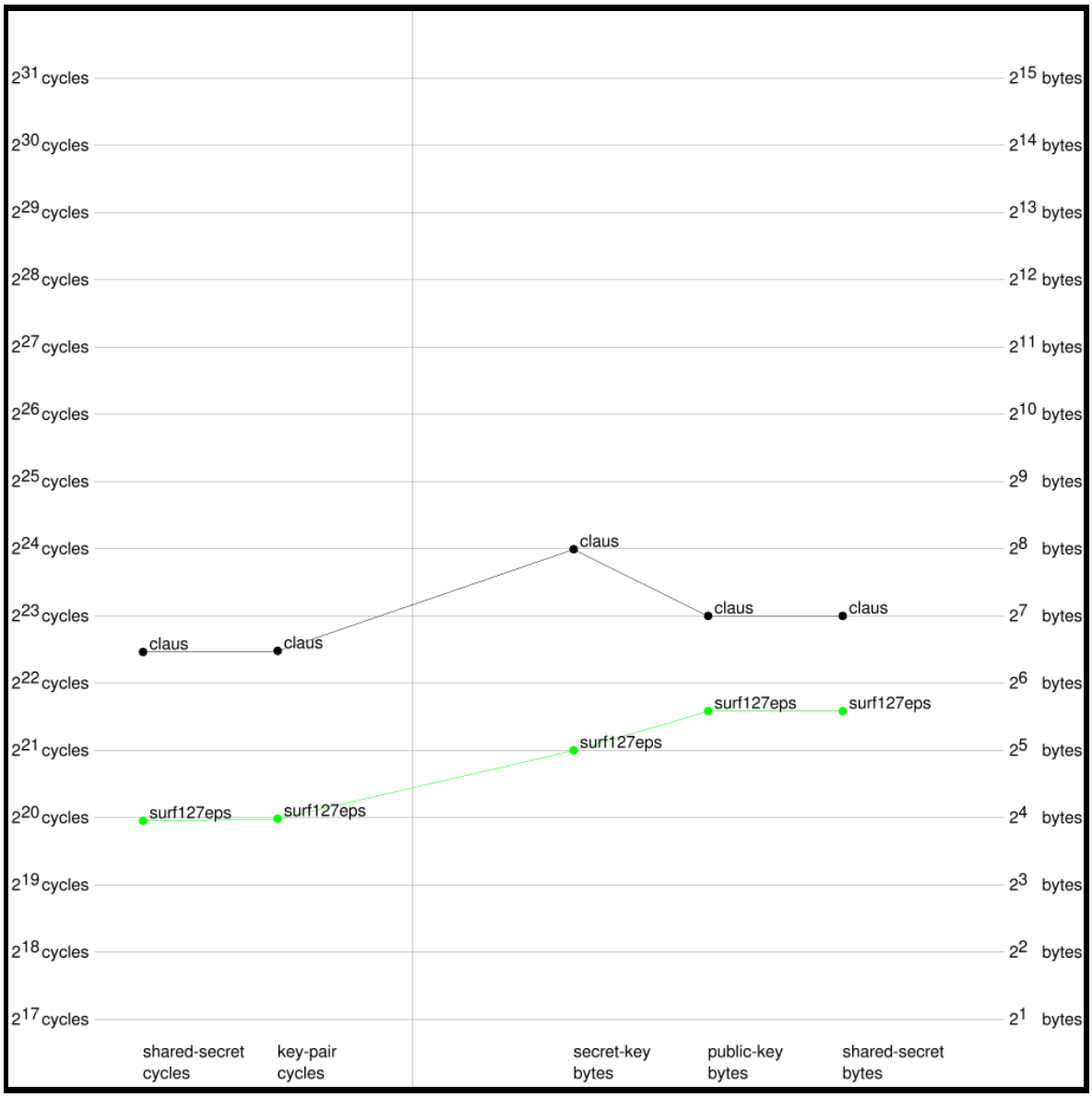
Secret key	
bytes	system
32	`curve25519`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
6582840	6593320	6642760	`surf127eps`
8156360	8175040	8197920	`curve25519`
65035120	65286760	65580320	`claus`

Shared secret	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

8.20 ppc64, 2000MHz, IBM PowerPC G5 970, geespaz



Cycles to generate a key pair			
quartile	median	quartile	system
1034160	1037640	1039860	`surf127eps`
5849280	5863860	5874660	`claus`

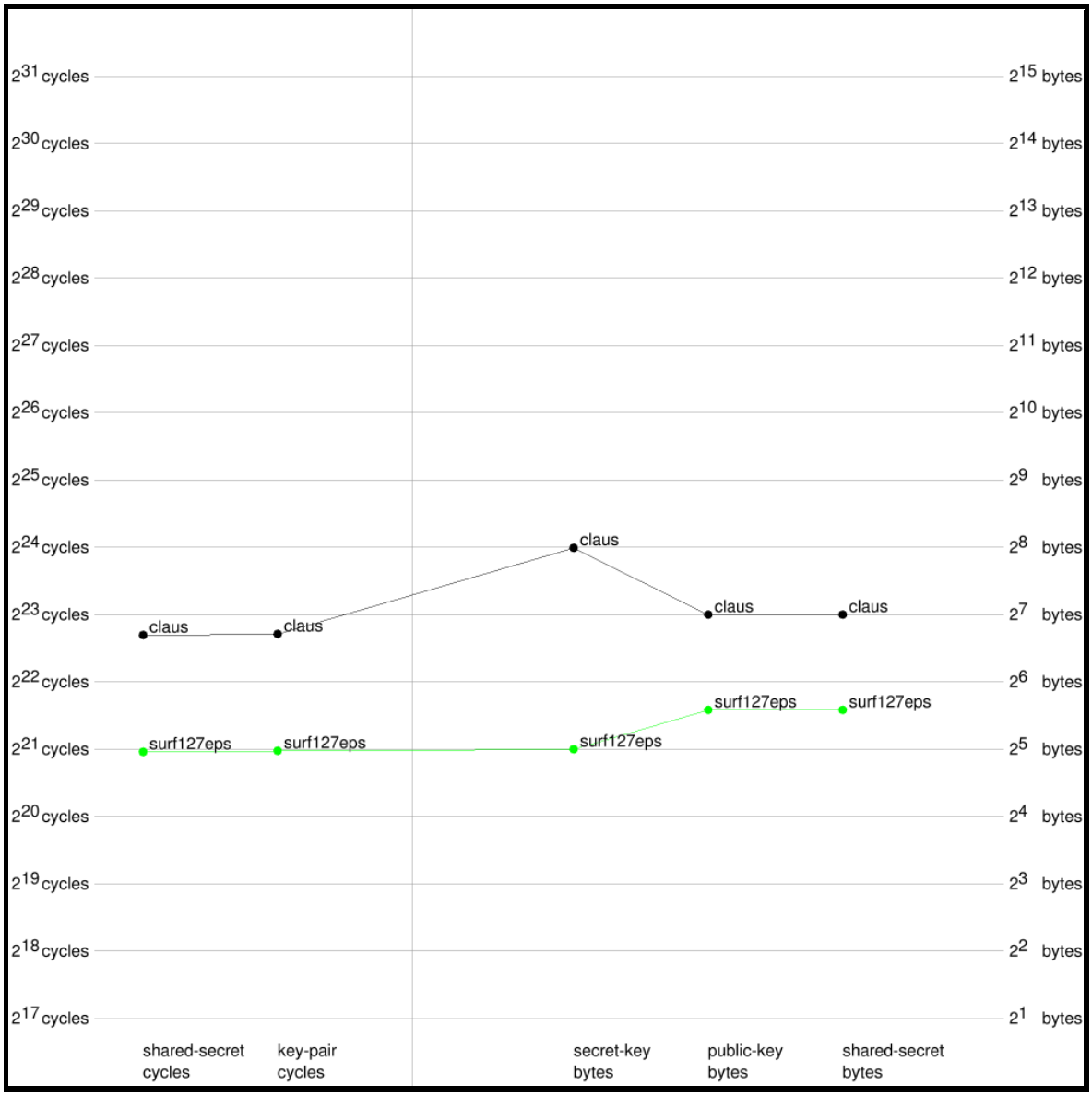
Secret key	
bytes	system
32	`surf127eps`
256	`claus`

Public key	
bytes	system
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
1015320	1016400	1017060	`surf127eps`
5790960	5803680	5815200	`claus`

Shared secret	
bytes	system
48	`surf127eps`
128	`claus`

8.21 ppc64, 2097MHz, IBM POWER5, `nmi0154`



Cycles to generate a key pair			
quartile	median	quartile	system
2064048	2070896	2076732	`surf127eps`
6874072	6887524	6899124	`claus`

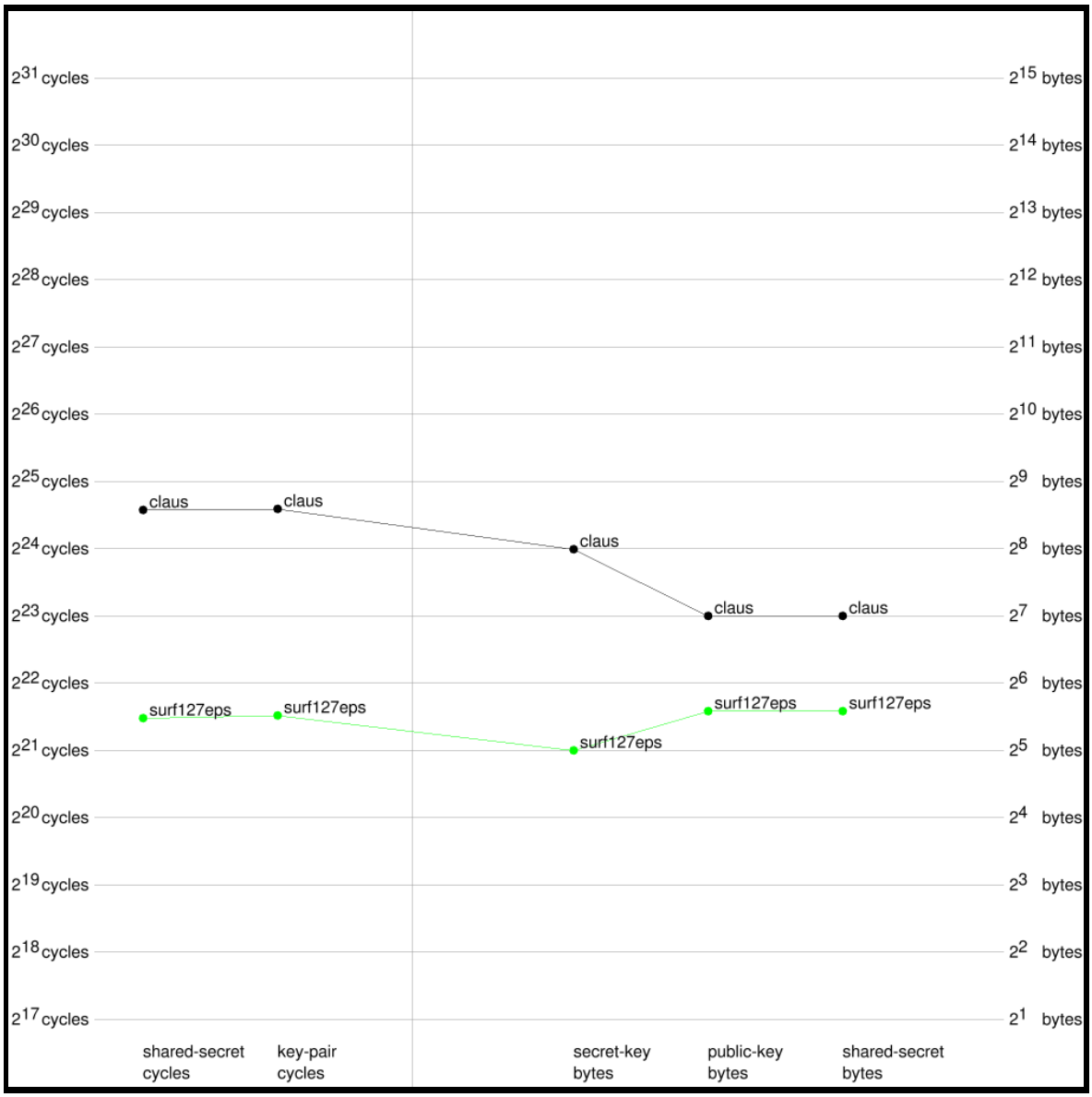
Secret key	
bytes	system
32	`surf127eps`
256	`claus`

Public key	
bytes	system
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
2040700	2045556	2050996	`surf127eps`
6812764	6821116	6835356	`claus`

Shared secret	
bytes	system
48	`surf127eps`
128	`claus`

8.22 ppc64, 3192MHz, IBM Cell PPE, `nmips3`



Cycles to generate a key pair			
quartile	median	quartile	system
3013960	3022920	3030680	`surf127eps`
25109400	25290200	25847680	`claus`

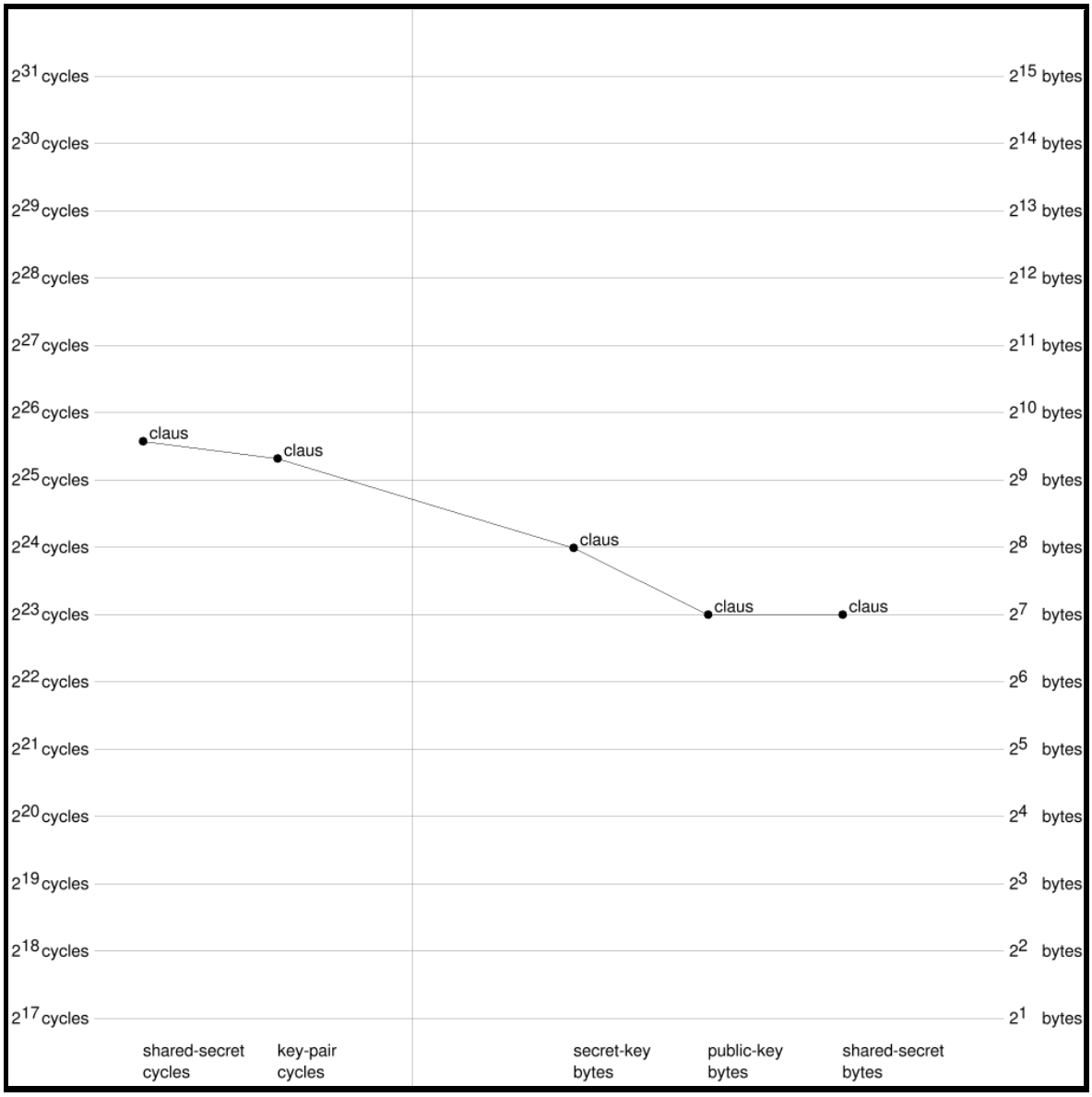
Secret key	
bytes	system
32	`surf127eps`
256	`claus`

Public key	
bytes	system
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
2926240	2938240	2944520	`surf127eps`
24923320	25026040	25632520	`claus`

Shared secret	
bytes	system
48	`surf127eps`
128	`claus`

8.23 sparcv9, 300MHz, Sun UltraSPARC IIi, `nmi0096`



Cycles to generate a key pair			
quartile	median	quartile	system
41885234	41975070	42240378	`claus`

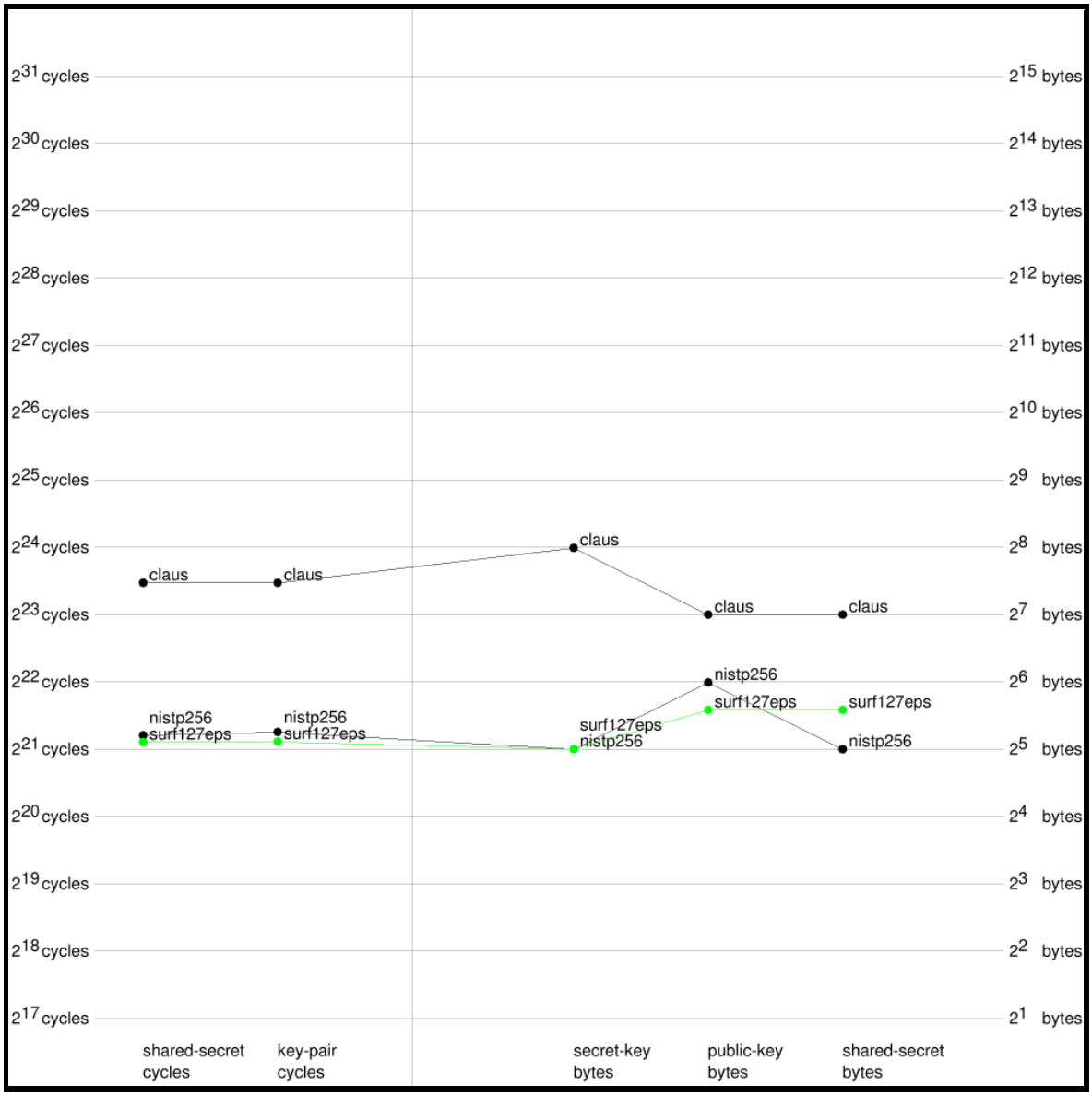
Secret key	
bytes	system
256	`claus`

Public key	
bytes	system
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
49953494	50108784	50363570	`claus`

Shared secret	
bytes	system
128	`claus`

8.24 sparcv9, 900MHz, Sun UltraSPARC III, `nmi0051`



Cycles to generate a key pair			
quartile	median	quartile	system
2263354	2271183	2276382	`surf127eps`
2477382	2515595	2546744	`nistp256`
11665767	11693971	11717520	`claus`

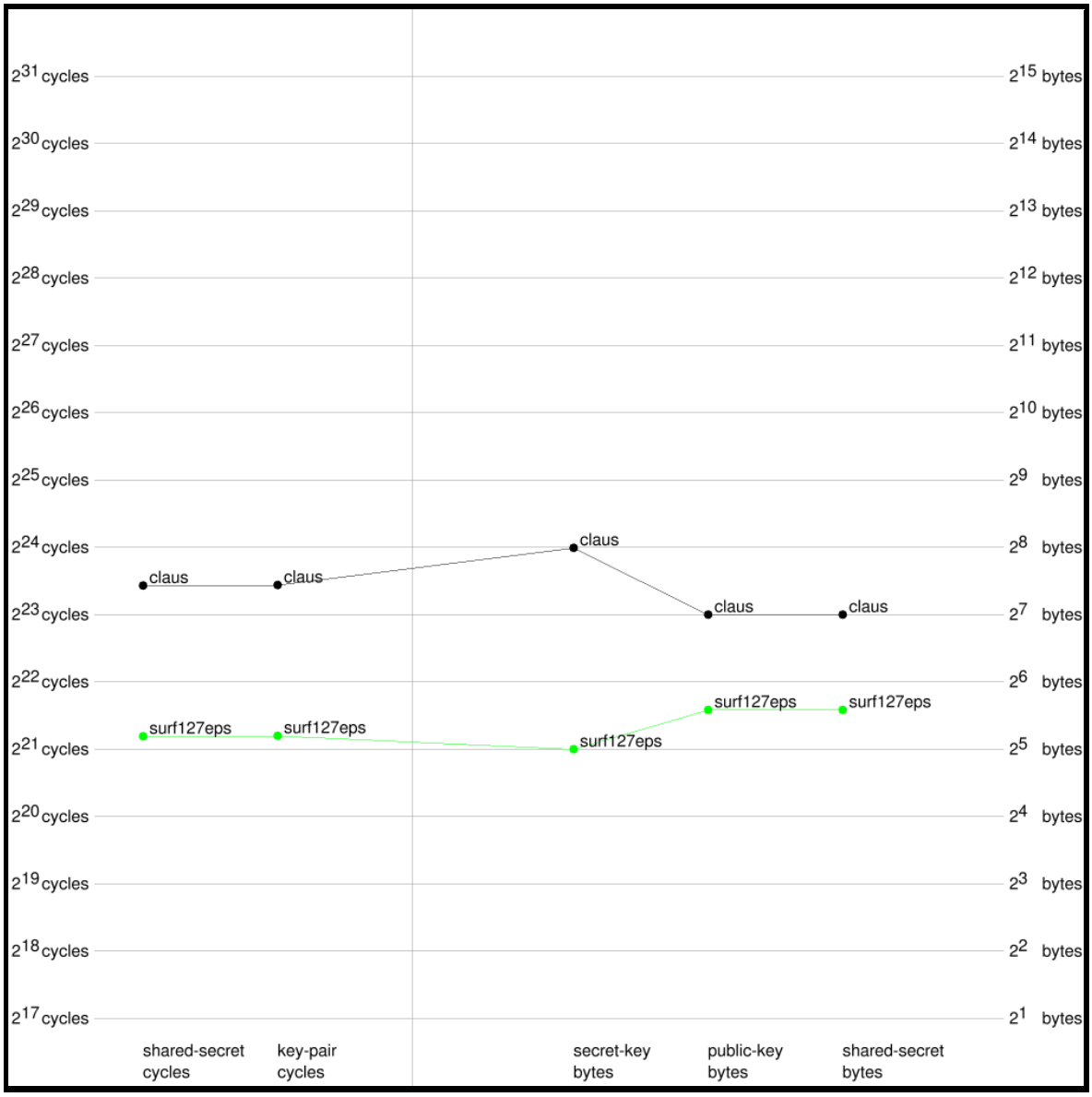
Secret key	
bytes	system
32	`nistp256`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
48	`surf127eps`
64	`nistp256`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
2256178	2260299	2263755	`surf127eps`
2426504	2432514	2528250	`nistp256`
11623505	11639559	11695568	`claus`

Shared secret	
bytes	system
32	`nistp256`
48	`surf127eps`
128	`claus`

8.25 sparcv9, 1200MHz, Sun UltraSPARC III, `nmisolaris10`



Cycles to generate a key pair			
quartile	median	quartile	system
2411361	2419984	2427738	`surf127eps`
11366675	11388037	11408036	`claus`

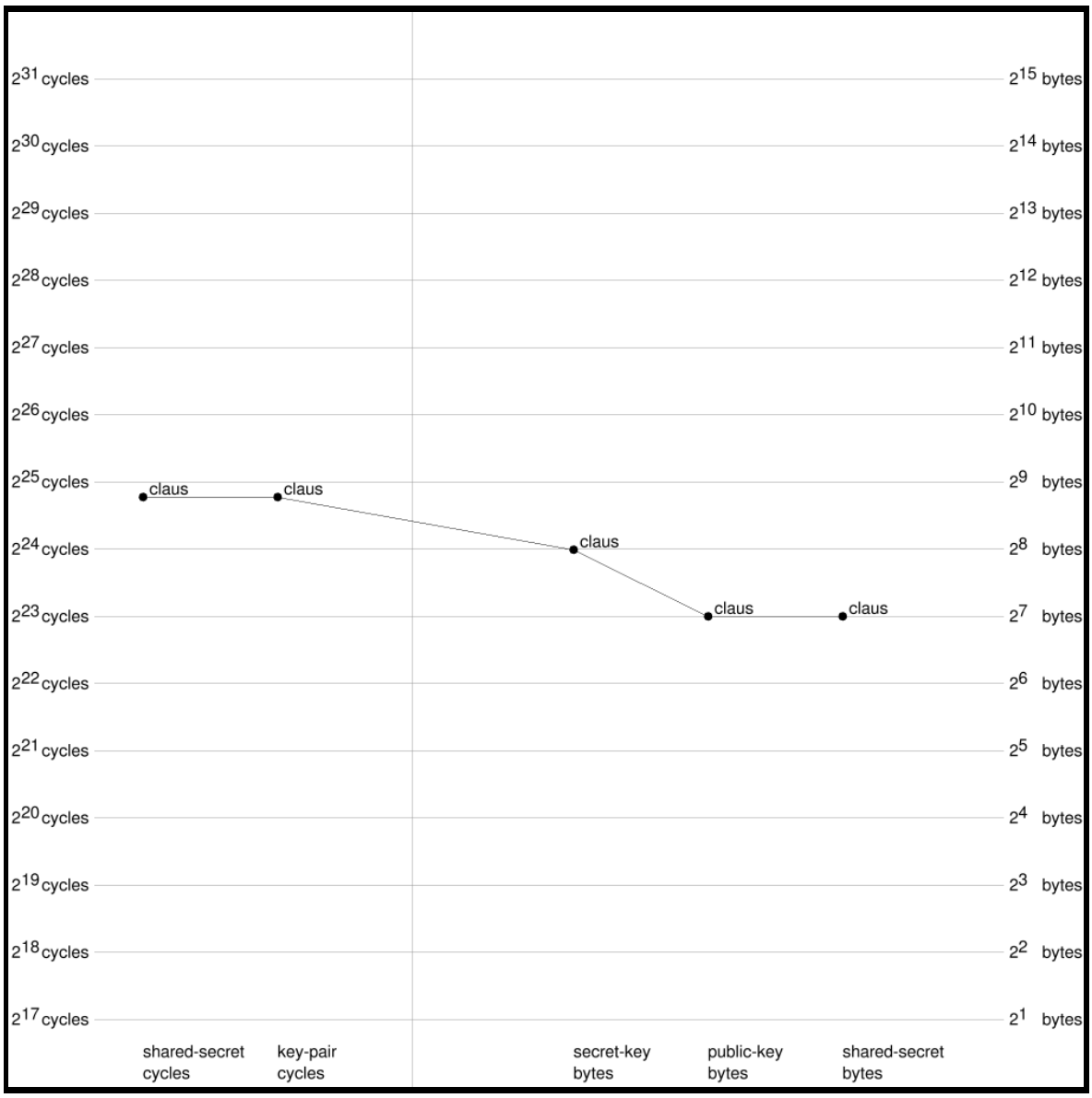
Secret key	
bytes	system
32	`surf127eps`
256	`claus`

Public key	
bytes	system
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
2392631	2397459	2403584	`surf127eps`
11337424	11346336	11370675	`claus`

Shared secret	
bytes	system
48	`surf127eps`
128	`claus`

8.26 x86, 1196MHz, Intel Celeron (6b1), `vieux`



Cycles to generate a key pair			
quartile	median	quartile	system
22096924	28868928	29075502	`claus`

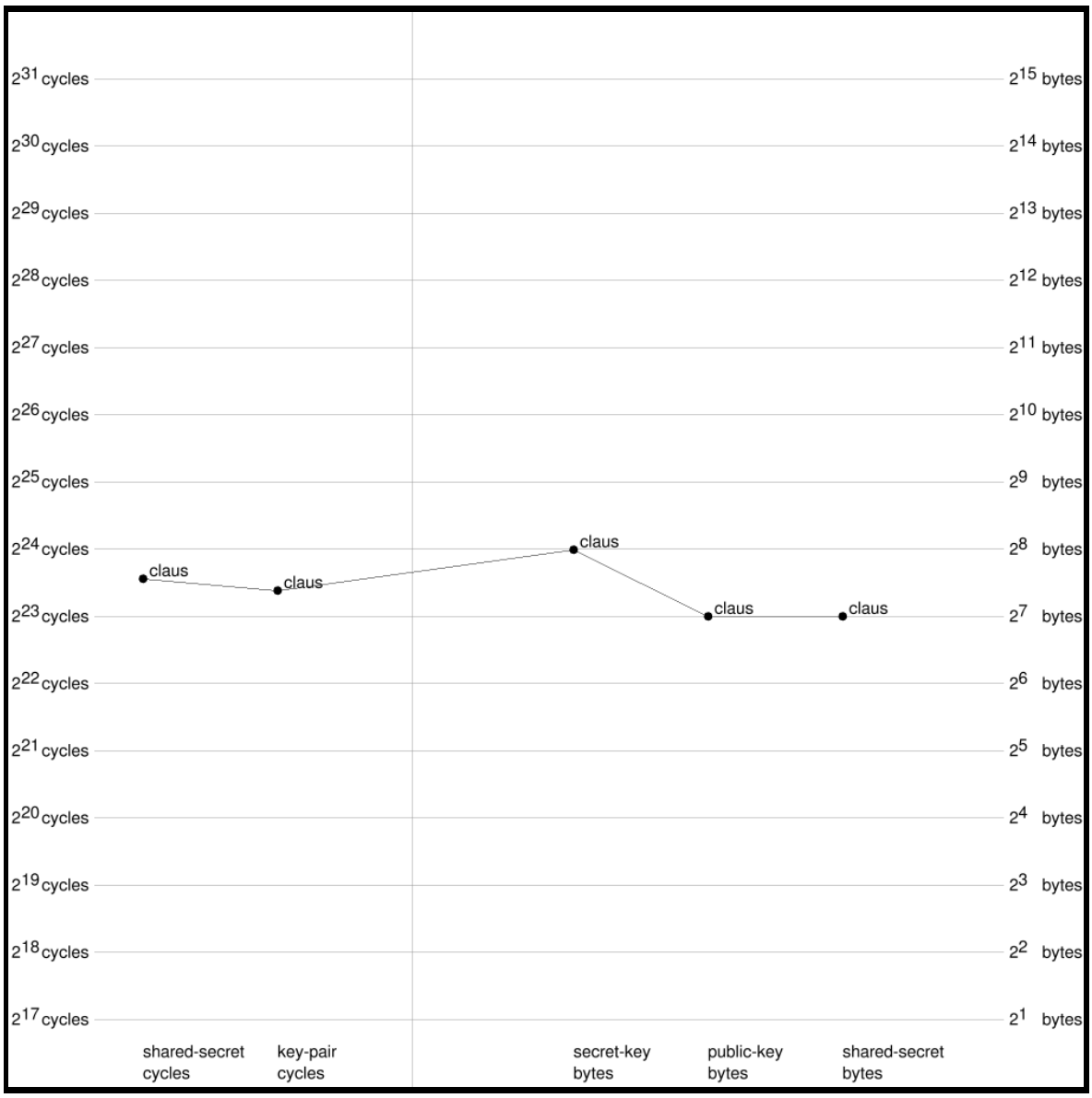
Secret key	
bytes	system
256	`claus`

Public key	
bytes	system
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
21984768	28763628	28931565	`claus`

Shared secret	
bytes	system
128	`claus`

8.27 x86, 1403MHz, AMD Opteron 240 (f58), `nmisles8amd64`



Cycles to generate a key pair			
quartile	median	quartile	system
10987177	10994242	11001346	`claus`

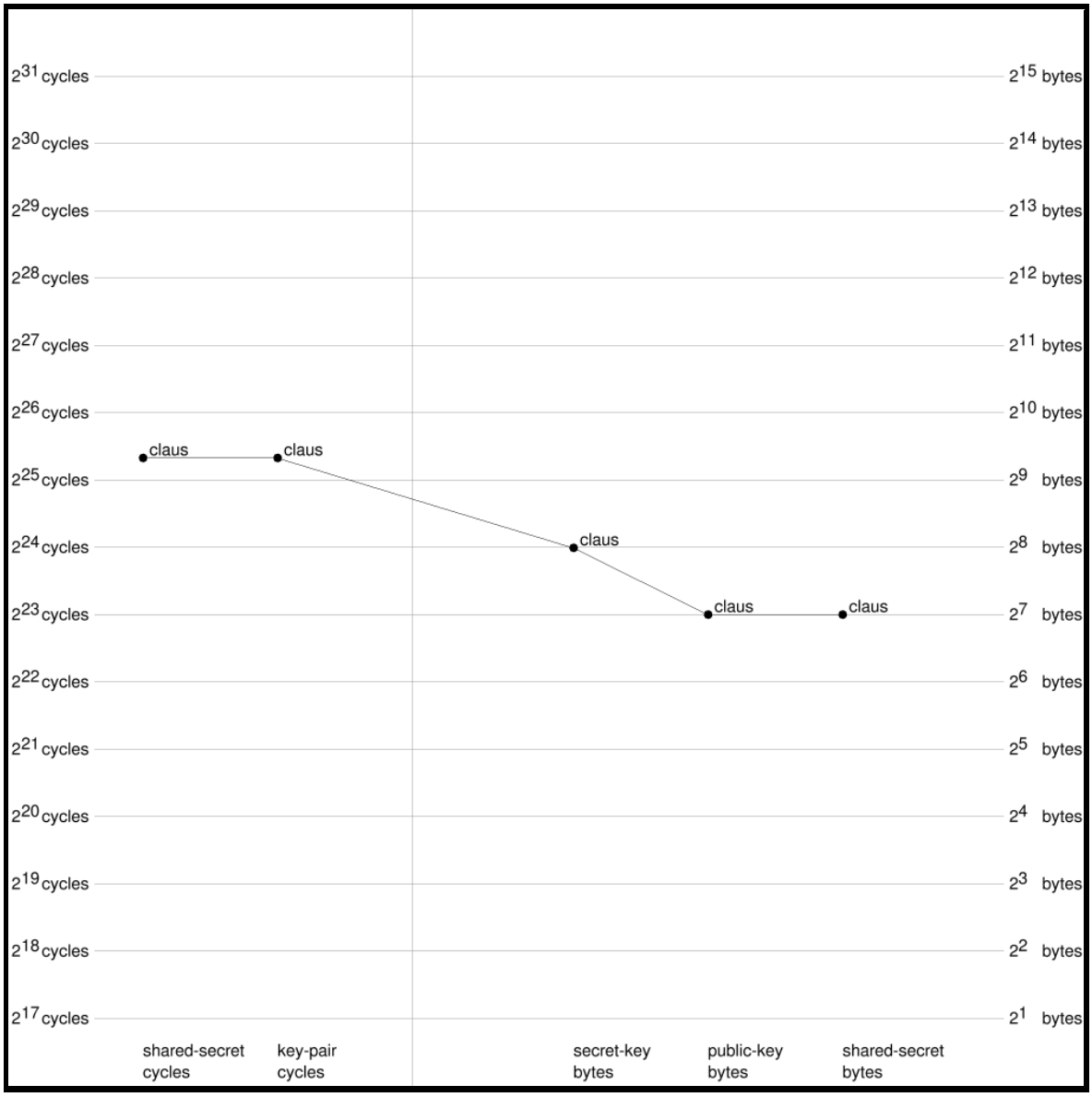
Secret key	
bytes	system
256	`claus`

Public key	
bytes	system
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
12387853	12409866	12412034	`claus`

Shared secret	
bytes	system
128	`claus`

8.28 x86, 1833MHz, Intel Core Duo, `nmi0068`



Cycles to generate a key pair			
quartile	median	quartile	system
42124907	42136270	42148876	`claus`

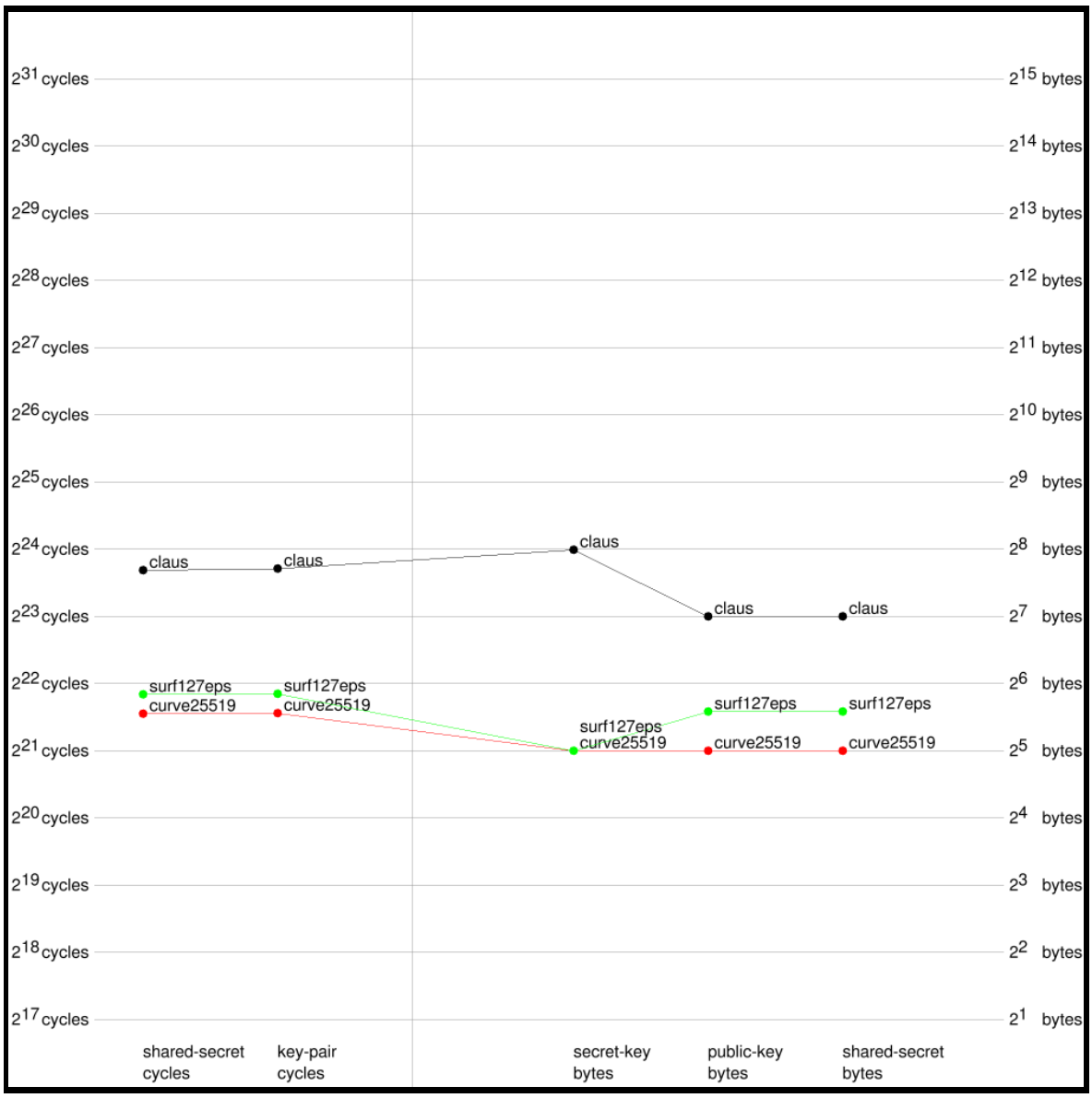
Secret key	
bytes	system
256	`claus`

Public key	
bytes	system
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
42117570	42123906	42131793	`claus`

Shared secret	
bytes	system
128	`claus`

8.29 x86, 2400MHz, Intel Pentium 4 (f24), `nmitest4`



Cycles to generate a key pair			
quartile	median	quartile	system
3089472	3101656	3109612	`curve25519`
3774876	3786700	3794888	`surf127eps`
13694544	13811440	13904416	`claus`

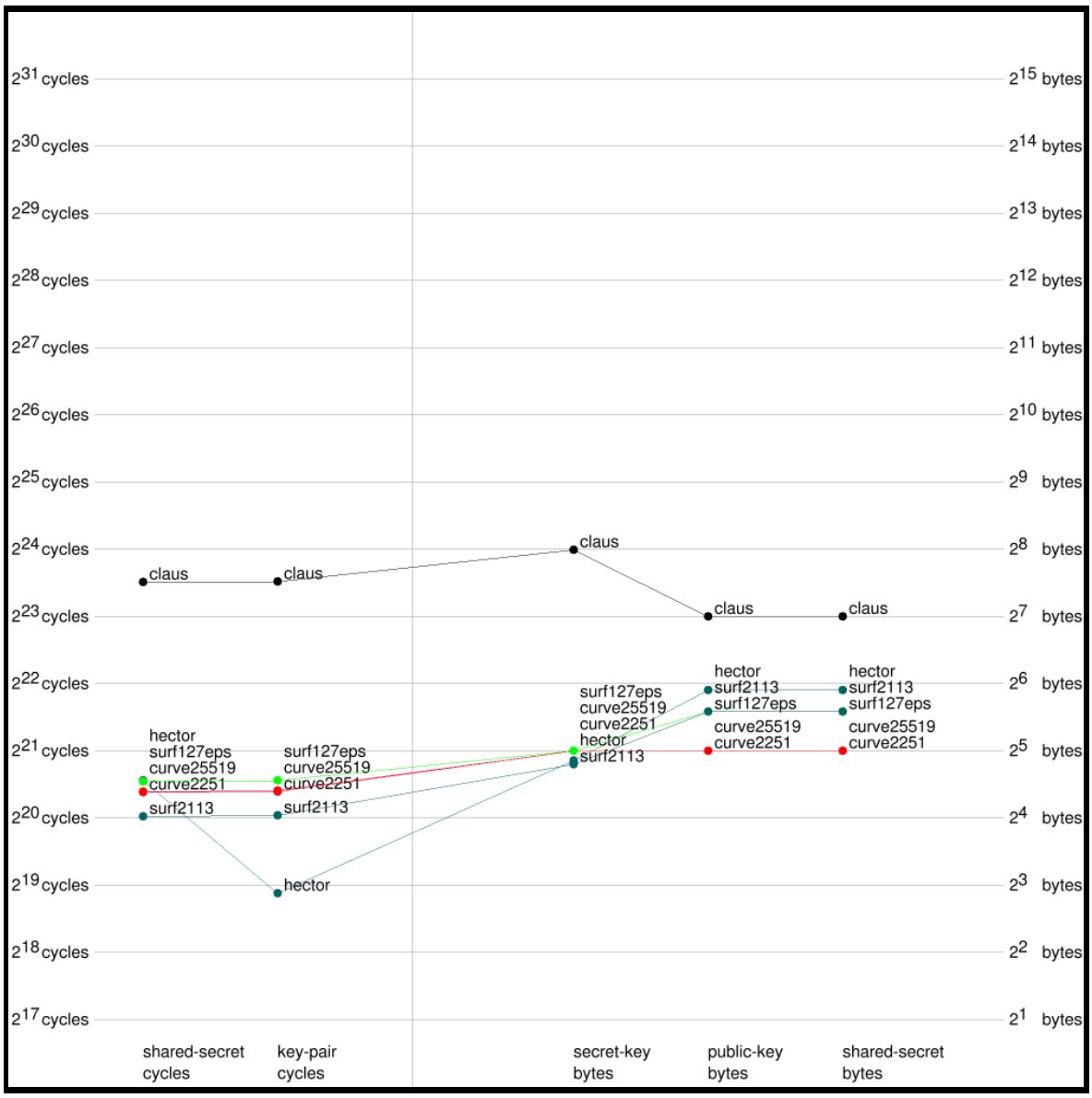
Secret key	
bytes	system
32	`curve25519`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
3082176	3086176	3090232	`curve25519`
3756036	3772208	3773380	`surf127eps`
13535748	13568280	13590696	`claus`

Shared secret	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

8.30 x86, 2400MHz, Intel Core 2 Duo (6fb), utrecht



Cycles to generate a key pair			
quartile	median	quartile	system
469458	484290	519138	`hector`
1076283	1081305	1084041	`surf2113`
1379205	1383084	1386198	`curve2251`
1389285	1394010	1396449	`curve25519`
1543968	1549863	1553634	`surf127eps`
12062907	12084453	12107664	`claus`

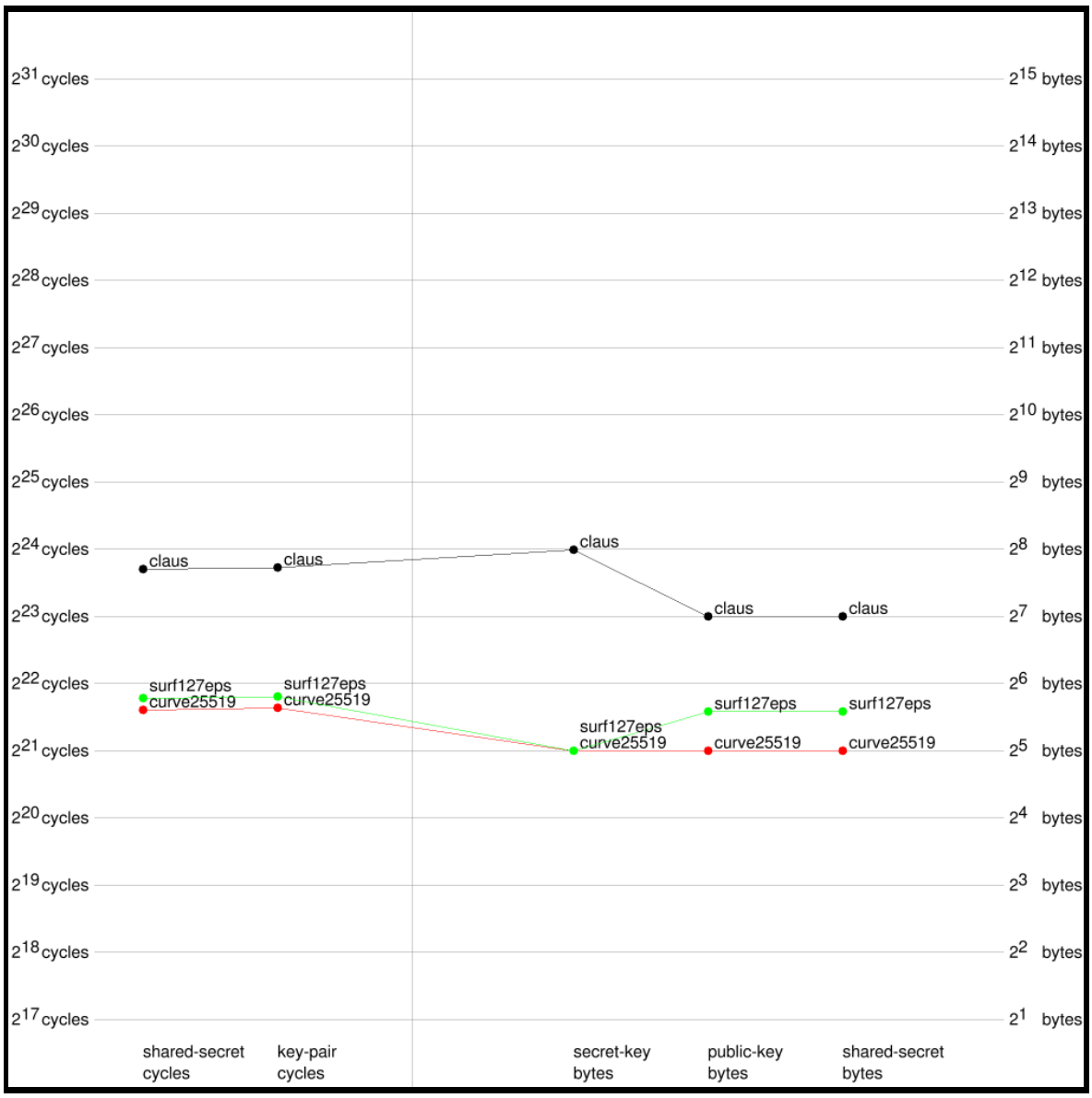
Secret key	
bytes	system
28	`surf2113`
29	`hector`
32	`curve2251`
32	`curve25519`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve2251`
32	`curve25519`
48	`surf127eps`
48	`surf2113`
60	`hector`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
1071126	1071765	1072368	`surf2113`
1371564	1374678	1375461	`curve2251`
1379151	1381113	1382553	`curve25519`
1525959	1533393	1538991	`surf127eps`
1544076	1550178	1556100	`hector`
12006036	12014226	12049092	`claus`

Shared secret	
bytes	system
32	`curve2251`
32	`curve25519`
48	`surf127eps`
48	`surf2113`
60	`hector`
128	`claus`

8.31 x86, 2401MHz, Intel Pentium 4 (f24), nmi0086



Cycles to generate a key pair			
quartile	median	quartile	system
3251692	3278916	3301688	`curve25519`
3670652	3686224	3702360	`surf127eps`
13836000	13895008	13934228	`claus`

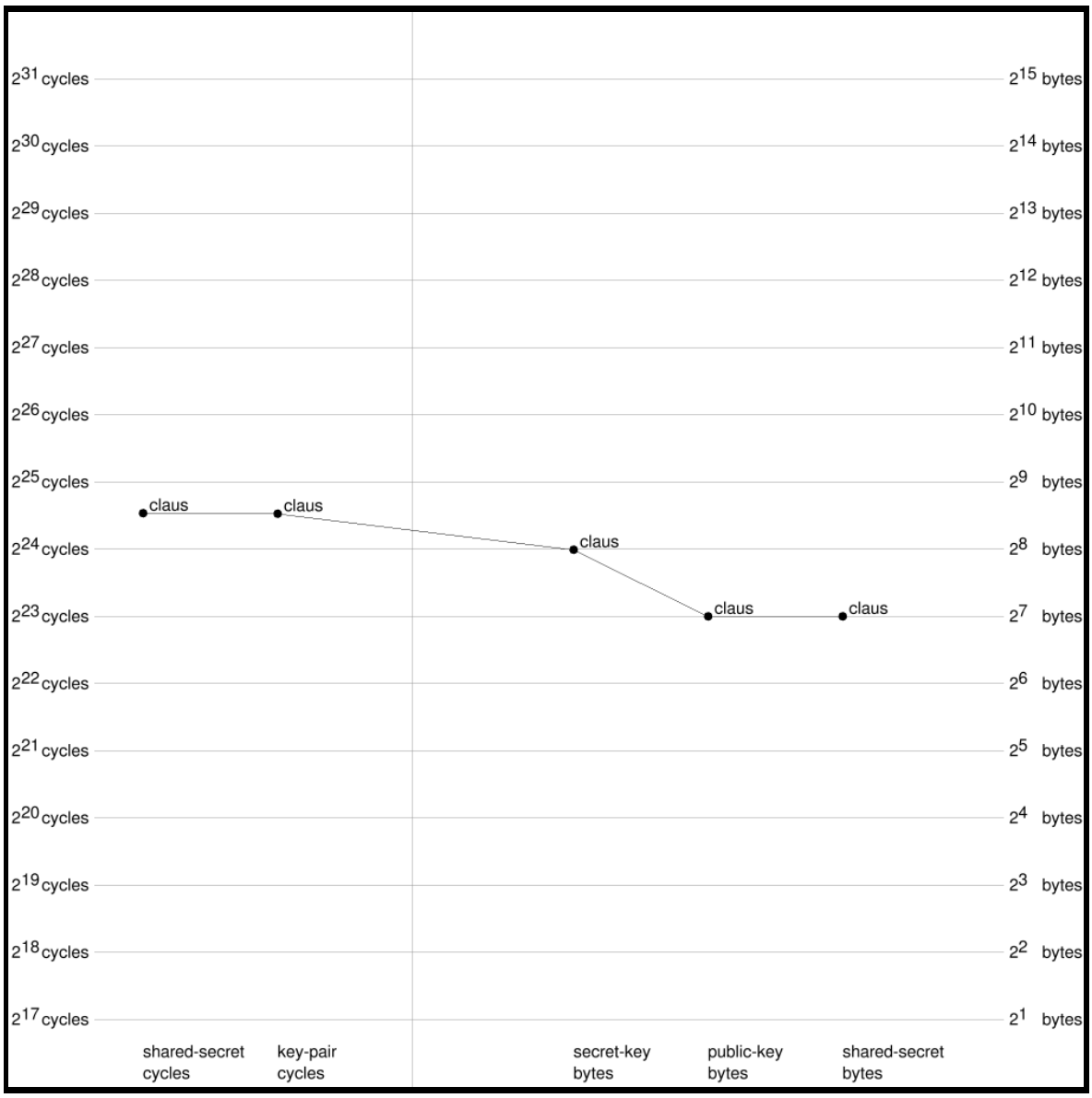
Secret key	
bytes	system
32	`curve25519`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
3188992	3206124	3222288	`curve25519`
3608304	3626724	3637960	`surf127eps`
13683812	13729572	13756476	`claus`

Shared secret	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

8.32 x86, 2658MHz, Intel Xeon (f25), `nmi0013`



Cycles to generate a key pair			
quartile	median	quartile	system
24223864	24276728	24324172	`claus`

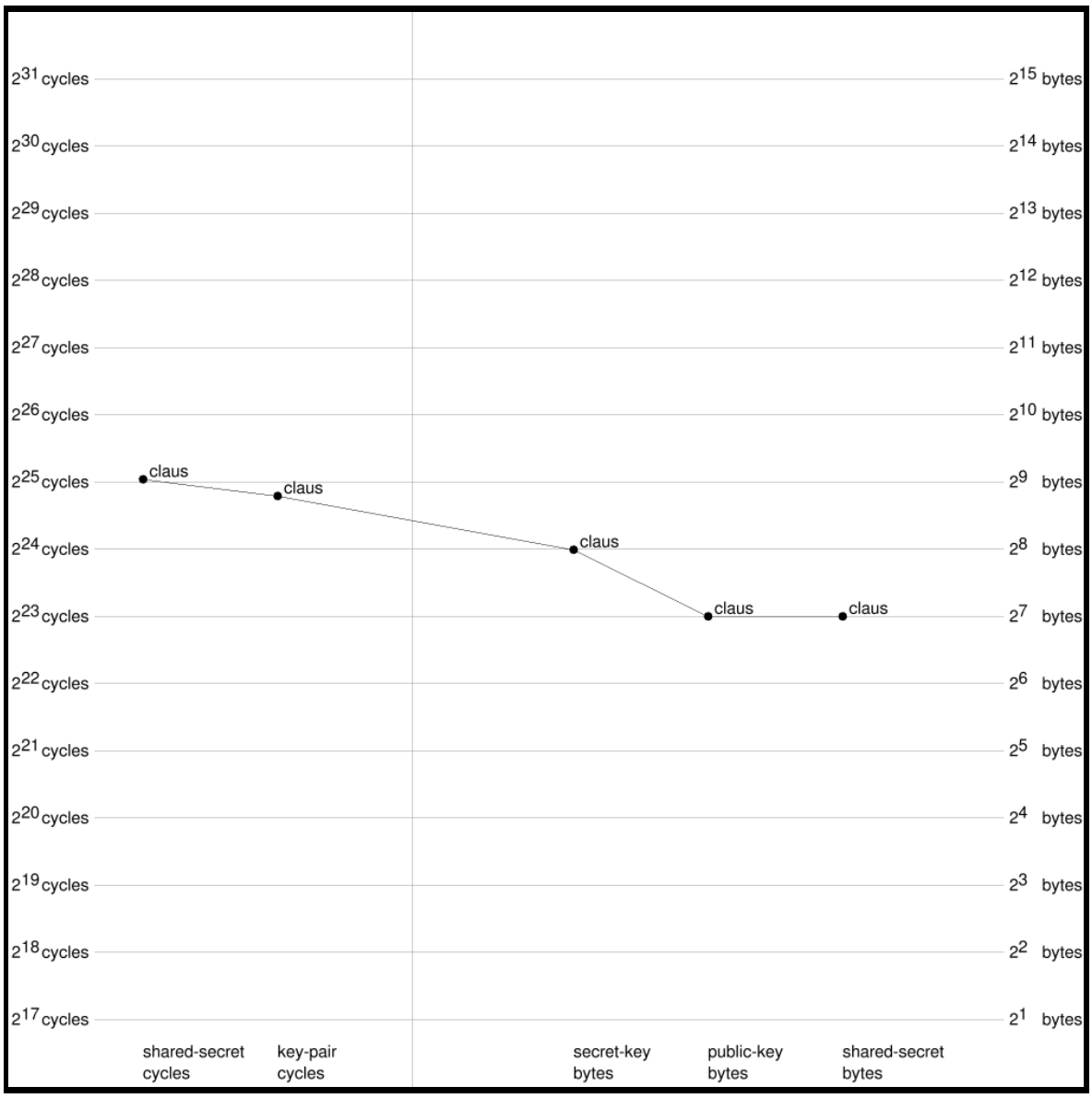
Secret key	
bytes	system
256	`claus`

Public key	
bytes	system
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
24356480	24390112	24460716	`claus`

Shared secret	
bytes	system
128	`claus`

8.33 x86, 2658MHz, Intel Xeon (f25), `nmibuild15`



Cycles to generate a key pair			
quartile	median	quartile	system
29065588	29102748	29142808	`claus`

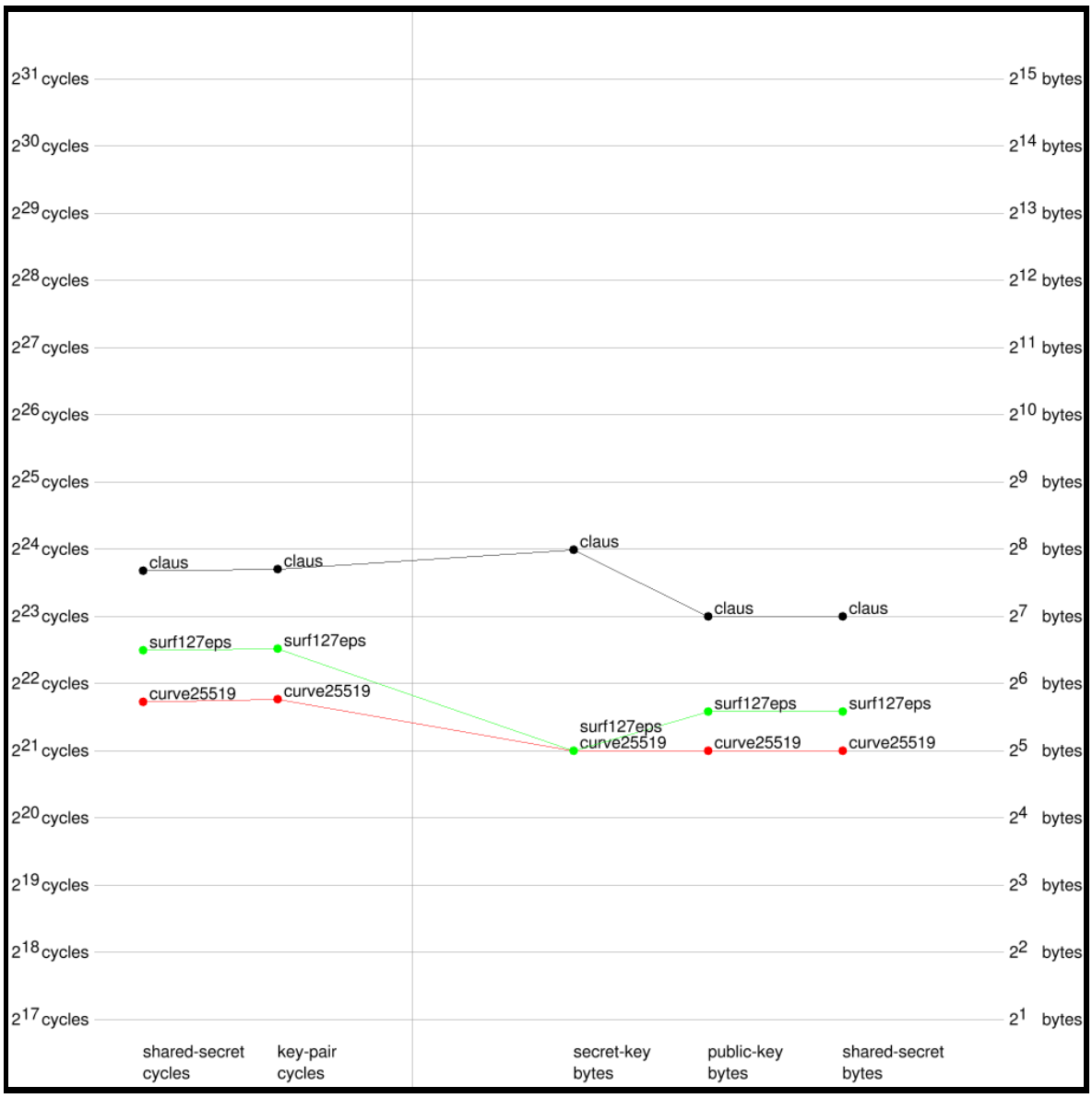
Secret key	
bytes	system
256	`claus`

Public key	
bytes	system
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
34507740	34566668	34627556	`claus`

Shared secret	
bytes	system
128	`claus`

8.34 x86, 2658MHz, Intel Xeon (f25), `nmibuild16`



Cycles to generate a key pair			
quartile	median	quartile	system
3561460	3576472	3585400	`curve25519`
6009608	6040116	6053568	`surf127eps`
13610104	13667424	13760828	`claus`

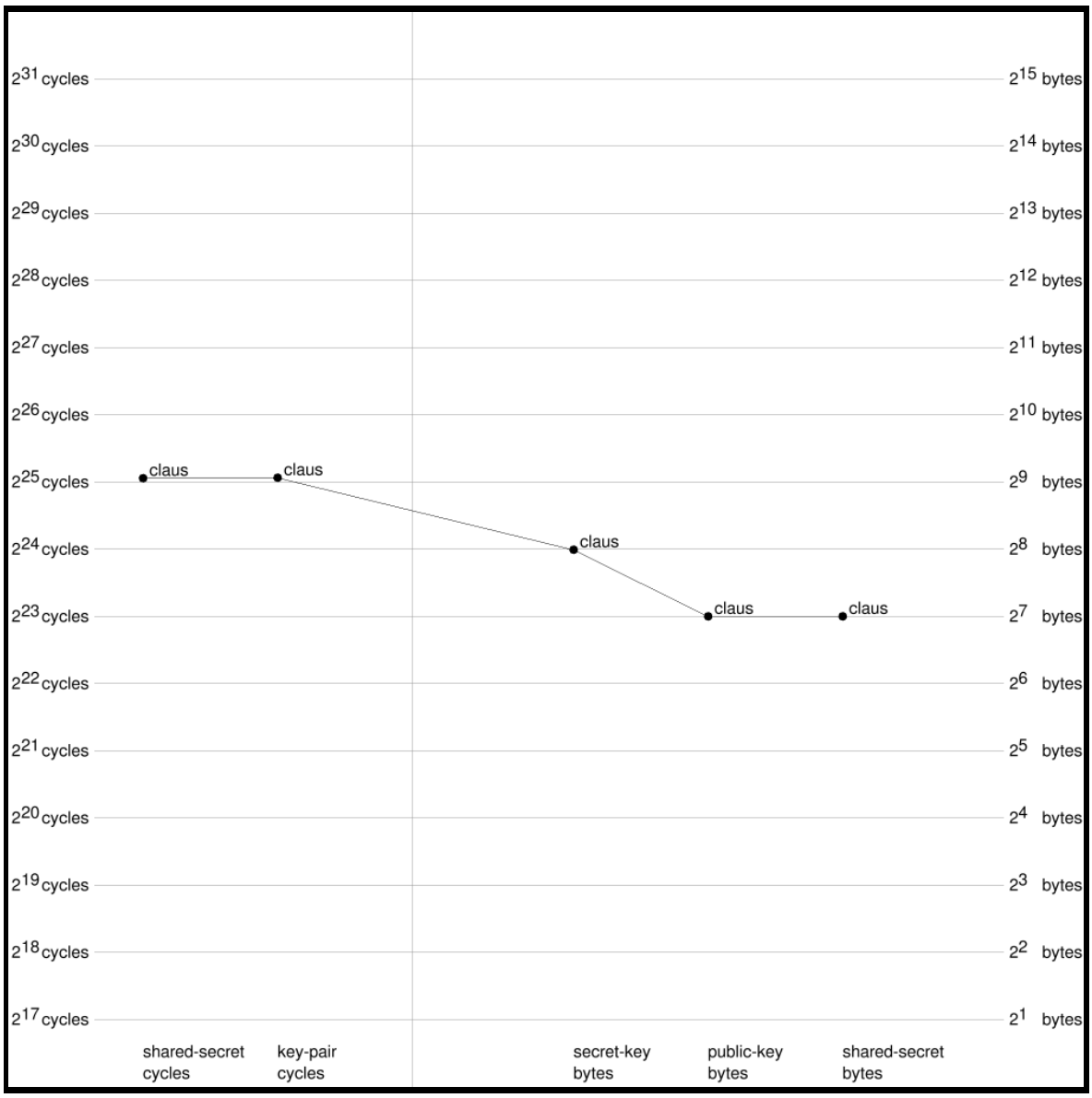
Secret key	
bytes	system
32	`curve25519`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
3422608	3487076	3526292	`curve25519`
5897868	5918696	5998512	`surf127eps`
13495392	13512944	13527900	`claus`

Shared secret	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

8.35 x86, 2658MHz, Intel Xeon (f25), `nmibuild22`



Cycles to generate a key pair			
quartile	median	quartile	system
35080428	35105964	35132516	`claus`

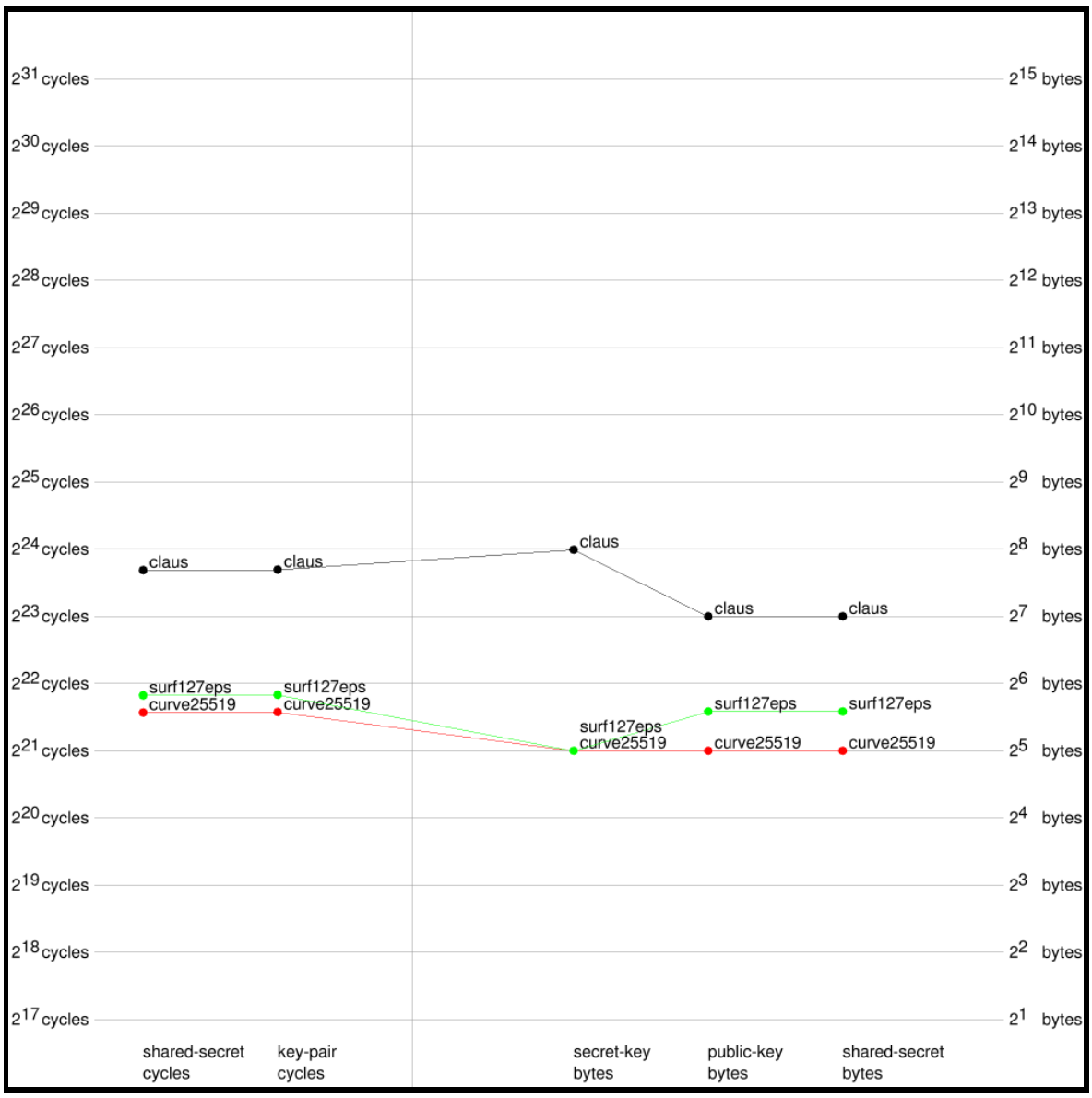
Secret key	
bytes	system
256	`claus`

Public key	
bytes	system
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
35040432	35069964	35158852	`claus`

Shared secret	
bytes	system
128	`claus`

8.36 x86, 2659MHz, Intel Xeon (f25), `nmibuild21`



Cycles to generate a key pair			
quartile	median	quartile	system
3123512	3135188	3149240	`curve25519`
3718476	3743628	3773812	`surf127eps`
13565036	13611240	13662416	`claus`

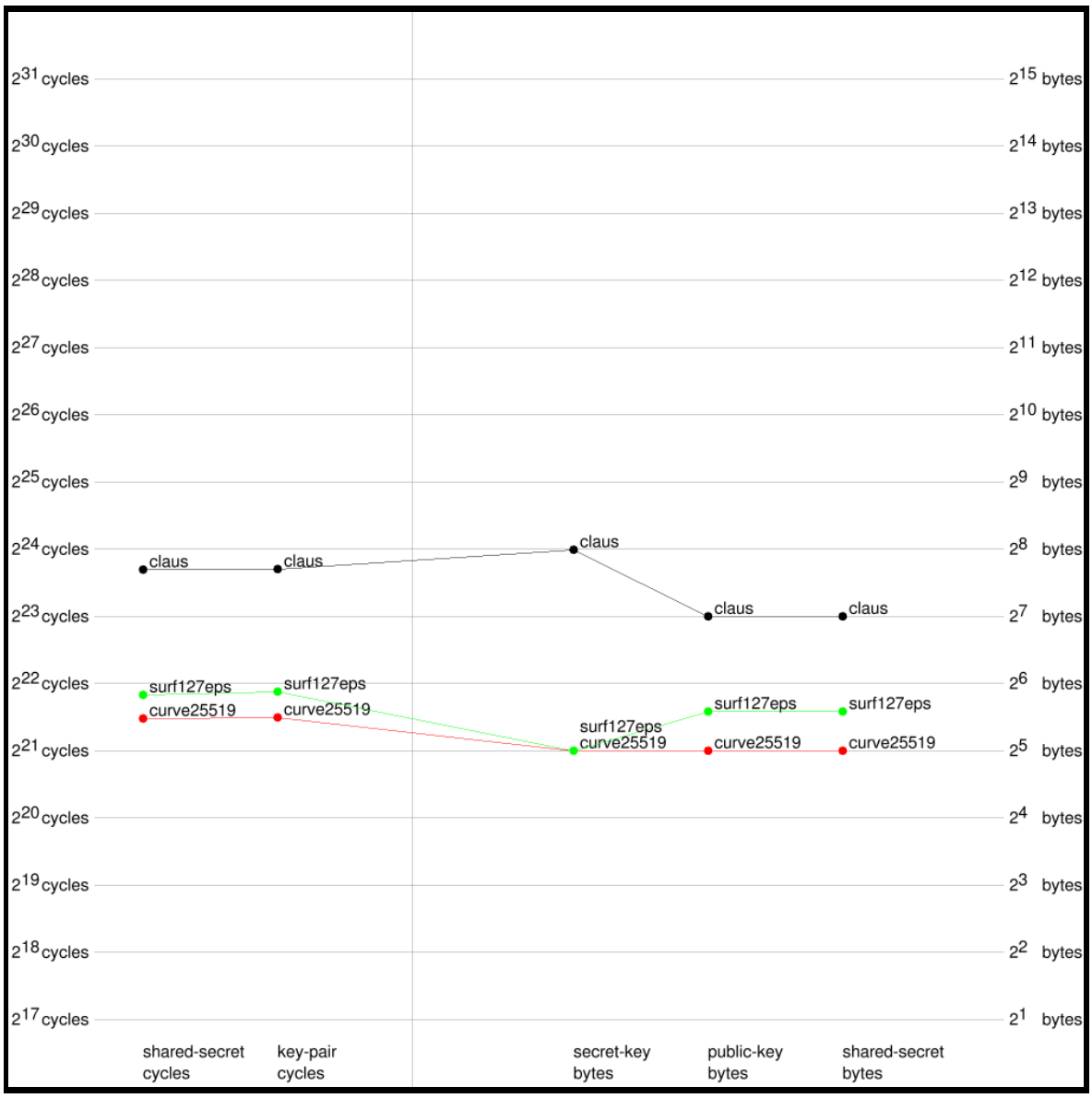
Secret key	
bytes	system
32	`curve25519`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
3113396	3120152	3128988	`curve25519`
3695824	3720680	3751912	`surf127eps`
13545384	13588552	13630312	`claus`

Shared secret	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

8.37 x86, 2659MHz, Intel Xeon (f25), nmibuild26



Cycles to generate a key pair			
quartile	median	quartile	system
2946804	2958020	2965964	`curve25519`
3821676	3869912	3934828	`surf127eps`
13646660	13721584	13784100	`claus`

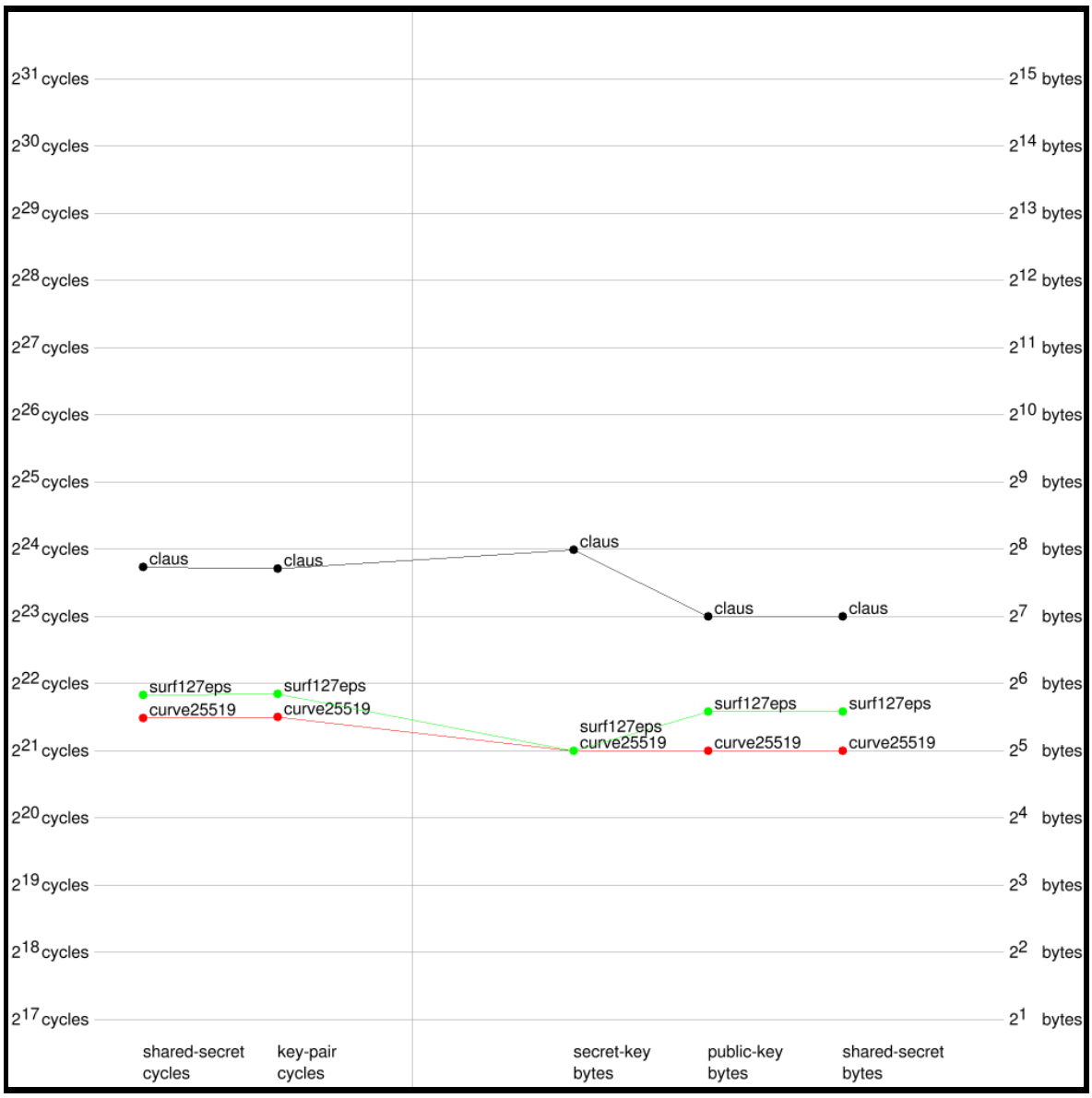
Secret key	
bytes	system
32	`curve25519`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
2923352	2929540	2936672	`curve25519`
3727340	3739572	3755456	`surf127eps`
13540604	13609728	13666392	`claus`

Shared secret	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

8.38 x86, 2667MHz, Intel Xeon (f25), `nmi0036`



Cycles to generate a key pair			
quartile	median	quartile	system
2968444	2980936	2994044	`curve25519`
3762000	3781332	3816968	`surf127eps`
13752444	13816440	13926944	`claus`

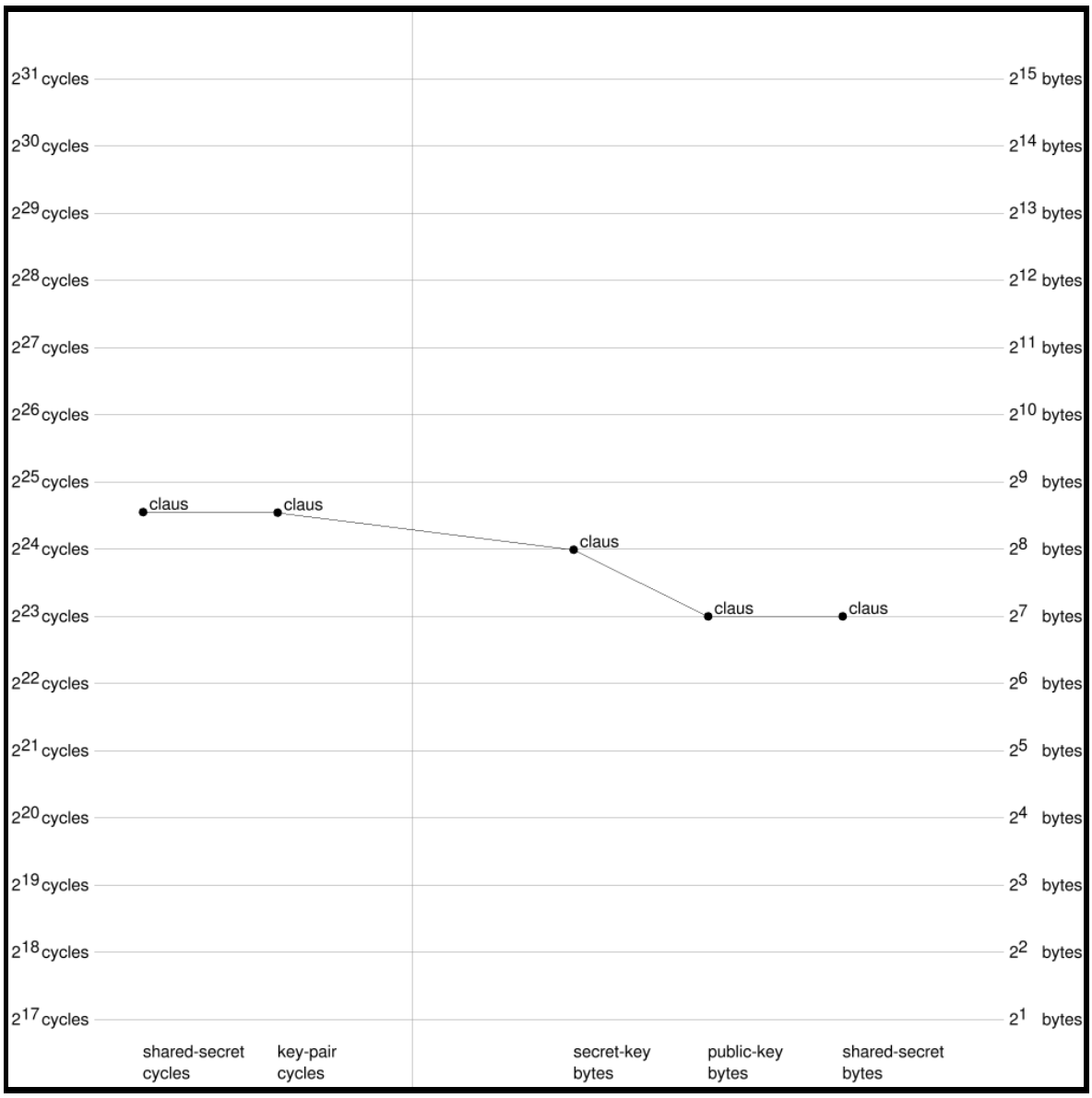
Secret key	
bytes	system
32	`curve25519`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
2940716	2949592	2959320	`curve25519`
3727392	3752672	3778072	`surf127eps`
13765364	13983296	14068584	`claus`

Shared secret	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

8.39 x86, 2791MHz, Intel Xeon (f27), nmi0024



Cycles to generate a key pair			
quartile	median	quartile	system
24506808	24523316	24542424	`claus`

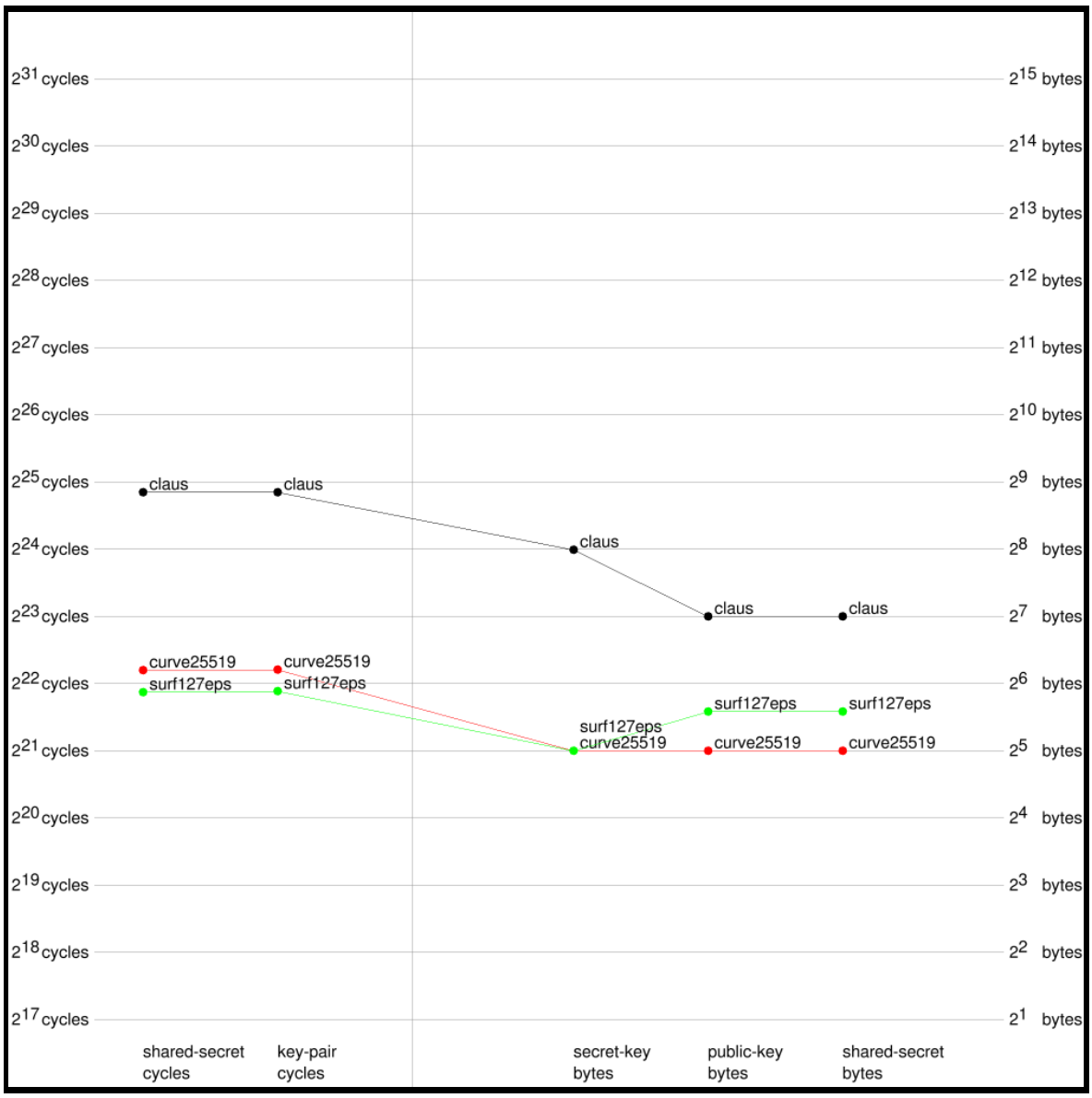
Secret key	
bytes	system
256	`claus`

Public key	
bytes	system
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
24620180	24650788	24868140	`claus`

Shared secret	
bytes	system
128	`claus`

8.40 x86, 2800MHz, Intel Xeon (f41), `nmi0057`



Cycles to generate a key pair			
quartile	median	quartile	system
3870475	3886029	3917704	`surf127eps`
4405247	4844868	4913706	`curve25519`
30180311	30270506	31320681	`claus`

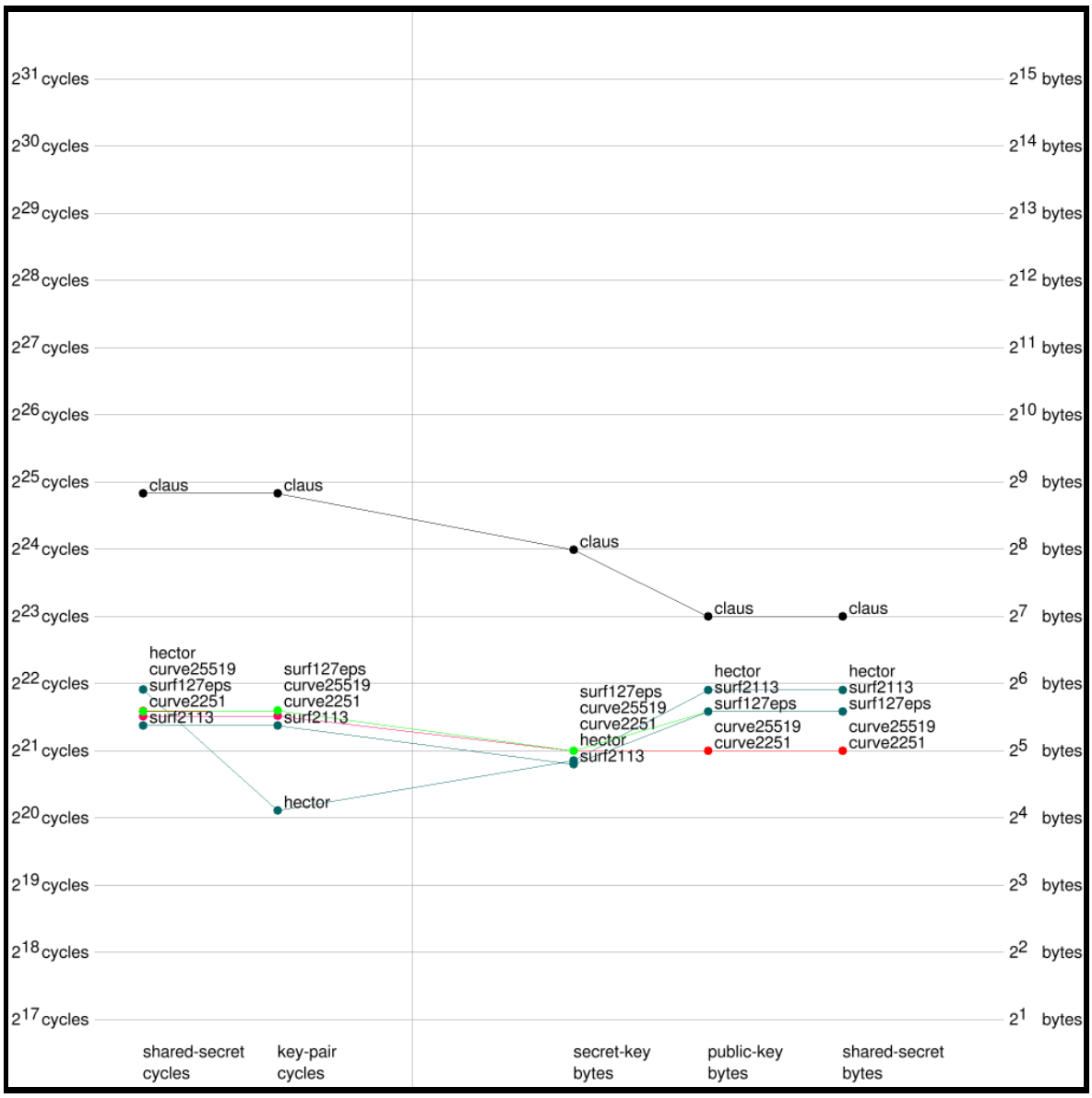
Secret key	
bytes	system
32	`curve25519`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
3844428	3855915	3870909	`surf127eps`
3266816	4822195	4889927	`curve25519`
30171596	30292346	30476012	`claus`

Shared secret	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

8.41 x86, 2800MHz, Intel Xeon (f41), nmi0063



Cycles to generate a key pair			
quartile	median	quartile	system
1106581	1133412	1181789	`hector`
2718835	2729993	2739947	`surf2113`
3002713	3014074	3024455	`curve2251`
3164742	3187800	3206504	`curve25519`
3183082	3195612	3206497	`surf127eps`
29946847	30005444	30066750	`claus`

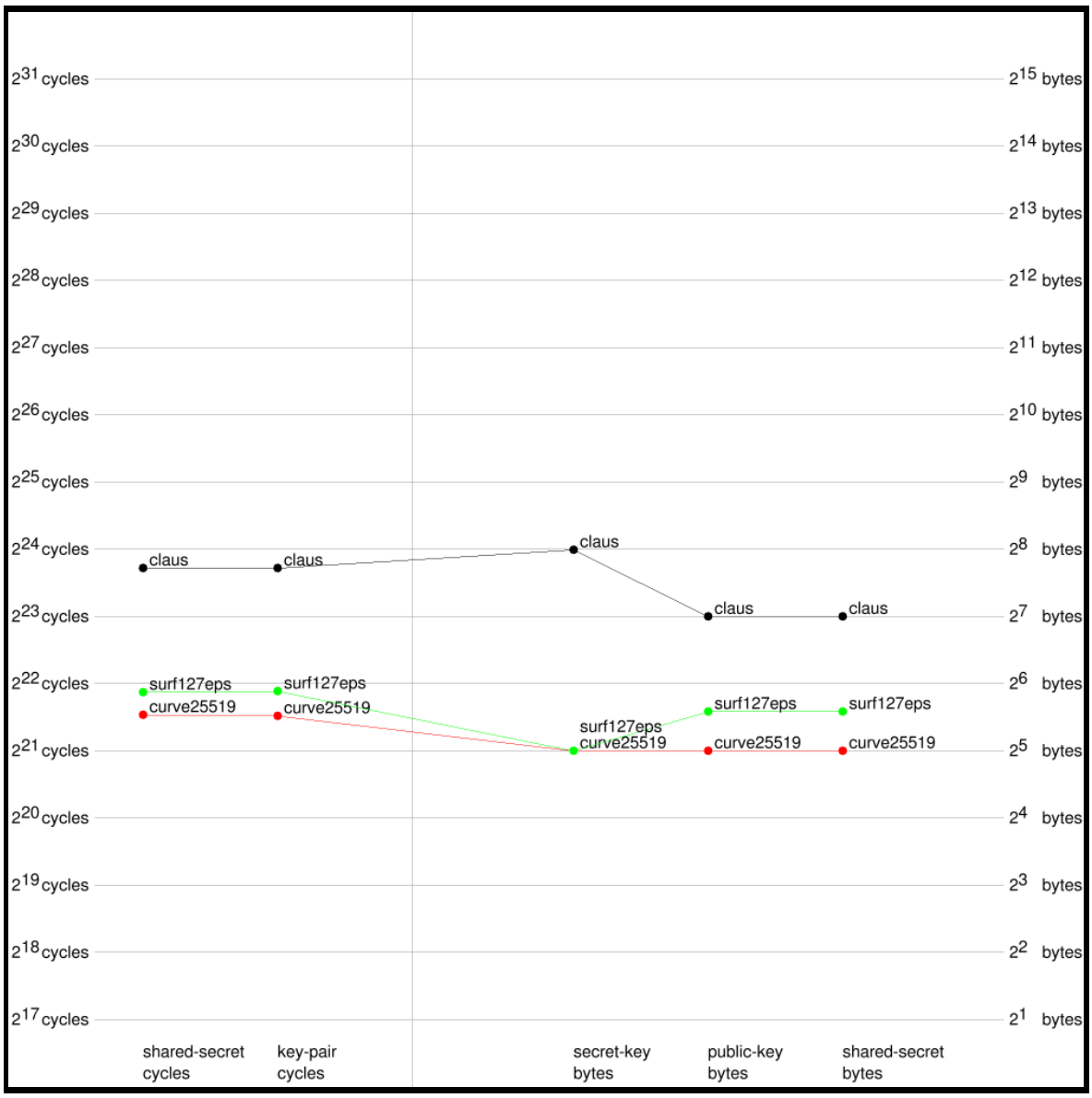
Secret key	
bytes	system
28	`surf2113`
29	`hector`
32	`curve2251`
32	`curve25519`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve2251`
32	`curve25519`
48	`surf127eps`
48	`surf2113`
60	`hector`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
2706718	2722174	2725184	`surf2113`
2986760	2992759	3001670	`curve2251`
3152086	3160346	3169621	`surf127eps`
3156853	3175900	3194240	`curve25519`
3935666	3958374	3975615	`hector`
29955163	29972852	30068556	`claus`

Shared secret	
bytes	system
32	`curve2251`
32	`curve25519`
48	`surf127eps`
48	`surf2113`
60	`hector`
128	`claus`

8.42 x86, 2801MHz, Intel Xeon (f41), nmi0060



Cycles to generate a key pair			
quartile	median	quartile	system
3000060	3017616	3040891	`curve25519`
3865491	3881745	3895262	`surf127eps`
13742967	13841562	13881497	`claus`

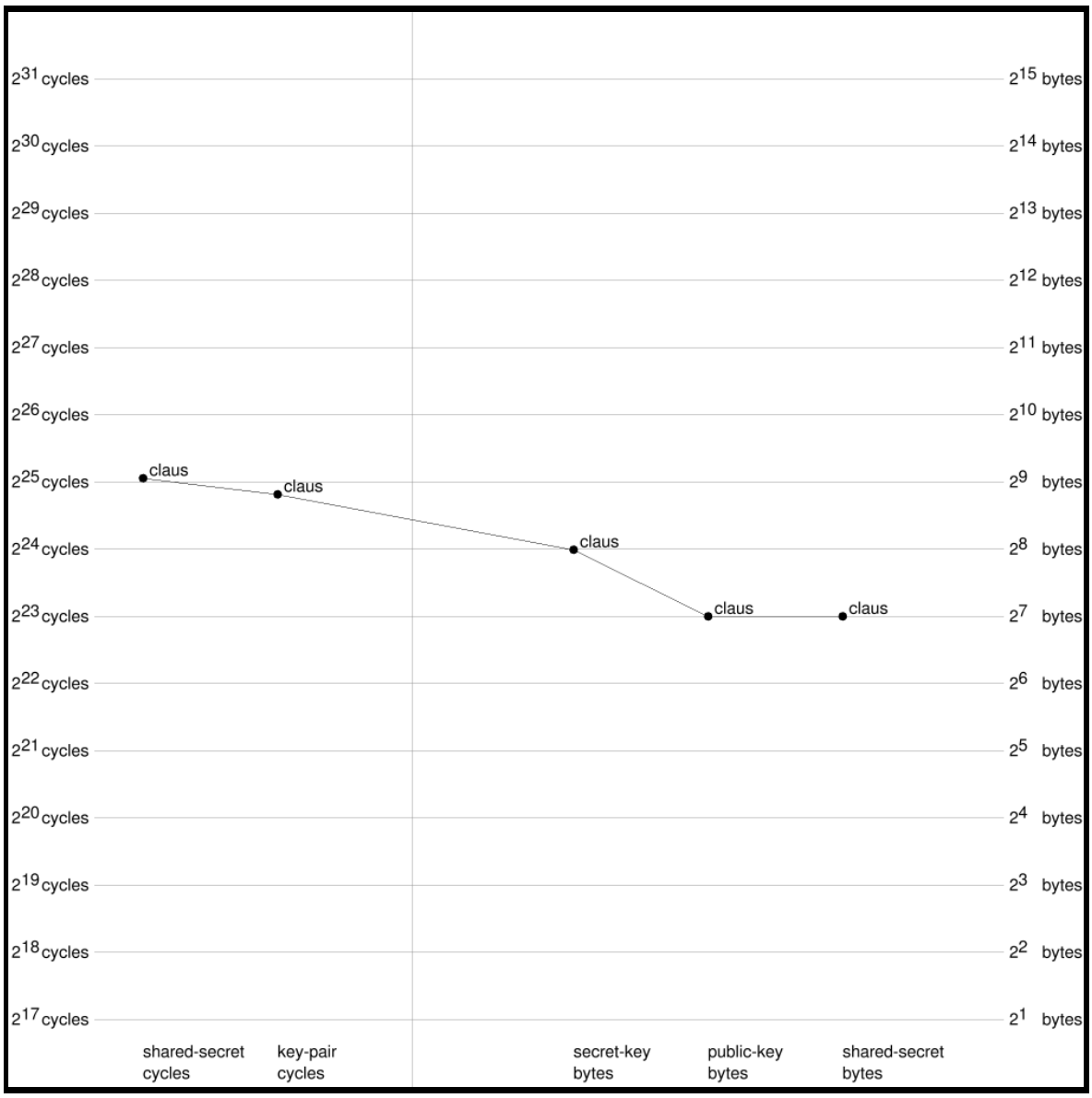
Secret key	
bytes	system
32	`curve25519`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
3016216	3051636	3065902	`curve25519`
3842342	3851624	3864532	`surf127eps`
13790308	13836137	13916392	`claus`

Shared secret	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

8.43 x86, 2801MHz, Intel Xeon (f41), `nmi0061`



Cycles to generate a key pair			
quartile	median	quartile	system
29557997	29577835	29596427	`claus`

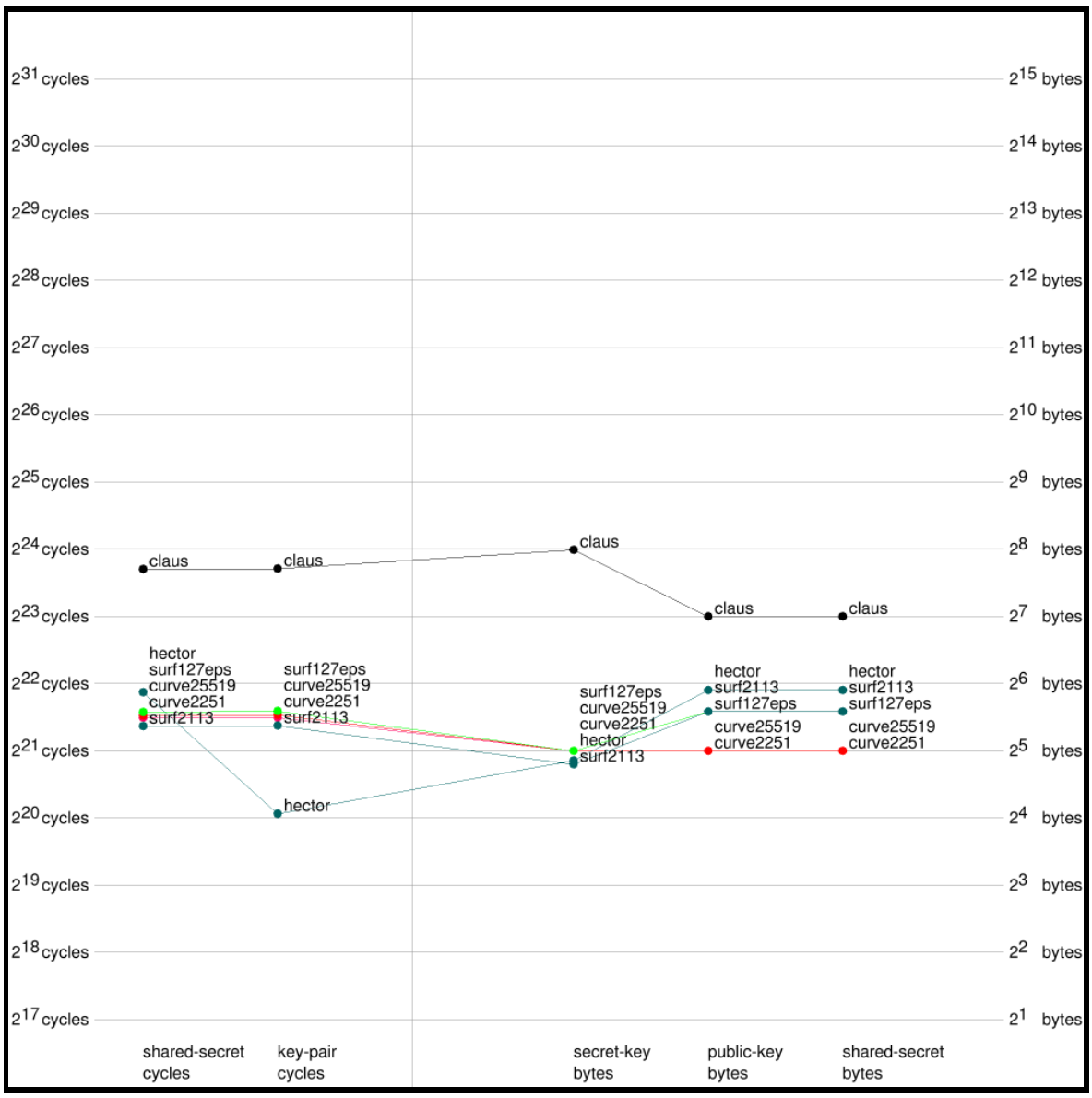
Secret key	
bytes	system
256	`claus`

Public key	
bytes	system
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
34895602	34915349	35077378	`claus`

Shared secret	
bytes	system
128	`claus`

8.44 x86, 2801MHz, Intel Xeon (f41), nmi0062



Cycles to generate a key pair			
quartile	median	quartile	system
1084671	1097411	1163631	`hector`
2718394	2729769	2736727	`surf2113`
2951214	2963219	2973432	`curve2251`
3039064	3056452	3070207	`curve25519`
3163307	3176747	3184405	`surf127eps`
13751640	13785947	13821738	`claus`

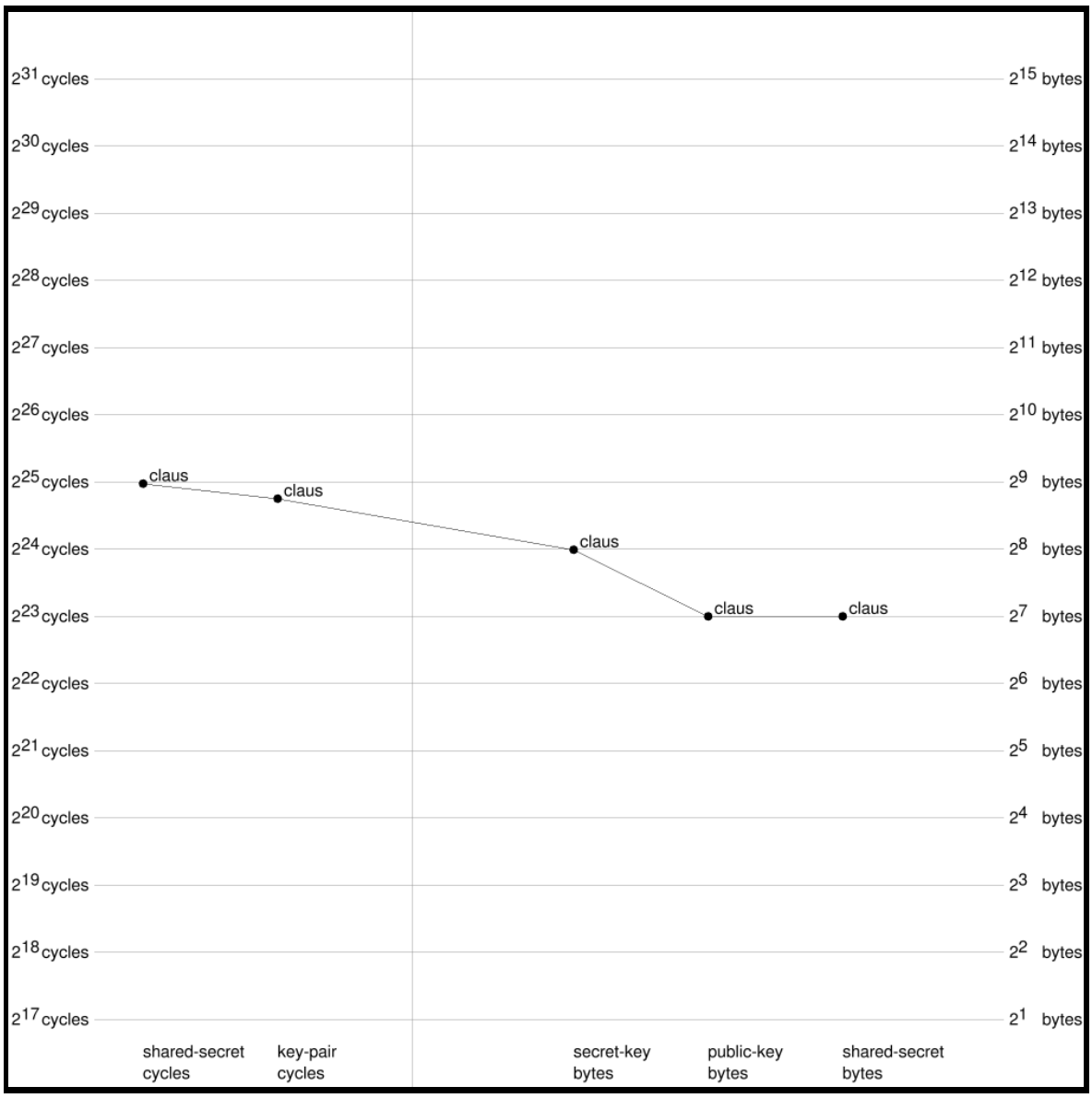
Secret key	
bytes	system
28	`surf2113`
29	`hector`
32	`curve2251`
32	`curve25519`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve2251`
32	`curve25519`
48	`surf127eps`
48	`surf2113`
60	`hector`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
2708699	2711282	2715713	`surf2113`
2948904	2957640	2969988	`curve2251`
3023559	3037167	3053932	`curve25519`
3137932	3143231	3148859	`surf127eps`
3835055	3855180	3867031	`hector`
13705160	13719748	13763715	`claus`

Shared secret	
bytes	system
32	`curve2251`
32	`curve25519`
48	`surf127eps`
48	`surf2113`
60	`hector`
128	`claus`

8.45 x86, 2802MHz, Intel Xeon (f29), `nmibuild40`



Cycles to generate a key pair			
quartile	median	quartile	system
28306844	28343020	28389836	`claus`

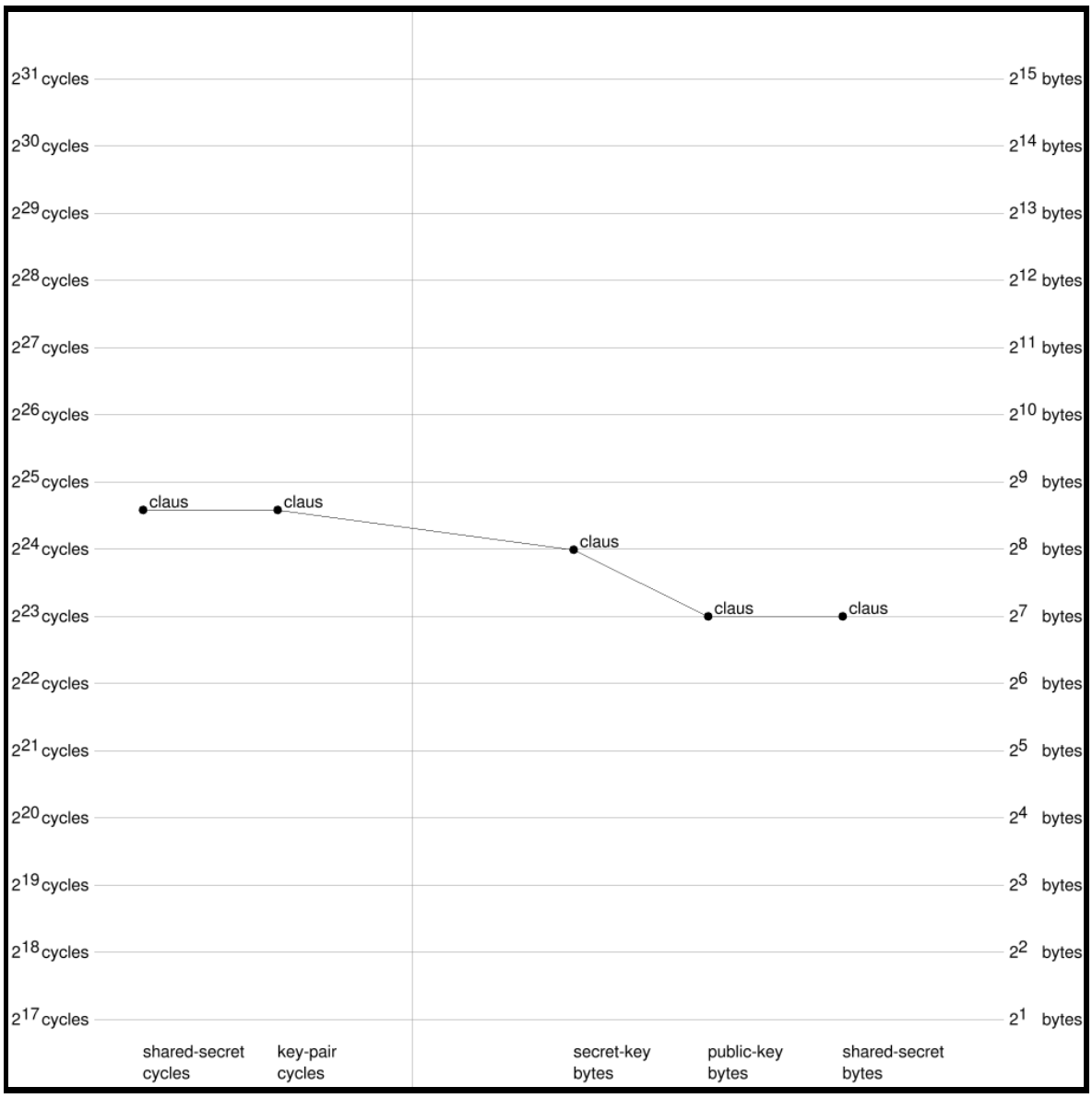
Secret key	
bytes	system
256	`claus`

Public key	
bytes	system
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
33065108	33119456	33203064	`claus`

Shared secret	
bytes	system
128	`claus`

8.46 x86, 2995MHz, Intel Xeon (f41), `nmi0079`



Cycles to generate a key pair			
quartile	median	quartile	system
25213635	25244940	25288297	`claus`

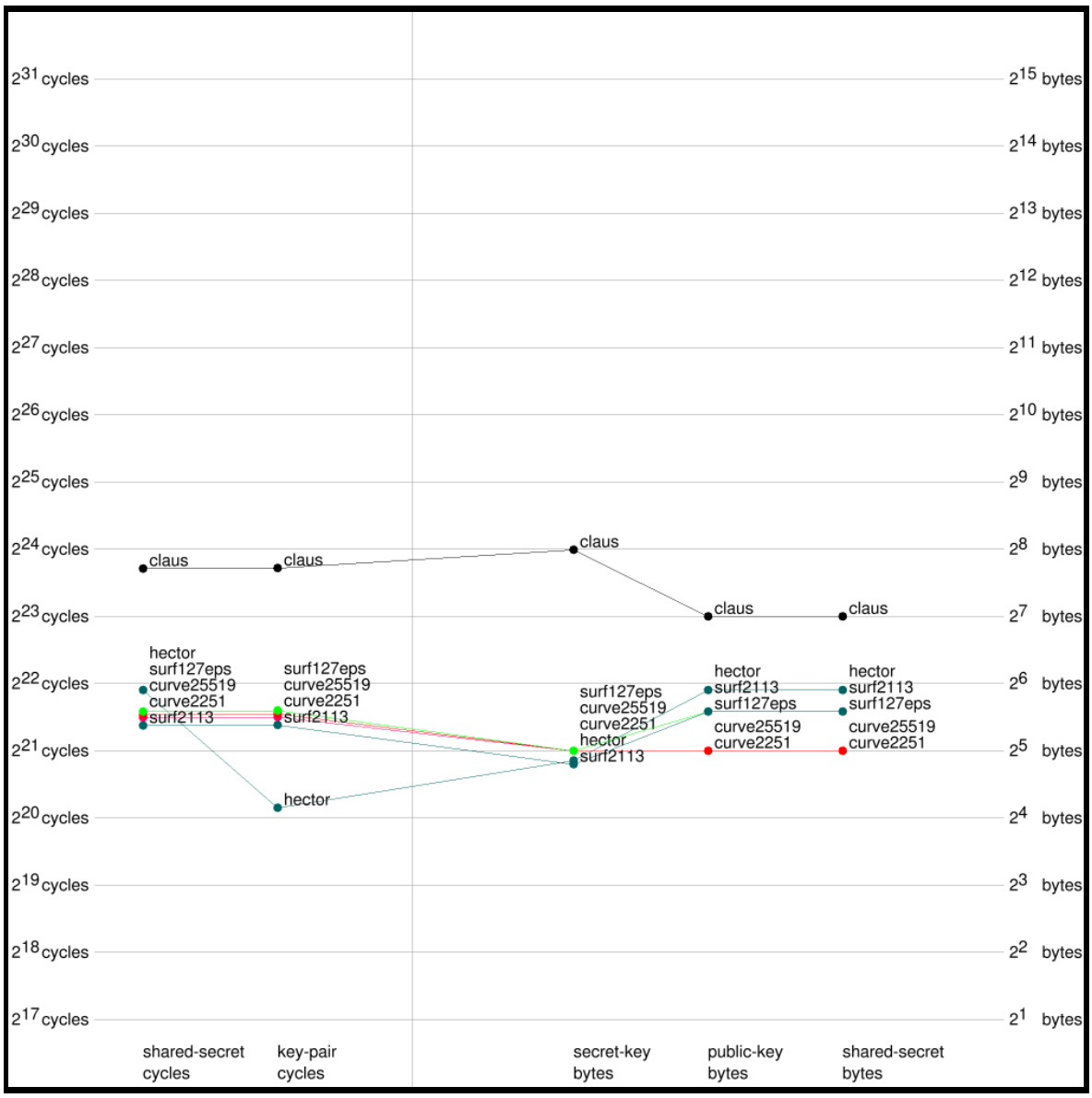
Secret key	
bytes	system
256	`claus`

Public key	
bytes	system
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
25171875	25199370	25229347	`claus`

Shared secret	
bytes	system
128	`claus`

8.47 x86, 2996MHz, Intel Xeon (f41), nmi0076



Cycles to generate a key pair			
quartile	median	quartile	system
1134503	1167930	1219500	`hector`
2723393	2736705	2746433	`surf2113`
2966333	2979915	2992822	`curve2251`
3075217	3087225	3105015	`curve25519`
3180878	3192825	3200978	`surf127eps`
13813260	13837673	13871467	`claus`

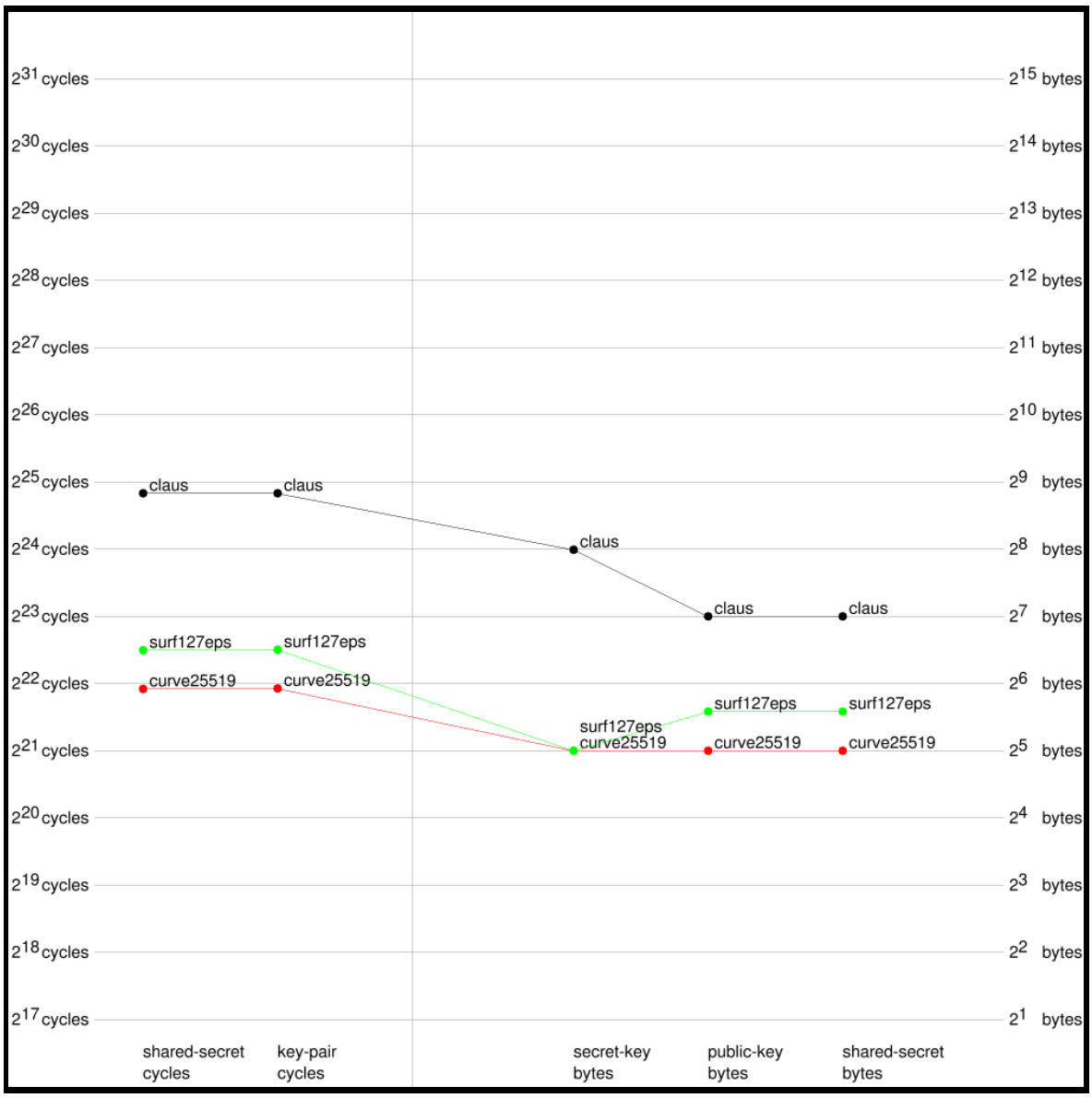
Secret key	
bytes	system
28	`surf2113`
29	`hector`
32	`curve2251`
32	`curve25519`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve2251`
32	`curve25519`
48	`surf127eps`
48	`surf2113`
60	`hector`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
2729827	2733863	2739240	`surf2113`
2953380	2959927	2976855	`curve2251`
3059565	3068812	3079920	`curve25519`
3152212	3157800	3163417	`surf127eps`
3912150	3927945	3940387	`hector`
13776727	13784805	13824690	`claus`

Shared secret	
bytes	system
32	`curve2251`
32	`curve25519`
48	`surf127eps`
48	`surf2113`
60	`hector`
128	`claus`

8.48 x86, 3000MHz, Intel Xeon (f4a), `nmi0090`



Cycles to generate a key pair			
quartile	median	quartile	system
3995250	4007197	4018500	`curve25519`
5951227	5971807	5994675	`surf127eps`
29958270	30006052	30065693	`claus`

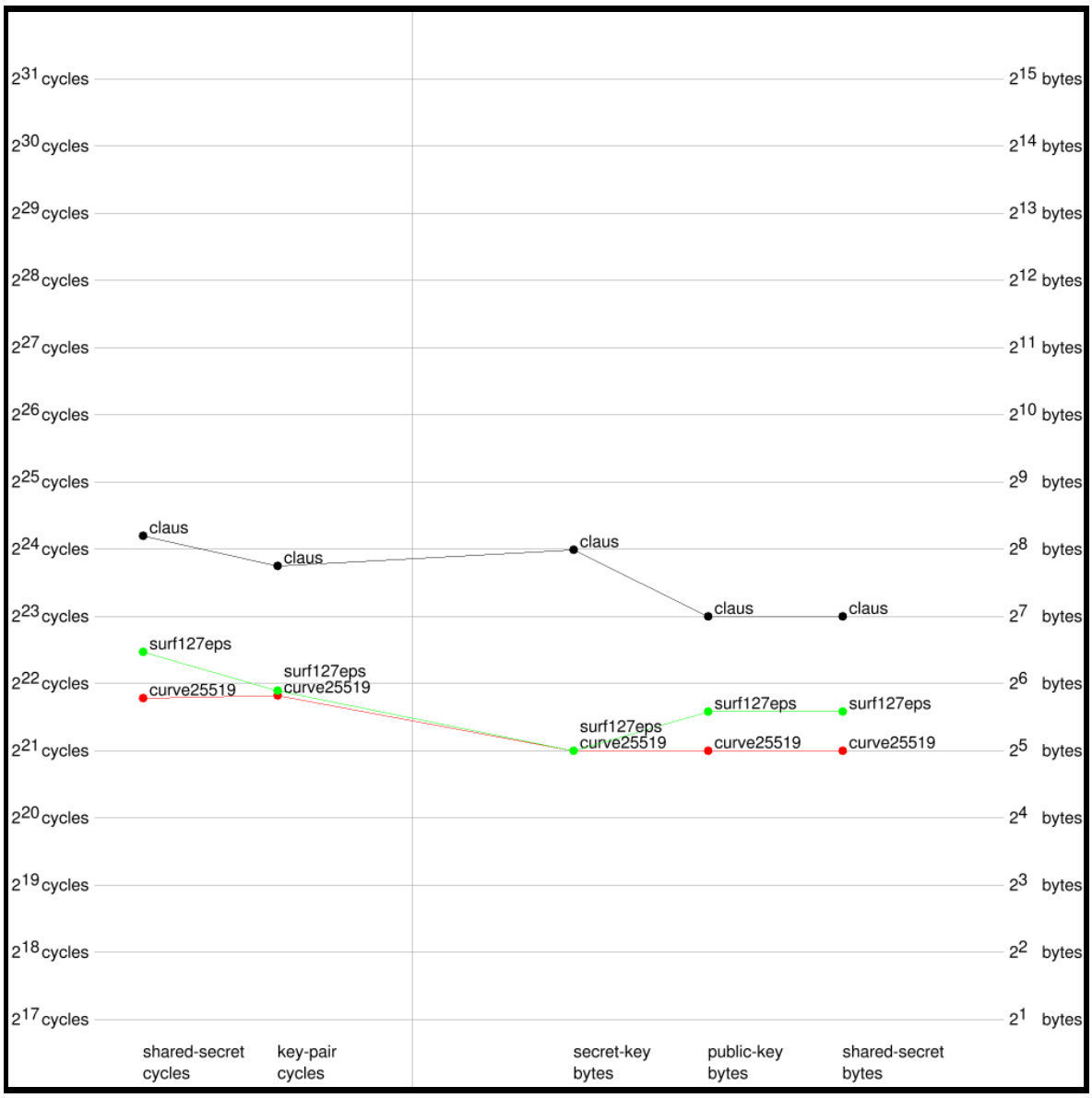
Secret key	
bytes	system
32	`curve25519`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
3922853	3980235	3989108	`curve25519`
5849550	5919750	5937780	`surf127eps`
29922930	29999033	30004905	`claus`

Shared secret	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

8.49 x86, 3000MHz, Intel Xeon (f4a), `nmi0102`



Cycles to generate a key pair			
quartile	median	quartile	system
3243503	3721035	4753200	`curve25519`
3885675	3903525	5925210	`surf127eps`
13834785	14181660	19744155	`claus`

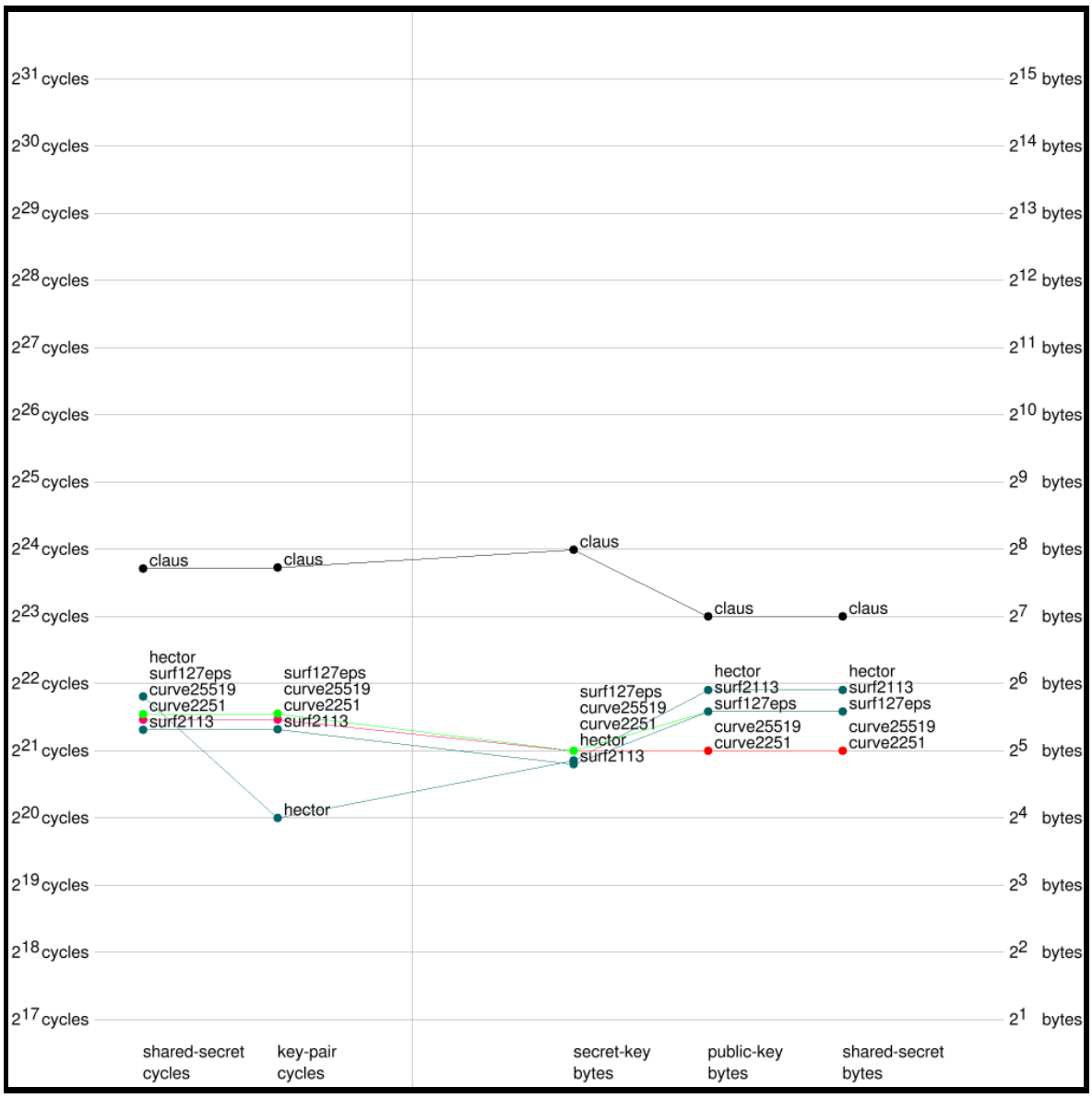
Secret key	
bytes	system
32	`curve25519`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
3226020	3622440	4750988	`curve25519`
3874485	5840835	6094980	`surf127eps`
14507843	19315215	24279487	`claus`

Shared secret	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

8.50 x86, 3391MHz, Intel Pentium D (f64), `nmi0099`



Cycles to generate a key pair			
quartile	median	quartile	system
1031152	1053252	1100563	`hector`
2608004	2620108	2629917	`surf2113`
2894794	2905521	2913528	`curve2251`
3046621	3079652	3108297	`curve25519`
3074280	3084514	3090039	`surf127eps`
13821510	13899166	14043360	`claus`

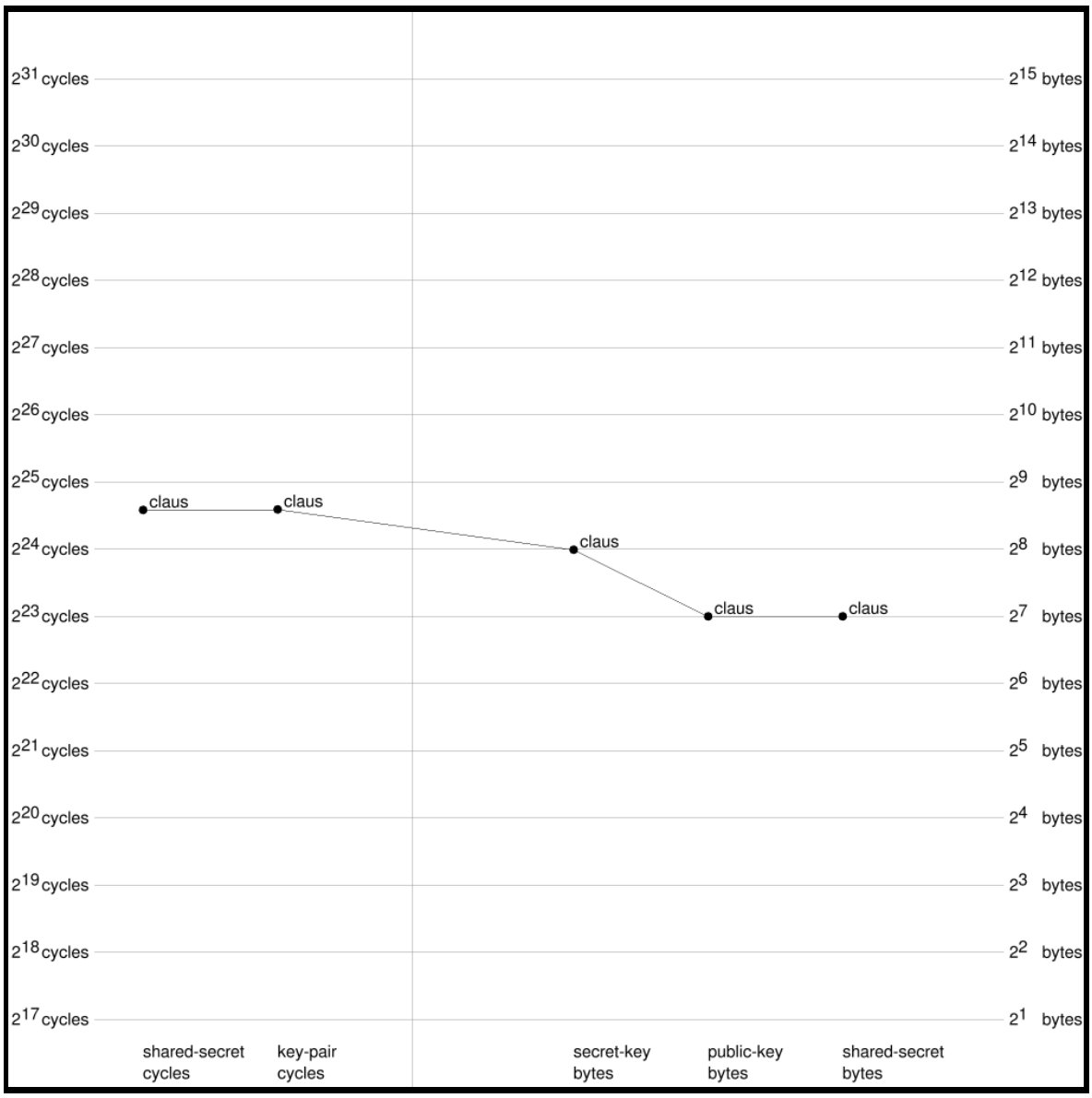
Secret key	
bytes	system
28	`surf2113`
29	`hector`
32	`curve2251`
32	`curve25519`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve2251`
32	`curve25519`
48	`surf127eps`
48	`surf2113`
60	`hector`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
2604417	2613784	2620074	`surf2113`
2893349	2897310	2902869	`curve2251`
3031729	3060680	3097587	`curve25519`
3059269	3066205	3069333	`surf127eps`
3648812	3673972	3689629	`hector`
13795143	13806227	13842930	`claus`

Shared secret	
bytes	system
32	`curve2251`
32	`curve25519`
48	`surf127eps`
48	`surf2113`
60	`hector`
128	`claus`

8.51 x86, 3392MHz, Intel Pentium D (f64), nmi0104



Cycles to generate a key pair			
quartile	median	quartile	system
25266301	25300165	25331955	`claus`

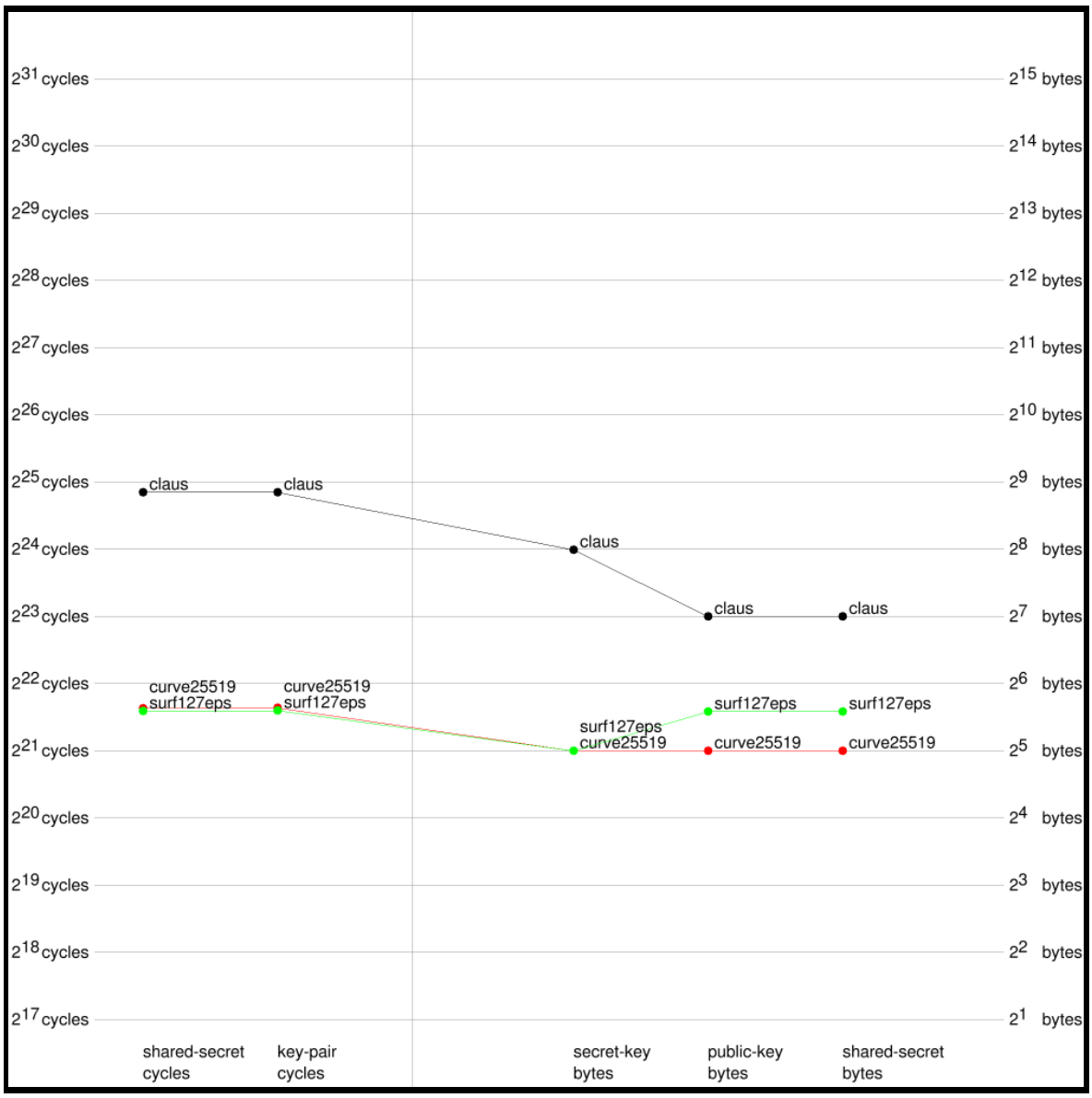
Secret key	
bytes	system
256	`claus`

Public key	
bytes	system
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
25184684	25216576	25244133	`claus`

Shared secret	
bytes	system
128	`claus`

8.52 x86, 3392MHz, Intel Pentium D (f64), `nmi0241`



Cycles to generate a key pair			
quartile	median	quartile	system
3176195	3187296	3195745	`surf127eps`
3268641	3283227	3294124	`curve25519`
30315250	30365621	30426855	`claus`

Secret key	
bytes	system
32	`curve25519`
32	`surf127eps`
256	`claus`

Public key	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

Cycles to compute a shared secret			
quartile	median	quartile	system
3155523	3161609	3167610	`surf127eps`
3255670	3258475	3261977	`curve25519`
30328085	30342501	30448955	`claus`

Shared secret	
bytes	system
32	`curve25519`
48	`surf127eps`
128	`claus`

Chapter 9

Measurements of public-key cryptosystems

9.1 Introduction

This chapter presents a series of graphs, one for each computer. There are seven horizontal positions on each graph:

- Time to encrypt a short message.
- Time to decrypt a short message.
- Time to compute a key pair.
- Space for a secret key.
- Space for a public key.
- Ciphertext overhead for a short message: more precisely, the difference between the space used by a short encrypted message and the space used by the original message.
- Ciphertext overhead for a long message.

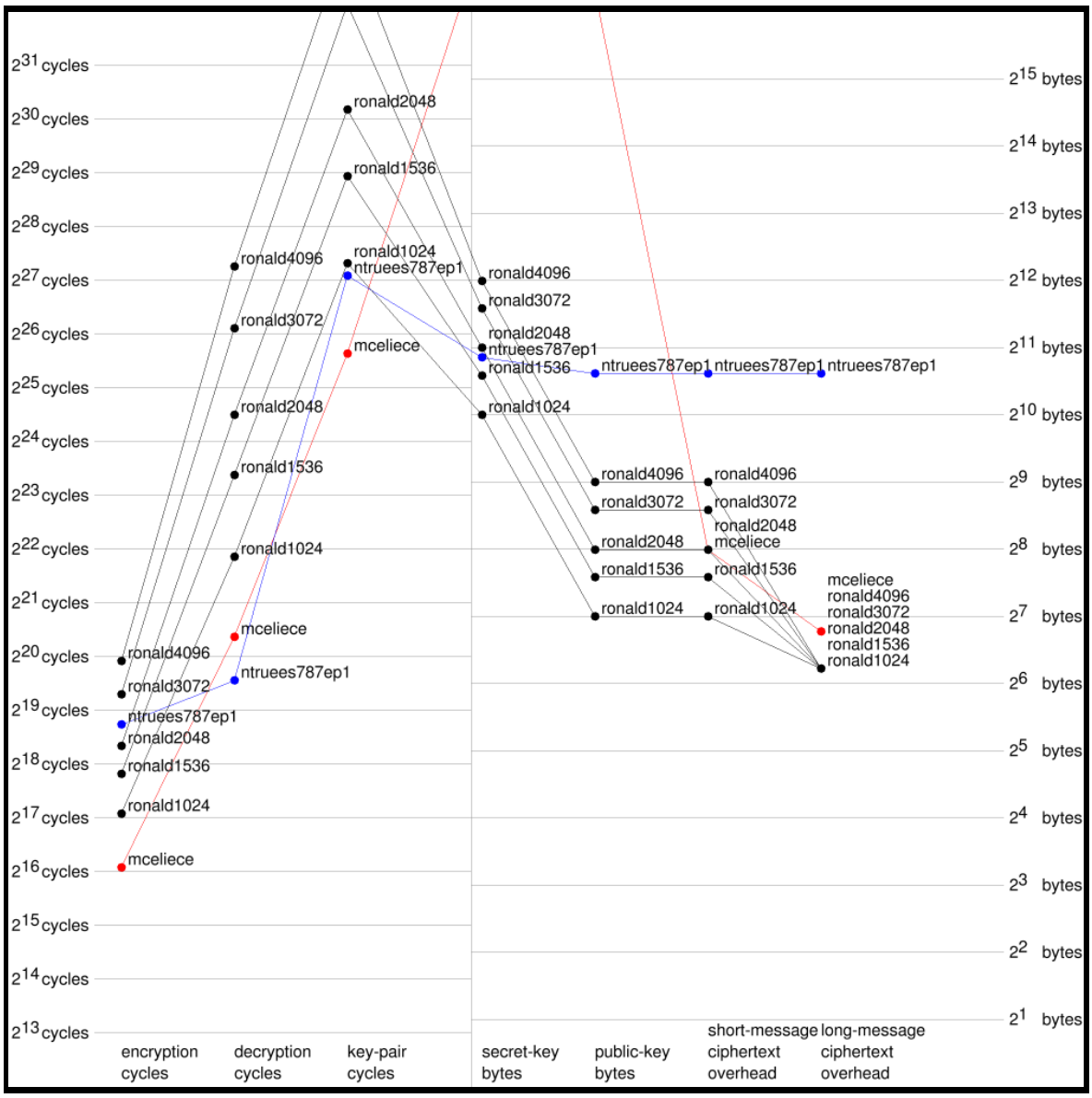
Each graph is a superimposition of several curves, one curve for each cryptosystem.

This chapter also presents a series of tables, eight for each computer. The first table shows the time, in cycles, to generate a key pair. Each row of the table lists

- the first quartile of many time measurements,
- the median of many time measurements,
- the third quartile of many time measurements, and
- the name of the signature system.

The second table shows the length of a secret key. The third table shows the length of a public key. The fourth table shows the time to encrypt a short message. The fifth table shows the time to decrypt a short message. The sixth, seventh, and eighth tables show the ciphertext overhead for, respectively, a 0-byte message, a 23-byte message, and a long message.

9.2 amd64, 1403MHz, AMD Opteron 240 (f58), `nmisles8amd64`



Cycles to generate a key pair			
quartile	median	quartile	system
48738789	52424124	57779331	`mceliece`
142572348	143160297	143513715	`ntruees787ep1`
118379135	168586970	264884063	`ronald1024`
314176228	517632313	761635274	`ronald1536`
813700211	1222218615	1977206553	`ronald2048`
3089450697	4763372801	7681274731	`ronald3072`
6289224404	11691185974	18282730408	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
68534	69473	70510	`mceliece`
137070	138623	140799	`ronald1024`
227605	231663	235825	`ronald1536`
329812	332837	336152	`ronald2048`
439562	439797	440224	`ntruees787ep1`
639850	648502	655097	`ronald3072`
989345	997276	1004456	`ronald4096`

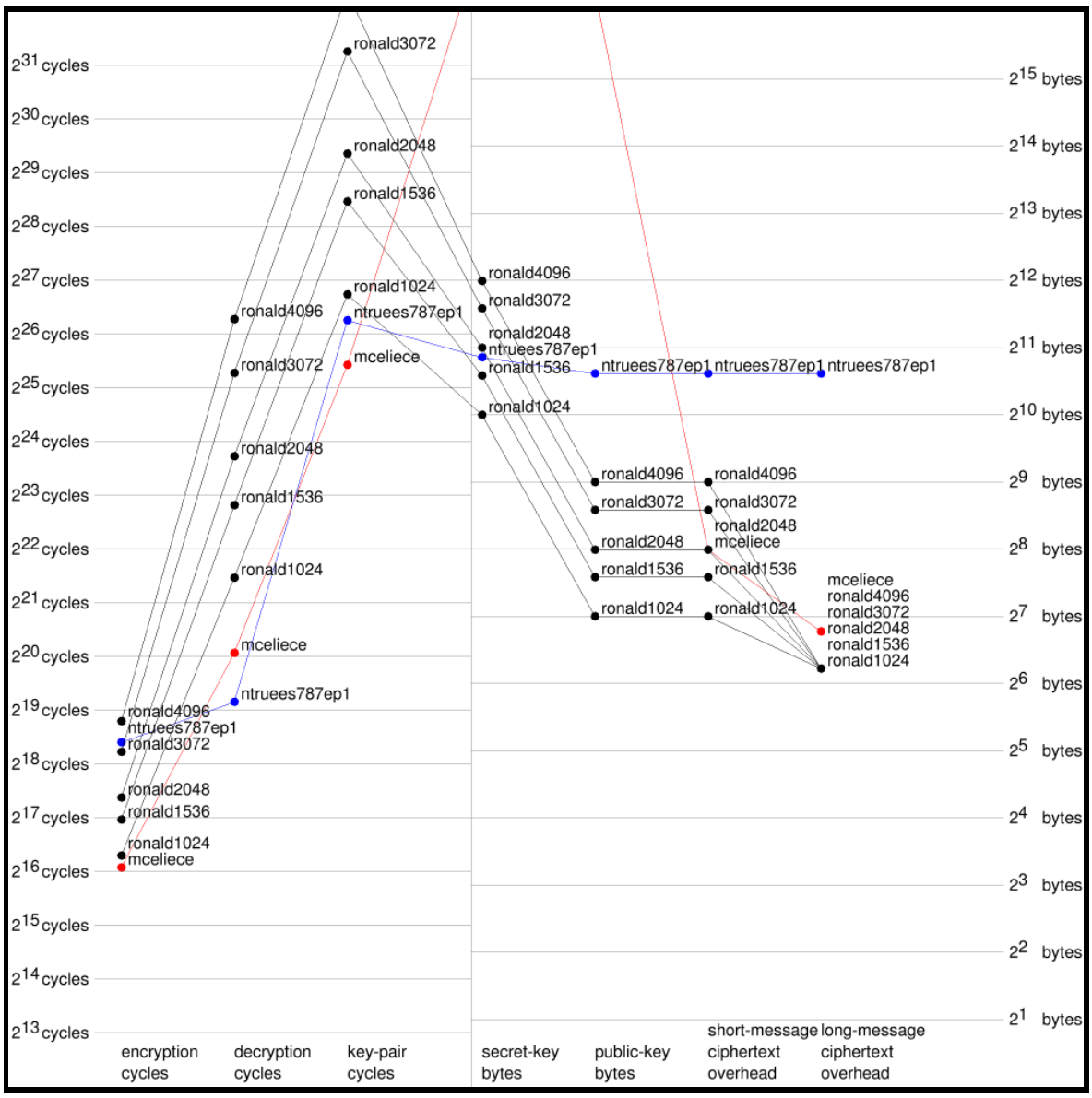
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
769862	774027	774208	`ntruees787ep1`
1355945	1361401	1368075	`mceliece`
3819747	3826109	3831512	`ronald1024`
10889563	10974806	11042385	`ronald1536`
23822812	23863377	24288703	`ronald2048`
72307613	72511086	73107425	`ronald3072`
160117093	161811219	161954156	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.3 amd64, 2400MHz, Intel Core 2 Duo (6fb), utrecht



Cycles to generate a key pair			
quartile	median	quartile	system
43606791	45446220	48259008	`mceliece`
80343765	80672013	80932626	`ntruees787ep1`
66538188	112559931	179167131	`ronald1024`
205613793	373598478	594934281	`ronald1536`
482270445	690044733	992475918	`ronald2048`
1293199686	2584139454	3894793920	`ronald3072`
3264666705	5568395958	7835179050	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
68652	69543	70434	`mceliece`
80361	80838	82224	`ronald1024`
125964	128718	129879	`ronald1536`
168624	170928	172800	`ronald2048`
305460	308241	310797	`ronald3072`
349614	350019	350325	`ntruees787ep1`
455229	458730	461214	`ronald4096`

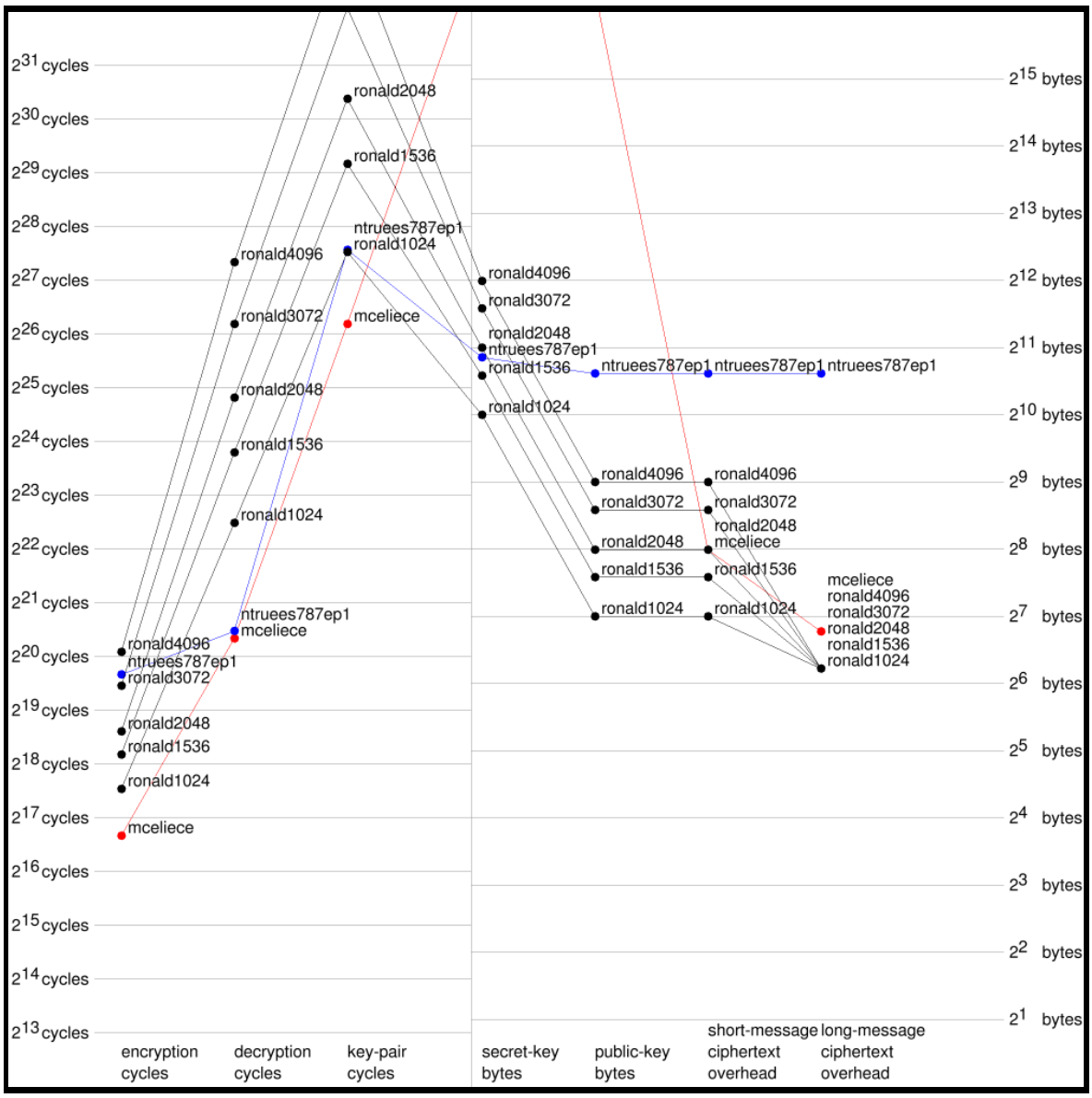
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
589158	589770	591516	`ntruees787ep1`
1103193	1106001	1113615	`mceliece`
2885697	2910519	2931651	`ronald1024`
7379001	7417449	7458966	`ronald1536`
13897332	13942602	14048172	`ronald2048`
39891060	40901418	41039424	`ronald3072`
81434457	81588564	82021266	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.4 amd64, 2800MHz, Intel Xeon (f41), nmi0056



Cycles to generate a key pair			
quartile	median	quartile	system
73929646	76870584	81366943	`mceliece`
137773664	194617969	309019333	`ronald1024`
199032113	200037432	200638137	`ntruees787ep1`
354231339	606322325	909931603	`ronald1536`
790400863	1406923616	1825344920	`ronald2048`
2609640992	4519931864	7859433757	`ronald3072`
6974977884	12185371023	24494008644	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
103845	104867	106757	`mceliece`
188552	190582	195762	`ronald1024`
295757	298165	304297	`ronald1536`
397068	401653	408625	`ronald2048`
719026	725620	732270	`ronald3072`
835436	837340	840231	`ntruees787ep1`
1113784	1120889	1128456	`ronald4096`

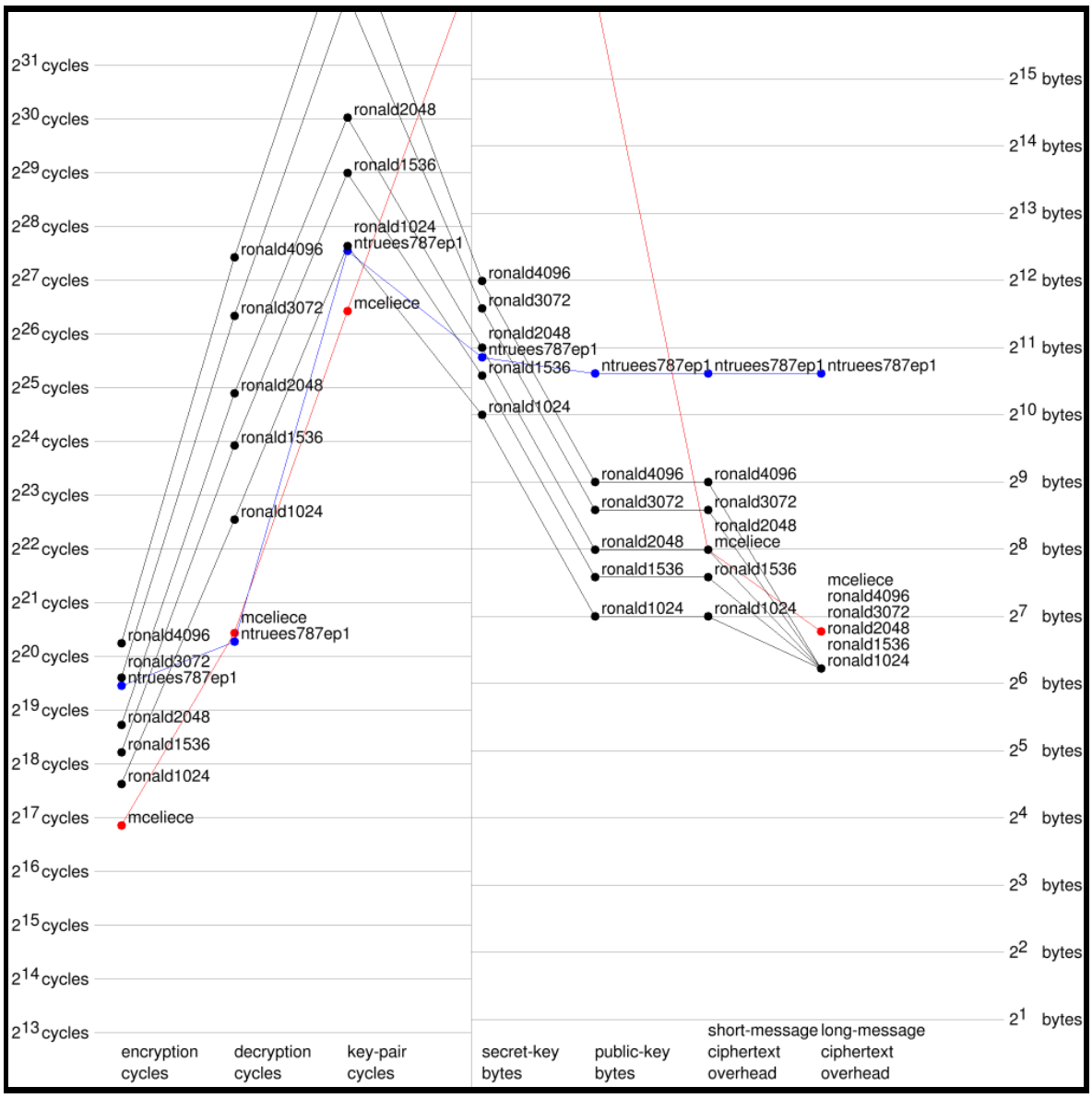
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1317183	1327361	1329811	`mceliece`
1465702	1467823	1471554	`ntruees787ep1`
5882898	5910975	5950658	`ronald1024`
14666183	14702331	14779352	`ronald1536`
29535317	29618890	29766800	`ronald2048`
76884906	77069048	77258713	`ronald3072`
170186835	170696386	171361260	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.5 amd64, 2800MHz, Intel Xeon (f41), nmi0057



Cycles to generate a key pair			
quartile	median	quartile	system
85467137	90919059	97548626	`mceliece`
196526120	197462153	197956535	`ntruees787ep1`
131293400	209313468	317810388	`ronald1024`
402612952	539772604	760711980	`ronald1536`
583317574	1101292738	1830579296	`ronald2048`
3608243184	5378021369	7532521598	`ronald3072`
7564403140	13740529670	21147901089	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
115801	119511	129234	`mceliece`
201817	203959	208803	`ronald1024`
301112	306383	312431	`ronald1536`
429513	435736	446180	`ronald2048`
721588	726117	730324	`ntruees787ep1`
791490	802011	814219	`ronald3072`
1238566	1252776	1261477	`ronald4096`

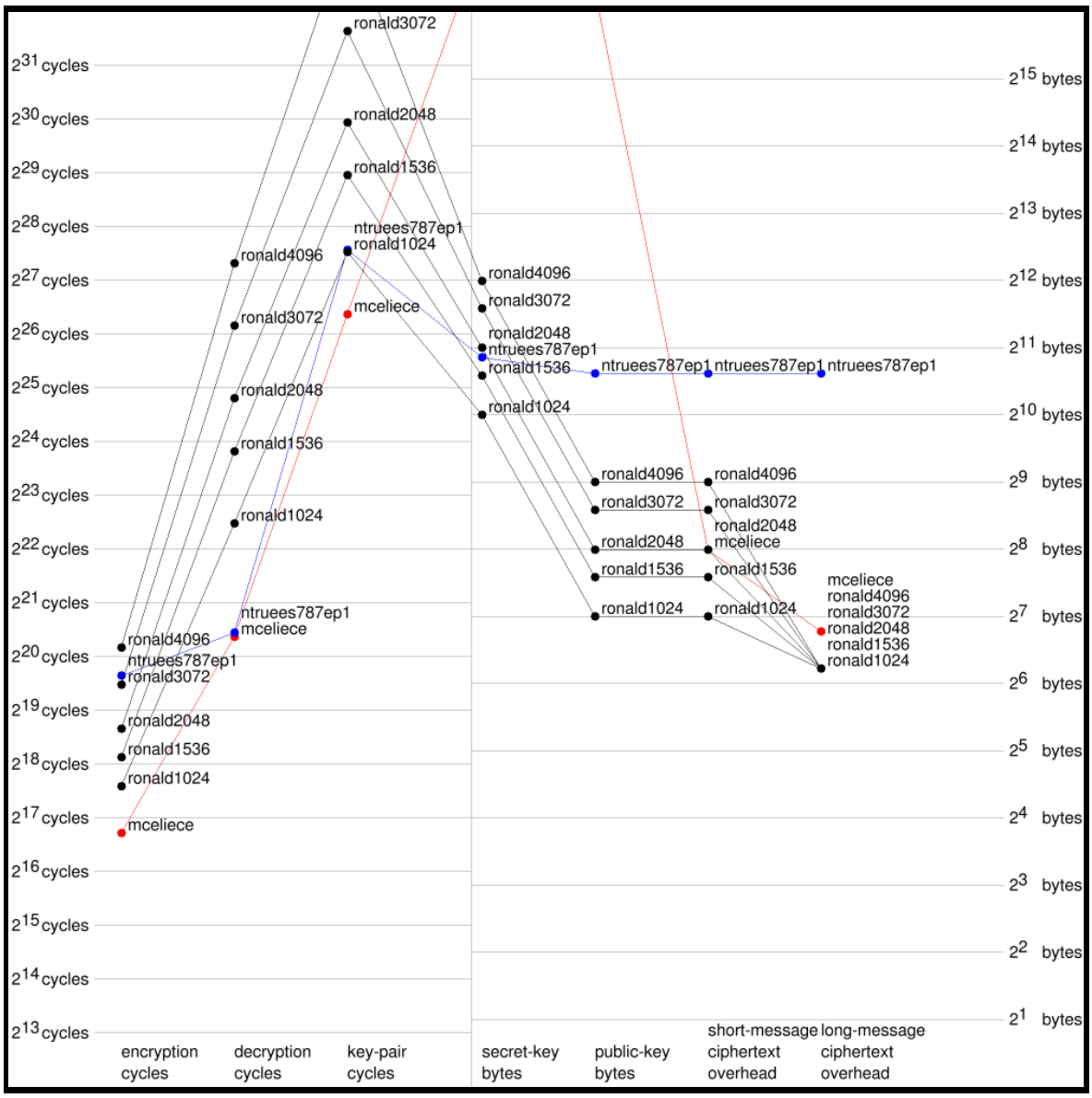
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1269373	1274042	1281756	`ntruees787ep1`
1417696	1422855	1434258	`mceliece`
6155037	6181175	6212178	`ronald1024`
15948212	16018751	16137149	`ronald1536`
31280781	31394286	31639013	`ronald2048`
84833434	85104432	85441881	`ronald3072`
181226605	182024129	183375185	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.6 amd64, 2800MHz, Intel Xeon (f41), nmi0063



Cycles to generate a key pair			
quartile	median	quartile	system
84238035	87239593	93770313	`mceliece`
114707530	194695522	315218470	`ronald1024`
198757356	199684352	200335079	`ntruees787ep1`
363321651	522470473	853527619	`ronald1536`
683051579	1030606010	1802681433	`ronald2048`
2295172740	3364977966	6005114073	`ronald3072`
6746497443	12383793142	16726014221	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
107065	108325	110215	`mceliece`
195104	197316	202699	`ronald1024`
282975	287945	294679	`ronald1536`
409227	415149	420343	`ronald2048`
730415	736134	743365	`ronald3072`
822157	826252	830277	`ntruees787ep1`
1176763	1184771	1193059	`ronald4096`

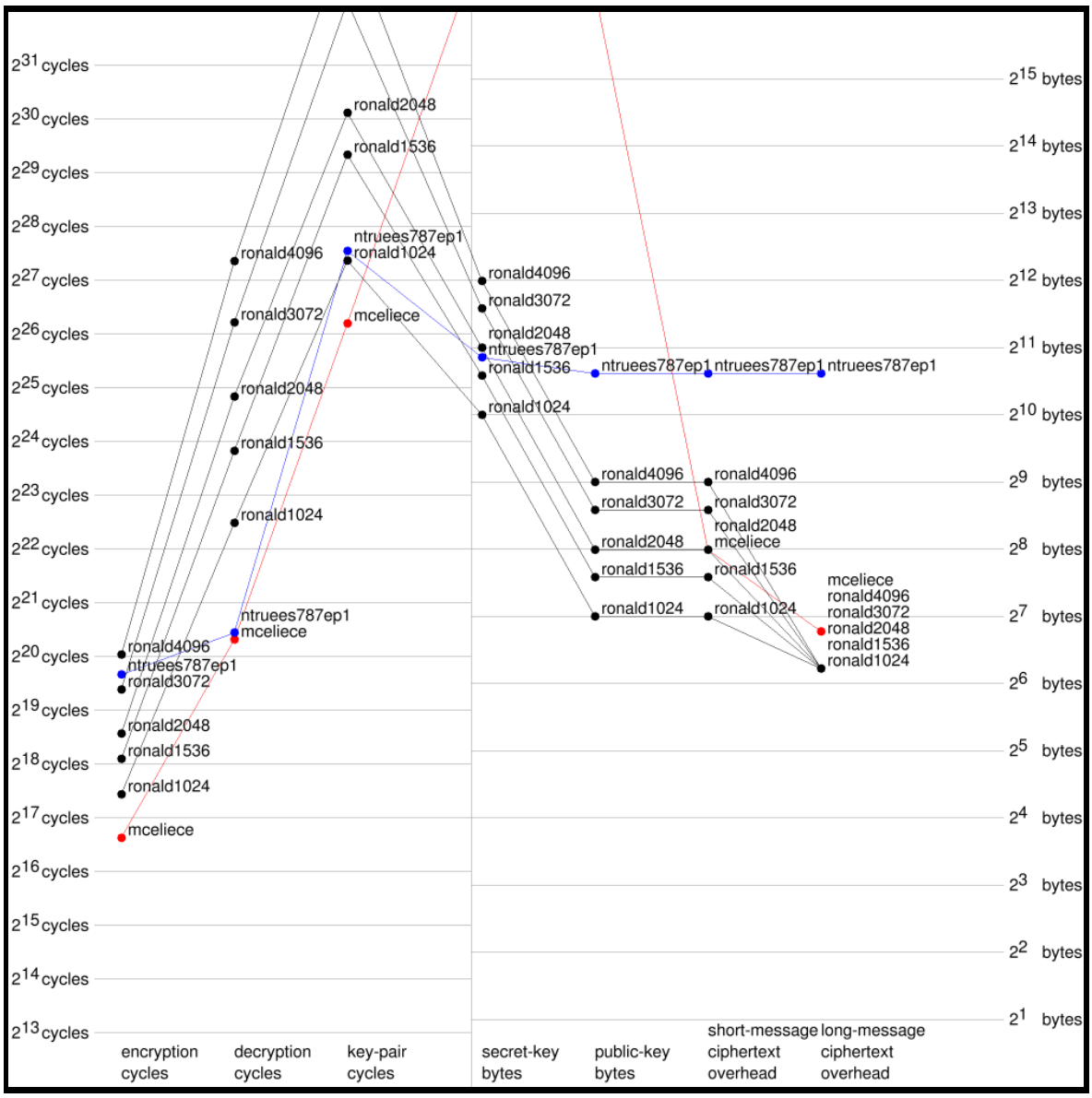
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1352834	1358623	1362221	`mceliece`
1430989	1436246	1440621	`ntruees787ep1`
5851146	5872944	5910464	`ronald1024`
14849520	14900270	14950152	`ronald1536`
29501556	29583666	29664572	`ronald2048`
74605692	75011930	75579161	`ronald3072`
167592495	167770554	168007609	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.7 amd64, 3000MHz, Intel Pentium D (f64), speed



Cycles to generate a key pair			
quartile	median	quartile	system
73585680	77176065	82488090	`mceliece`
123133125	174420615	267160965	`ronald1024`
196614585	197619435	198415770	`ntruees787ep1`
428982570	680519895	990928230	`ronald1536`
653538690	1169753355	1980886665	`ronald2048`
2549340570	4926630330	7745781465	`ronald3072`
7022864925	12411315270	18124072875	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
100230	101580	103545	`mceliece`
176640	177915	184440	`ronald1024`
279000	281625	291870	`ronald1536`
380670	390165	393915	`ronald2048`
684855	687960	693825	`ronald3072`
836235	838245	840570	`ntruees787ep1`
1077795	1085115	1093995	`ronald4096`

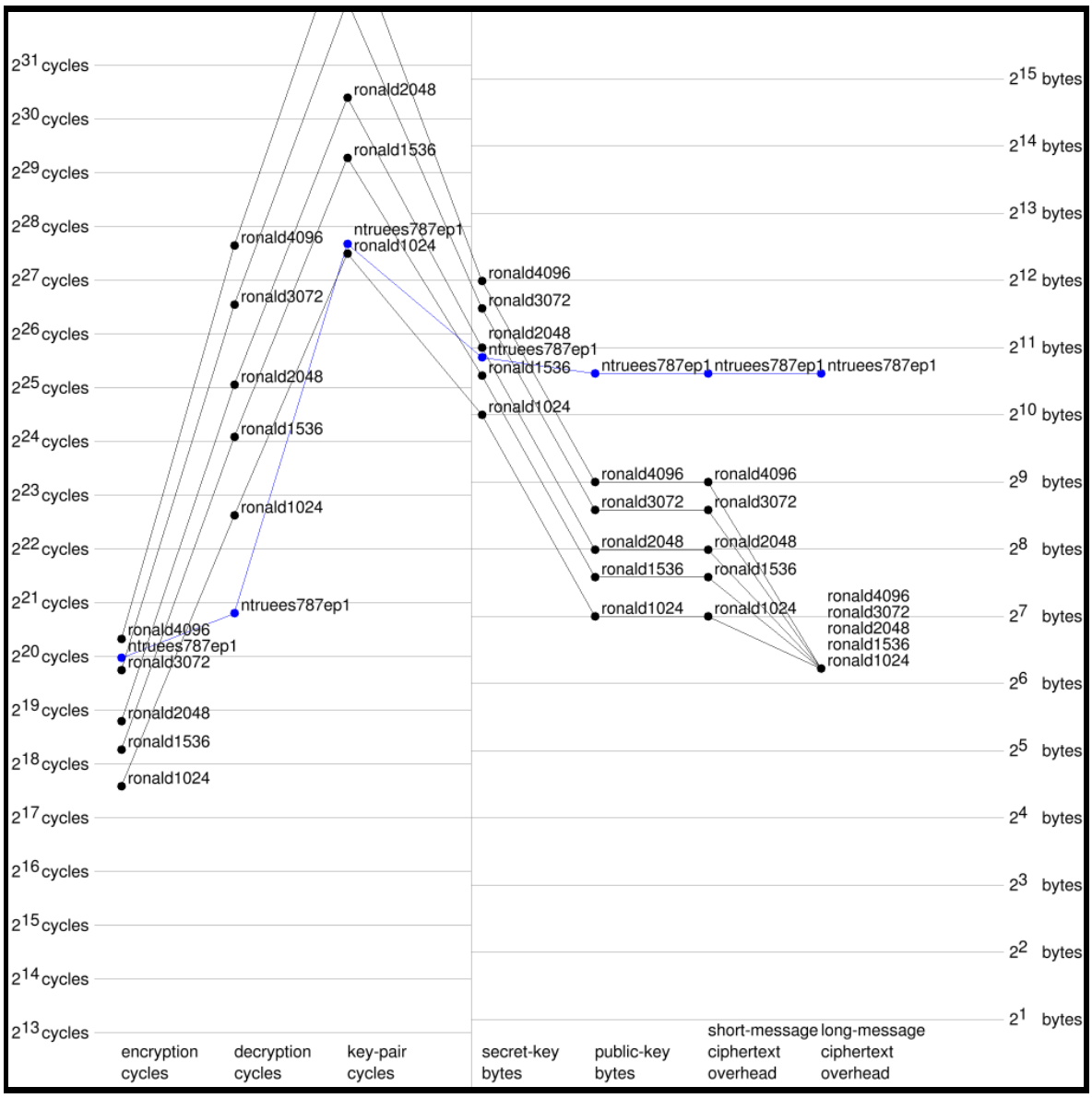
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1305360	1310880	1318770	`mceliece`
1435605	1438575	1441170	`ntruees787ep1`
5875005	5903445	5952390	`ronald1024`
14911590	14995050	15067365	`ronald1536`
30102075	30214335	30328095	`ronald2048`
77691120	78192495	78685770	`ronald3072`
172685565	173397930	174080775	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.8 amd64, 3000MHz, Intel Xeon (f4a), `nmi0090`



Cycles to generate a key pair			
quartile	median	quartile	system
120888172	191099753	316646213	`ronald1024`
215483093	216390997	217100842	`ntruees787ep1`
383631195	653327438	922906027	`ronald1536`
802095337	1421355990	2202078840	`ronald2048`
3424316588	4954458345	8118767715	`ronald3072`
9490839165	13954826820	22346355307	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
193500	198383	203768	`ronald1024`
311032	318225	322470	`ronald1536`
451170	456540	461760	`ronald2048`
877125	882105	891630	`ronald3072`
1033763	1036200	1041240	`ntruees787ep1`
1313917	1320405	1330935	`ronald4096`

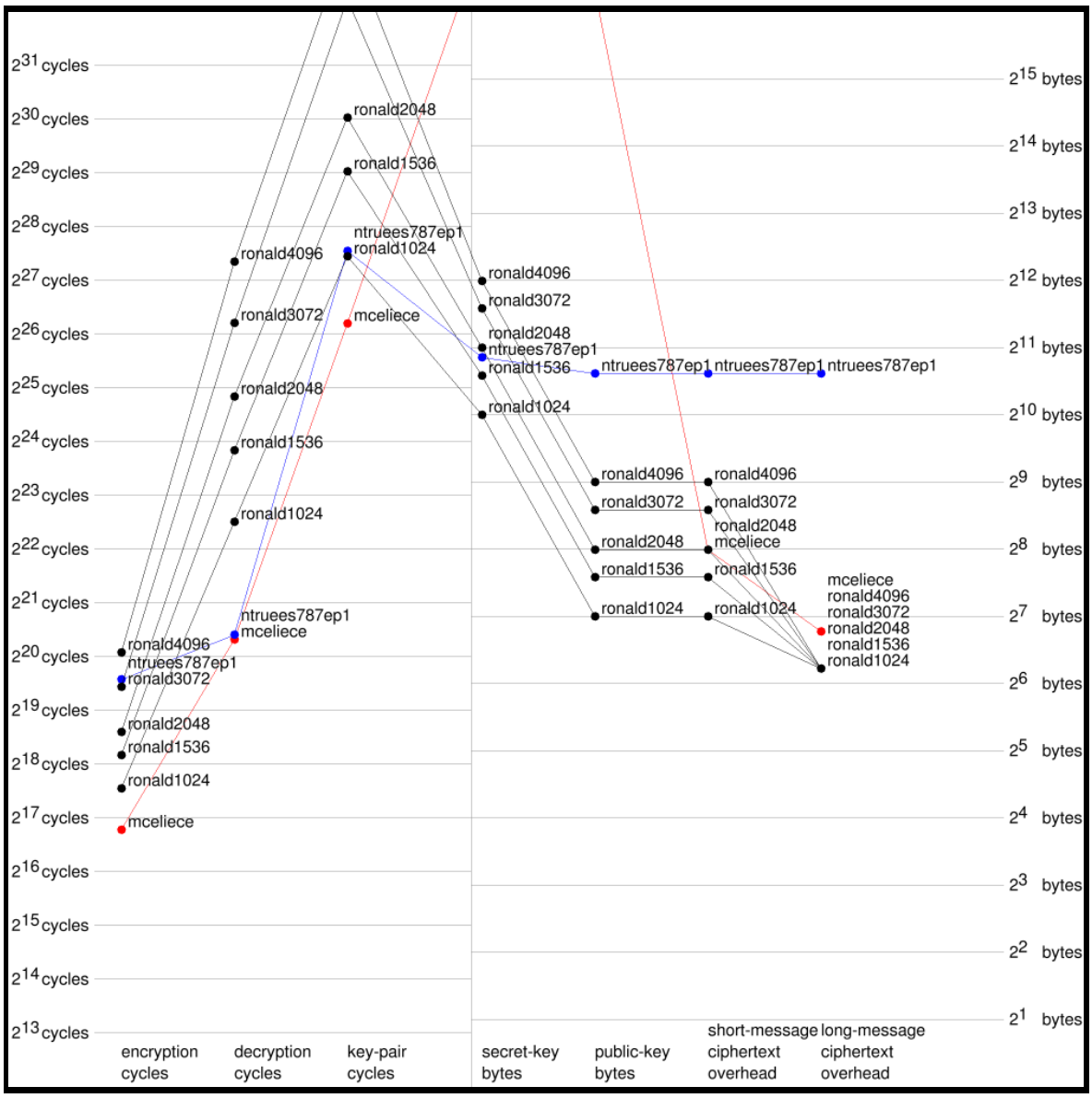
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1843642	1846875	1850993	`ntruees787ep1`
6473977	6503977	6543488	`ronald1024`
17823142	17916660	17961023	`ronald1536`
34917675	35046038	35097097	`ronald2048`
98243017	98414872	98625412	`ronald3072`
211446863	211708350	211984777	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
1573	`ntruees787ep1`

9.9 amd64, 3392MHz, Intel Pentium D (f64), nmi0104



Cycles to generate a key pair			
quartile	median	quartile	system
74452316	77109110	82939770	`mceliece`
112161784	184032548	266441221	`ronald1024`
196527956	197485974	198114090	`ntruees787ep1`
378381818	551290467	938071050	`ronald1536`
690715967	1100562150	1753275518	`ronald2048`
2473255081	5042072109	6891528255	`ronald3072`
7370912224	11025074872	17770093914	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
111214	112659	114223	`mceliece`
190026	192644	197183	`ronald1024`
292978	295273	299370	`ronald1536`
393397	397953	402985	`ronald2048`
706231	711637	718505	`ronald3072`
785043	786590	788477	`ntruees787ep1`
1104184	1112140	1117580	`ronald4096`

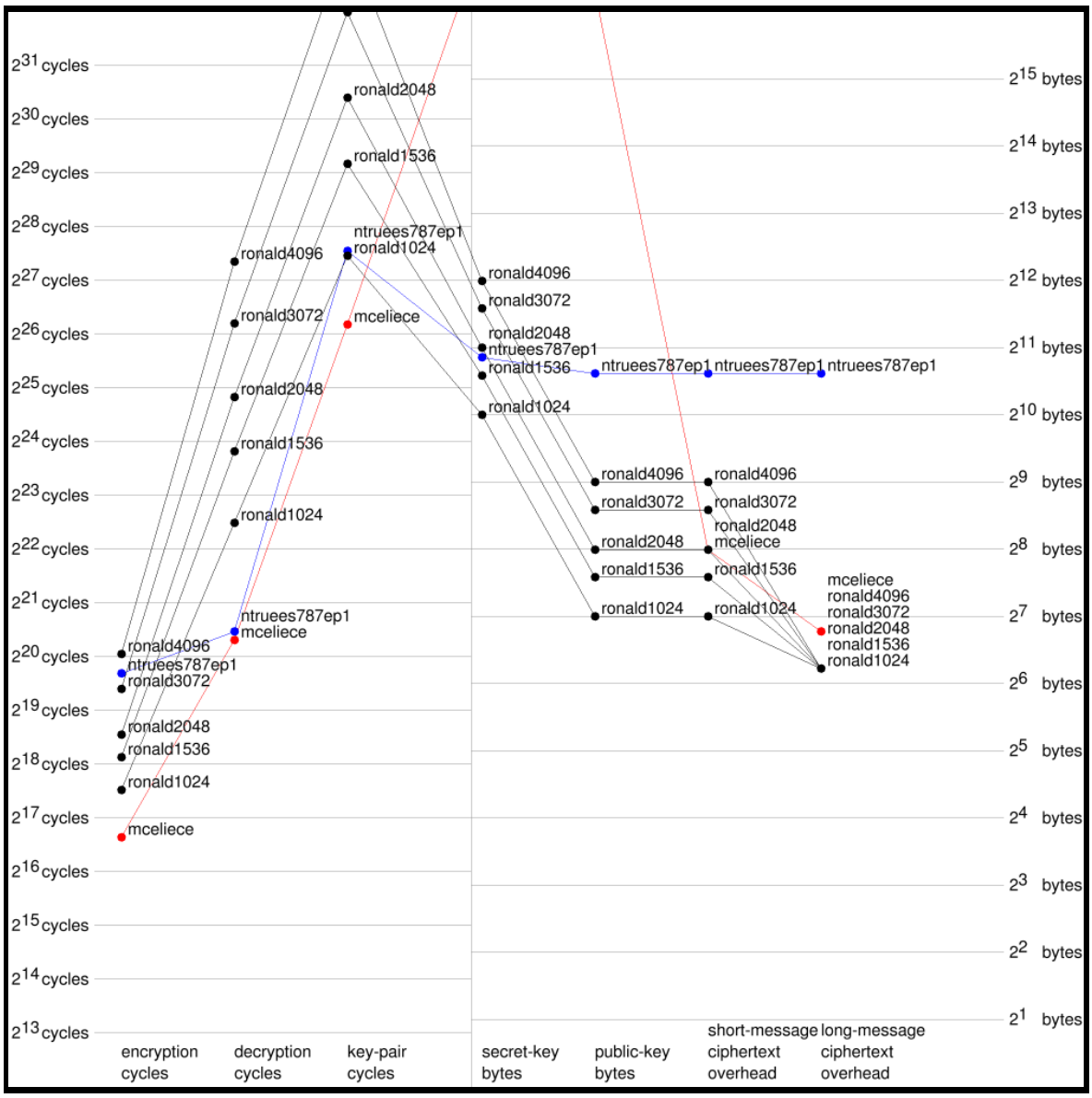
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1315460	1317007	1328975	`mceliece`
1396227	1399882	1402670	`ntruees787ep1`
5936536	5981263	6036139	`ronald1024`
14999457	15097105	15136239	`ronald1536`
30121705	30185744	30251704	`ronald2048`
77766772	78016332	78270618	`ronald3072`
171498193	171859732	172250800	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.10 amd64, 3392MHz, Intel Pentium D (f64), nmi0161



Cycles to generate a key pair			
quartile	median	quartile	system
73536679	76438511	80901674	`mceliece`
132577356	185249527	295609957	`ronald1024`
196343336	197345707	197870310	`ntruees787ep1`
304798406	607652165	817351772	`ronald1536`
756359784	1426112371	1963392798	`ronald2048`
3198241671	4293678185	6538425403	`ronald3072`
6907990052	11192915192	18650287410	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
101184	102578	104533	`mceliece`
188173	189227	194837	`ronald1024`
284206	286960	292638	`ronald1536`
381429	385781	391085	`ronald2048`
689401	693311	699771	`ronald3072`
847314	849728	851479	`ntruees787ep1`
1083121	1089190	1096925	`ronald4096`

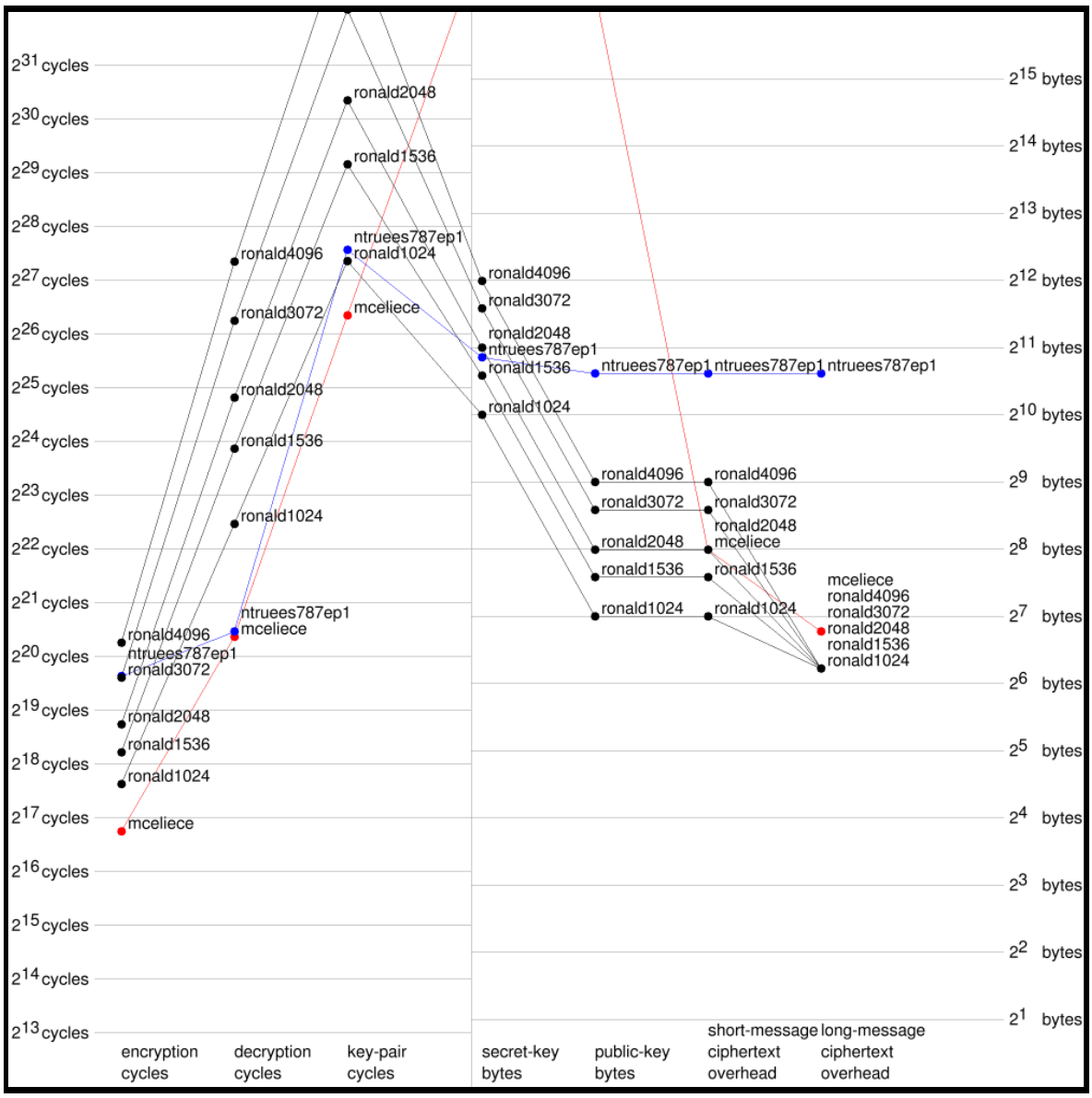
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1303798	1305396	1319030	`mceliece`
1458447	1460521	1463530	`ntruees787ep1`
5897487	5928342	5961033	`ronald1024`
14863372	14883806	14916769	`ronald1536`
29841732	29940434	30071963	`ronald2048`
77267975	77446679	77570201	`ronald3072`
171037527	171254107	171612688	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.11 amd64, 3392MHz, Intel Pentium D (f64), nmi0241



Cycles to generate a key pair			
quartile	median	quartile	system
83091223	85673659	91405277	`mceliece`
117637025	172991847	283286198	`ronald1024`
199847138	200399536	201230921	`ntruees787ep1`
371236140	601149648	885752700	`ronald1536`
804915014	1376492890	2153588067	`ronald2048`
2657505671	4417317179	6500651046	`ronald3072`
7742905000	13188623698	20410159234	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
109123	110585	112472	`mceliece`
200056	202929	208250	`ronald1024`
302413	306561	314602	`ronald1536`
435812	440776	450840	`ronald2048`
798388	804576	812430	`ronald3072`
817122	819910	825350	`ntruees787ep1`
1254005	1262930	1278247	`ronald4096`

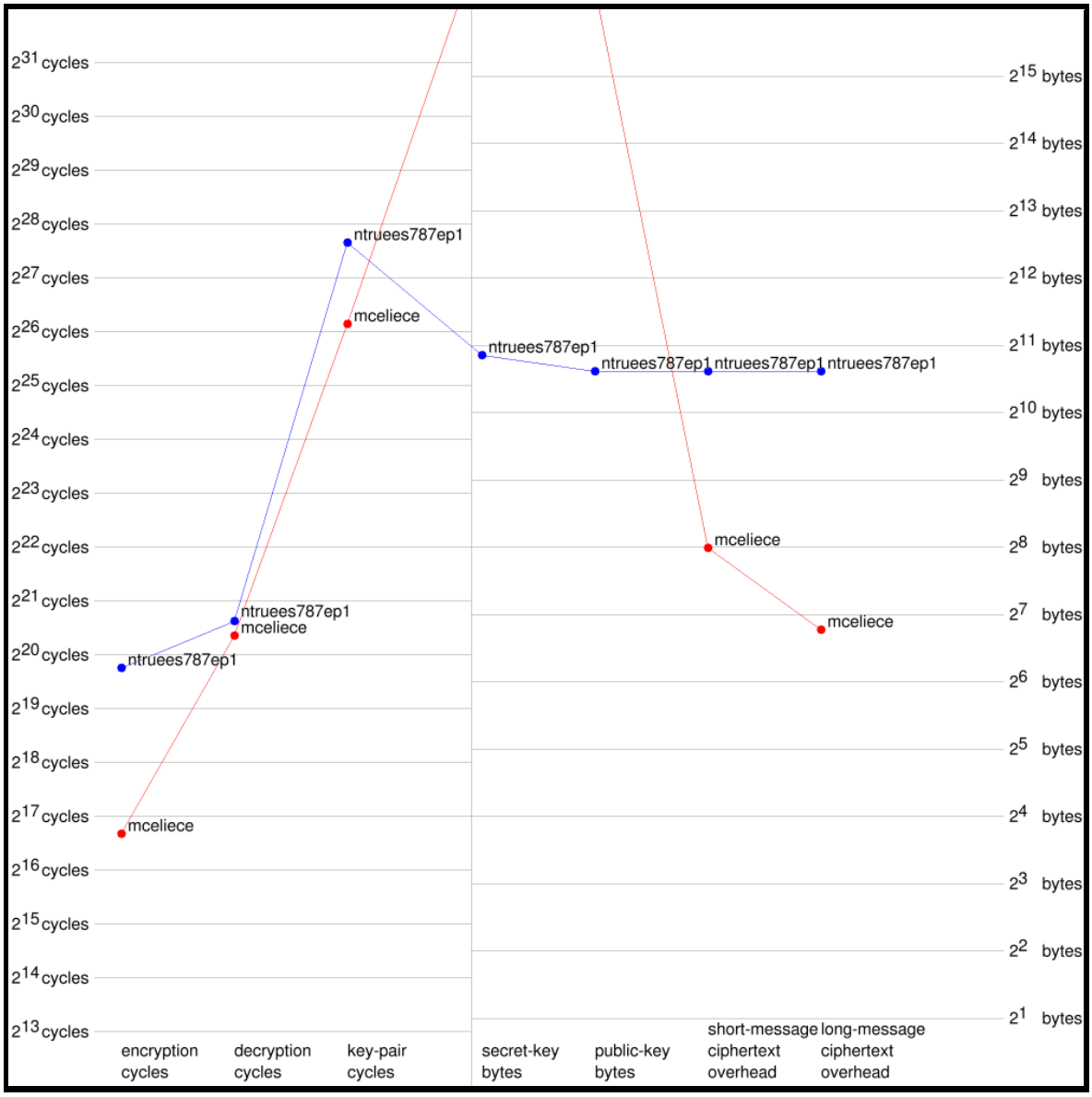
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1353251	1364318	1369299	`mceliece`
1450168	1455744	1464193	`ntruees787ep1`
5758580	5836457	5878668	`ronald1024`
15255120	15354655	15423998	`ronald1536`
29509093	29620426	29815382	`ronald2048`
80099971	80210828	80357572	`ronald3072`
171374739	172158082	172805153	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.12 ia64, 900MHz, HP Itanium II, nmi0025



Cycles to generate a key pair			
quartile	median	quartile	system
71584416	74526764	80206544	`mceliece`
204532447	212805564	295506535	`ntruees787ep1`

Secret key	
bytes	system
1854	`ntruees787ep1`
137282	`mceliece`

Public key	
bytes	system
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
104613	105695	107318	`mceliece`
890776	891413	891861	`ntruees787ep1`

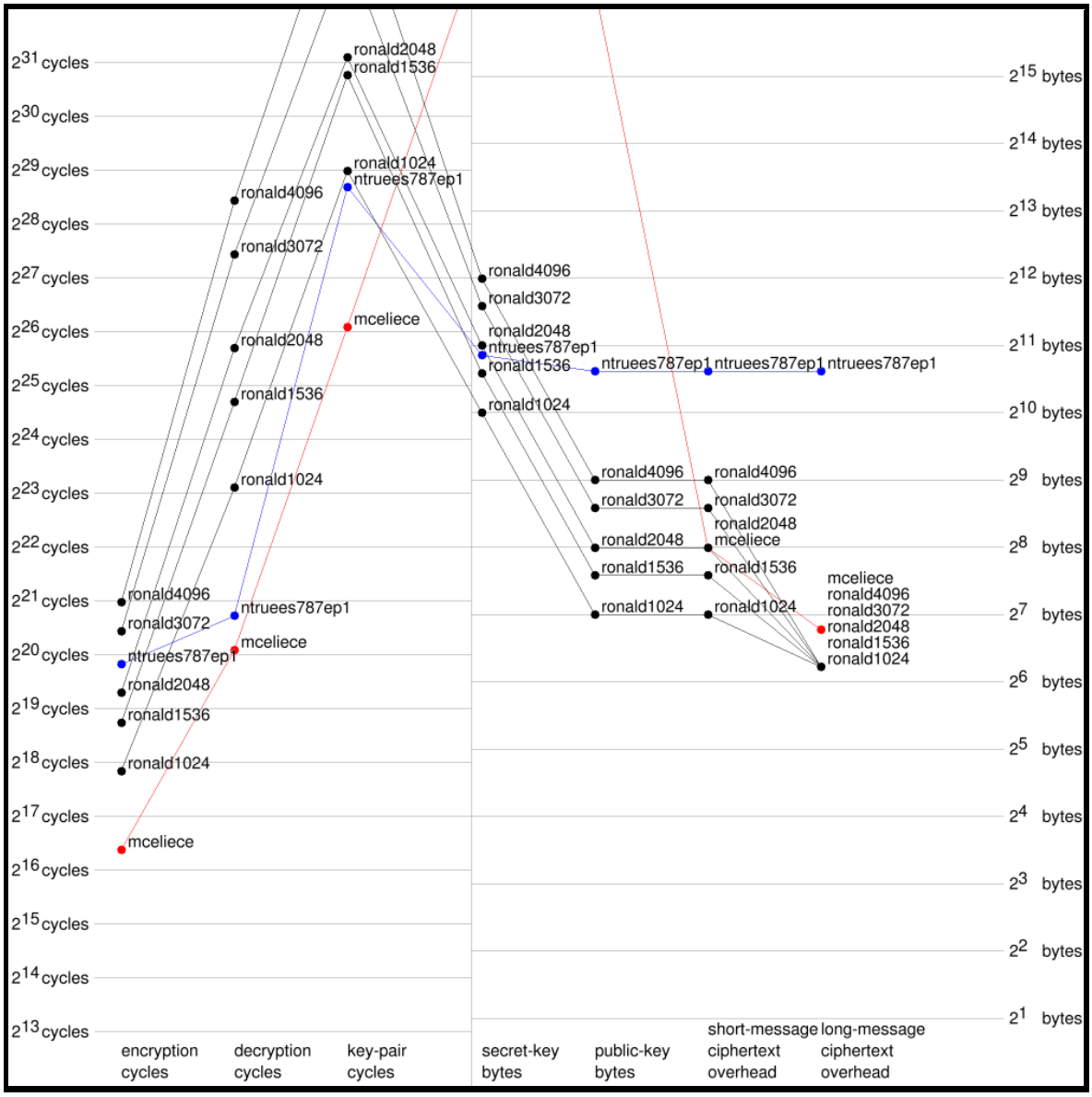
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1338471	1351677	1353842	`mceliece`
1629450	1629706	1629953	`ntruees787ep1`

Encrypting 0 bytes	
bytes	system
256	`mceliece`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
233	`mceliece`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
110	`mceliece`
1573	`ntruees787ep1`

9.13 ia64, 997MHz, HP Itanium II, `nmi0020`



Cycles to generate a key pair			
quartile	median	quartile	system
67882454	71473492	79307646	`mceliece`
371835585	435228562	561045709	`ntruees787ep1`
367259272	535486805	860714035	`ronald1024`
1184552895	1837105551	2557087729	`ronald1536`
1638589160	2315086930	3695419300	`ronald2048`
5316170555	9174624958	15581474640	`ronald3072`
12841159650	25684510502	44166119078	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
84812	85818	87398	`mceliece`
233866	235334	239426	`ronald1024`
435687	438694	441822	`ronald1536`
642927	646586	650717	`ronald2048`
934271	936178	938380	`ntruees787ep1`
1421696	1426359	1431329	`ronald3072`
2070652	2076040	2081142	`ronald4096`

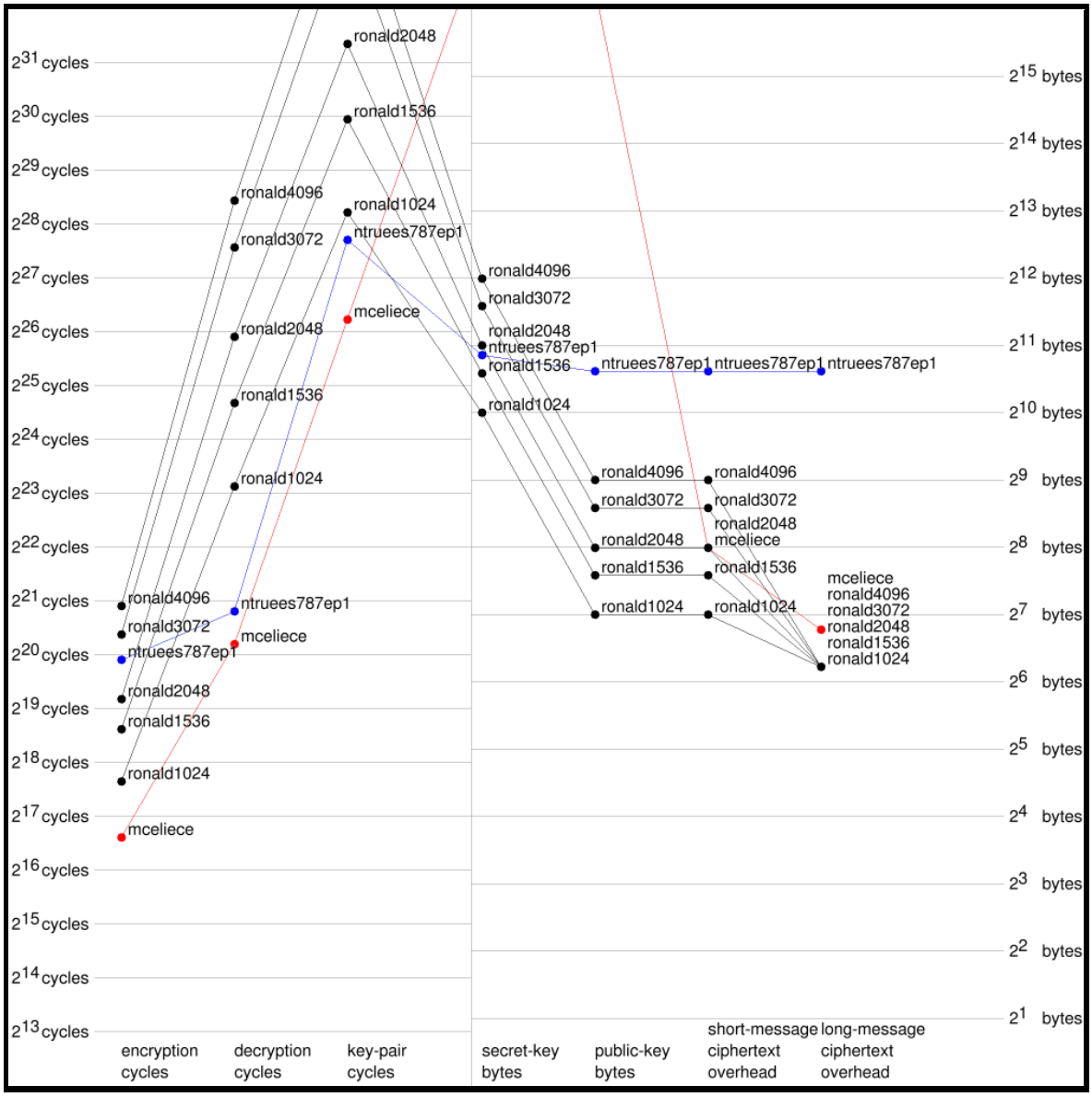
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1112963	1122318	1126151	`mceliece`
1740408	1741705	1743887	`ntruees787ep1`
9073316	9100578	9149773	`ronald1024`
26646309	27341242	78391166	`ronald1536`
54681242	54727277	54797381	`ronald2048`
182957876	183067766	183305887	`ronald3072`
366261535	366375232	366497069	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.14 ia64, 997MHz, HP Itanium II, `nmi0058`



Cycles to generate a key pair			
quartile	median	quartile	system
70926670	78968154	93627533	`mceliece`
195003698	220211858	271097732	`ntruees787ep1`
167528707	314405020	498626580	`ronald1024`
554599620	1039480413	1527589920	`ronald1536`
1609642422	2754235415	3826615515	`ronald2048`
7479107448	12669544520	17460186685	`ronald3072`
15815396360	26693638350	37739132712	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
99338	100448	102322	`mceliece`
205062	206075	211152	`ronald1024`
401241	405098	415775	`ronald1536`
594765	597658	602522	`ronald2048`
988054	988582	989011	`ntruees787ep1`
1362052	1367741	1373248	`ronald3072`
1979606	1982086	1991615	`ronald4096`

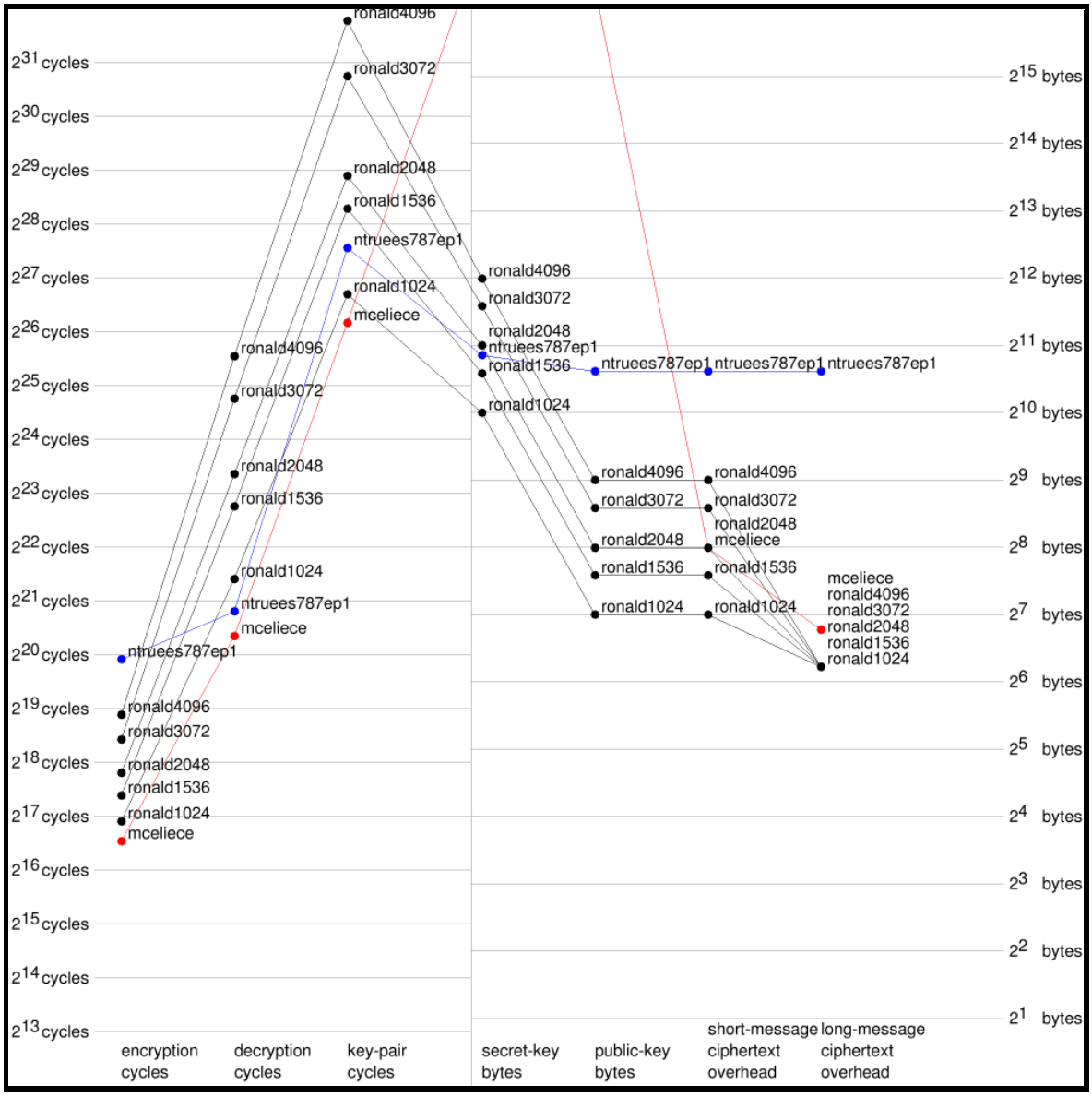
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1199323	1206499	1210468	`mceliece`
1839893	1840096	1840669	`ntruees787ep1`
9125082	9181182	9743284	`ronald1024`
26658629	26966873	30837007	`ronald1536`
54908612	63483041	93343140	`ronald2048`
184705522	199943664	256905022	`ronald3072`
365453604	366180654	371965923	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.15 ia64, 1396MHz, HP Itanium II, nmi0065



Cycles to generate a key pair			
quartile	median	quartile	system
72779100	75997986	82259524	`mceliece`
78599054	109308871	168751245	`ronald1024`
197349370	198096154	198559461	`ntruees787ep1`
161452266	328256548	494631960	`ronald1536`
291441679	503274262	847754179	`ronald2048`
1259099106	1815073858	3310795418	`ronald3072`
2018295229	3700999203	5961110496	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
94942	95851	97269	`mceliece`
123291	123581	126417	`ronald1024`
171640	172389	177461	`ronald1536`
225327	230972	231695	`ronald2048`
348905	353196	359555	`ronald3072`
484576	487532	493844	`ronald4096`
993946	995268	995759	`ntruees787ep1`

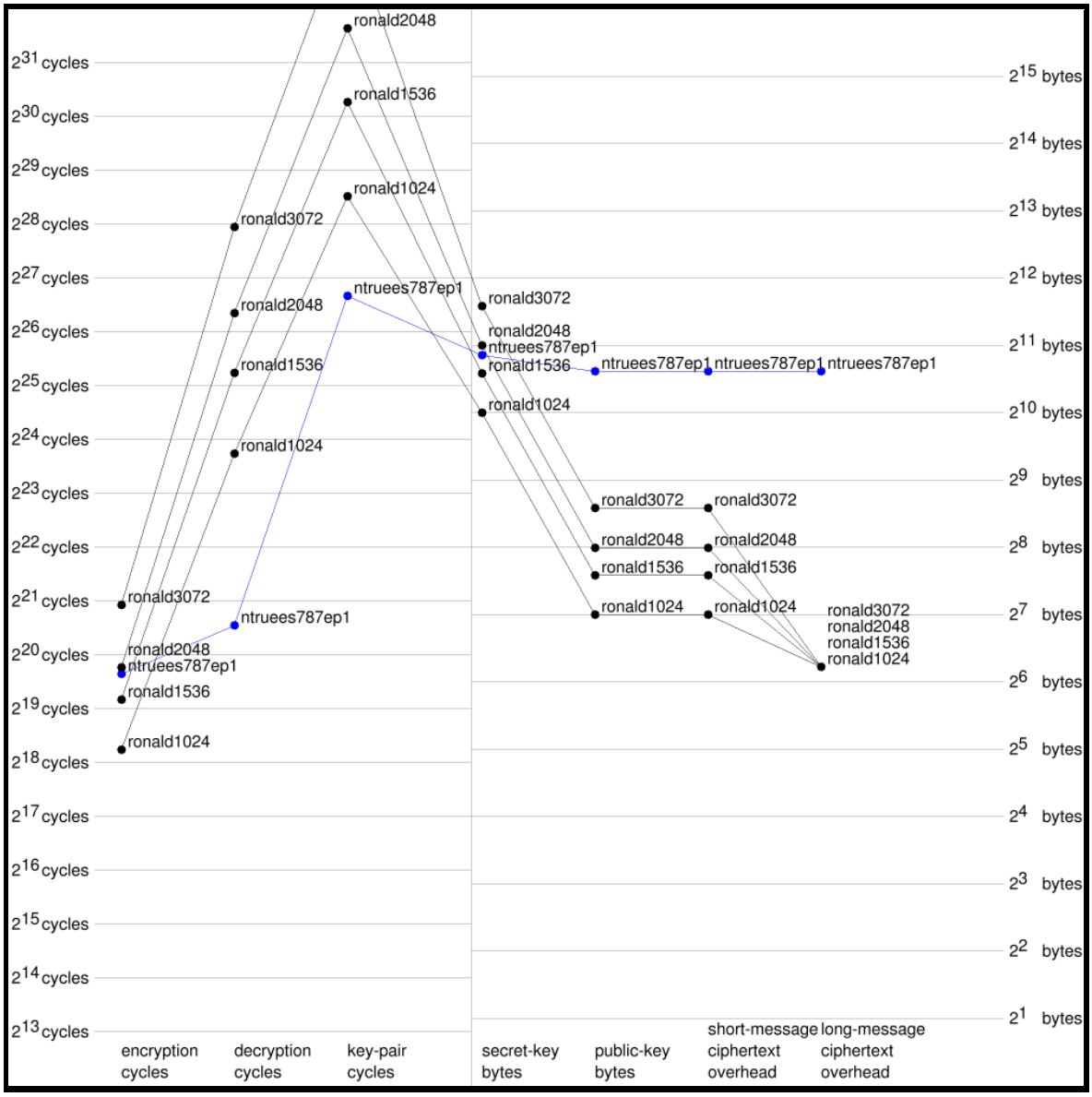
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1326593	1338990	1340745	`mceliece`
1838701	1839015	1841336	`ntruees787ep1`
2788458	2794632	2801432	`ronald1024`
7118249	7143258	7170341	`ronald1536`
10794131	10805299	10824571	`ronald2048`
28479341	28524688	28571194	`ronald3072`
49162232	49200648	49239593	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.16 ppc32, 400MHz, Motorola PowerPC G4 7400, `nmi0042`



Cycles to generate a key pair			
quartile	median	quartile	system
106554096	106986560	107268400	`ntruees787ep1`
288758176	386586352	586622272	`ronald1024`
933714672	1302447984	2373984960	`ronald1536`
2252371184	3369650400	5149027344	`ronald2048`
7683867904	13167030208	21576925488	`ronald3072`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
1574	`ntruees787ep1`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
309424	311472	313456	`ronald1024`
589504	590976	595424	`ronald1536`
824064	824288	824848	`ntruees787ep1`
893584	896080	901456	`ronald2048`
2004912	2008976	2012608	`ronald3072`

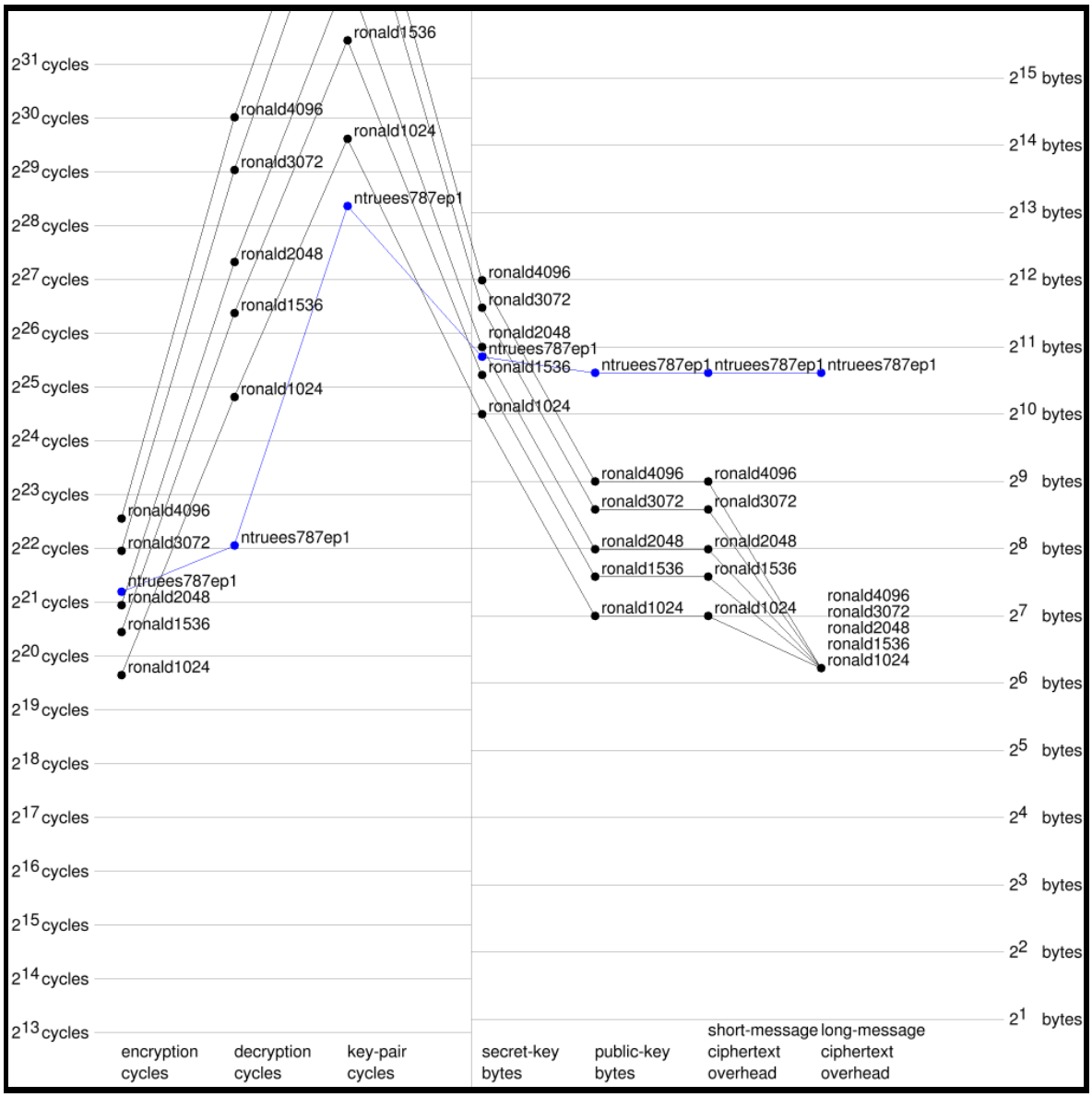
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1539840	1540272	1541248	`ntruees787ep1`
13966400	14018208	14032448	`ronald1024`
39629824	39676976	39835504	`ronald1536`
85277232	85672992	85933584	`ronald2048`
259886864	260090480	260393600	`ronald3072`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
1573	`ntruees787ep1`

9.17 ppc32, 3192MHz, IBM Cell PPE, `nmips3`



Cycles to generate a key pair			
quartile	median	quartile	system
345775080	347171440	348663720	`ntruees787ep1`
542930880	827912360	1237157080	`ronald1024`
2038584320	2938521640	4808311040	`ronald1536`
4849733720	6900750480	11096723240	`ronald2048`
21965726520	35651586480	48782196920	`ronald3072`
46083201040	69256375560	116859326080	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
820400	824480	836880	`ronald1024`
1426920	1436400	1448680	`ronald1536`
2016400	2031920	2050240	`ronald2048`
2403960	2409760	2414360	`ntruees787ep1`
4063000	4087960	4110120	`ronald3072`
6170480	6188240	6224560	`ronald4096`

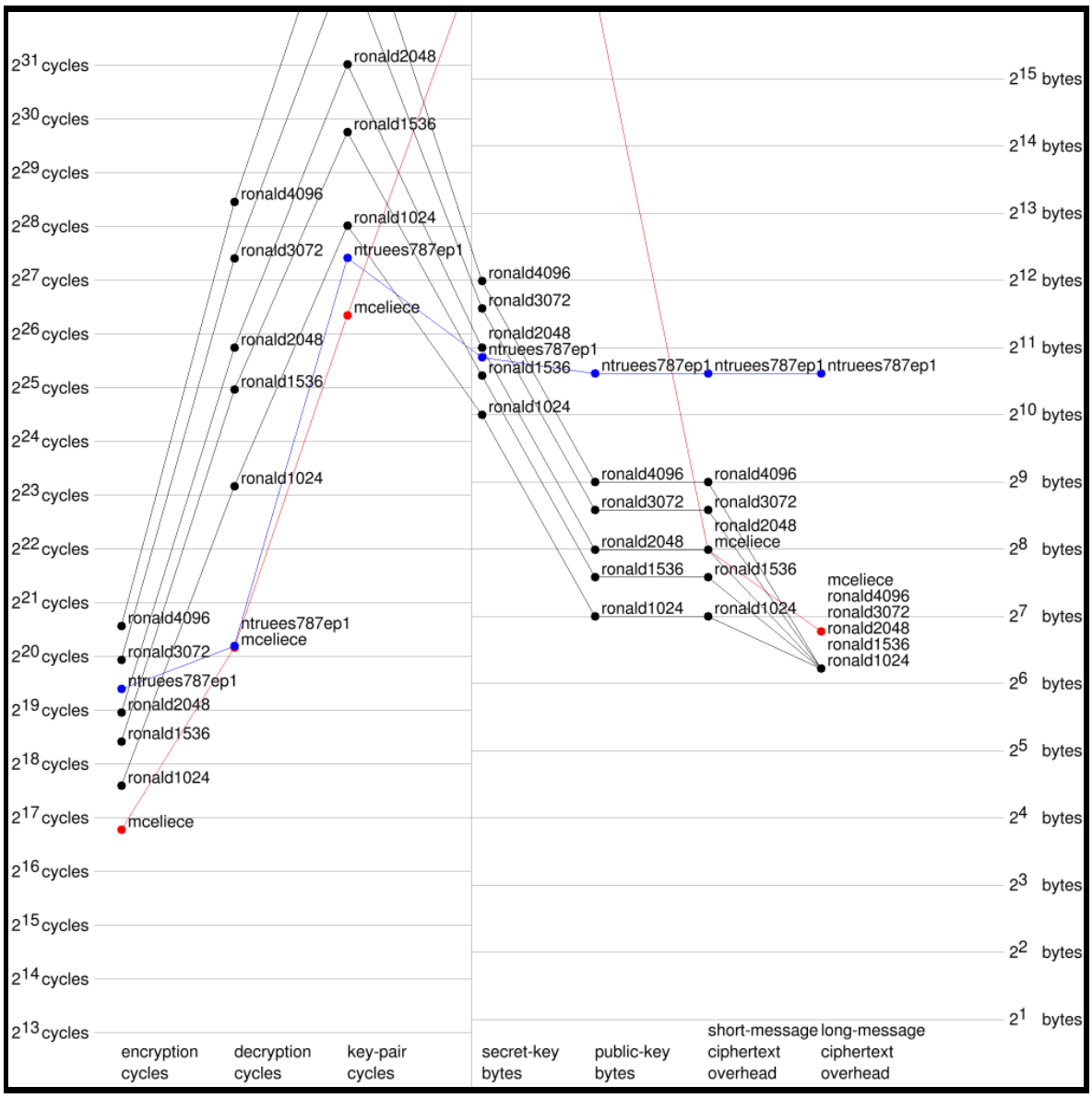
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
4379800	4382600	4391160	`ntruees787ep1`
29102360	29735560	29822400	`ronald1024`
87196560	87801840	87969000	`ronald1536`
168161600	169293840	170035440	`ronald2048`
554361680	555239640	558796360	`ronald3072`
1088270160	1091435240	1097666760	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
1573	`ntruees787ep1`

9.18 x86, 1196MHz, Intel Celeron (6b1), `vieux`



Cycles to generate a key pair			
quartile	median	quartile	system
82725252	85664124	92098464	`mceliece`
179887992	180772500	182130492	`ntruees787ep1`
178426392	272722032	410625888	`ronald1024`
595905252	911277096	1532270604	`ronald1536`
1453247448	2181264324	4058268792	`ronald2048`
5187521400	8523800868	16531117848	`ronald3072`
15546040080	27211738764	38356798560	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
111458	112884	115662	`mceliece`
198084	199068	203186	`ronald1024`
348153	351560	357576	`ronald1536`
507130	512047	516411	`ronald2048`
693476	693945	695024	`ntruees787ep1`
1006355	1010694	1020684	`ronald3072`
1557604	1565701	1576047	`ronald4096`

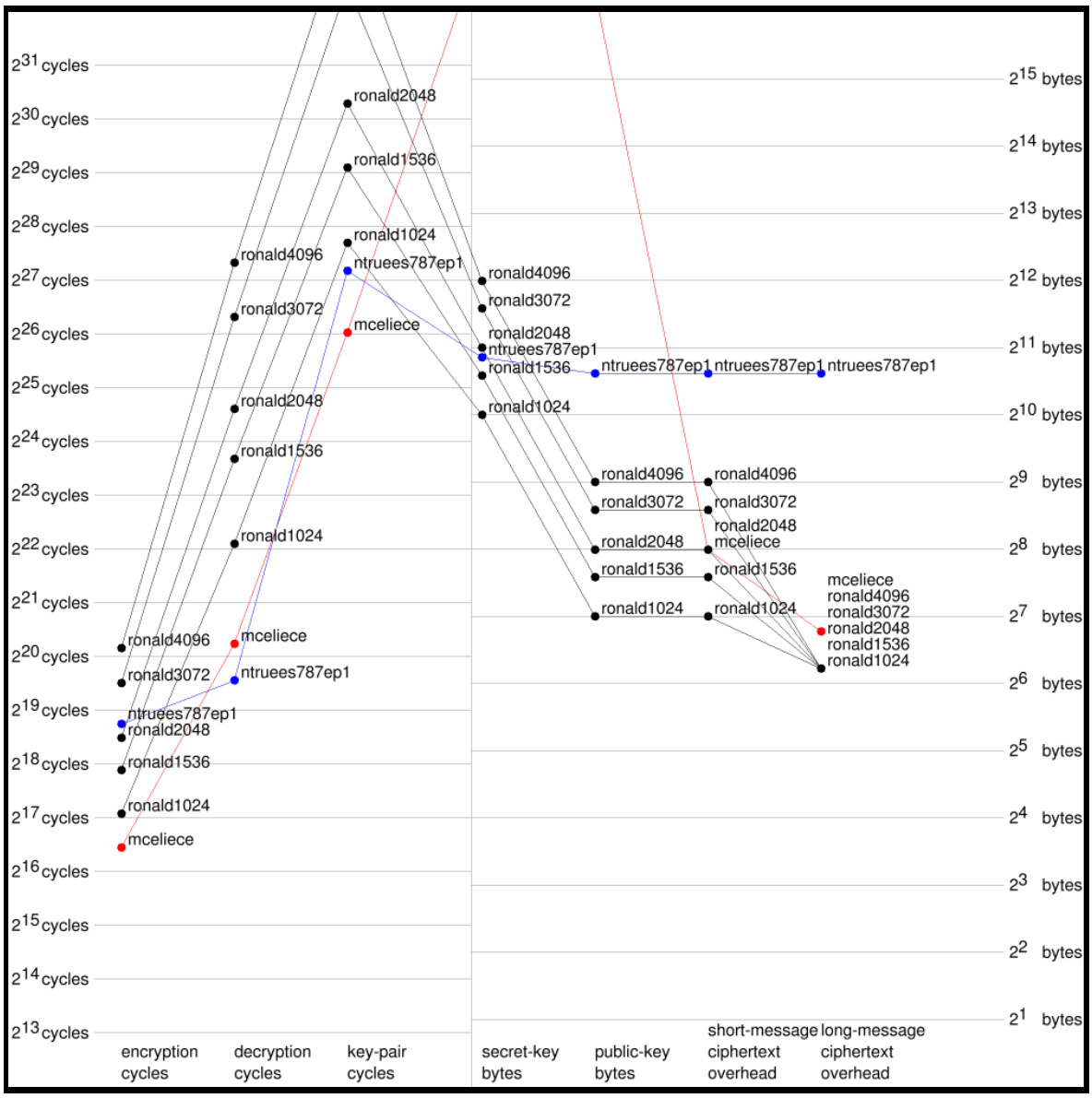
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1172505	1185977	1206295	`mceliece`
1207688	1208177	1214100	`ntruees787ep1`
9393231	9478937	16069920	`ronald1024`
26156764	32941859	33078552	`ronald1536`
56532840	56808432	63469548	`ronald2048`
178400652	178690236	179201676	`ronald3072`
363332808	369402024	370297668	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.19 x86, 1403MHz, AMD Opteron 240 (f58), `nmisles8amd64`



Cycles to generate a key pair			
quartile	median	quartile	system
64617891	68798527	75780731	`mceliece`
151958900	152642610	153041708	`ntruees787ep1`
133368366	219026974	334565050	`ronald1024`
397237812	579191105	913713752	`ronald1536`
868628506	1321185921	1956853522	`ronald2048`
3915639315	6055829981	9134924755	`ronald3072`
8519139513	14856485703	23184456356	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
89017	90141	91559	`mceliece`
137873	138776	140840	`ronald1024`
241408	244513	245559	`ronald1536`
365386	368413	371434	`ronald2048`
440955	441260	441640	`ntruees787ep1`
745452	748819	752154	`ronald3072`
1169041	1173235	1176213	`ronald4096`

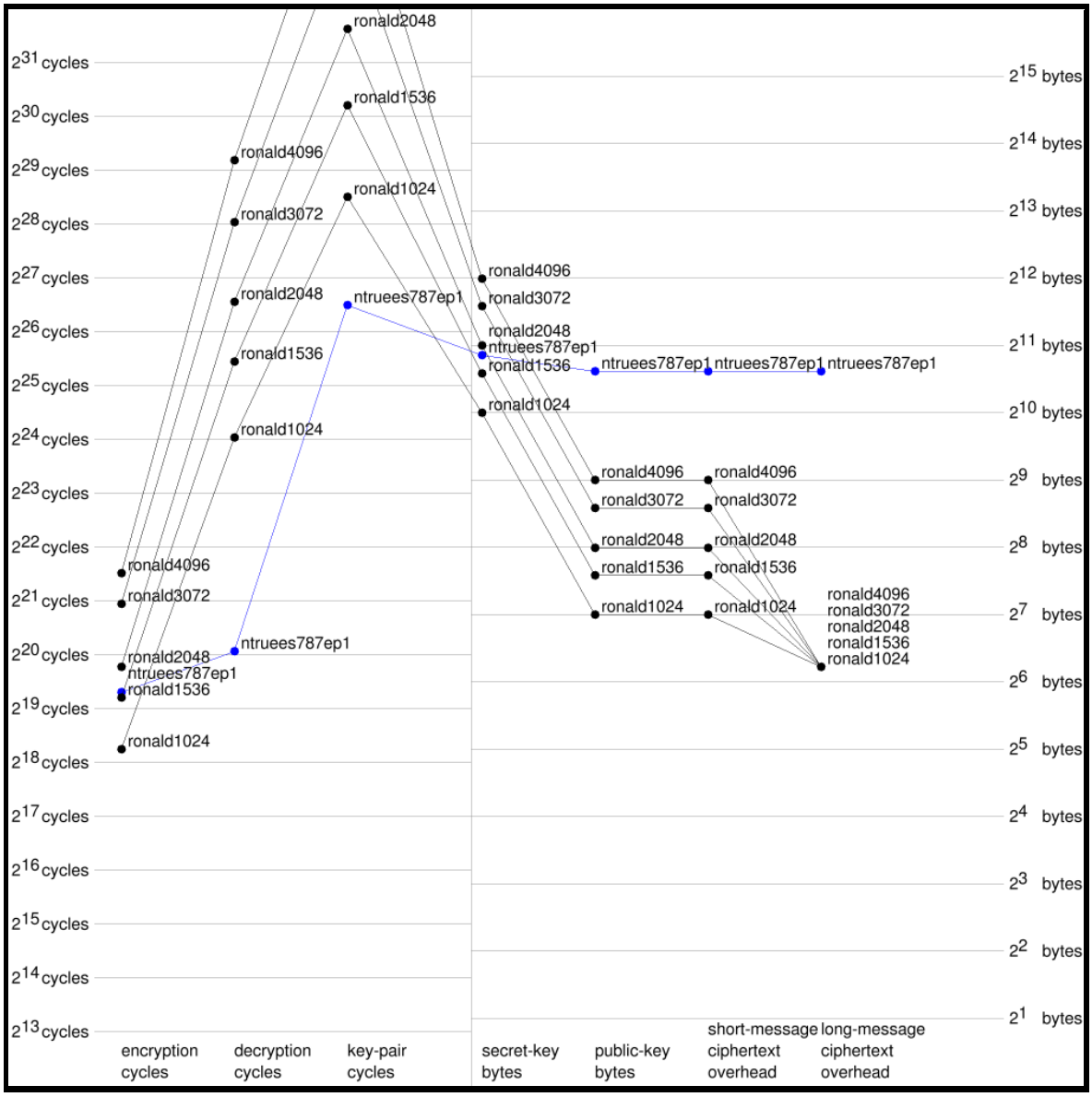
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
774529	775320	775689	`ntruees787ep1`
1241371	1245195	1253224	`mceliece`
4501544	4506999	4541197	`ronald1024`
13437724	13467095	13485500	`ronald1536`
25599309	25637343	25680874	`ronald2048`
84000100	84092603	84269010	`ronald3072`
169078032	169284220	169367008	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.20 x86, 1833MHz, Intel Core Duo, `nmi0068`



Cycles to generate a key pair			
quartile	median	quartile	system
94779047	95093449	95347802	`ntruees787ep1`
253585068	382855847	518421079	`ronald1024`
735538782	1250415881	1915255452	`ronald1536`
2118868400	3342087738	5151804405	`ronald2048`
6965847119	13049045372	19675257888	`ronald3072`
24835508445	39073634622	62227107888	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
309881	312455	317449	`ronald1024`
604285	607200	612205	`ronald1536`
644589	651035	651541	`ntruees787ep1`
904442	906422	911130	`ronald2048`
2034648	2038839	2045516	`ronald3072`
3002186	3011096	3020798	`ronald4096`

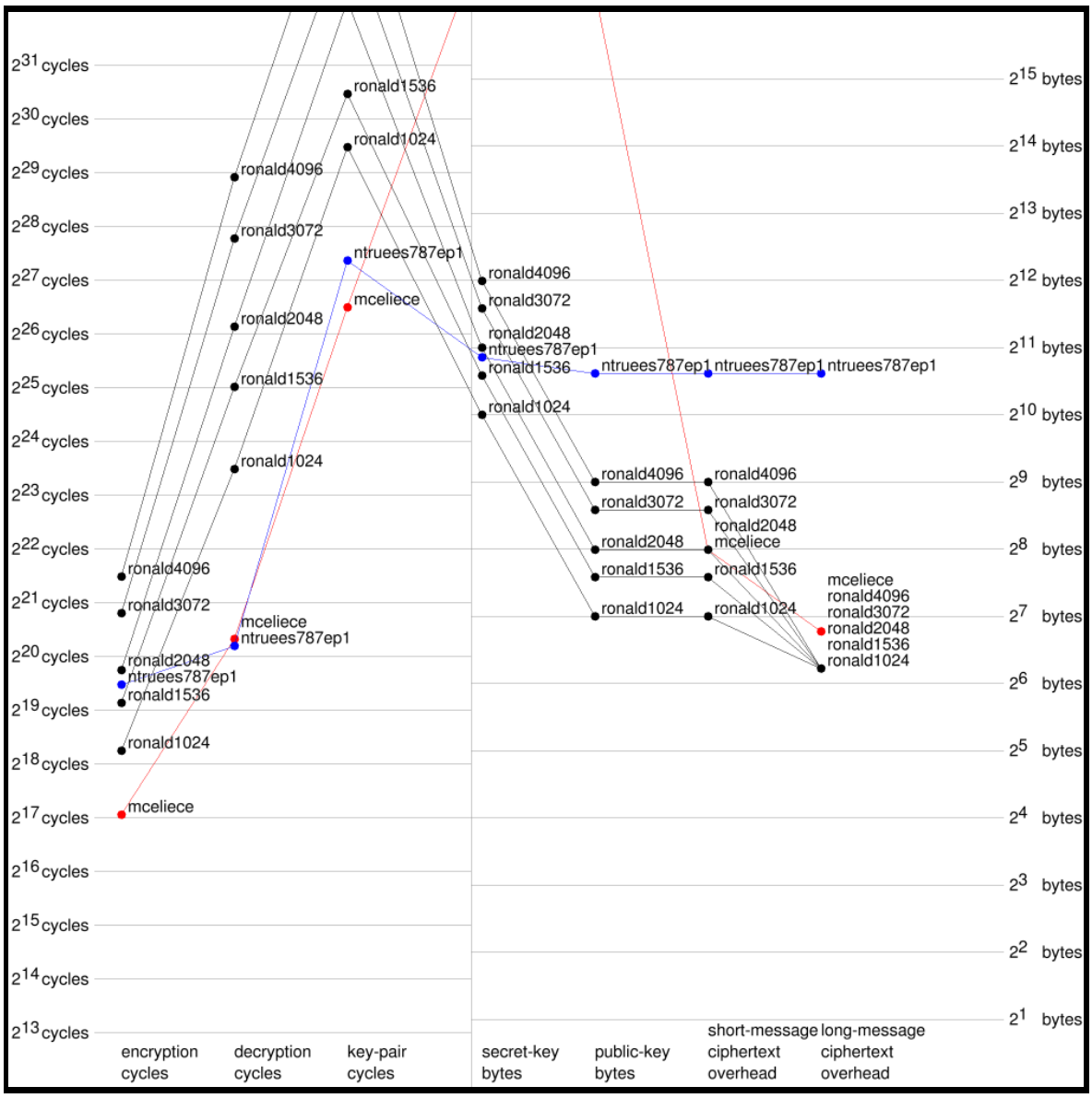
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1102442	1102497	1102937	`ntruees787ep1`
17333415	17361256	17391110	`ronald1024`
45807311	45882320	45949299	`ronald1536`
99308638	99381557	99508618	`ronald2048`
276989405	277121416	277451141	`ronald3072`
612654438	613076310	615560836	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
1573	`ntruees787ep1`

9.21 x86, 2400MHz, Intel Pentium 4 (f24), `nmitest4`



Cycles to generate a key pair			
quartile	median	quartile	system
91910108	95013072	101322432	`mceliece`
172671588	173518992	174058732	`ntruees787ep1`
421928804	752572260	1161461716	`ronald1024`
994909956	1494691084	2215731468	`ronald1536`
3046290156	4956826068	6685394308	`ronald2048`
8637026600	12848751108	22803309560	`ronald3072`
20598342876	36953850976	59465596176	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
134312	137124	139036	`mceliece`
308832	312272	314632	`ronald1024`
574176	577724	582948	`ronald1536`
728404	731284	733824	`ntruees787ep1`
876696	882832	890436	`ronald2048`
1842148	1850580	1863036	`ronald3072`
2940000	2953080	2982108	`ronald4096`

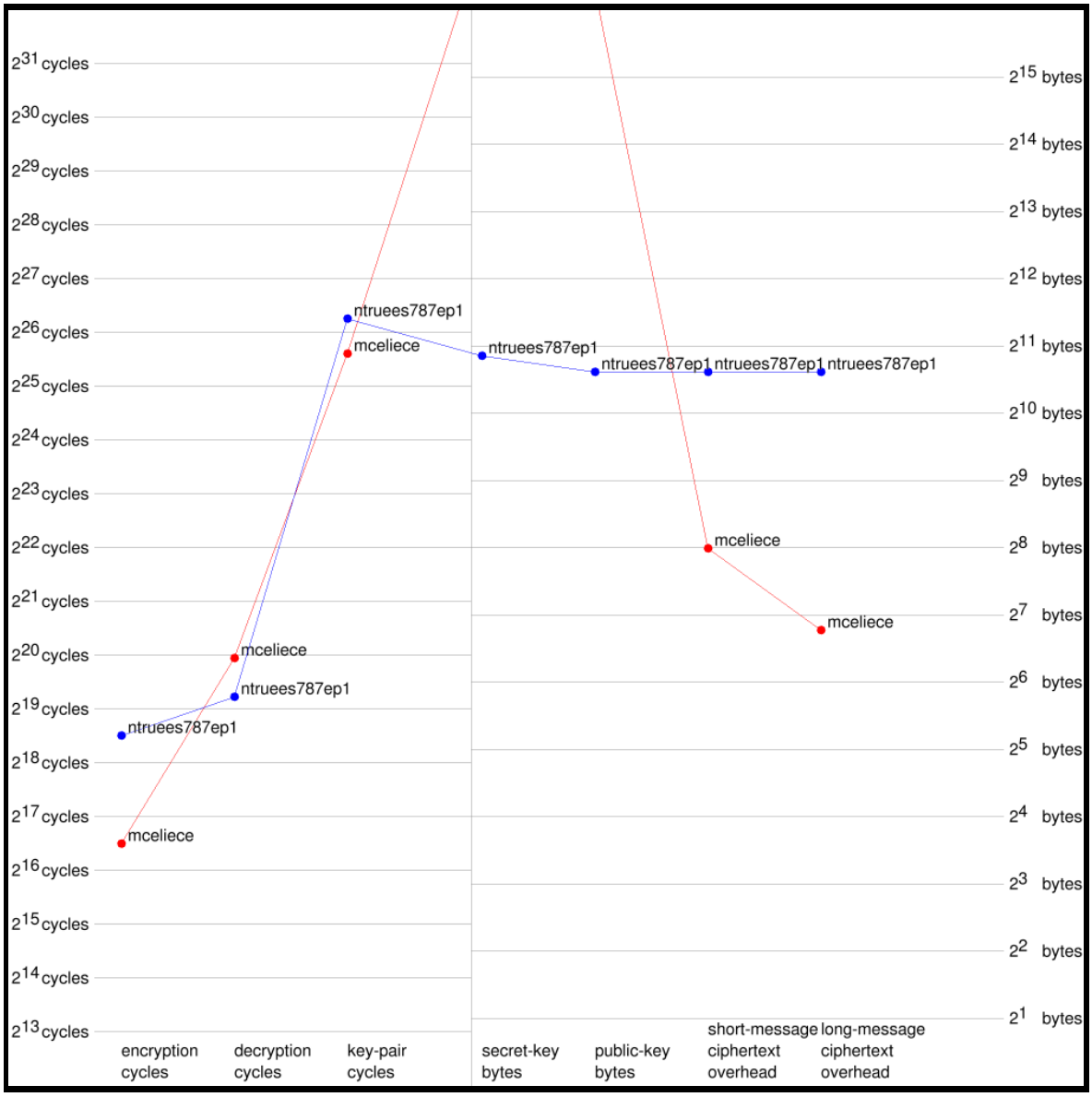
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1208600	1211772	1217972	`ntruees787ep1`
1311980	1319728	1332440	`mceliece`
11783736	11857516	11905084	`ronald1024`
33678864	34109124	34459776	`ronald1536`
74277316	74446412	74656500	`ronald2048`
230356896	231237804	232107344	`ronald3072`
508012296	508389136	509207356	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.22 x86, 2400MHz, Intel Core 2 Duo (6fb), utrecht



Cycles to generate a key pair			
quartile	median	quartile	system
49420287	51407640	54420912	`mceliece`
80201601	80546103	80776692	`ntruees787ep1`

Secret key	
bytes	system
1854	`ntruees787ep1`
137282	`mceliece`

Public key	
bytes	system
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
92016	93240	94284	`mceliece`
373500	373887	374229	`ntruees787ep1`

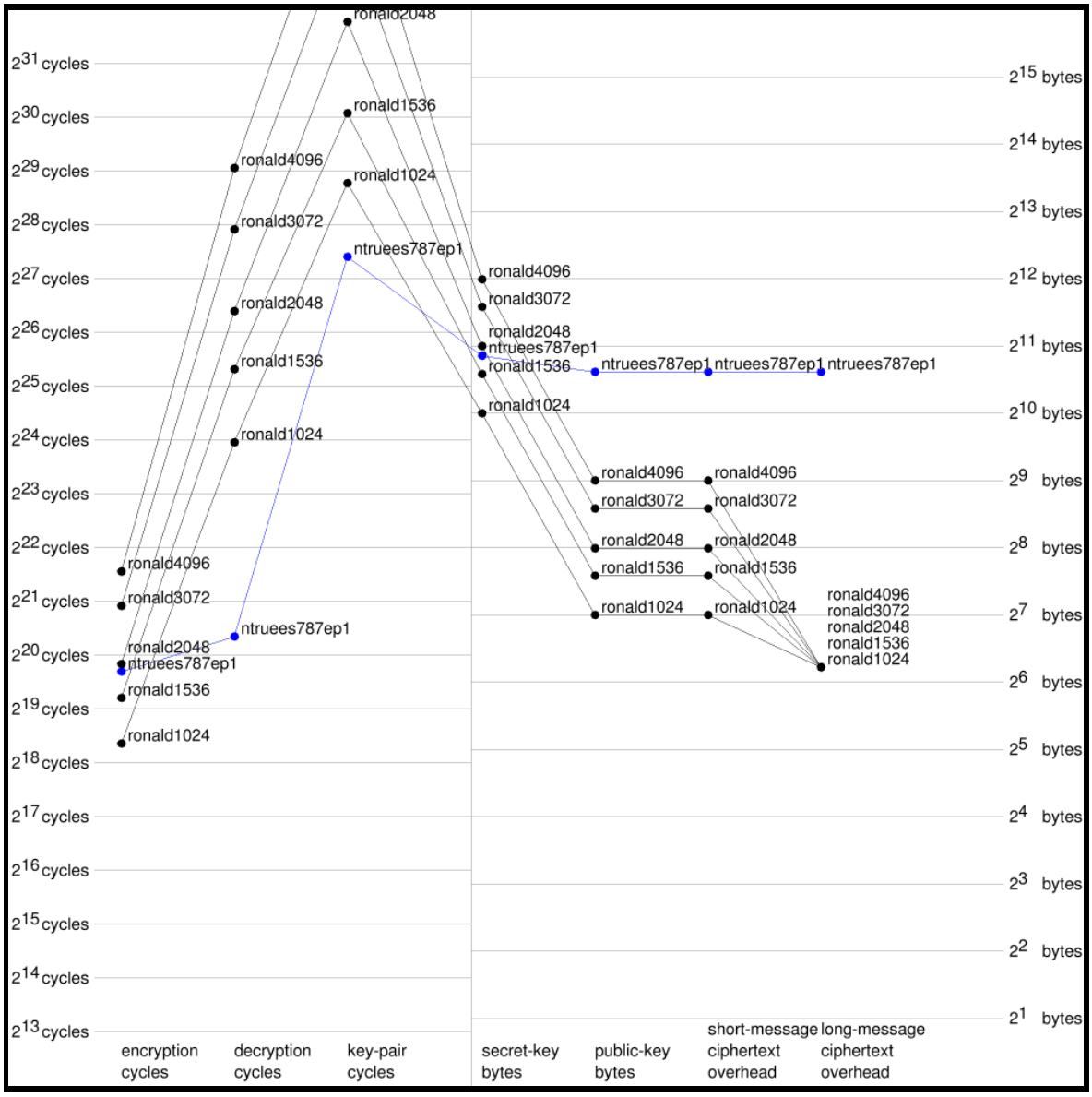
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
615744	617004	617967	`ntruees787ep1`
1003428	1015128	1017972	`mceliece`

Encrypting 0 bytes	
bytes	system
256	`mceliece`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
233	`mceliece`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
110	`mceliece`
1573	`ntruees787ep1`

9.23 x86, 2401MHz, Intel Pentium 4 (f24), nmi0086



Cycles to generate a key pair			
quartile	median	quartile	system
178124312	179001400	179515392	`ntruees787ep1`
315374036	463959424	637018084	`ronald1024`
694964916	1138521060	1732933528	`ronald1536`
2253397148	3695793912	5786590464	`ronald2048`
6717804264	12252068856	18089867572	`ronald3072`
15866148636	35401089672	57691536284	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
335732	337988	343164	`ronald1024`
601064	608012	614040	`ronald1536`
848468	852820	861272	`ntruees787ep1`
936372	943740	954636	`ronald2048`
1992328	1997404	2003628	`ronald3072`
3092796	3101232	3109604	`ronald4096`

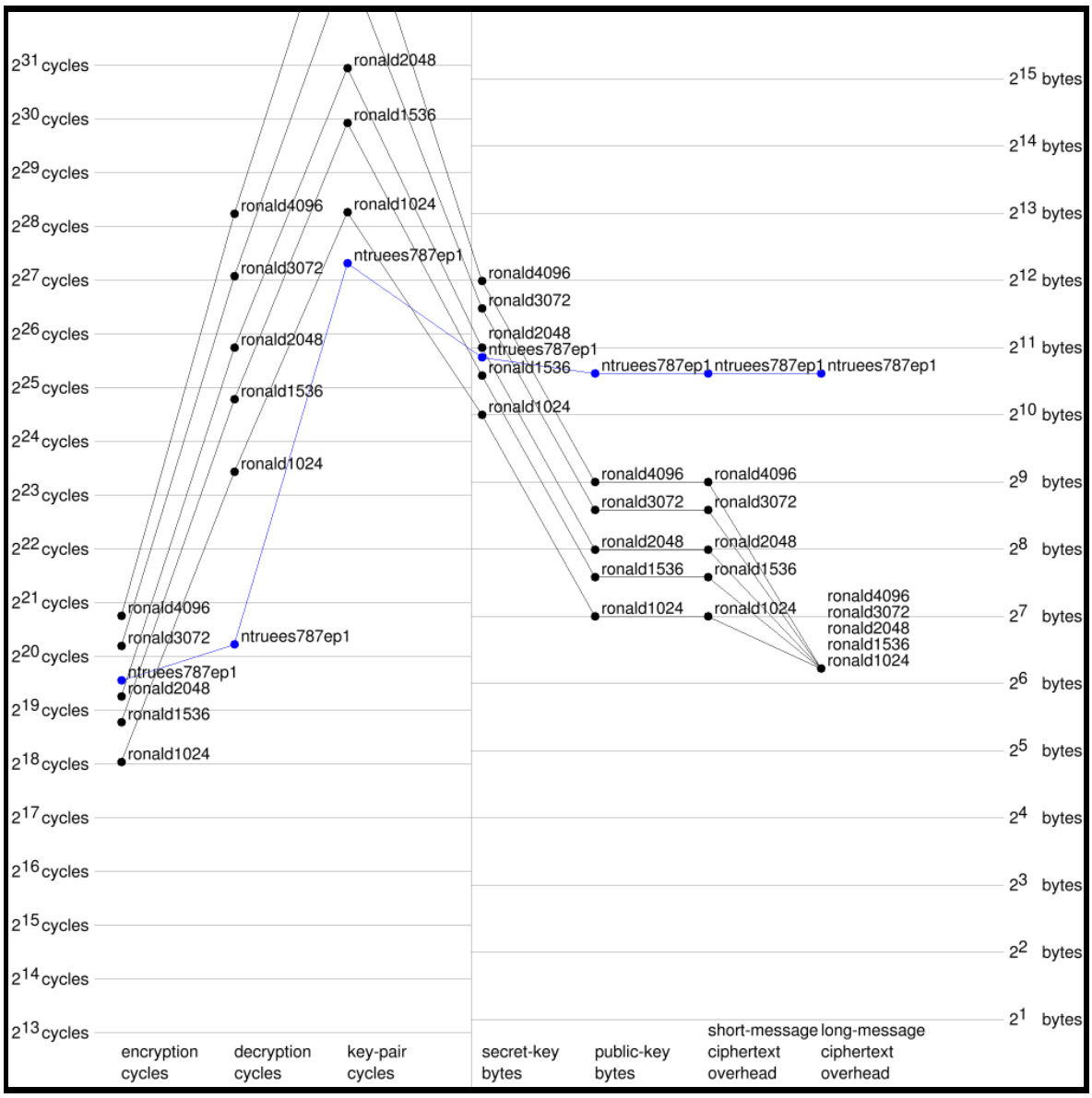
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1334408	1340912	1366092	`ntruees787ep1`
16169140	16324840	17274044	`ronald1024`
41949304	42152400	42370888	`ronald1536`
88861744	89137928	89554028	`ronald2048`
253841520	254837464	255867708	`ronald3072`
560797188	561858244	563614284	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
1573	`ntruees787ep1`

9.24 x86, 2658MHz, Intel Xeon (f25), `nmi0013`



Cycles to generate a key pair			
quartile	median	quartile	system
167173376	167910244	168800416	`ntruees787ep1`
223037648	325816860	530645516	`ronald1024`
630900224	1027507500	1602432444	`ronald1536`
1251687784	2080350836	3667845740	`ronald2048`
4738786500	8253235640	12744485060	`ronald3072`
17345728200	29385742800	43242533440	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
269148	270676	274228	`ronald1024`
450008	453252	458136	`ronald1536`
625048	630948	635828	`ronald2048`
774348	776920	778448	`ntruees787ep1`
1194820	1209908	1220132	`ronald3072`
1780700	1785708	1795792	`ronald4096`

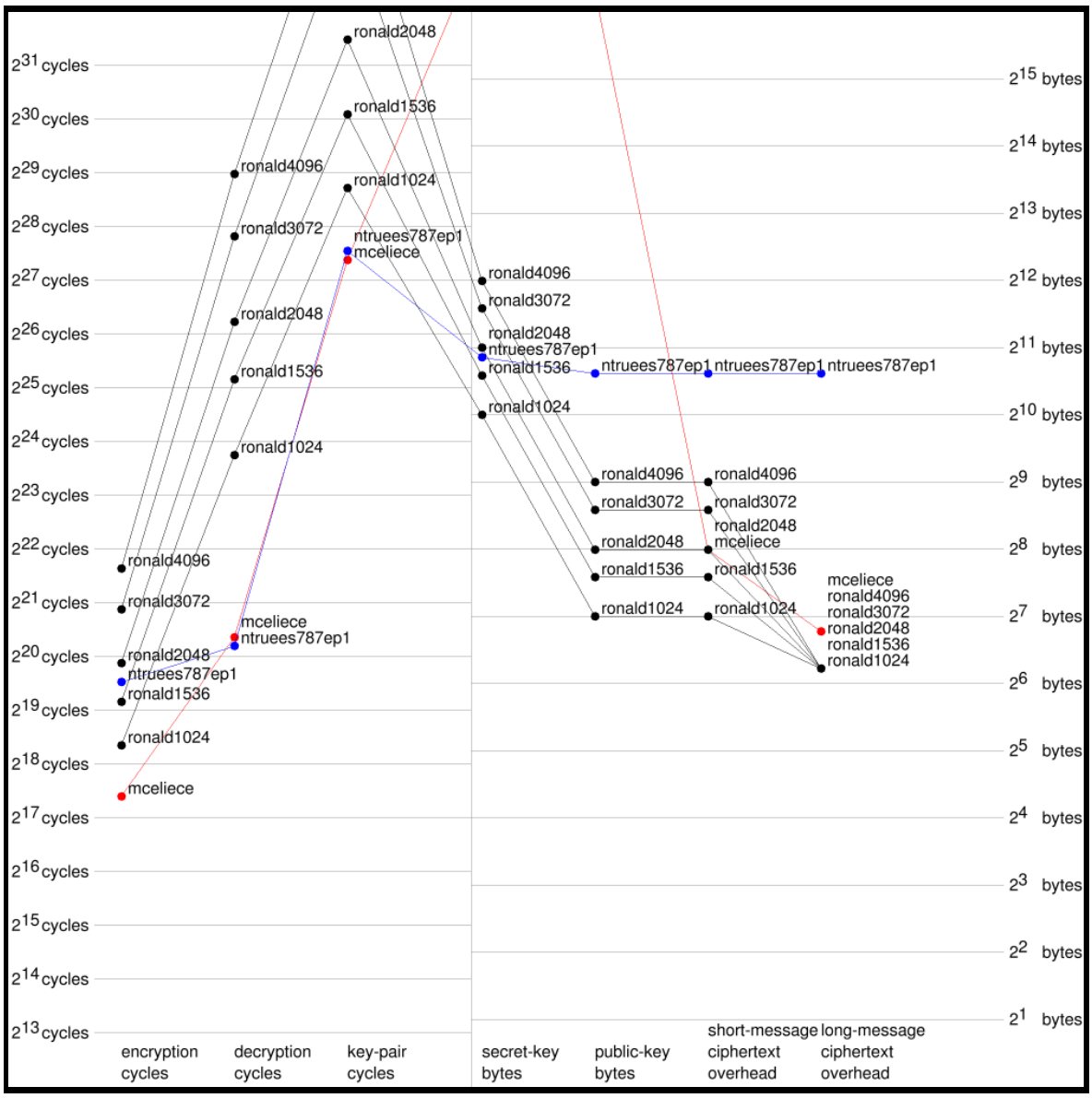
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1230504	1232312	1237156	`ntruees787ep1`
11366800	11423572	11473272	`ronald1024`
28318032	29097520	30362212	`ronald1536`
56469804	56628652	56798376	`ronald2048`
141059076	142267144	144173060	`ronald3072`
317280768	317897452	319125984	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
1573	`ntruees787ep1`

9.25 x86, 2658MHz, Intel Xeon (f25), `nmibuild15`



Cycles to generate a key pair			
quartile	median	quartile	system
171656260	175310008	180902520	`mceliece`
196923768	197717040	198316732	`ntruees787ep1`
240778576	443908616	632133536	`ronald1024`
764136552	1148414312	2016831524	`ronald1536`
1727117836	2997920824	4608528996	`ronald2048`
7810368364	14184227260	21131642060	`ronald3072`
24879861260	40191301116	58619001100	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
170516	172972	176780	`mceliece`
331656	335028	340652	`ronald1024`
584684	587104	593044	`ronald1536`
757624	760052	765776	`ntruees787ep1`
962404	967200	970684	`ronald2048`
1932380	1939244	1945084	`ronald3072`
3281316	3286800	3294108	`ronald4096`

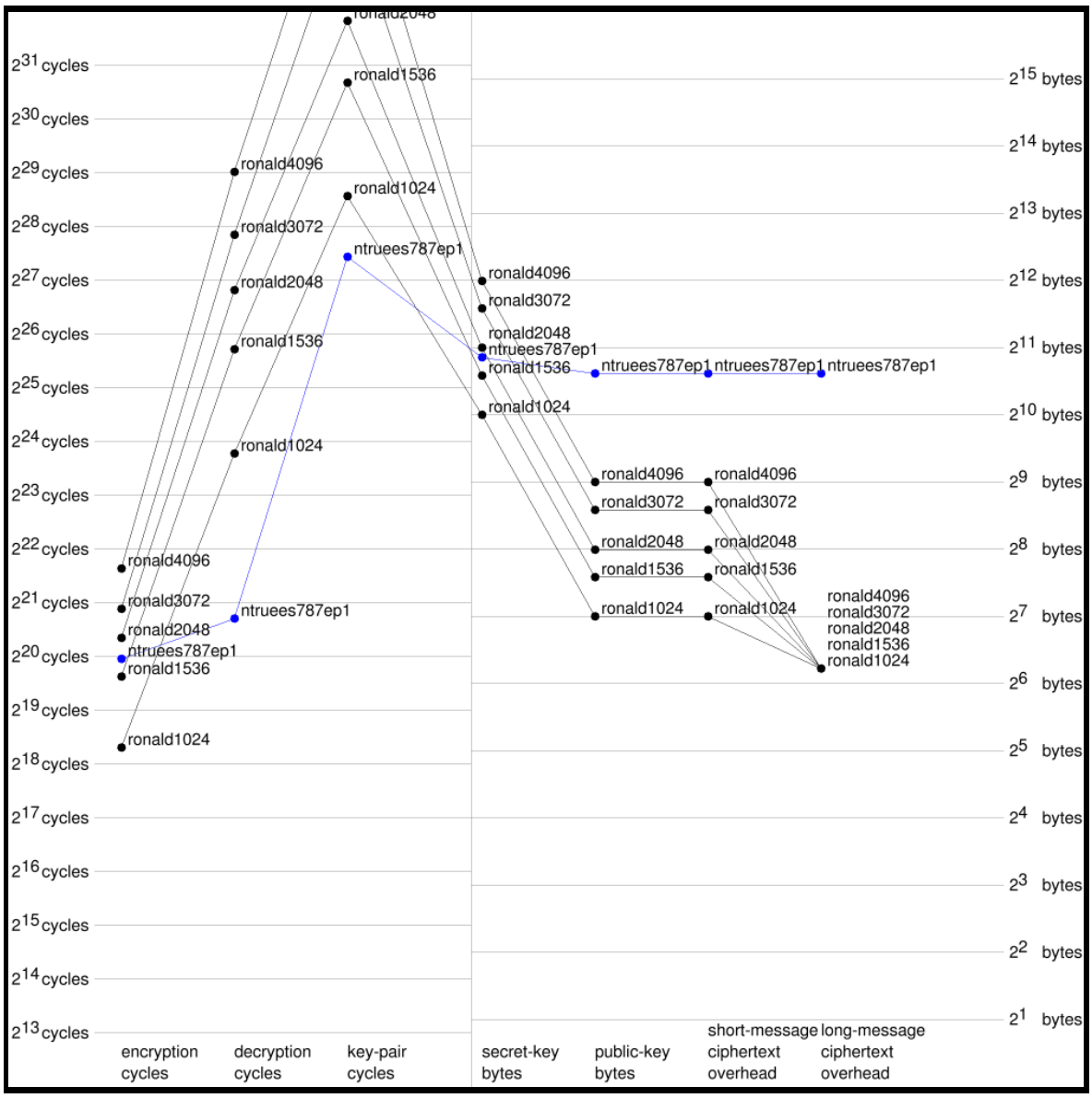
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1203824	1207584	1212568	`ntruees787ep1`
1337160	1346256	1358456	`mceliece`
14153668	14194940	14265676	`ronald1024`
37322696	37497712	37875784	`ronald1536`
78377272	78778288	80513272	`ronald2048`
236009400	237125560	237774300	`ronald3072`
531049152	532631396	535251612	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.26 x86, 2658MHz, Intel Xeon (f25), `nmibuild16`



Cycles to generate a key pair			
quartile	median	quartile	system
180937524	182408284	232359308	`ntruees787ep1`
276777428	401083648	620578252	`ronald1024`
971571192	1730112788	2513513844	`ronald1536`
2244265488	3835827884	6071094312	`ronald2048`
9989479326	16427339502	23347848940	`ronald3072`
27562737296	44645425314	72622559316	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
321324	326556	328920	`ronald1024`
577036	816812	822828	`ronald1536`
1016752	1020336	1274872	`ntruees787ep1`
949028	1337380	1344344	`ronald2048`
1941808	1955700	2786592	`ronald3072`
3267128	3278604	4719940	`ronald4096`

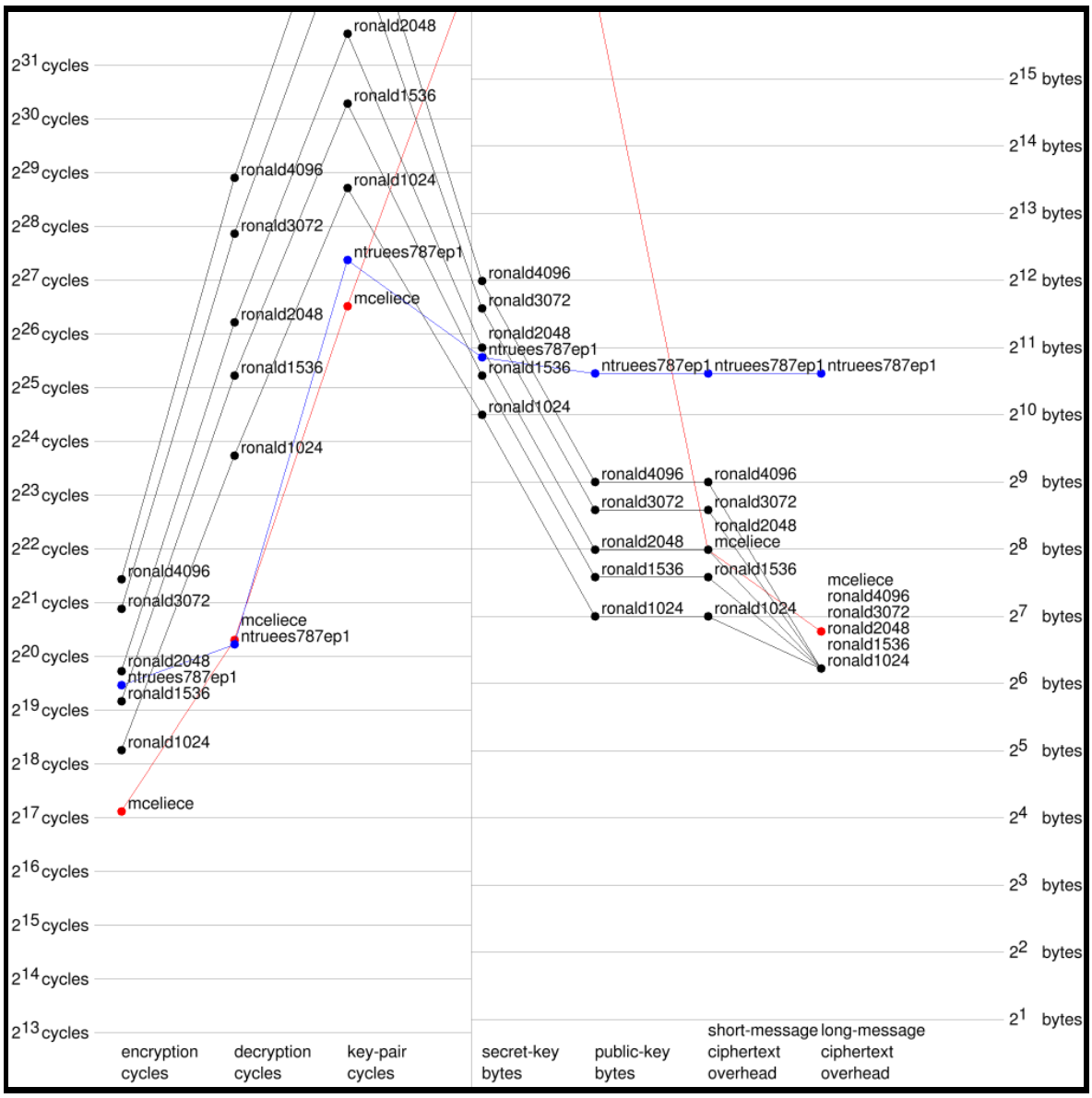
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1712536	1716256	2162564	`ntruees787ep1`
14442828	14502468	14583392	`ronald1024`
39244720	55399648	55904736	`ronald1536`
82316252	119198668	119978308	`ronald2048`
242294416	243509484	244390240	`ronald3072`
542911872	544701520	546507364	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
1573	`ntruees787ep1`

9.27 x86, 2658MHz, Intel Xeon (f25), `nmibuild22`



Cycles to generate a key pair			
quartile	median	quartile	system
92722580	96787540	104156700	`mceliece`
174144232	174991364	175532636	`ntruees787ep1`
292475252	443358520	689923000	`ronald1024`
799352060	1316372976	1948434736	`ronald1536`
2223894588	3247523776	5180761092	`ronald2048`
7170522300	13427014304	17914041580	`ronald3072`
22402827980	34709391180	51387614800	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
140244	143164	150948	`mceliece`
312356	314364	319272	`ronald1024`
587460	591576	598024	`ronald1536`
726616	728172	731380	`ntruees787ep1`
866616	873740	882204	`ronald2048`
1937156	1944844	1953620	`ronald3072`
2846436	2853540	2865240	`ronald4096`

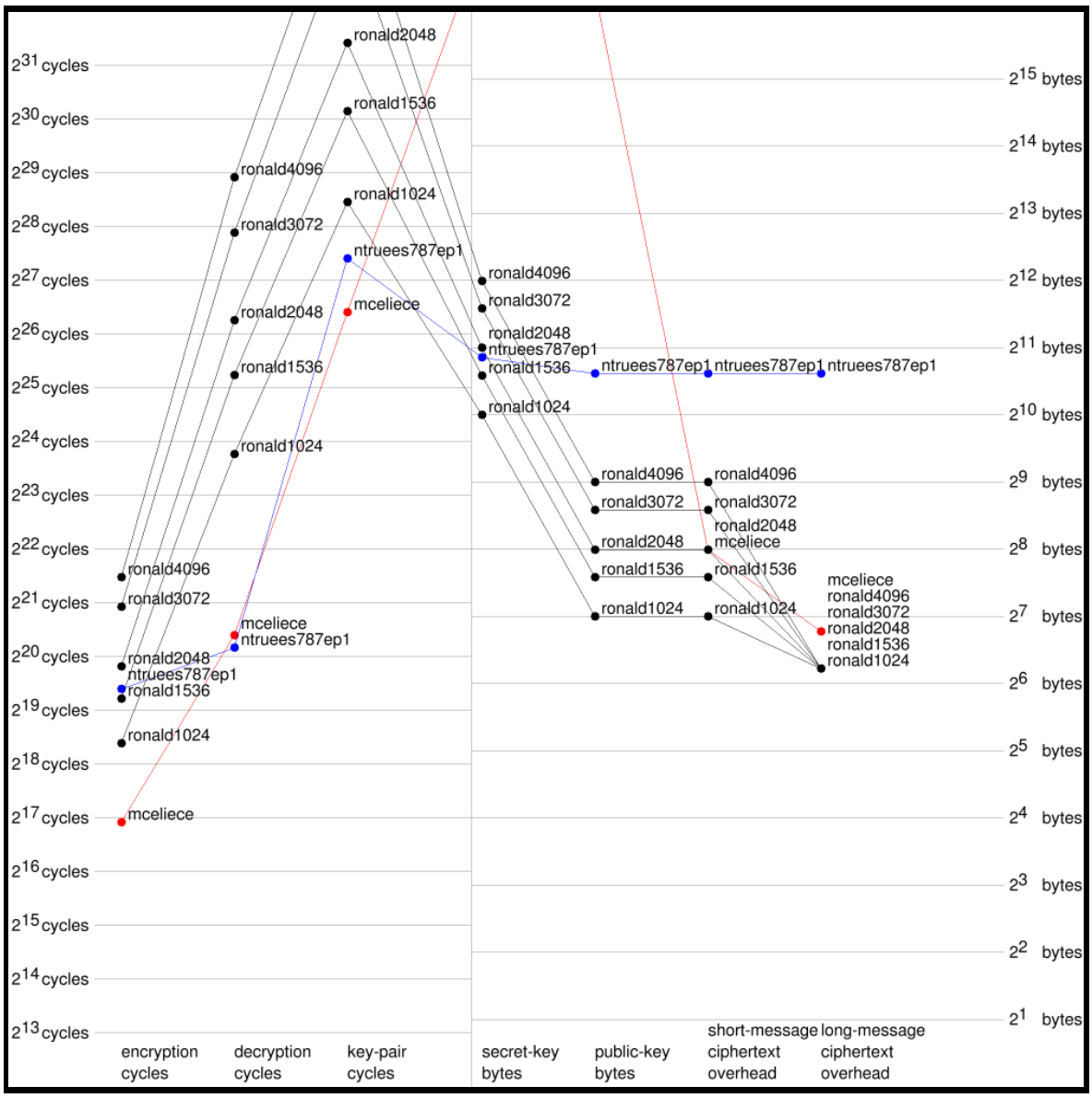
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1232732	1234076	1237184	`ntruees787ep1`
1289760	1308008	1337400	`mceliece`
13977860	14052416	14259720	`ronald1024`
39145956	39407168	39710368	`ronald1536`
78371272	78535052	78797496	`ronald2048`
244435512	245323564	246303380	`ronald3072`
503482096	505020792	505950956	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.28 x86, 2659MHz, Intel Xeon (f25), `nmibuild21`



Cycles to generate a key pair			
quartile	median	quartile	system
86400600	89338652	93838620	mceliece
177746056	178514484	178968216	ntruees787ep1
262274780	370170844	572305352	ronald1024
873876244	1196383328	1762092116	ronald1536
1779466536	2891327820	5090098620	ronald2048
7891041022	13113703544	21246724142	ronald3072
19290987340	31740342996	48930800620	ronald4096

Secret key	
bytes	system
1024	ronald1024
1536	ronald1536
1854	ntruees787ep1
2048	ronald2048
3072	ronald3072
4096	ronald4096
137282	mceliece

Public key	
bytes	system
128	ronald1024
192	ronald1536
256	ronald2048
384	ronald3072
512	ronald4096
1574	ntruees787ep1
81408	mceliece

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
121240	124400	127096	mceliece
340152	345120	350016	ronald1024
607428	613076	620988	ronald1536
687000	692304	702596	ntruees787ep1
921360	927228	934376	ronald2048
1992988	2004700	2019864	ronald3072
2922224	2933724	2951096	ronald4096

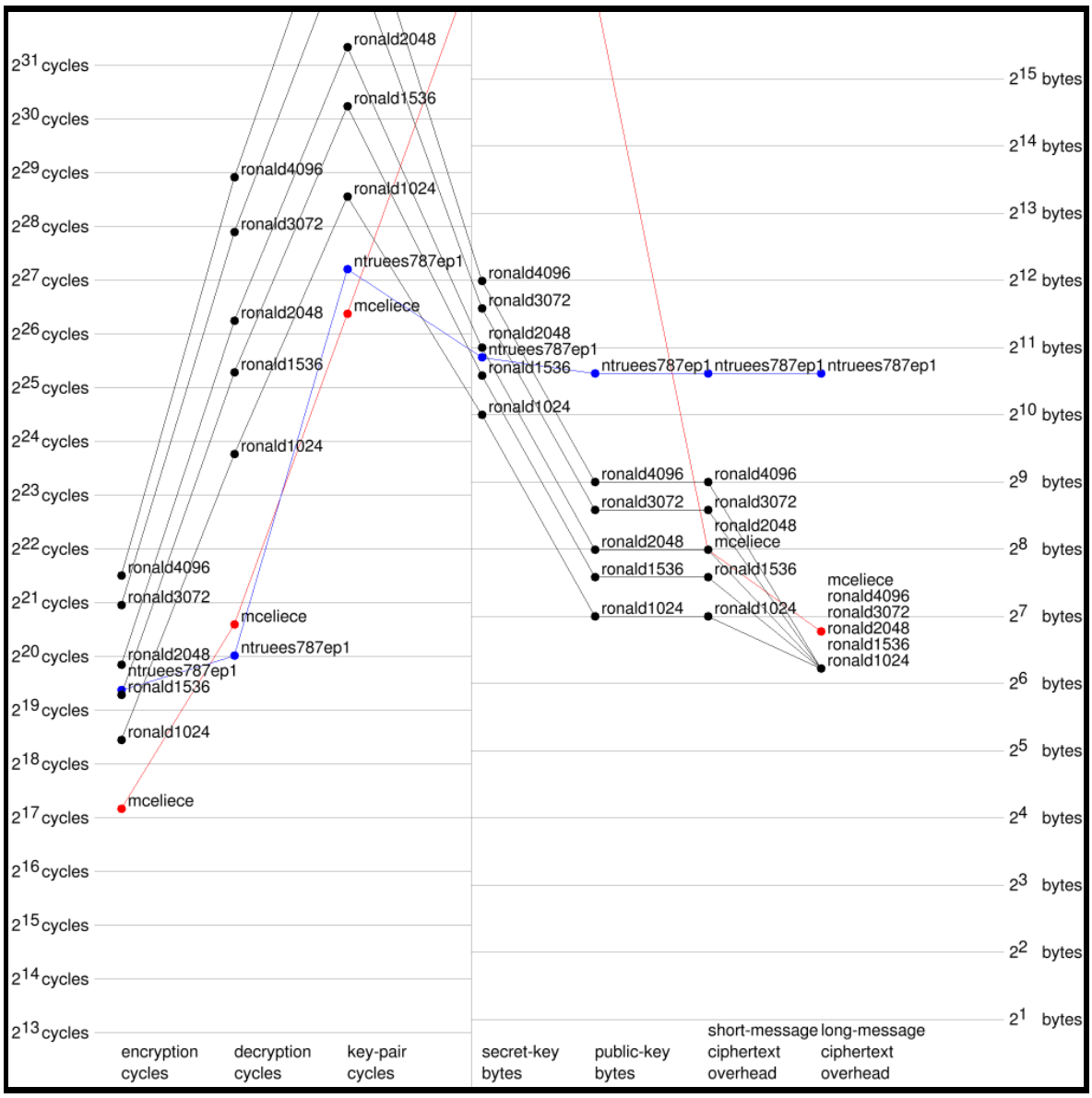
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1179380	1186208	1196728	ntruees787ep1
1360576	1384244	1394688	mceliece
14250940	14326020	14628672	ronald1024
39467500	39773260	40387388	ronald1536
80059644	80528020	81124756	ronald2048
248164836	249542088	250667296	ronald3072
506784724	507958240	509369352	ronald4096

Encrypting 0 bytes	
bytes	system
128	ronald1024
192	ronald1536
256	mceliece
256	ronald2048
384	ronald3072
512	ronald4096
1574	ntruees787ep1

Encrypting 23 bytes	
bytes	system
105	ronald1024
169	ronald1536
233	mceliece
233	ronald2048
361	ronald3072
489	ronald4096
1551	ntruees787ep1

Encrypting many bytes	
bytes	system
75	ronald1024
75	ronald1536
75	ronald2048
75	ronald3072
75	ronald4096
110	mceliece
1573	ntruees787ep1

9.29 x86, 2659MHz, Intel Xeon (f25), `nmibuild26`



Cycles to generate a key pair			
quartile	median	quartile	system
83864480	87647660	94006760	`mceliece`
155620516	156290668	156837924	`ntruees787ep1`
241591172	397594164	514615140	`ronald1024`
845367708	1275693764	2195545780	`ronald1536`
1491040220	2719735780	4119601560	`ronald2048`
7801936364	11231612540	15889169908	`ronald3072`
18656758586	32711076508	51303266620	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
146652	148324	150468	`mceliece`
357356	359692	365740	`ronald1024`
634800	642612	649128	`ronald1536`
682468	685788	692528	`ntruees787ep1`
941016	948288	957104	`ronald2048`
2032444	2044348	2987856	`ronald3072`
2986064	2996888	3013544	`ronald4096`

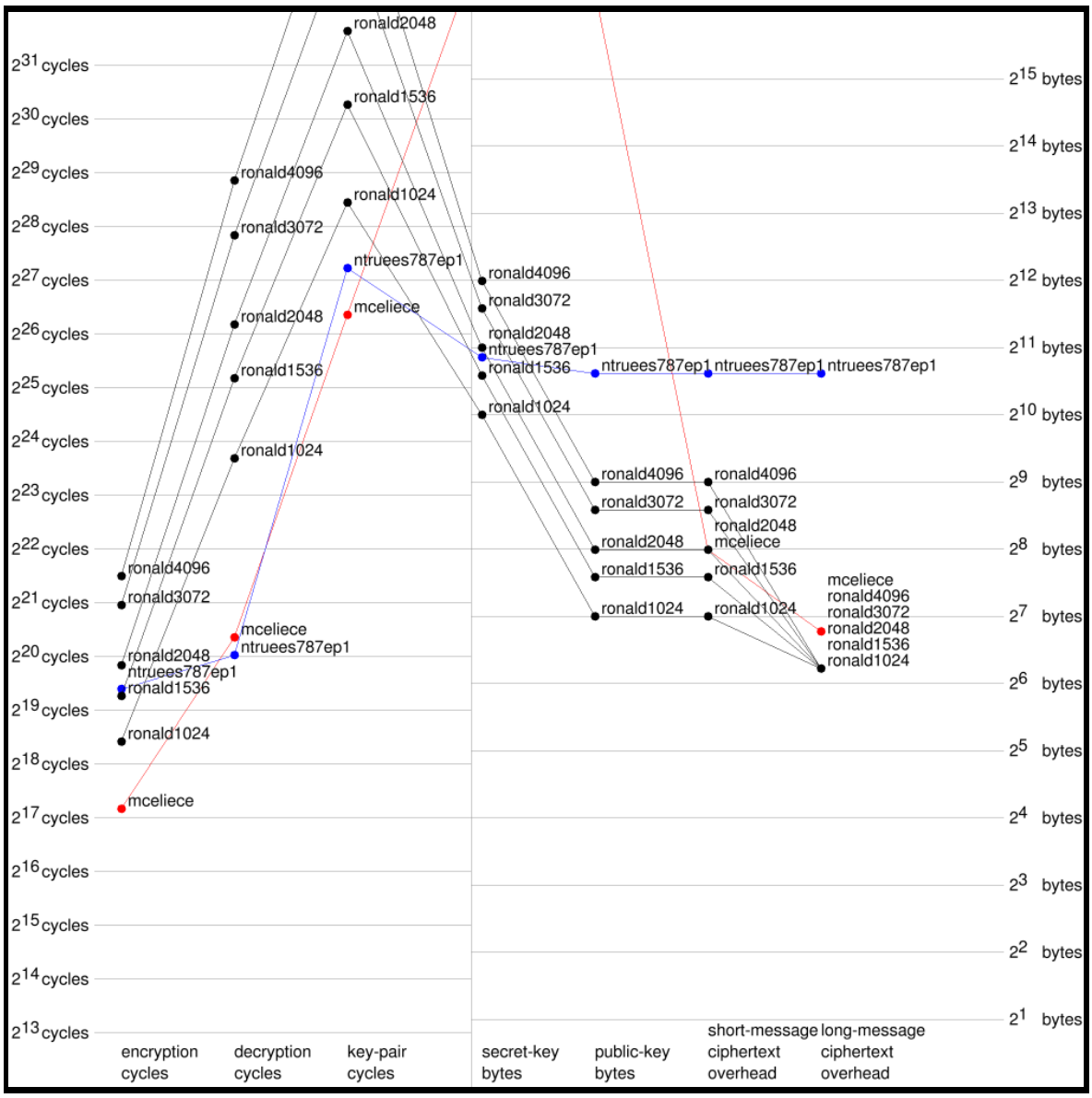
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1059172	1067564	1072232	`ntruees787ep1`
1547992	1594764	1662008	`mceliece`
14301752	14387676	14491236	`ronald1024`
40789404	41115784	41525108	`ronald1536`
80107824	80286960	80507020	`ronald2048`
250484912	251976192	253426516	`ronald3072`
510340184	511199656	512099052	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.30 x86, 2667MHz, Intel Xeon (f25), `nmi0036`



Cycles to generate a key pair			
quartile	median	quartile	system
83451680	86201120	93062900	`mceliece`
156467724	157555836	158540292	`ntruees787ep1`
261353548	367366348	549805512	`ronald1024`
641798100	1299561732	2200161496	`ronald1536`
1832234896	3346551598	5067629082	`ronald2048`
8071442420	12832566556	20366876698	`ronald3072`
21163945602	35411034040	52628092720	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
145388	147568	149440	`mceliece`
349992	352260	357916	`ronald1024`
629164	633640	641664	`ronald1536`
689212	692892	712712	`ntruees787ep1`
934436	944476	956420	`ronald2048`
2029724	2051988	2071416	`ronald3072`
2974944	2983976	2995176	`ronald4096`

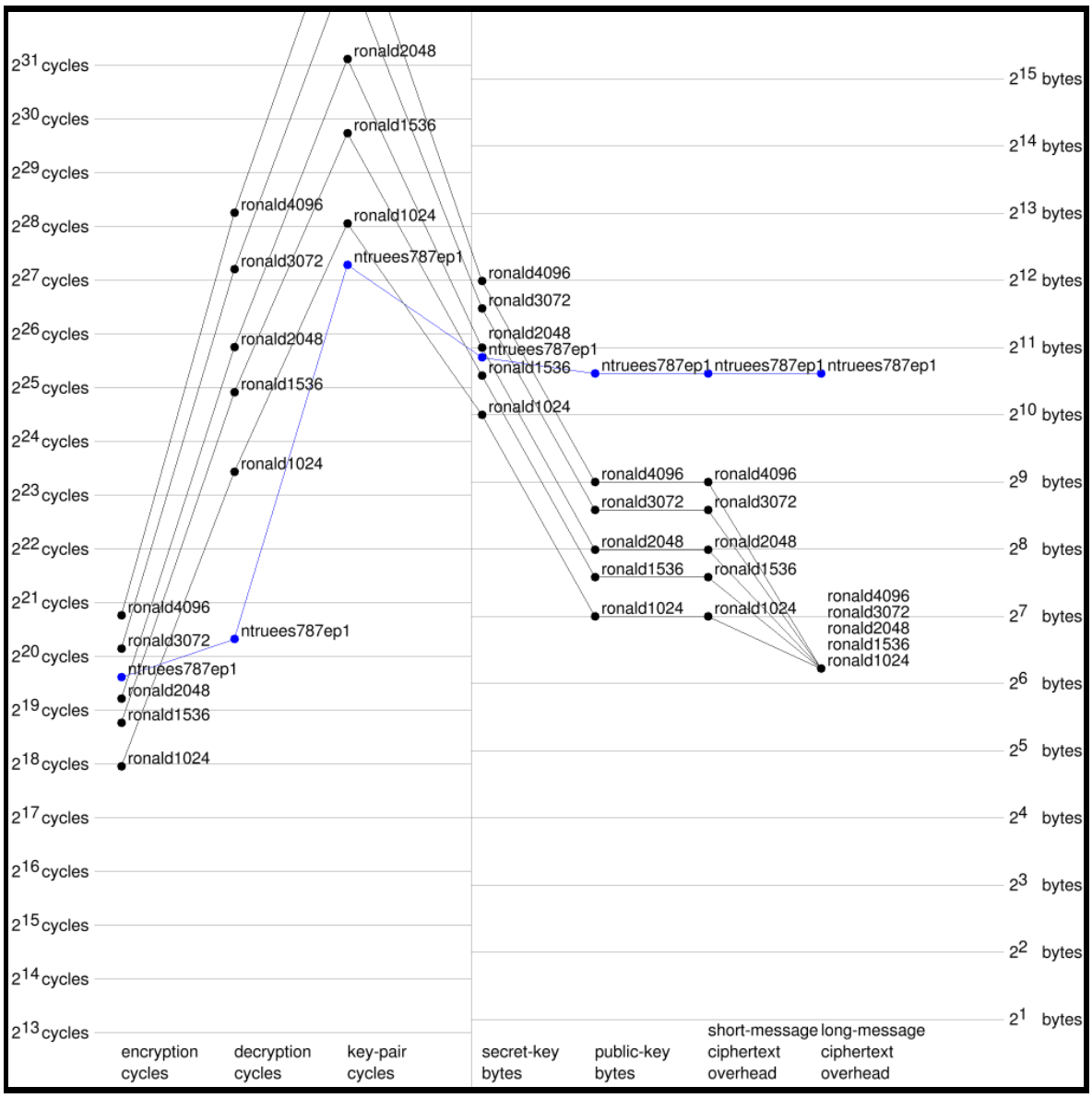
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1066504	1075572	1091676	`ntruees787ep1`
1328892	1346304	1360296	`mceliece`
13463092	13562036	13688592	`ronald1024`
37717576	38089480	38608140	`ronald1536`
75915920	76425524	77018384	`ronald2048`
238837540	241401516	244876254	`ronald3072`
487685716	490102892	493590252	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.31 x86, 2791MHz, Intel Xeon (f27), nmi0024



Cycles to generate a key pair			
quartile	median	quartile	system
164217384	165012180	165535564	`ntruees787ep1`
196063724	281369208	382796736	`ronald1024`
515215192	902735988	1324019196	`ronald1536`
1453751992	2348725504	3890588740	`ronald2048`
5412467392	7797590112	12591064660	`ronald3072`
13002532470	20558569458	35809998294	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
253388	255680	259636	`ronald1024`
441480	447384	454064	`ronald1536`
602504	611884	620040	`ronald2048`
806260	808268	810144	`ntruees787ep1`
1163156	1168976	1178004	`ronald3072`
1781828	1788576	1797152	`ronald4096`

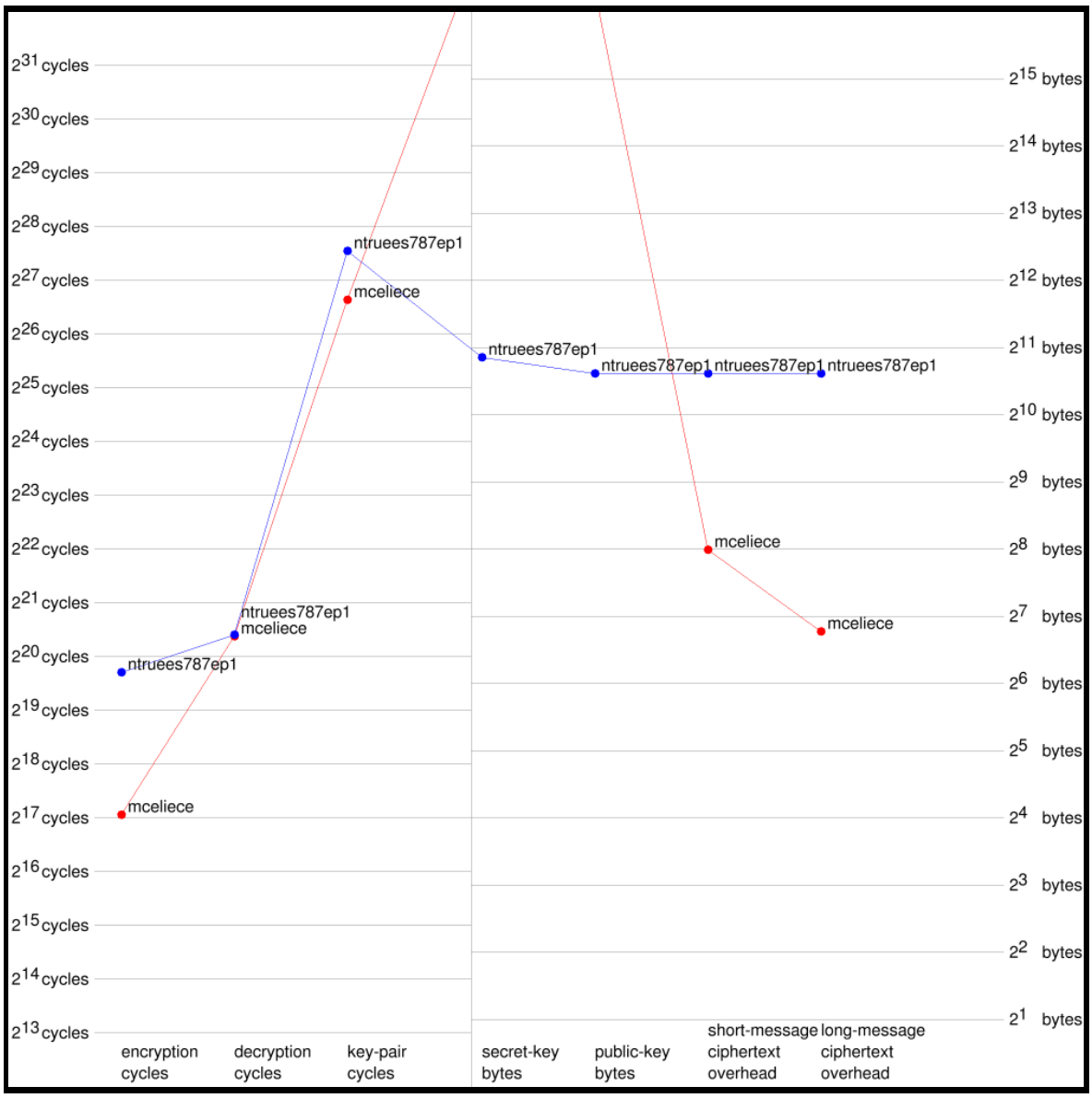
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1295768	1318812	1432376	`ntruees787ep1`
11325784	11407244	11455804	`ronald1024`
30613760	31956620	32778928	`ronald1536`
56628272	56911020	57305856	`ronald2048`
154182788	155689624	156593980	`ronald3072`
320465424	322086964	324617532	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
1573	`ntruees787ep1`

9.32 x86, 2800MHz, Intel Xeon (f41), nmi0057



Cycles to generate a key pair			
quartile	median	quartile	system
95357402	104750520	131766838	`mceliece`
196242102	197255016	202218163	`ntruees787ep1`

Secret key	
bytes	system
1854	`ntruees787ep1`
137282	`mceliece`

Public key	
bytes	system
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
133903	137193	213262	`mceliece`
820491	862582	1421532	`ntruees787ep1`

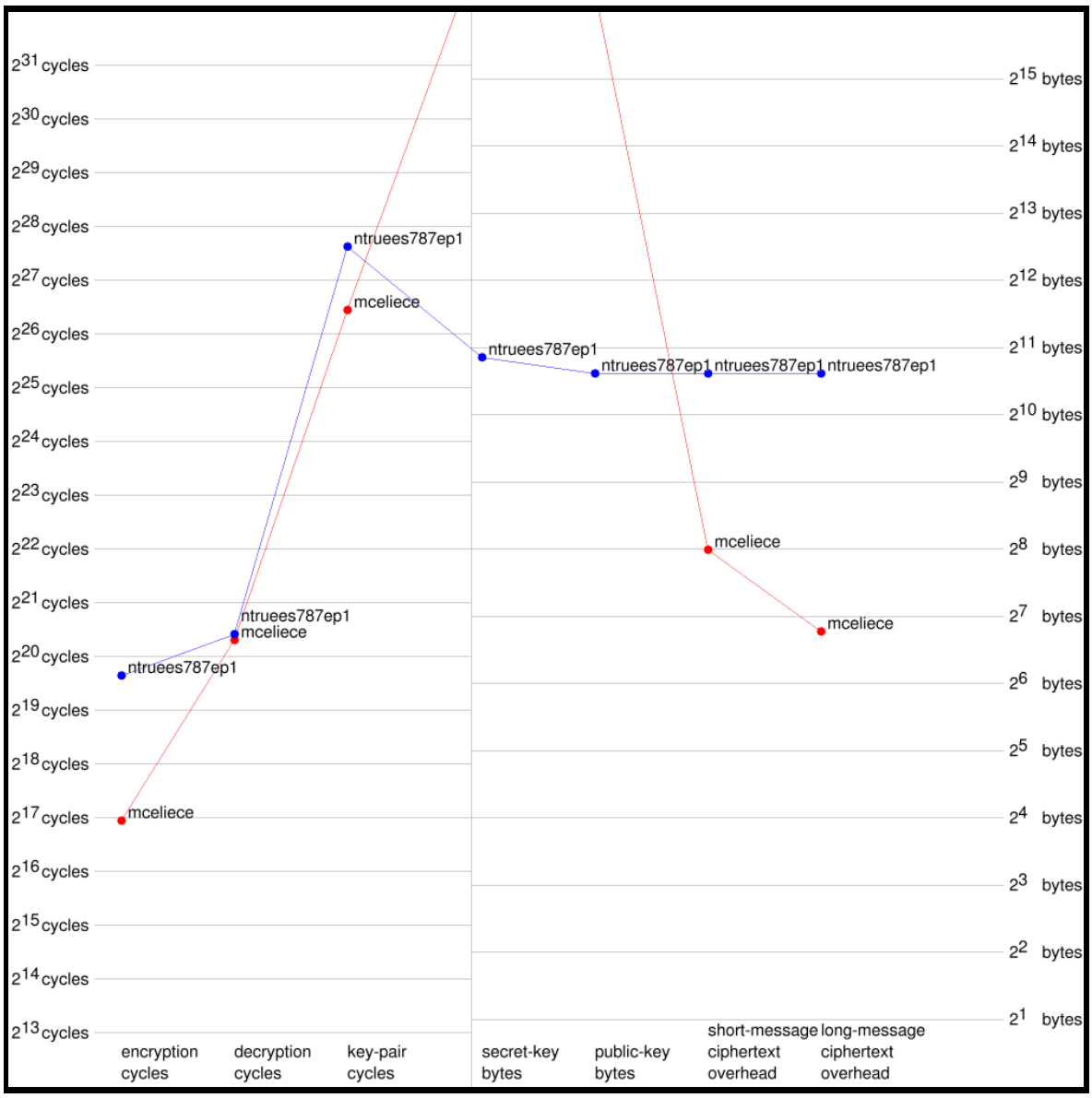
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1354934	1372021	2154628	`mceliece`
1381527	1396731	2395771	`ntruees787ep1`

Encrypting 0 bytes	
bytes	system
256	`mceliece`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
233	`mceliece`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
110	`mceliece`
1573	`ntruees787ep1`

9.33 x86, 2800MHz, Intel Xeon (f41), nmi0063



Cycles to generate a key pair			
quartile	median	quartile	system
88798983	91703283	97477786	`mceliece`
207800971	208761987	209366822	`ntruees787ep1`

Secret key	
bytes	system
1854	`ntruees787ep1`
137282	`mceliece`

Public key	
bytes	system
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
125104	127015	129444	`mceliece`
820666	825216	841190	`ntruees787ep1`

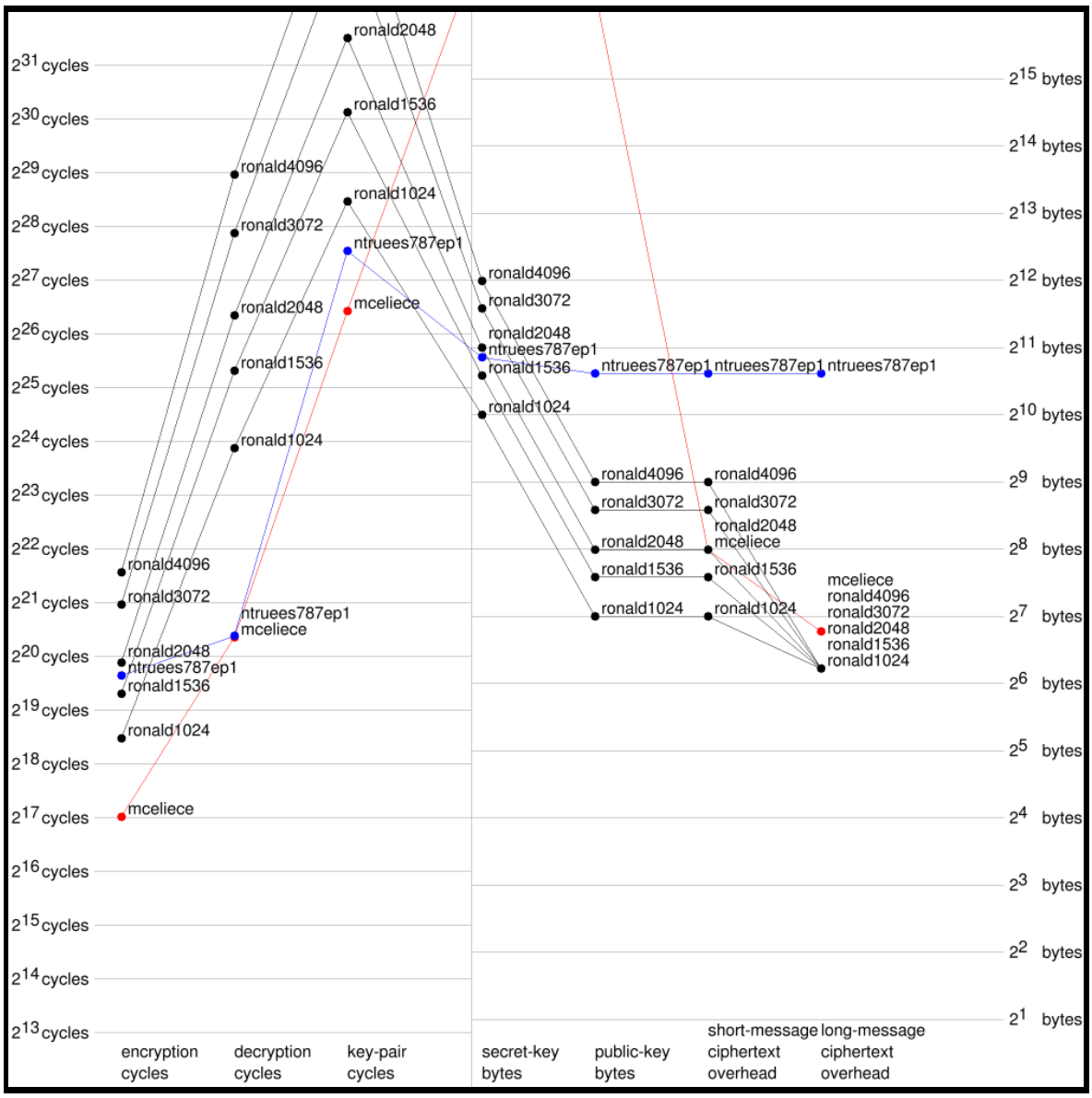
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1291710	1301552	1307299	`mceliece`
1399321	1409821	1416303	`ntruees787ep1`

Encrypting 0 bytes	
bytes	system
256	`mceliece`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
233	`mceliece`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
110	`mceliece`
1573	`ntruees787ep1`

9.34 x86, 2801MHz, Intel Xeon (f41), nmi0060



Cycles to generate a key pair			
quartile	median	quartile	system
87959501	90755707	95349744	`mceliece`
195853917	196793450	197743252	`ntruees787ep1`
268050314	372270843	613191005	`ronald1024`
739405247	1179389890	1752901500	`ronald1536`
1775240320	3059281407	4867310910	`ronald2048`
7320495700	12189128021	18652901687	`ronald3072`
17742882458	30968627823	49307388872	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
131432	133140	135240	`mceliece`
364798	367262	373002	`ronald1024`
645764	650972	658371	`ronald1536`
817859	824089	830599	`ntruees787ep1`
965426	973126	977578	`ronald2048`
2050867	2066918	2081961	`ronald3072`
3106677	3116169	3126578	`ronald4096`

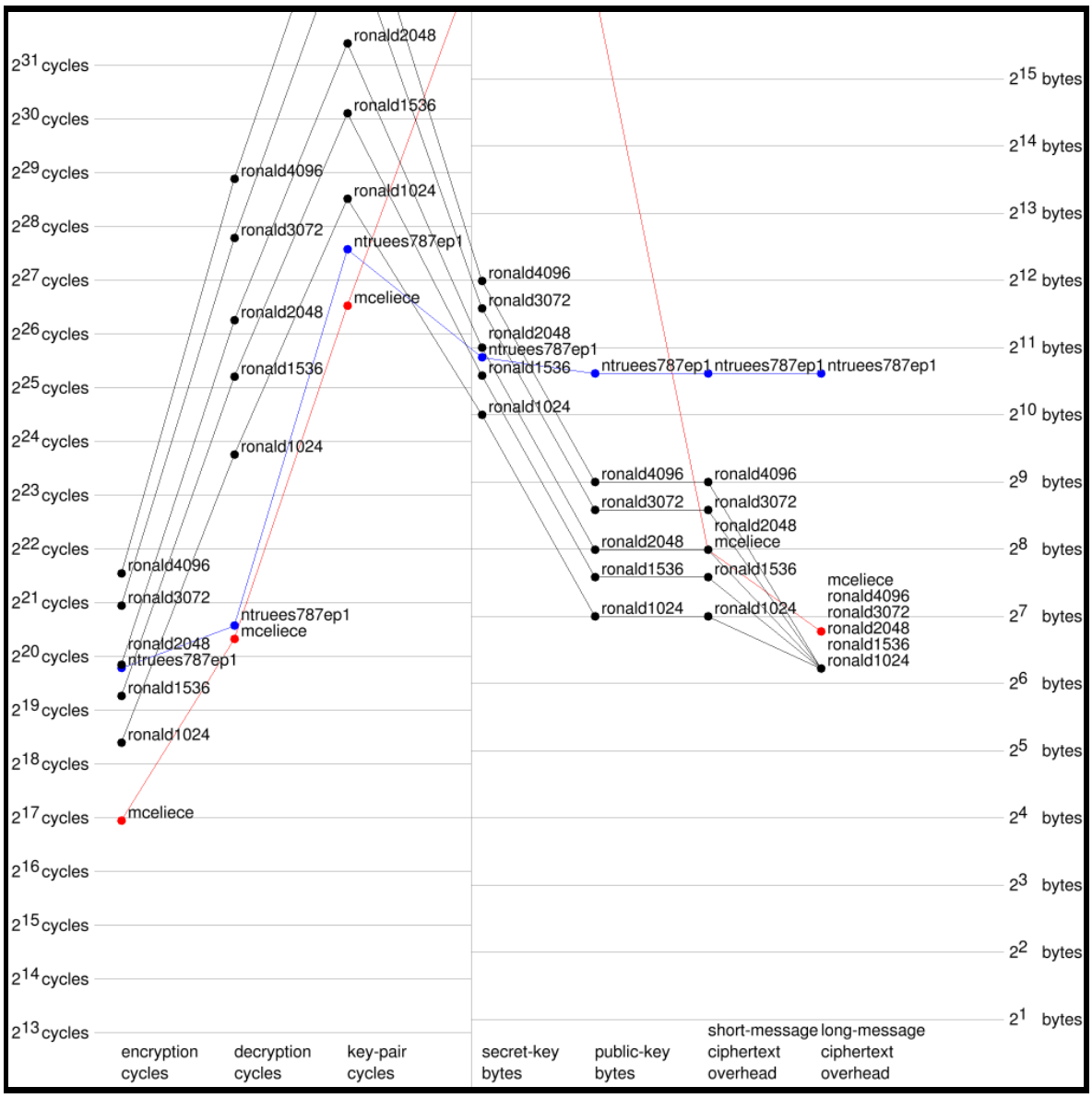
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1344924	1351217	1363201	`mceliece`
1373897	1380890	1393063	`ntruees787ep1`
15452423	15497881	15565606	`ronald1024`
42095886	42173691	42270067	`ronald1536`
85627654	85764973	85887655	`ronald2048`
247039450	247311148	248082030	`ronald3072`
526288266	526845473	529482611	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.35 x86, 2801MHz, Intel Xeon (f41), nmi0061



Cycles to generate a key pair			
quartile	median	quartile	system
93821021	96949062	101721074	`mceliece`
200224850	200956840	201912088	`ntruees787ep1`
256997503	386357370	593877760	`ronald1024`
810368601	1163977479	1903316002	`ronald1536`
1516581640	2853332818	4393858952	`ronald2048`
8370153603	13104894726	20322638217	`ronald3072`
23404707718	34716035046	53540012316	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
125552	127183	129087	`mceliece`
344771	347564	354200	`ronald1024`
628810	633073	639751	`ronald1536`
903679	909433	919359	`ntruees787ep1`
944524	948542	954625	`ronald2048`
2028376	2033997	2049796	`ronald3072`
3079370	3089135	3097164	`ronald4096`

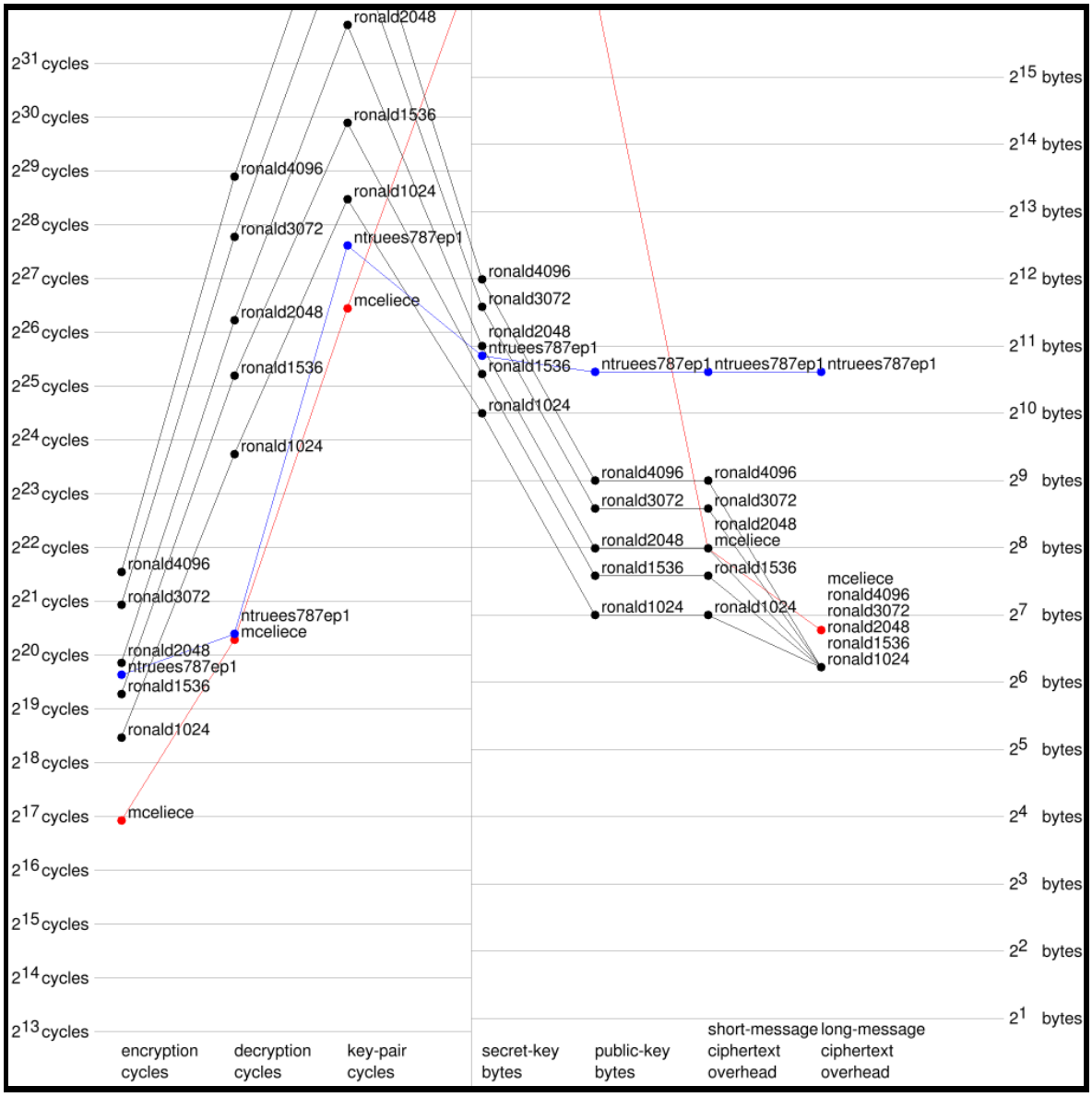
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1311912	1318534	1326507	`mceliece`
1557563	1567993	1579389	`ntruees787ep1`
14207214	14246169	14307790	`ronald1024`
38945480	39043851	39259584	`ronald1536`
80286381	80444630	80547187	`ronald2048`
232204210	232555554	234395847	`ronald3072`
499371453	500058013	500953187	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.36 x86, 2801MHz, Intel Xeon (f41), nmi0062



Cycles to generate a key pair			
quartile	median	quartile	system
88801489	91849513	97205906	mceliece
205802583	206653636	207212600	ntruees787ep1
219885211	375719701	497198163	ronald1024
644633563	1004555426	1758240134	ronald1536
1811016718	3544726353	4544664852	ronald2048
7848272124	12866856226	21653689911	ronald3072
16509435537	33735731883	50318840831	ronald4096

Secret key	
bytes	system
1024	ronald1024
1536	ronald1536
1854	ntruees787ep1
2048	ronald2048
3072	ronald3072
4096	ronald4096
137282	mceliece

Public key	
bytes	system
128	ronald1024
192	ronald1536
256	ronald2048
384	ronald3072
512	ronald4096
1574	ntruees787ep1
81408	mceliece

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
123081	125104	128352	mceliece
360689	363132	368802	ronald1024
633647	640668	648165	ronald1536
818580	821961	826280	ntruees787ep1
947765	953141	959763	ronald2048
2010715	2019143	2026234	ronald3072
3066798	3080868	3089387	ronald4096

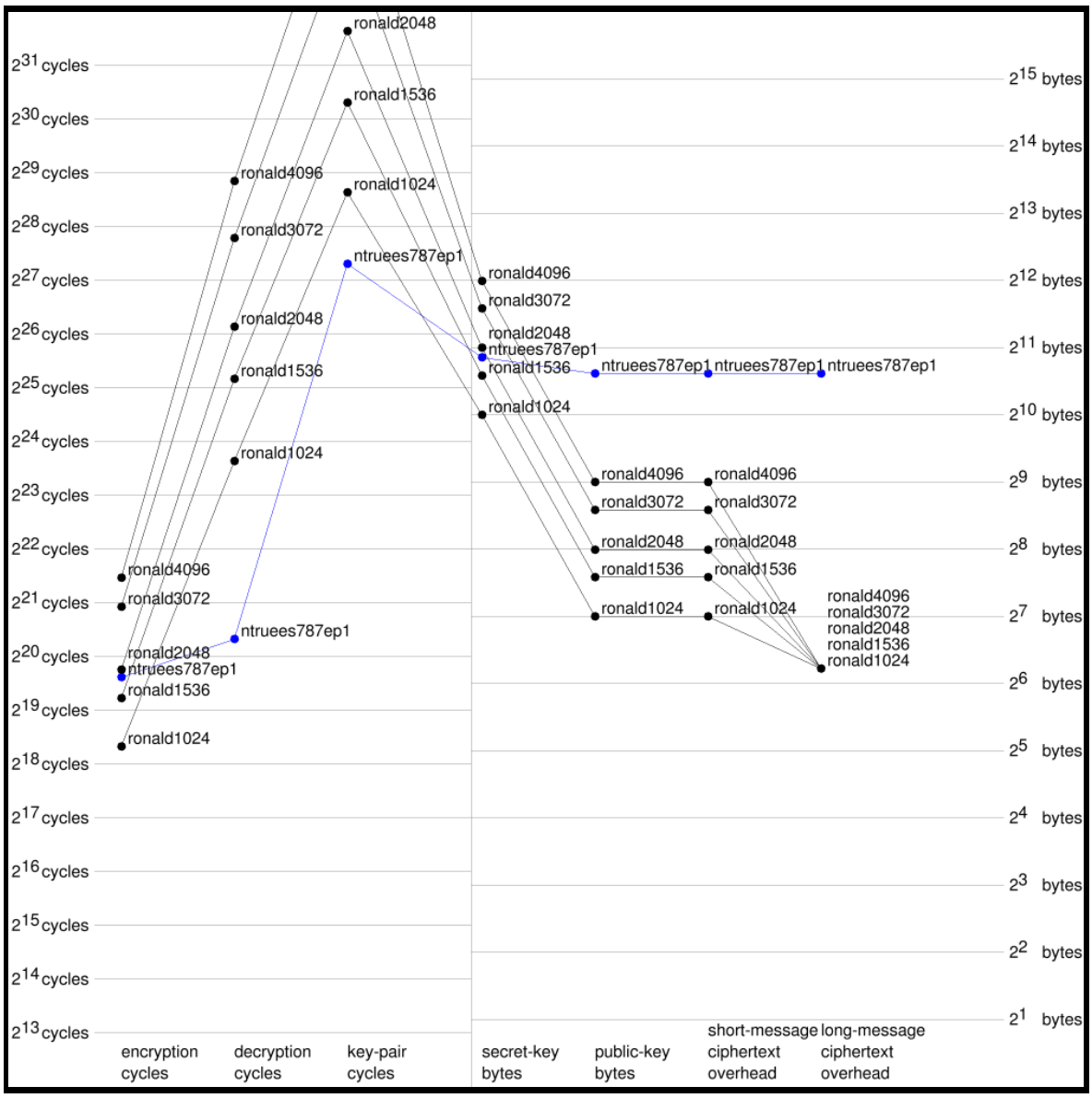
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1281028	1286257	1294300	mceliece
1387806	1392524	1397186	ntruees787ep1
13983683	14023191	14047712	ronald1024
38549406	38625881	38720605	ronald1536
79113727	79199918	79334682	ronald2048
231601265	231870464	232162252	ronald3072
500406375	501095098	501726764	ronald4096

Encrypting 0 bytes	
bytes	system
128	ronald1024
192	ronald1536
256	mceliece
256	ronald2048
384	ronald3072
512	ronald4096
1574	ntruees787ep1

Encrypting 23 bytes	
bytes	system
105	ronald1024
169	ronald1536
233	mceliece
233	ronald2048
361	ronald3072
489	ronald4096
1551	ntruees787ep1

Encrypting many bytes	
bytes	system
75	ronald1024
75	ronald1536
75	ronald2048
75	ronald3072
75	ronald4096
110	mceliece
1573	ntruees787ep1

9.37 x86, 2802MHz, Intel Xeon (f29), `nmibuild40`



Cycles to generate a key pair			
quartile	median	quartile	system
165669004	166573008	167369956	`ntruees787ep1`
276928984	420177696	617419424	`ronald1024`
940853380	1332912504	2059742748	`ronald1536`
2029481832	3368521824	5254491332	`ronald2048`
6500902736	12578354820	20384343084	`ronald3072`
18824432804	35059902992	50280295568	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
322080	330136	335232	`ronald1024`
608704	618000	631892	`ronald1536`
803780	808224	815796	`ntruees787ep1`
887292	893948	900640	`ronald2048`
1982184	2004636	2032852	`ronald3072`
2909600	2917100	2930296	`ronald4096`

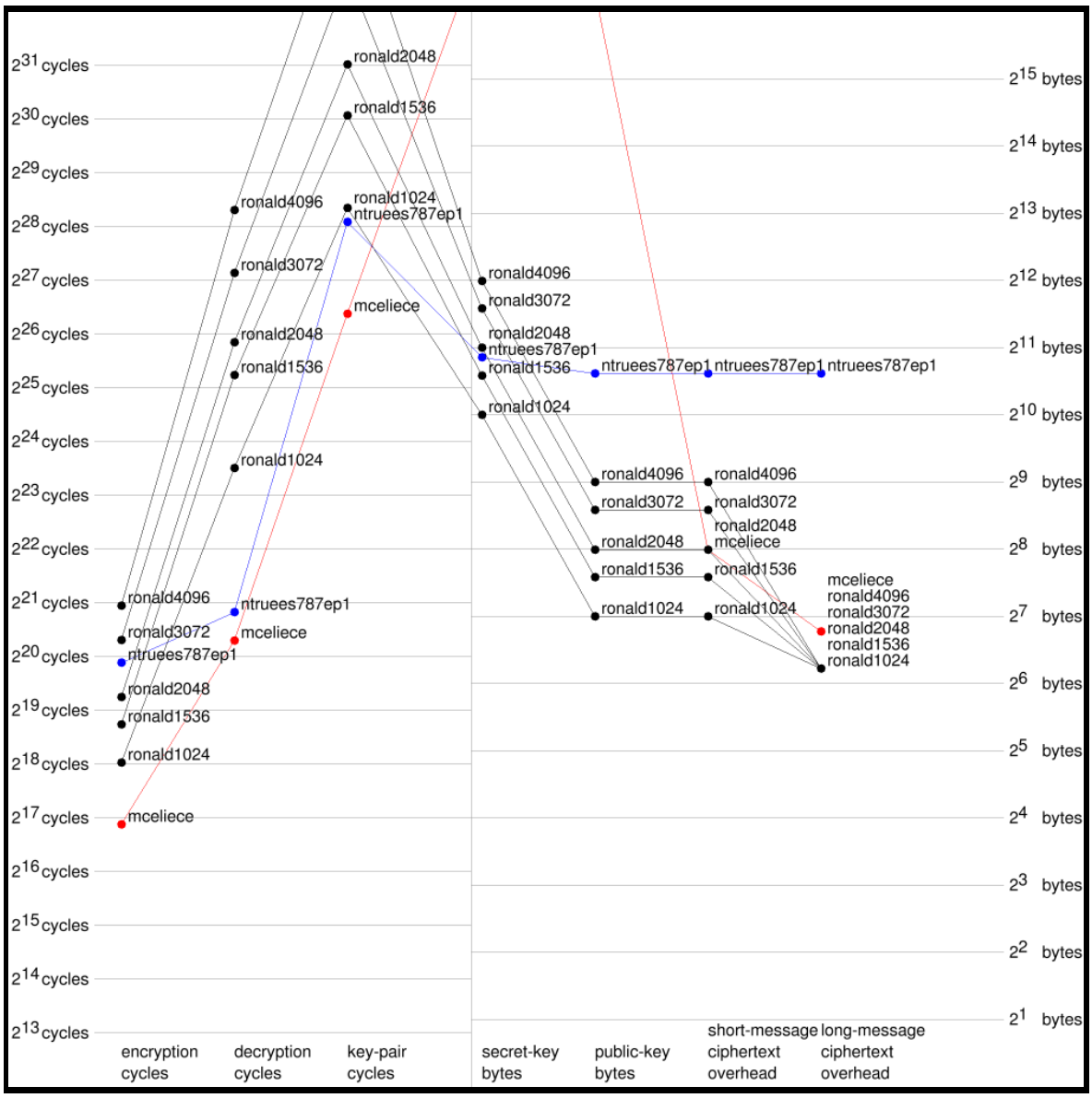
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1313784	1322588	1330912	`ntruees787ep1`
13044224	13119072	13167728	`ronald1024`
37059896	37947744	38551036	`ronald1536`
74198228	74372580	75045780	`ronald2048`
231713452	233476160	235607592	`ronald3072`
484748264	485835496	487154844	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
1573	`ntruees787ep1`

9.38 x86, 2995MHz, Intel Xeon (f41), `nmi0079`



Cycles to generate a key pair			
quartile	median	quartile	system
84584115	87706672	94821705	`mceliece`
199560533	286349077	326484397	`ntruees787ep1`
230931510	343227240	536434838	`ronald1024`
640283565	1133251770	1632289140	`ronald1536`
1166664203	2178734985	3337908360	`ronald2048`
4185559860	7095589064	11198527575	`ronald3072`
15508787227	22050803857	35097450263	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
120068	121433	123585	`mceliece`
265665	268058	271485	`ronald1024`
433500	439140	455333	`ronald1536`
619995	625357	631215	`ronald2048`
865733	977062	1494427	`ntruees787ep1`
1298212	1304775	1319355	`ronald3072`
2019930	2029627	2040240	`ronald4096`

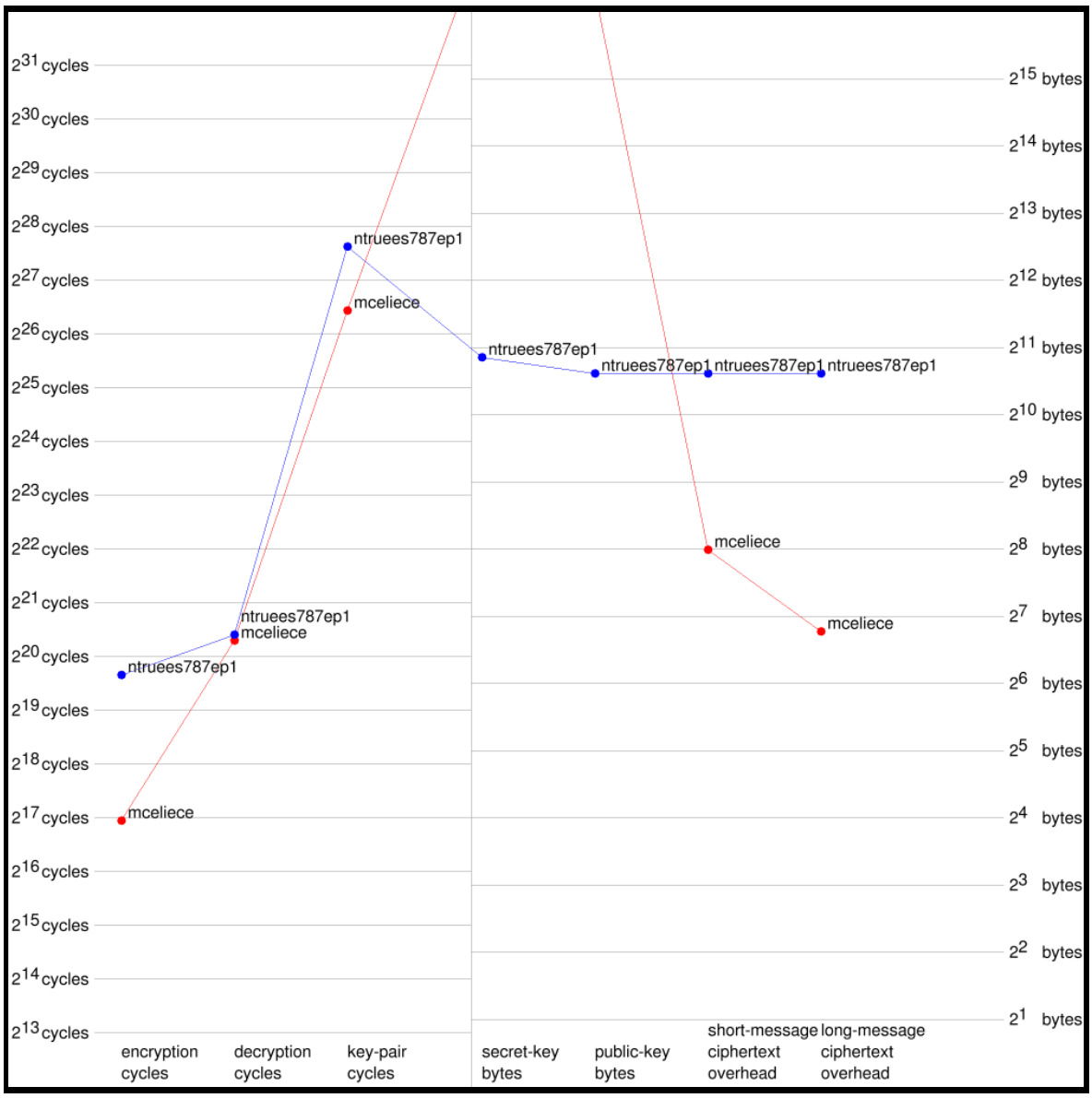
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1279710	1292250	1296885	`mceliece`
1502685	1874587	2611927	`ntruees787ep1`
11977815	12026812	12086190	`ronald1024`
29364487	39628785	49321905	`ronald1536`
60370440	60649725	60895365	`ronald2048`
138577643	147911010	169210755	`ronald3072`
333304905	333719640	334415362	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.39 x86, 2996MHz, Intel Xeon (f41), nmi0076



Cycles to generate a key pair			
quartile	median	quartile	system
87872903	91670985	97095052	`mceliece`
206757428	207908940	208372215	`ntruees787ep1`

Secret key	
bytes	system
1854	`ntruees787ep1`
137282	`mceliece`

Public key	
bytes	system
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
125392	126877	128910	`mceliece`
826178	830955	838327	`ntruees787ep1`

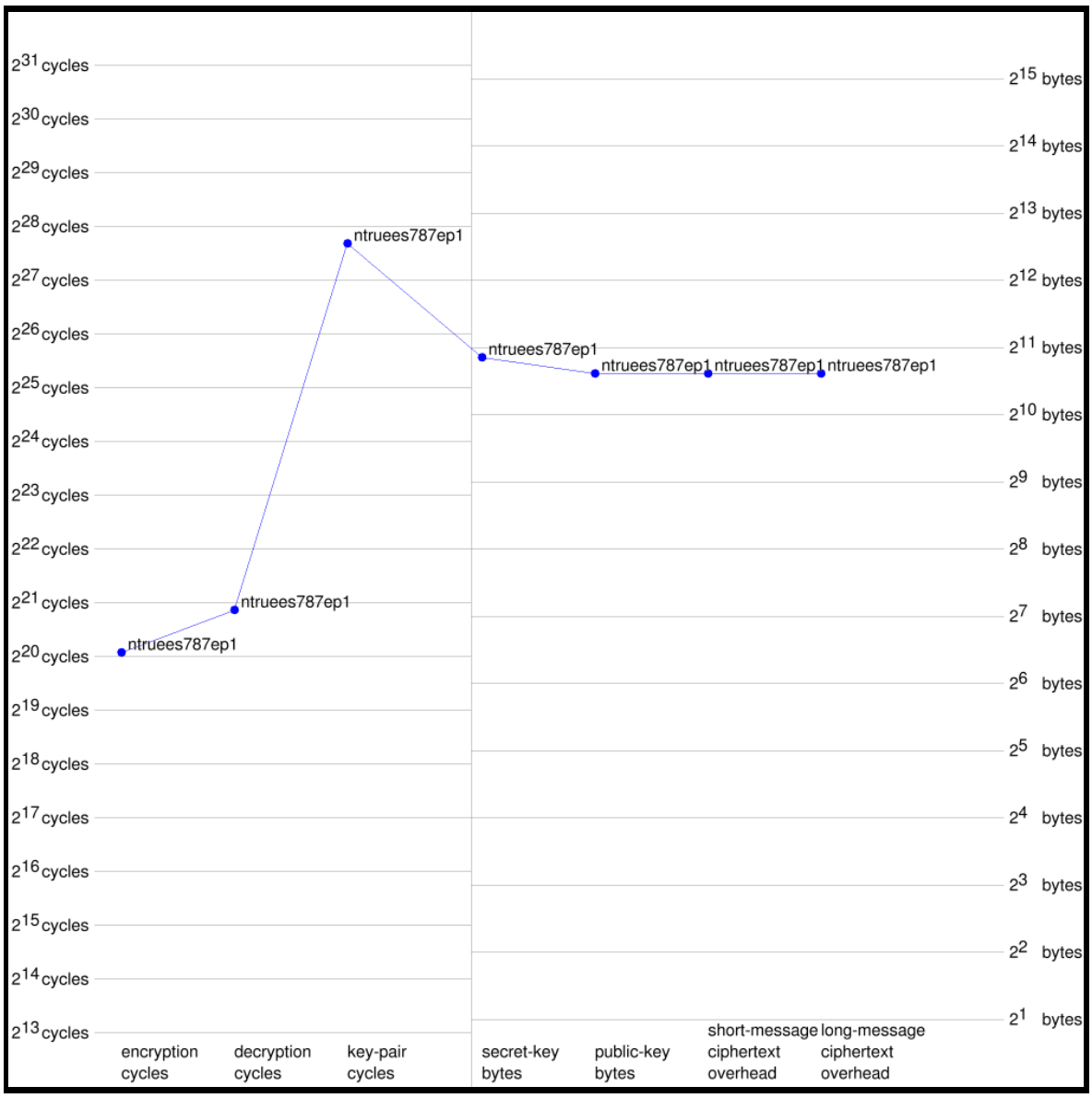
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1283145	1298160	1301512	`mceliece`
1385445	1395187	1403407	`ntruees787ep1`

Encrypting 0 bytes	
bytes	system
256	`mceliece`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
233	`mceliece`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
110	`mceliece`
1573	`ntruees787ep1`

9.40 x86, 3000MHz, Intel Xeon (f4a), nmi0090



Cycles to generate a key pair			
quartile	median	quartile	system
216577470	217372958	217979978	`ntruees787ep1`

Secret key	
bytes	system
1854	`ntruees787ep1`

Public key	
bytes	system
1574	`ntruees787ep1`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
1111200	1113195	1118085	`ntruees787ep1`

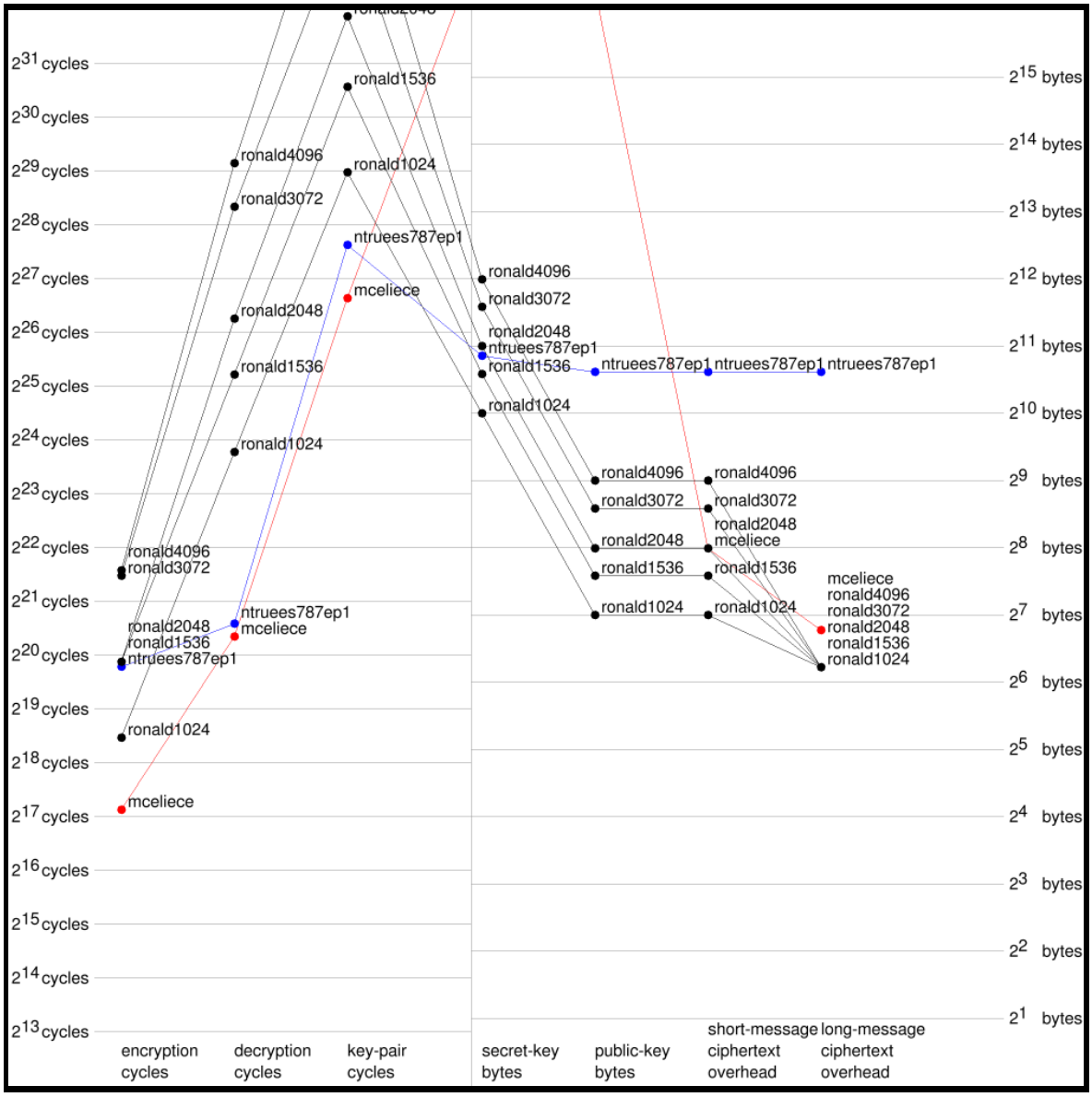
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1922678	1927658	1932240	`ntruees787ep1`

Encrypting 0 bytes	
bytes	system
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
1573	`ntruees787ep1`

9.41 x86, 3000MHz, Intel Xeon (f4a), nmi0102



Cycles to generate a key pair			
quartile	median	quartile	system
101755035	105265957	115591710	`mceliece`
206925240	208189763	232012305	`ntruees787ep1`
317502705	532951447	823204073	`ronald1024`
1016466960	1598296958	2674621530	`ronald1536`
2367808155	3961409280	6099724350	`ronald2048`
8789632432	14891918228	22450334528	`ronald3072`
32654235435	50557973707	72931606815	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
142170	143580	146437	`mceliece`
360758	365100	565252	`ronald1024`
905152	908460	1577940	`ntruees787ep1`
961695	969045	1421745	`ronald2048`
658200	970290	999773	`ronald1536`
2063332	2935110	2982135	`ronald3072`
3112710	3148057	4501913	`ronald4096`

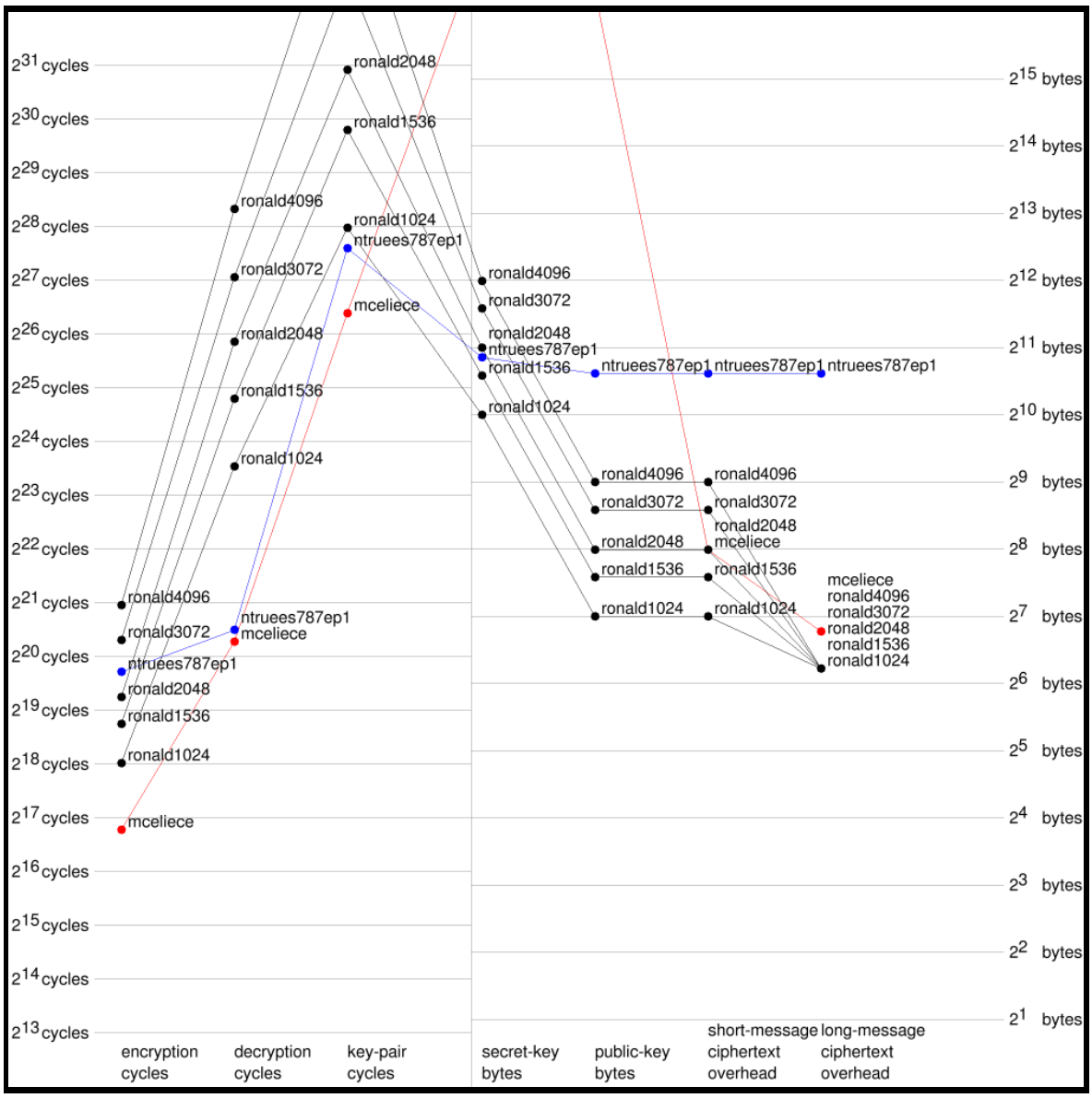
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1325790	1337842	1490738	`mceliece`
1583025	1587113	2712405	`ntruees787ep1`
14420460	14494043	21717398	`ronald1024`
39156240	39230512	39378637	`ronald1536`
80385457	80556045	80782395	`ronald2048`
241742340	341570790	350530297	`ronald3072`
558021457	595913040	631864118	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.42 x86, 3391MHz, Intel Pentium D (f64), nmi0099



Cycles to generate a key pair			
quartile	median	quartile	system
83167825	87991422	101534982	`mceliece`
202523465	203532840	205958944	`ntruees787ep1`
159984620	265161886	391074698	`ronald1024`
587194977	938065576	1297471484	`ronald1536`
1365994234	2039718293	2926937311	`ronald2048`
3554258680	6907791067	11014342585	`ronald3072`
15340421087	26411413486	46048988612	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
110993	112642	114240	`mceliece`
264197	267223	271660	`ronald1024`
437291	441354	448460	`ronald1536`
616692	623866	629629	`ronald2048`
865538	867374	873171	`ntruees787ep1`
1298834	1306110	1315460	`ronald3072`
2035325	2043383	2058258	`ronald4096`

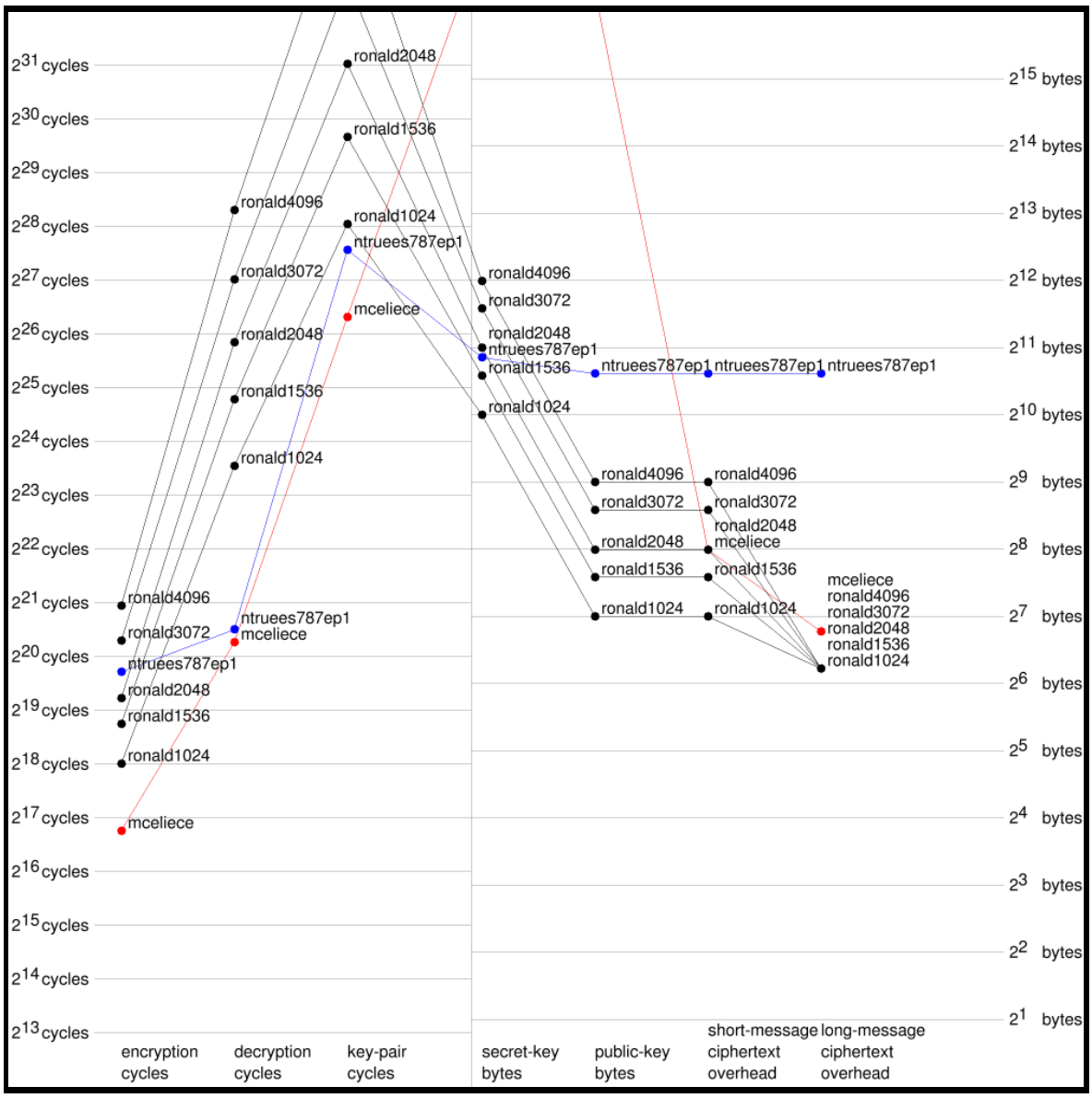
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1268999	1279114	1285676	`mceliece`
1482842	1487857	1493314	`ntruees787ep1`
12234764	12269053	12323368	`ronald1024`
29199965	29279916	29356025	`ronald1536`
60826646	61057642	61284286	`ronald2048`
137920847	140036021	152579403	`ronald3072`
335155510	339529627	379140630	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.43 x86, 3392MHz, Intel Pentium D (f64), `nmi0104`



Cycles to generate a key pair			
quartile	median	quartile	system
81055711	84103114	90077645	`mceliece`
199402112	200480184	201016381	`ntruees787ep1`
202945082	279055442	437313185	`ronald1024`
486110937	859894663	1426328747	`ronald1536`
1193563064	2206230777	2909424676	`ronald2048`
4112397053	6443197761	9304445032	`ronald3072`
14919174568	23692525626	42526809884	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
109718	111163	113084	`mceliece`
262327	265693	270283	`ronald1024`
438617	442153	445740	`ronald1536`
615315	619021	625430	`ronald2048`
865266	867119	868683	`ntruees787ep1`
1289501	1295298	1300228	`ronald3072`
2024054	2030956	2038963	`ronald4096`

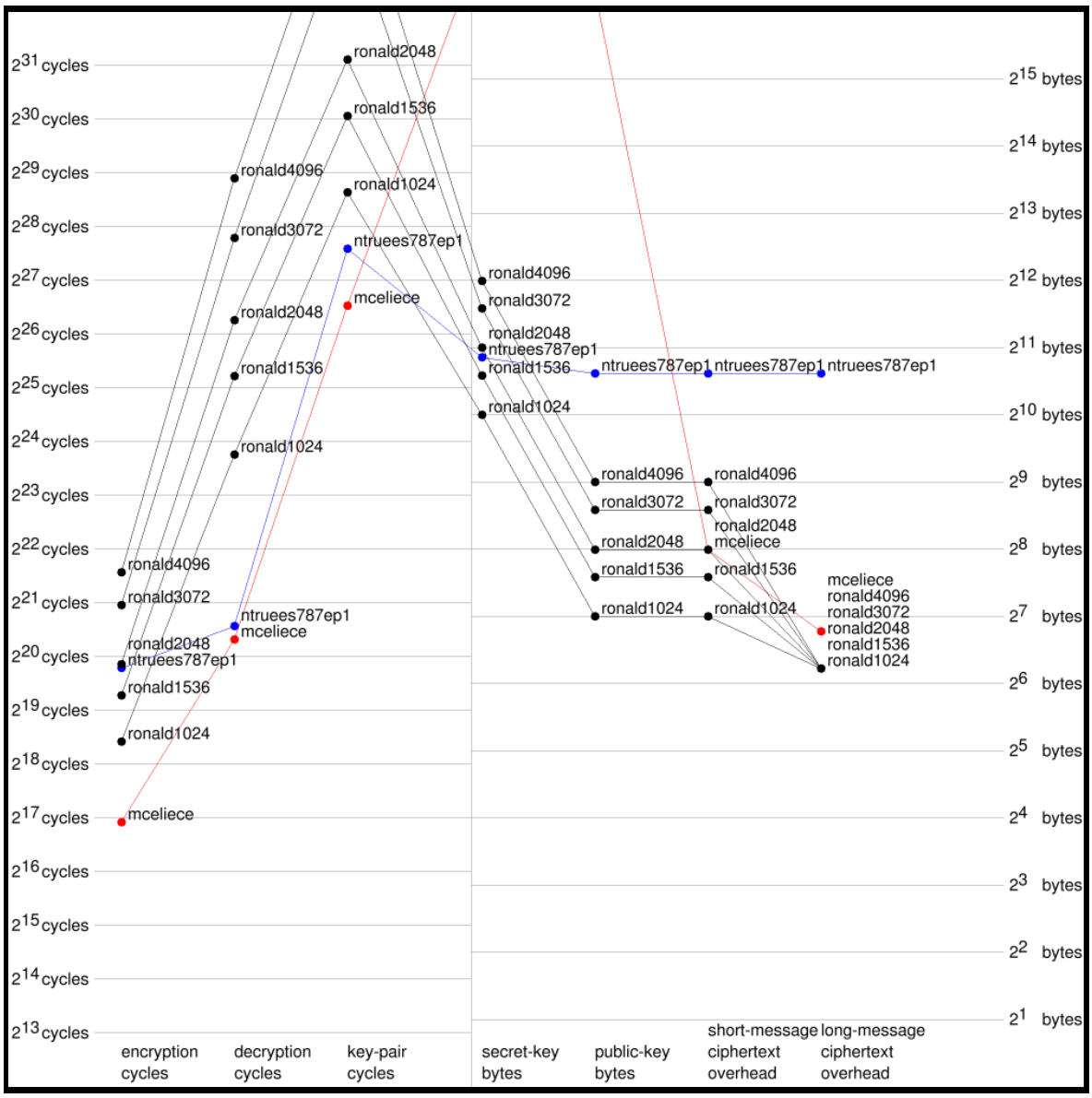
Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1264749	1266551	1276122	`mceliece`
1496663	1498839	1501287	`ntruees787ep1`
12230225	12305654	12363913	`ronald1024`
28995625	29074131	29160015	`ronald1536`
60617546	60745590	60905169	`ronald2048`
136322133	136519826	136759475	`ronald3072`
333088055	333683021	334646666	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

9.44 x86, 3392MHz, Intel Pentium D (f64), `nmi0241`



Cycles to generate a key pair			
quartile	median	quartile	system
93826451	97142454	104099534	`mceliece`
202490502	203402739	204101558	`ntruees787ep1`
248281838	419609266	534015101	`ronald1024`
639165796	1122918306	1746192774	`ronald1536`
1486645359	2327164799	4433084186	`ronald2048`
8433660033	14615189799	22247250345	`ronald3072`
19951038517	34680512992	54007461313	`ronald4096`

Secret key	
bytes	system
1024	`ronald1024`
1536	`ronald1536`
1854	`ntruees787ep1`
2048	`ronald2048`
3072	`ronald3072`
4096	`ronald4096`
137282	`mceliece`

Public key	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`
81408	`mceliece`

Cycles to encrypt 59 bytes			
quartile	median	quartile	system
123471	124712	127160	`mceliece`
348466	352971	360230	`ronald1024`
632400	638061	642974	`ronald1536`
907545	912237	920550	`ntruees787ep1`
947376	953411	963883	`ronald2048`
2039762	2046035	2054671	`ronald3072`
3111170	3116967	3123393	`ronald4096`

Cycles to decrypt 59 bytes			
quartile	median	quartile	system
1301469	1314168	1322413	`mceliece`
1556061	1562742	1584961	`ntruees787ep1`
14163193	14213785	14275155	`ronald1024`
39061767	39131433	39192208	`ronald1536`
80531278	80801935	81135781	`ronald2048`
232882082	233409252	234111981	`ronald3072`
503343956	503794660	505033603	`ronald4096`

Encrypting 0 bytes	
bytes	system
128	`ronald1024`
192	`ronald1536`
256	`mceliece`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
1574	`ntruees787ep1`

Encrypting 23 bytes	
bytes	system
105	`ronald1024`
169	`ronald1536`
233	`mceliece`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`
1551	`ntruees787ep1`

Encrypting many bytes	
bytes	system
75	`ronald1024`
75	`ronald1536`
75	`ronald2048`
75	`ronald3072`
75	`ronald4096`
110	`mceliece`
1573	`ntruees787ep1`

Chapter 10

Measurements of public-key signature systems

10.1 Introduction

This chapter presents a series of graphs, one for each computer. There are seven horizontal positions on each graph:

- Time to verify a signed message.
- Time to sign a message.
- Time to compute a key pair.
- Space for a secret key.
- Space for a public key.
- Space for a signature on a short message.
- Space for a signature on a long message: more precisely, the difference between the space used by a long signed message and the space used by the original unsigned message. This can be smaller than the space for a signature on a short message for signature systems that support "message recovery."

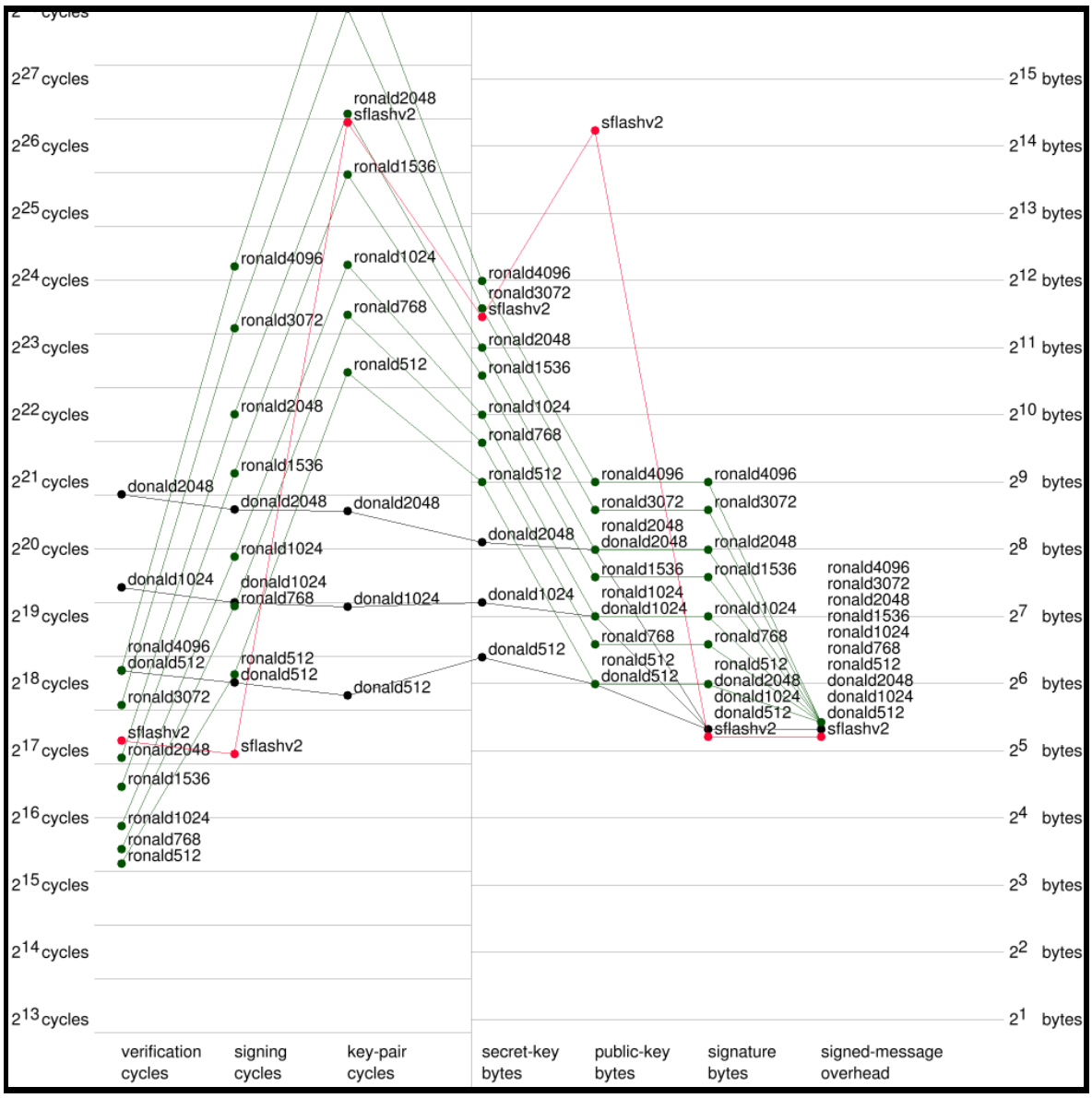
Each graph is a superimposition of several curves, one curve for each signature system.

This chapter also presents a series of tables, eight for each computer. The first table shows the time, in cycles, to generate a key pair. Each row of the table lists

- the first quartile of many time measurements,
- the median of many time measurements,
- the third quartile of many time measurements, and
- the name of the signature system.

The second table shows the length of a secret key. The third table shows the time to sign a short message. The fourth table shows the length of a public key. The fifth table shows the time to verify a signature on a short message. The sixth, seventh, and eighth tables show the space for a signature on, respectively, a 0-byte message, a 23-byte message, and a long message.

10.2 amd64, 1403MHz, AMD Opteron 240 (f58), `nmisles8amd64`



Cycles to generate a key pair			
quartile	median	quartile	system
632520	639944	647807	donald512
1979664	2001171	2018110	donald1024
6833818	6895157	6946186	donald2048
27197251	41265724	62480396	ronald512
57224667	86385342	127474840	ronald768
110193109	165061556	251046522	ronald1024
312699688	528457959	741731949	ronald1536
1034718511	1034780866	1034867593	sflashv2
827061579	1152921589	2035295232	ronald2048
2523358755	4490268006	7280890018	ronald3072
7823823572	14033247022	19732259266	ronald4096

Secret key	
bytes	system
84	donald512
148	donald1024
276	donald2048
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096

Cycles to sign 59 bytes			
quartile	median	quartile	system
299942	300068	300098	sflashv2
745351	752178	759821	donald512
834019	834994	854319	ronald512
1971610	2015649	2019294	ronald768
2105069	2121154	2134350	donald1024
3820550	3828192	3878430	ronald1024
6954505	7006353	7074632	donald2048
11028868	11169115	11206621	ronald1536
23876795	23896422	23976777	ronald2048
72628718	72723363	73359568	ronald3072
160164255	161395372	161833766	ronald4096

Public key	
bytes	system
64	donald512
64	ronald512
96	ronald768
128	donald1024
128	ronald1024
192	ronald1536
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2

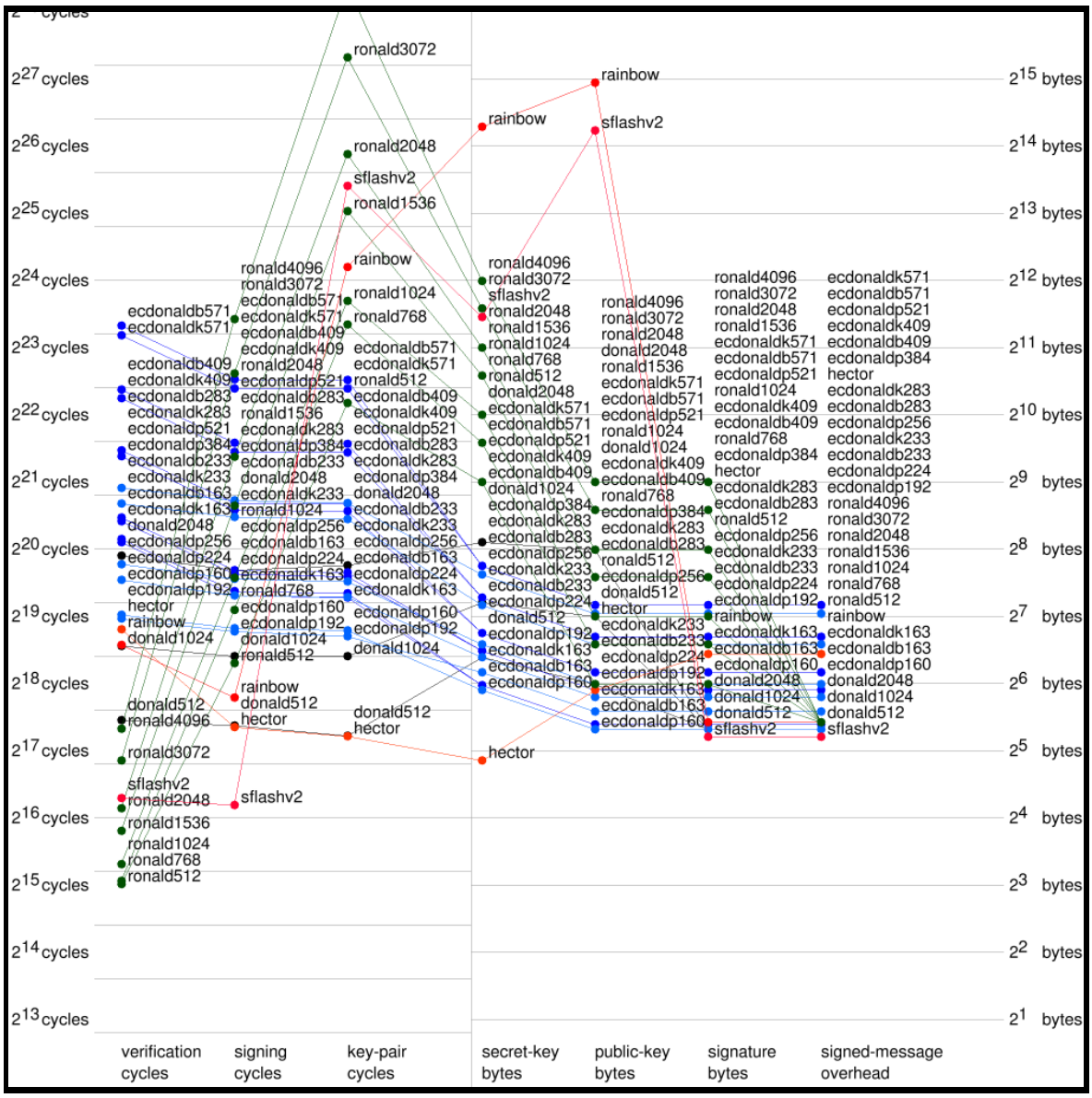
Cycles to verify 59 bytes			
quartile	median	quartile	system
72606	73189	76450	ronald512
86847	87882	90498	ronald768
116095	118149	122145	ronald1024
192758	196437	198056	ronald1536
277954	285018	288824	ronald2048
356651	356757	356952	sflashv2
560008	565418	567676	ronald3072
875450	876385	884463	donald512
881357	884324	893730	ronald4096
2567621	2570236	2573452	donald1024
8518974	8532263	8587553	donald2048

Signing 0 bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
41	`ronald512`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.3 amd64, 2400MHz, Intel Core 2 Duo (6fb), `utrecht`



Cycles to generate a key pair			
quartile	median	quartile	system
374319	376290	403452	`hector`
378468	379845	381798	`donald512`
1059444	1061397	1063962	`donald1024`
1349550	1369692	1403793	`ecdonaldp192`
1452366	1475928	1527939	`ecdonaldp160`
2233629	2252403	2273823	`ecdonaldk163`
2240577	2276865	2333052	`ecdonaldp224`
2358270	2381058	2398140	`ecdonaldb163`
2754369	2779137	2809350	`ecdonaldp256`
2953125	2964834	2983437	`ecdonaldk233`
3106971	3123666	3142422	`ecdonaldb233`
3407724	3410451	3417867	`donald2048`
6154596	6183675	6226740	`ecdonaldp384`
6870762	6894333	6953382	`ecdonaldk283`
7418484	7572816	7859304	`ecdonaldb283`
7603443	7634916	7693821	`ecdonaldp521`
14586840	14629518	14651397	`ecdonaldk409`
16363431	16385274	16433730	`ecdonaldb409`
16679313	27676449	40480461	`ronald512`
33095043	33369876	33520005	`ecdonaldk571`
37001907	37364904	37594899	`ecdonaldb571`
49569597	76041234	117760158	`ronald768`
62405964	103408803	165835575	`ronald1024`
159886962	160653717	161181207	`rainbow`
215343405	329046255	491980770	`ronald1536`
456345441	456395427	456593103	`sflashv2`
355613382	684557793	1026616680	`ronald2048`
1593342387	2383907058	3716336943	`ronald3072`
3054962349	5991845076	9455902902	`ronald4096`

Secret key	
bytes	system
29	hector
60	ecdonaldp160
63	ecdonaldb163
63	ecdonaldk163
72	ecdonaldp192
84	donald512
84	ecdonaldp224
90	ecdonaldb233
90	ecdonaldk233
96	ecdonaldp256
108	ecdonaldb283
108	ecdonaldk283
144	ecdonaldp384
148	donald1024
156	ecdonaldb409
156	ecdonaldk409
198	ecdonaldp521
216	ecdonaldb571
216	ecdonaldk571
276	donald2048
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096
20107	rainbow

Cycles to sign 59 bytes			
quartile	median	quartile	system
154539	155331	155565	sflashv2
401283	423477	448758	hector
428571	434133	438840	donald512
618381	620568	621630	rainbow
954306	965502	984429	ronald512
1048401	1056735	1063224	donald1024
1442754	1456641	1468350	ecdonaldp192
1505934	1519227	1539648	ecdonaldp160
1907739	1917135	1930518	ronald768
2290599	2313405	2335581	ecdonaldk163
2299743	2320731	2349495	ecdonaldp224
2431233	2454912	2482632	ecdonaldb163
2863323	2881413	2898765	ecdonaldp256
2906379	2924307	2953413	ronald1024
3040641	3053268	3069171	ecdonaldk233
3196026	3215088	3240198	donald2048
3206547	3219849	3253185	ecdonaldb233
6328485	6380397	6474753	ecdonaldp384
6929757	6967935	7035795	ecdonaldk283
7361946	7392942	7430391	ronald1536
7528194	7627356	7686234	ecdonaldb283
7830630	7885170	7928514	ecdonaldp521
13857705	13885992	13928031	ronald2048
14770917	14796720	14821002	ecdonaldk409
16500627	16549101	16583985	ecdonaldb409
33267276	33444180	33650550	ecdonaldk571
37217268	37607121	37681578	ecdonaldb571
39733245	40549950	40887252	ronald3072
81436005	81506610	81571059	ronald4096

Public key	
bytes	system
40	ecdonaldp160
42	ecdonaldb163
42	ecdonaldk163
48	ecdonaldp192
56	ecdonaldp224
60	ecdonaldb233
60	ecdonaldk233
60	hector
64	donald512
64	ecdonaldp256
64	ronald512
72	ecdonaldb283
72	ecdonaldk283
96	ecdonaldp384
96	ronald768
104	ecdonaldb409
104	ecdonaldk409
128	donald1024
128	ronald1024
132	ecdonaldp521
144	ecdonaldb571
144	ecdonaldk571
192	ronald1536
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2
31680	rainbow

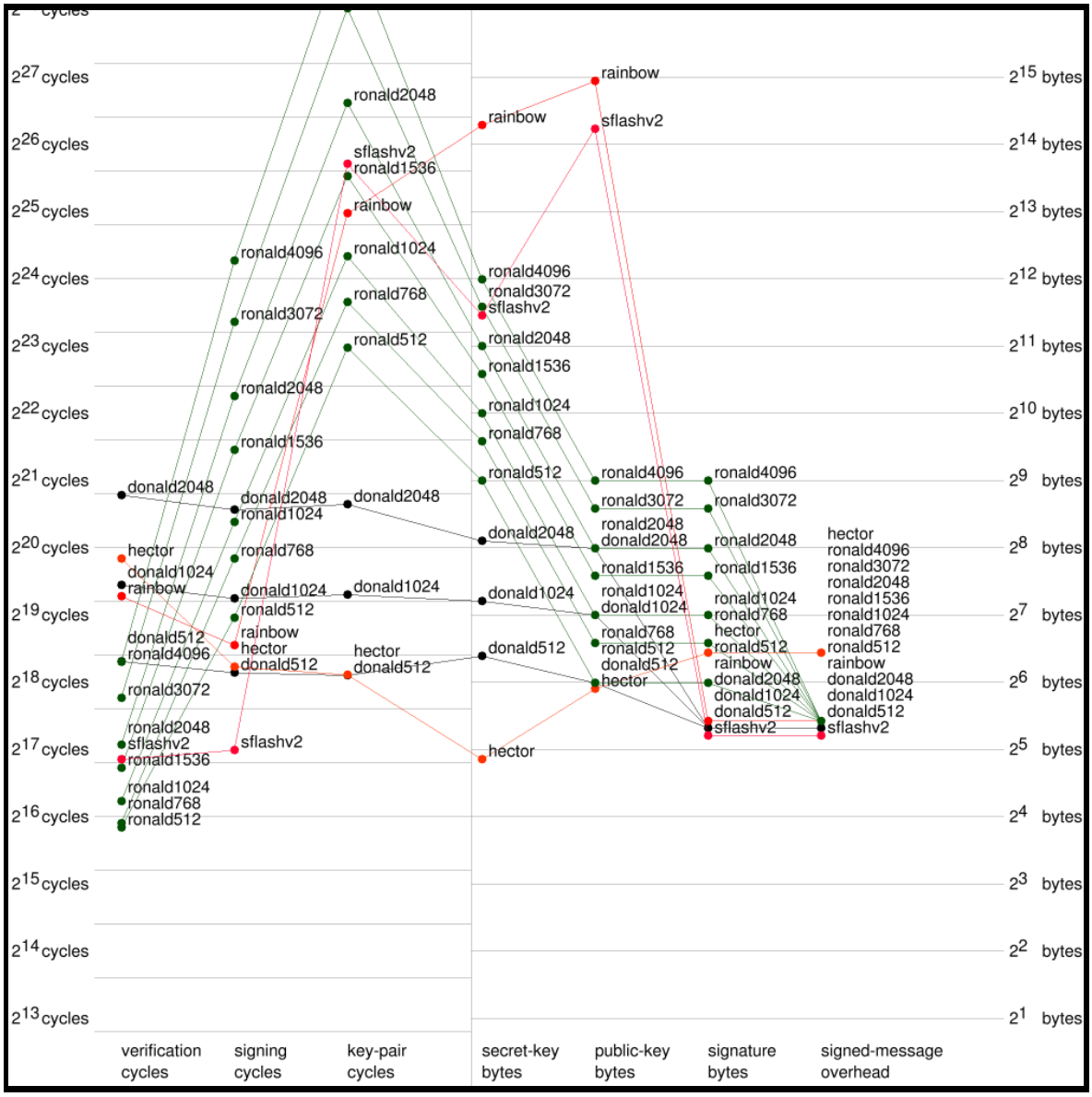
Cycles to verify 59 bytes			
quartile	median	quartile	system
55881	56043	56214	ronald512
57816	58383	58905	ronald768
71883	72423	72819	ronald1024
110583	111177	111609	ronald1536
148689	149139	150174	ronald2048
170019	170127	170658	sflashv2
275733	276516	277371	ronald3072
414396	414882	415611	ronald4096
463545	464121	466380	donald512
1200186	1207935	1224621	donald1024
1227303	1227492	1232415	rainbow
1501434	1502892	1529190	hector
1707390	1724229	1736325	ecdonaldp192
1787337	1800675	1814868	ecdonaldp160
2807514	2826585	2858967	ecdonaldp224
3462417	3471993	3491451	ecdonaldp256
3788928	3863178	3879225	donald2048
4553307	4597740	4727907	ecdonaldk163
4755420	4816188	4858713	ecdonaldb163
5998815	6042492	6066396	ecdonaldk233
6294060	6333993	6500727	ecdonaldb233
7534899	7574139	7672788	ecdonaldp384
9229815	9273645	9331893	ecdonaldp521
13916502	13963068	14043447	ecdonaldk283
14962761	15073074	15215787	ecdonaldb283
29429532	29470554	29552301	ecdonaldk409
32990976	33060618	33114690	ecdonaldb409
66244491	66582594	66903138	ecdonaldk571
74620764	75140622	75290067	ecdonaldb571

Signing 0 bytes	
bytes	system
37	sflashv2
40	donald1024
40	donald2048
40	donald512
40	ecdonaldp160
42	ecdonaldb163
42	ecdonaldk163
43	rainbow
48	ecdonaldp192
56	ecdonaldp224
60	ecdonaldb233
60	ecdonaldk233
64	ecdonaldp256
64	ronald512
72	ecdonaldb283
72	ecdonaldk283
87	hector
96	ecdonaldp384
96	ronald768
104	ecdonaldb409
104	ecdonaldk409
128	ronald1024
132	ecdonaldp521
144	ecdonaldb571
144	ecdonaldk571
192	ronald1536
256	ronald2048
384	ronald3072
512	ronald4096

Signing 23 bytes	
bytes	system
37	sflashv2
40	donald1024
40	donald2048
40	donald512
40	ecdonaldp160
41	ronald512
42	ecdonaldb163
42	ecdonaldk163
43	rainbow
48	ecdonaldp192
56	ecdonaldp224
60	ecdonaldb233
60	ecdonaldk233
64	ecdonaldp256
72	ecdonaldb283
72	ecdonaldk283
73	ronald768
87	hector
96	ecdonaldp384
104	ecdonaldb409
104	ecdonaldk409
105	ronald1024
132	ecdonaldp521
144	ecdonaldb571
144	ecdonaldk571
169	ronald1536
233	ronald2048
361	ronald3072
489	ronald4096

Signing many bytes	
bytes	system
37	sflashv2
40	donald1024
40	donald2048
40	donald512
40	ecdonaldp160
42	ecdonaldb163
42	ecdonaldk163
43	rainbow
43	ronald1024
43	ronald1536
43	ronald2048
43	ronald3072
43	ronald4096
43	ronald512
43	ronald768
48	ecdonaldp192
56	ecdonaldp224
60	ecdonaldb233
60	ecdonaldk233
64	ecdonaldp256
72	ecdonaldb283
72	ecdonaldk283
87	hector
96	ecdonaldp384
104	ecdonaldb409
104	ecdonaldk409
132	ecdonaldp521
144	ecdonaldb571
144	ecdonaldk571

10.4 amd64, 2800MHz, Intel Xeon (f41), `nmi0056`



Cycles to generate a key pair			
quartile	median	quartile	system
808367	811580	819056	donald512
803649	817579	845215	hector
2293039	2297841	2305688	donald1024
7334348	7369901	7405146	donald2048
34029163	55612697	75187784	ronald512
74897277	100022055	160421828	ronald768
108688272	179726820	257942237	ronald1024
307876744	314313300	315661892	rainbow
354638361	506536247	777574693	ronald1536
593088671	593399002	593932423	sflashv2
682371515	1303363215	1819489672	ronald2048
2394171290	4387859665	7045717413	ronald3072
5908123522	11675770127	19685307642	ronald4096

Secret key	
bytes	system
29	hector
84	donald512
148	donald1024
276	donald2048
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096
20107	rainbow

Cycles to sign 59 bytes			
quartile	median	quartile	system
310037	311388	313229	sflashv2
838278	843178	850080	donald512
881531	910987	945133	hector
1198379	1199912	1212631	rainbow
1696660	1708063	1730309	ronald512
2172345	2186667	2206659	donald1024
3643913	3671465	3694698	ronald768
5850089	5882548	5923610	ronald1024
6822683	6862499	6918758	donald2048
14796565	14875980	14973287	ronald1536
29561595	29669304	29762936	ronald2048
77009912	77178255	77358260	ronald3072
170533006	171036250	171504242	ronald4096

Public key	
bytes	system
60	hector
64	donald512
64	ronald512
96	ronald768
128	donald1024
128	ronald1024
192	ronald1536
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2
31680	rainbow

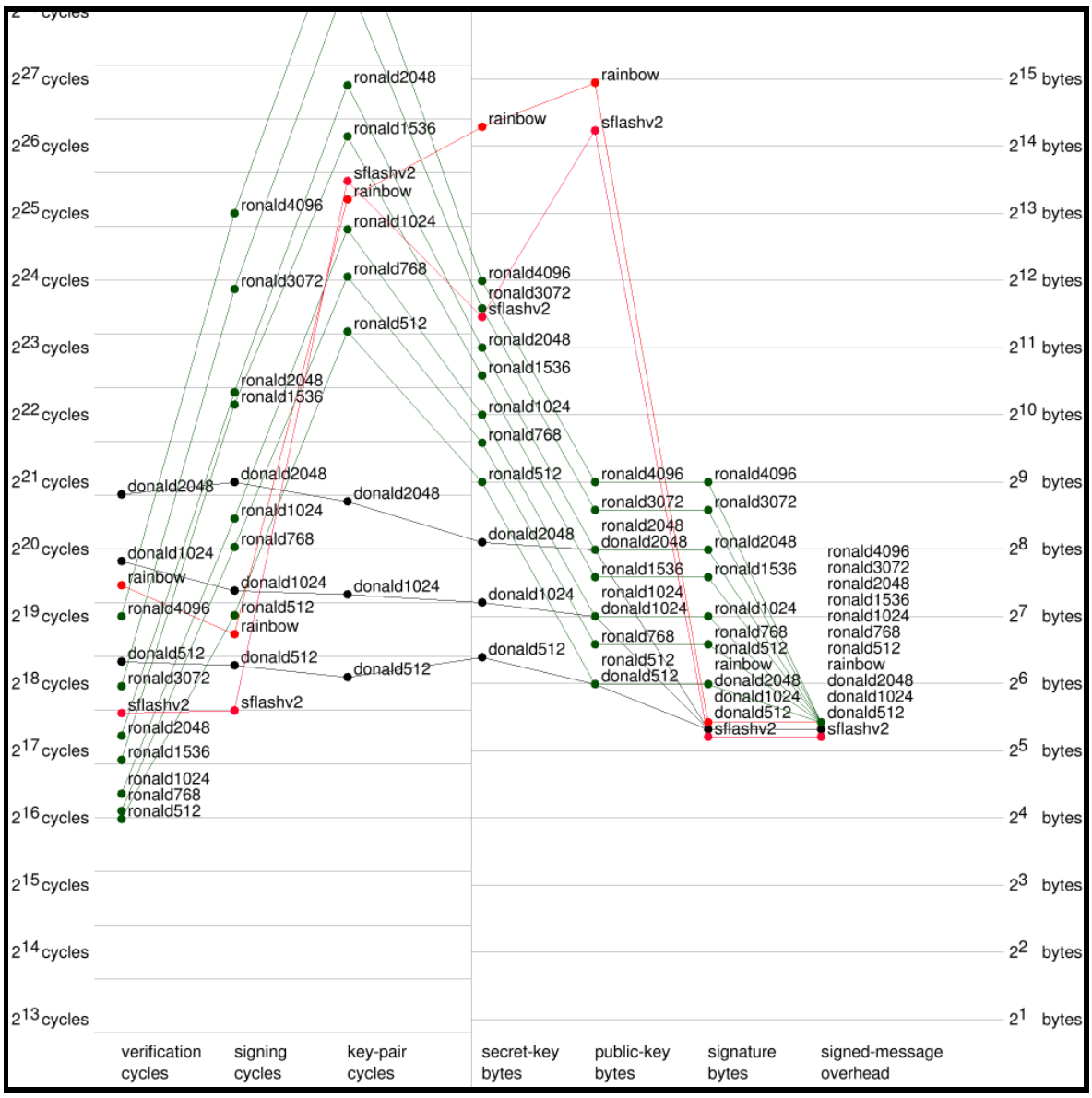
Cycles to verify 59 bytes			
quartile	median	quartile	system
112567	114240	114583	ronald512
120428	121009	124180	ronald768
156072	160881	162288	ronald1024
240702	246883	247975	ronald1536
274750	275590	289989	sflashv2
330309	332570	336154	ronald2048
606851	608580	611289	ronald3072
968485	970823	974610	ronald4096
966791	976528	983633	donald512
2262029	2262932	2264717	rainbow
2564660	2614913	2641156	donald1024
3645285	3656758	3707949	hector
8271235	8327256	8394687	donald2048

Signing 0 bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`rainbow`
64	`ronald512`
87	`hector`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
41	`ronald512`
43	`rainbow`
73	`ronald768`
87	`hector`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`rainbow`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`
87	`hector`

10.5 amd64, 2800MHz, Intel Xeon (f41), nmi0057



Cycles to generate a key pair			
quartile	median	quartile	system
796355	807464	826035	donald512
2326611	2345819	4051257	donald1024
7656201	7813729	13658120	donald2048
46956469	69487467	128813944	ronald512
88479230	141527526	194756758	ronald768
183495277	260773212	414375164	ronald1024
361236932	384832504	438803155	rainbow
464302594	486878917	899809904	sflashv2
463324694	860438285	1379076223	ronald1536
885189816	1665649195	2426478929	ronald2048
4277233233	6544332382	10046124508	ronald3072
11112996440	18024506395	33709340287	ronald4096

Secret key	
bytes	system
84	donald512
148	donald1024
276	donald2048
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096
20107	rainbow

Cycles to sign 59 bytes			
quartile	median	quartile	system
330008	527576	534128	sflashv2
920430	942788	1528380	donald512
1403346	1411914	1430324	rainbow
1770440	1791587	1808793	ronald512
2452394	2470944	4132072	donald1024
3867122	4312693	6300329	ronald768
6197212	6243916	6326943	ronald1024
7813463	10043894	14024745	donald2048
17859919	27143900	27484156	ronald1536
31695209	31833858	44661344	ronald2048
85370040	120852900	146867315	ronald3072
317693334	319732679	321415668	ronald4096

Public key	
bytes	system
64	donald512
64	ronald512
96	ronald768
128	donald1024
128	ronald1024
192	ronald1536
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2
31680	rainbow

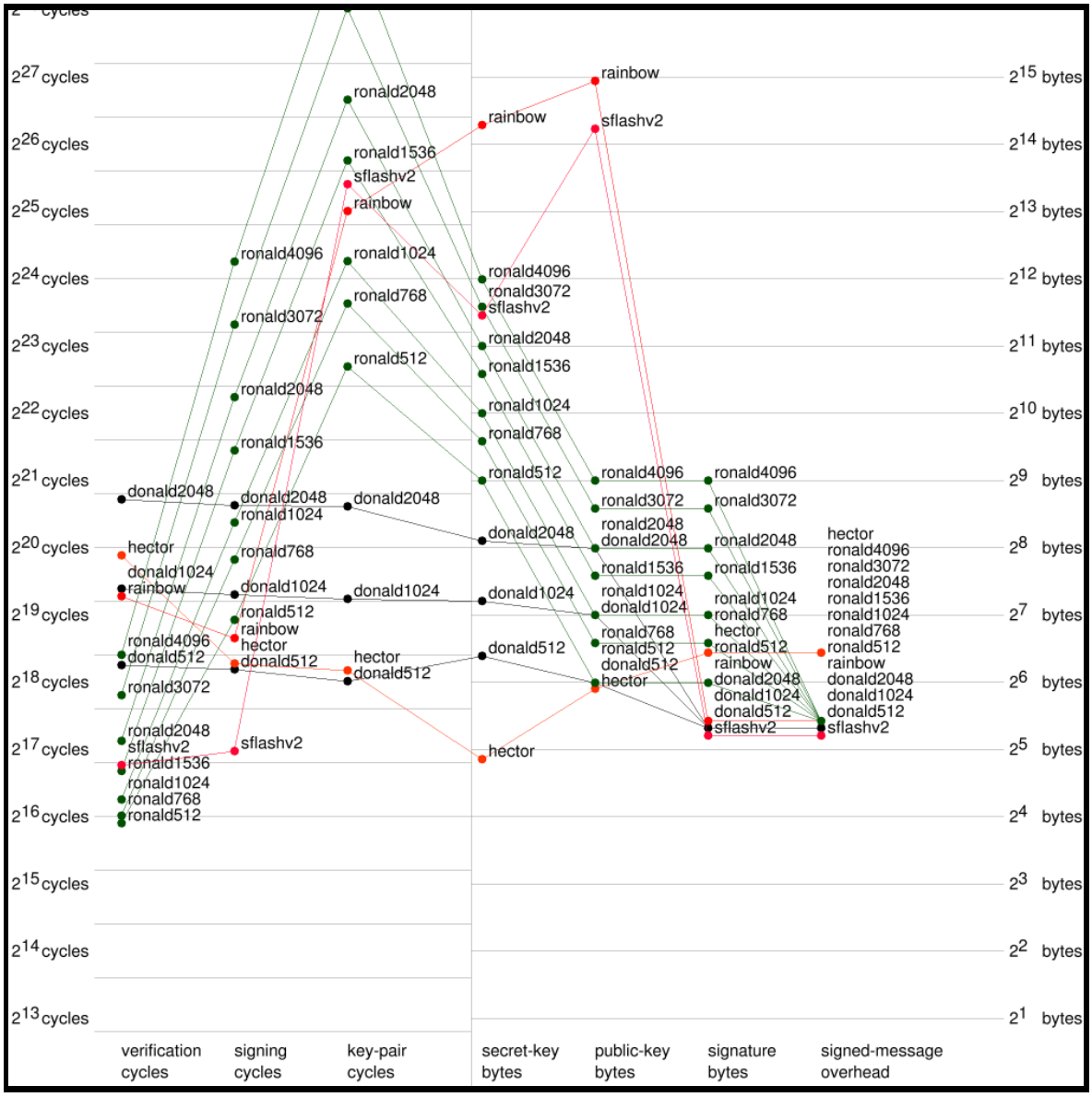
Cycles to verify 59 bytes			
quartile	median	quartile	system
127960	129766	131257	ronald512
137809	144193	245154	ronald768
174951	179641	183295	ronald1024
261681	277403	460915	ronald1536
373611	379435	405685	ronald2048
296289	509250	519456	sflashv2
707378	716394	1231762	ronald3072
972685	990668	1025780	donald512
1125908	1773562	1799707	ronald4096
2635577	2642129	2654603	rainbow
2671004	3608745	4482184	donald1024
8409625	8555155	10570882	donald2048

Signing 0 bytes	
bytes	system
37	sflashv2
40	donald1024
40	donald2048
40	donald512
43	rainbow
64	ronald512
96	ronald768
128	ronald1024
192	ronald1536
256	ronald2048
384	ronald3072
512	ronald4096

Signing 23 bytes	
bytes	system
37	sflashv2
40	donald1024
40	donald2048
40	donald512
41	ronald512
43	rainbow
73	ronald768
105	ronald1024
169	ronald1536
233	ronald2048
361	ronald3072
489	ronald4096

Signing many bytes	
bytes	system
37	sflashv2
40	donald1024
40	donald2048
40	donald512
43	rainbow
43	ronald1024
43	ronald1536
43	ronald2048
43	ronald3072
43	ronald4096
43	ronald512
43	ronald768

10.6 amd64, 2800MHz, Intel Xeon (f41), `nmi0063`



Cycles to generate a key pair			
quartile	median	quartile	system
751828	756861	762895	donald512
842051	864759	899010	hector
2165527	2174522	2180087	donald1024
7130368	7159859	7167524	donald2048
30121217	43495284	63347438	ronald512
61222518	97686330	152884830	ronald768
104667206	169042699	310918524	ronald1024
320379122	323353772	325106572	rainbow
454662376	454788544	454988156	sflashv2
358412803	618280257	866782903	ronald1536
786808134	1352529136	1974696451	ronald2048
2509481737	4394433330	6649833183	ronald3072
8602203036	12509658978	17886785696	ronald4096

Secret key	
bytes	system
29	hector
84	donald512
148	donald1024
276	donald2048
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096
20107	rainbow

Cycles to sign 59 bytes			
quartile	median	quartile	system
305900	307391	310968	sflashv2
873019	880747	886053	donald512
923650	949851	995722	hector
1305150	1311156	1317428	rainbow
1656291	1665965	1680672	ronald512
2283841	2295356	2302146	donald1024
3606603	3625671	3651284	ronald768
5781874	5811421	5837881	ronald1024
7257712	7287532	7298095	donald2048
14767060	14807723	14892388	ronald1536
29325849	29392503	29452360	ronald2048
74786614	74907357	75058228	ronald3072
167570326	167777820	168238651	ronald4096

Public key	
bytes	system
60	hector
64	donald512
64	ronald512
96	ronald768
128	donald1024
128	ronald1024
192	ronald1536
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2
31680	rainbow

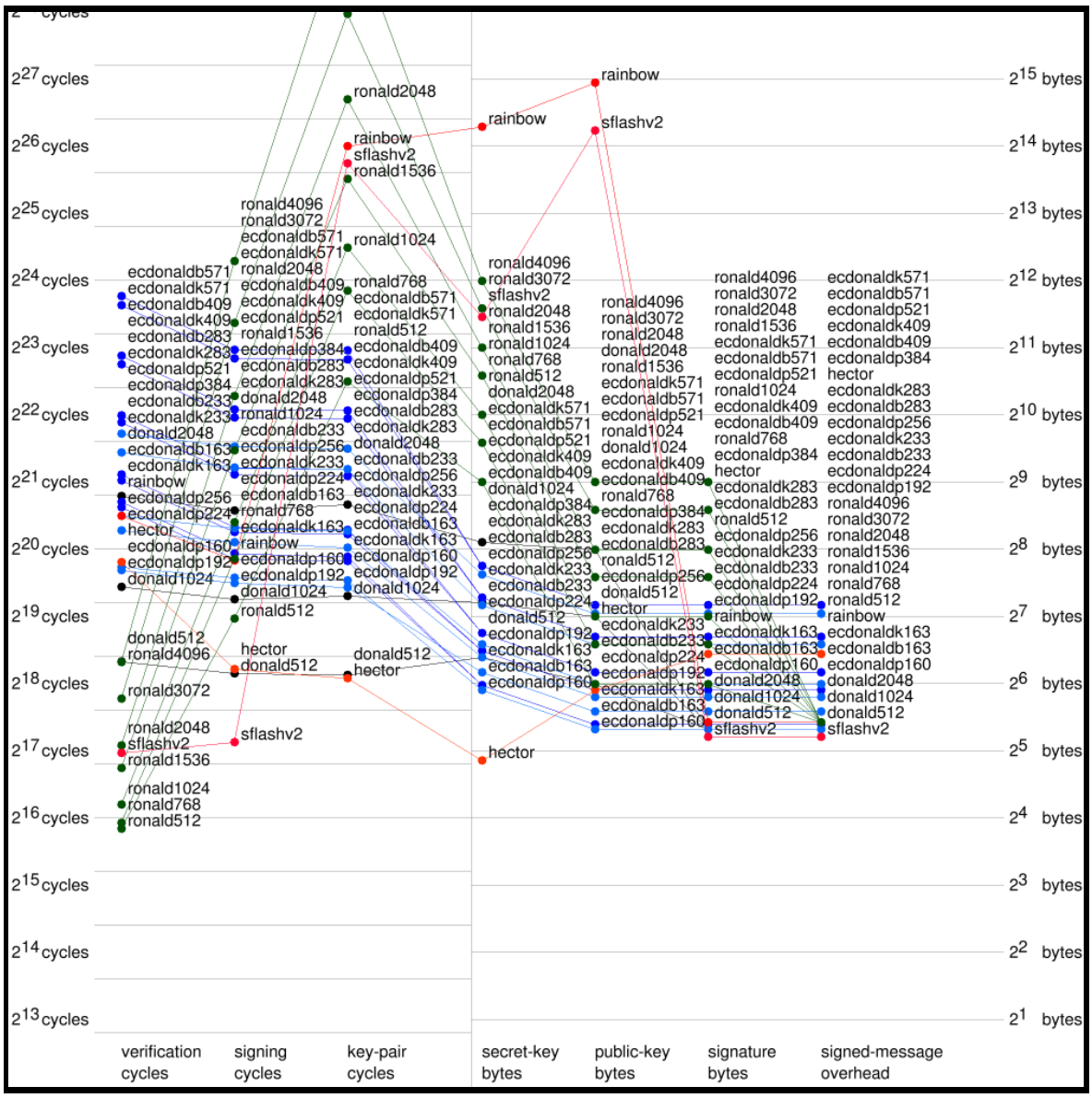
Cycles to verify 59 bytes			
quartile	median	quartile	system
120043	121191	122017	ronald512
127624	133231	135275	ronald768
162568	164143	167538	ronald1024
233751	237839	241465	ronald1536
253330	255045	257096	sflashv2
347144	349041	351092	ronald2048
625660	629769	638449	ronald3072
919023	925939	933814	donald512
1056447	1060087	1063888	ronald4096
2234862	2256212	2268315	rainbow
2459275	2478714	2499084	donald1024
3807853	3823757	3879288	hector
7806925	7829563	7856534	donald2048

Signing 0 bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`rainbow`
64	`ronald512`
87	`hector`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
41	`ronald512`
43	`rainbow`
73	`ronald768`
87	`hector`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`rainbow`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`
87	`hector`

10.7 amd64, 3000MHz, Intel Pentium D (f64), speed



Cycles to generate a key pair			
quartile	median	quartile	system
793260	796800	835350	`hector`
821355	828510	834045	`donald512`
2290380	2299500	2304390	`donald1024`
2552175	2577660	2592555	`ecdonaldp192`
2781030	2823240	2912850	`ecdonaldp160`
3562575	3603585	3629895	`ecdonaldk163`
3800130	3817875	3835350	`ecdonaldb163`
4260900	4305810	4375380	`ecdonaldp224`
5073315	5113365	5140290	`ecdonaldk233`
5274690	5310510	5372250	`ecdonaldp256`
5353395	5399265	5566335	`ecdonaldb233`
7451595	7479270	7585440	`donald2048`
10761675	10825665	10880175	`ecdonaldk283`
11747175	11785050	11860245	`ecdonaldb283`
11710815	11804415	11906055	`ecdonaldp384`
15313245	15373695	15510645	`ecdonaldp521`
22595730	22652910	22755840	`ecdonaldk409`
25169880	25253460	25336680	`ecdonaldb409`
26244735	36536790	58934730	`ronald512`
48478680	48617400	48735390	`ecdonaldk571`
54417345	54548805	54708345	`ecdonaldb571`
72235440	118448490	157961265	`ronald768`
122987220	205899510	306236445	`ronald1024`
365456805	499435740	841747890	`ronald1536`
603805470	609534645	614894505	`sflashv2`
750905145	760277400	761911140	`rainbow`
973360665	1393226415	2375945535	`ronald2048`
2947073805	4197513300	7206882900	`ronald3072`
9503456220	14957181465	21916229670	`ronald4096`

Secret key	
bytes	system
29	hector
60	ecdonaldp160
63	ecdonaldb163
63	ecdonaldk163
72	ecdonaldp192
84	donald512
84	ecdonaldp224
90	ecdonaldb233
90	ecdonaldk233
96	ecdonaldp256
108	ecdonaldb283
108	ecdonaldk283
144	ecdonaldp384
148	donald1024
156	ecdonaldb409
156	ecdonaldk409
198	ecdonaldp521
216	ecdonaldb571
216	ecdonaldk571
276	donald2048
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096
20107	rainbow

Cycles to sign 59 bytes			
quartile	median	quartile	system
347415	348525	350430	sflashv2
844365	848955	854130	donald512
865320	895170	930600	hector
1706715	1723560	1747530	ronald512
2195160	2209170	2245440	donald1024
2703750	2727330	2751630	ecdonaldp192
2874585	2909850	2941500	ecdonaldp160
3630375	3650205	3677115	rainbow
3687645	3704985	3726075	ecdonaldk163
3695565	3725610	3804795	ronald768
3941430	3969555	3991485	ecdonaldb163
4524600	4612545	4678200	ecdonaldp224
5200590	5238810	5284920	ecdonaldk233
5462175	5513280	5553090	ecdonaldp256
5548845	5609745	5651610	ecdonaldb233
5920200	5953110	5997525	ronald1024
6881010	6934650	6991515	donald2048
10963620	11045130	11085165	ecdonaldk283
11960265	12009870	12197400	ecdonaldb283
11945115	12034875	12138960	ecdonaldp384
14962350	15023655	15085005	ronald1536
15664755	15776775	15893235	ecdonaldp521
22932585	23056245	23530410	ecdonaldk409
25520550	25601100	25665030	ecdonaldb409
30193365	30287535	30376080	ronald2048
49002690	49155480	49242120	ecdonaldk571
54847365	55022985	55152615	ecdonaldb571
77807175	78014250	78429135	ronald3072
172439760	173037945	173542065	ronald4096

Public key	
bytes	system
40	ecdonaldp160
42	ecdonaldb163
42	ecdonaldk163
48	ecdonaldp192
56	ecdonaldp224
60	ecdonaldb233
60	ecdonaldk233
60	hector
64	donald512
64	ecdonaldp256
64	ronald512
72	ecdonaldb283
72	ecdonaldk283
96	ecdonaldp384
96	ronald768
104	ecdonaldb409
104	ecdonaldk409
128	donald1024
128	ronald1024
132	ecdonaldp521
144	ecdonaldb571
144	ecdonaldk571
192	ronald1536
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2
31680	rainbow

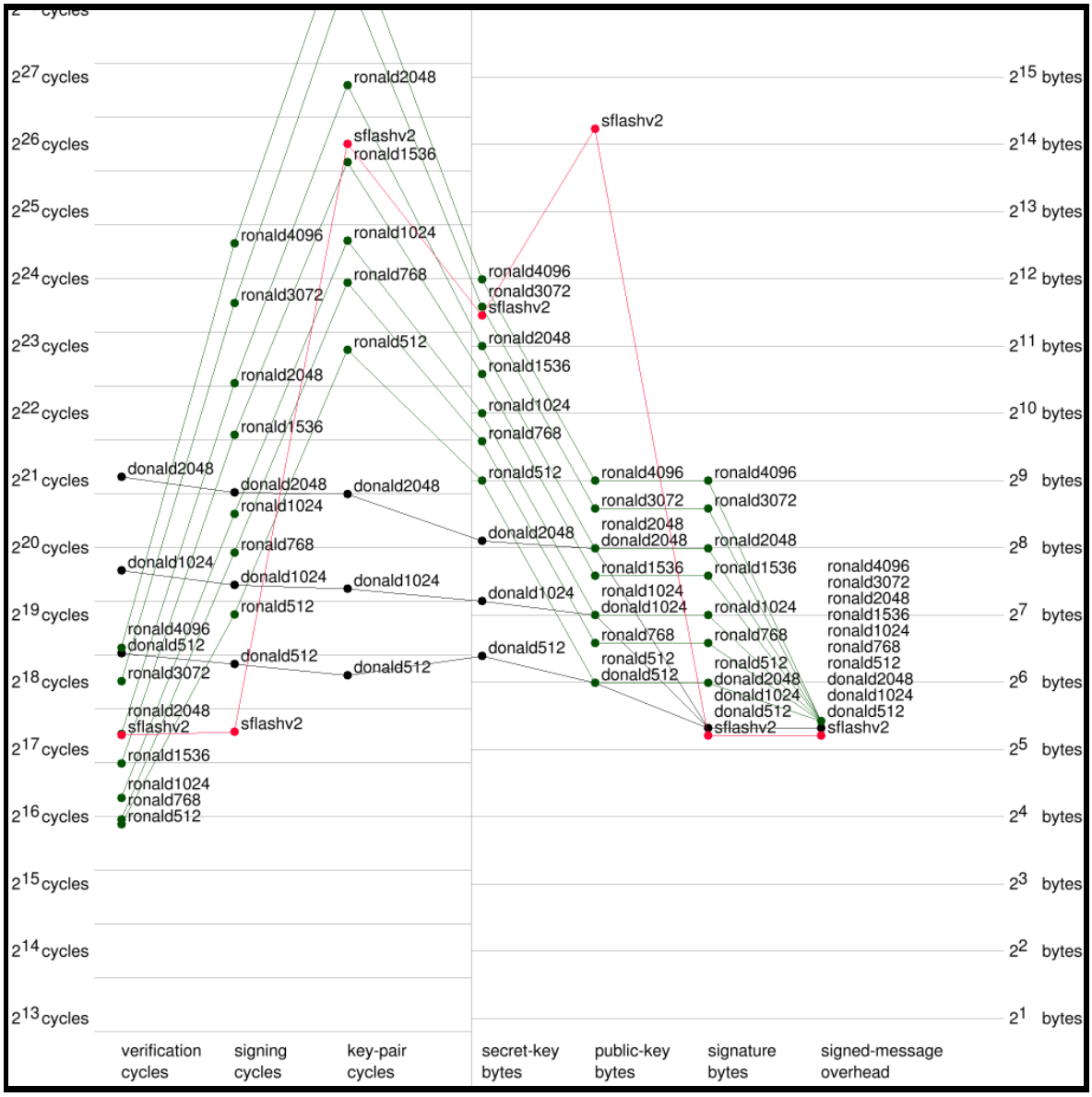
Cycles to verify 59 bytes			
quartile	median	quartile	system
113460	114270	114900	ronald512
122460	123180	124455	ronald768
154935	156480	157605	ronald1024
249930	251025	252495	ronald1536
281430	303840	315015	sflashv2
332625	334680	336315	ronald2048
609960	612990	615045	ronald3072
981075	985035	988560	ronald4096
983640	988020	994095	donald512
2567700	2582685	2592420	donald1024
3173295	3203460	3224490	ecdonaldp192
3330825	3358500	3433365	ecdonaldp160
3563610	3573195	3632565	hector
5314275	5356380	5470395	ecdonaldp224
6445665	6451305	6455325	rainbow
6438855	6476550	6560370	ecdonaldp256
7198350	7227480	7282770	ecdonaldk163
7722735	7761765	7814925	ecdonaldb163
8313150	8336565	8356710	donald2048
10191960	10235910	10331430	ecdonaldk233
10995975	11050500	11190195	ecdonaldb233
14580030	14629485	14773740	ecdonaldp384
18584250	18697455	18808245	ecdonaldp521
21398895	21552240	21875685	ecdonaldk283
23590455	23650410	23776200	ecdonaldb283
45533415	45708795	45939735	ecdonaldk409
50819040	50953455	51105885	ecdonaldb409
97977975	98177655	98581875	ecdonaldk571
109902000	110181150	112366305	ecdonaldb571

Signing 0 bytes	
bytes	system
37	sflashv2
40	donald1024
40	donald2048
40	donald512
40	ecdonaldp160
42	ecdonaldb163
42	ecdonaldk163
43	rainbow
48	ecdonaldp192
56	ecdonaldp224
60	ecdonaldb233
60	ecdonaldk233
64	ecdonaldp256
64	ronald512
72	ecdonaldb283
72	ecdonaldk283
87	hector
96	ecdonaldp384
96	ronald768
104	ecdonaldb409
104	ecdonaldk409
128	ronald1024
132	ecdonaldp521
144	ecdonaldb571
144	ecdonaldk571
192	ronald1536
256	ronald2048
384	ronald3072
512	ronald4096

Signing 23 bytes	
bytes	system
37	sflashv2
40	donald1024
40	donald2048
40	donald512
40	ecdonaldp160
41	ronald512
42	ecdonaldb163
42	ecdonaldk163
43	rainbow
48	ecdonaldp192
56	ecdonaldp224
60	ecdonaldb233
60	ecdonaldk233
64	ecdonaldp256
72	ecdonaldb283
72	ecdonaldk283
73	ronald768
87	hector
96	ecdonaldp384
104	ecdonaldb409
104	ecdonaldk409
105	ronald1024
132	ecdonaldp521
144	ecdonaldb571
144	ecdonaldk571
169	ronald1536
233	ronald2048
361	ronald3072
489	ronald4096

Signing many bytes	
bytes	system
37	sflashv2
40	donald1024
40	donald2048
40	donald512
40	ecdonaldp160
42	ecdonaldb163
42	ecdonaldk163
43	rainbow
43	ronald1024
43	ronald1536
43	ronald2048
43	ronald3072
43	ronald4096
43	ronald512
43	ronald768
48	ecdonaldp192
56	ecdonaldp224
60	ecdonaldb233
60	ecdonaldk233
64	ecdonaldp256
72	ecdonaldb283
72	ecdonaldk283
87	hector
96	ecdonaldp384
104	ecdonaldb409
104	ecdonaldk409
132	ecdonaldp521
144	ecdonaldb571
144	ecdonaldk571

10.8 amd64, 3000MHz, Intel Xeon (f4a), `nmi0090`



Cycles to generate a key pair			
quartile	median	quartile	system
808650	814718	819810	donald512
2458200	2477228	2497012	donald1024
8364660	8427195	8510310	donald2048
36499342	54037380	71924340	ronald512
89903183	128475660	179601127	ronald768
131967855	220382543	317897790	ronald1024
335724585	604400250	1027763618	ronald1536
764556067	764953335	765614205	sflashv2
881047822	1637841855	2441384235	ronald2048
4149239422	6769777800	10148544375	ronald3072
7248114698	14067979020	24386016825	ronald4096

Secret key	
bytes	system
84	donald512
148	donald1024
276	donald2048
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096

Cycles to sign 59 bytes			
quartile	median	quartile	system
392310	393630	396600	sflashv2
934995	939720	949980	donald512
1777785	1787610	1808085	ronald512
2586060	2612063	2633655	donald1024
3941078	3956693	3977985	ronald768
6474825	6499537	6537195	ronald1024
8527252	8616090	8688233	donald2048
17921918	17987610	18048068	ronald1536
35009962	35055450	35137748	ronald2048
98290590	98387017	98468078	ronald3072
211899900	212330662	212807820	ronald4096

Public key	
bytes	system
64	donald512
64	ronald512
96	ronald768
128	donald1024
128	ronald1024
192	ronald1536
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2

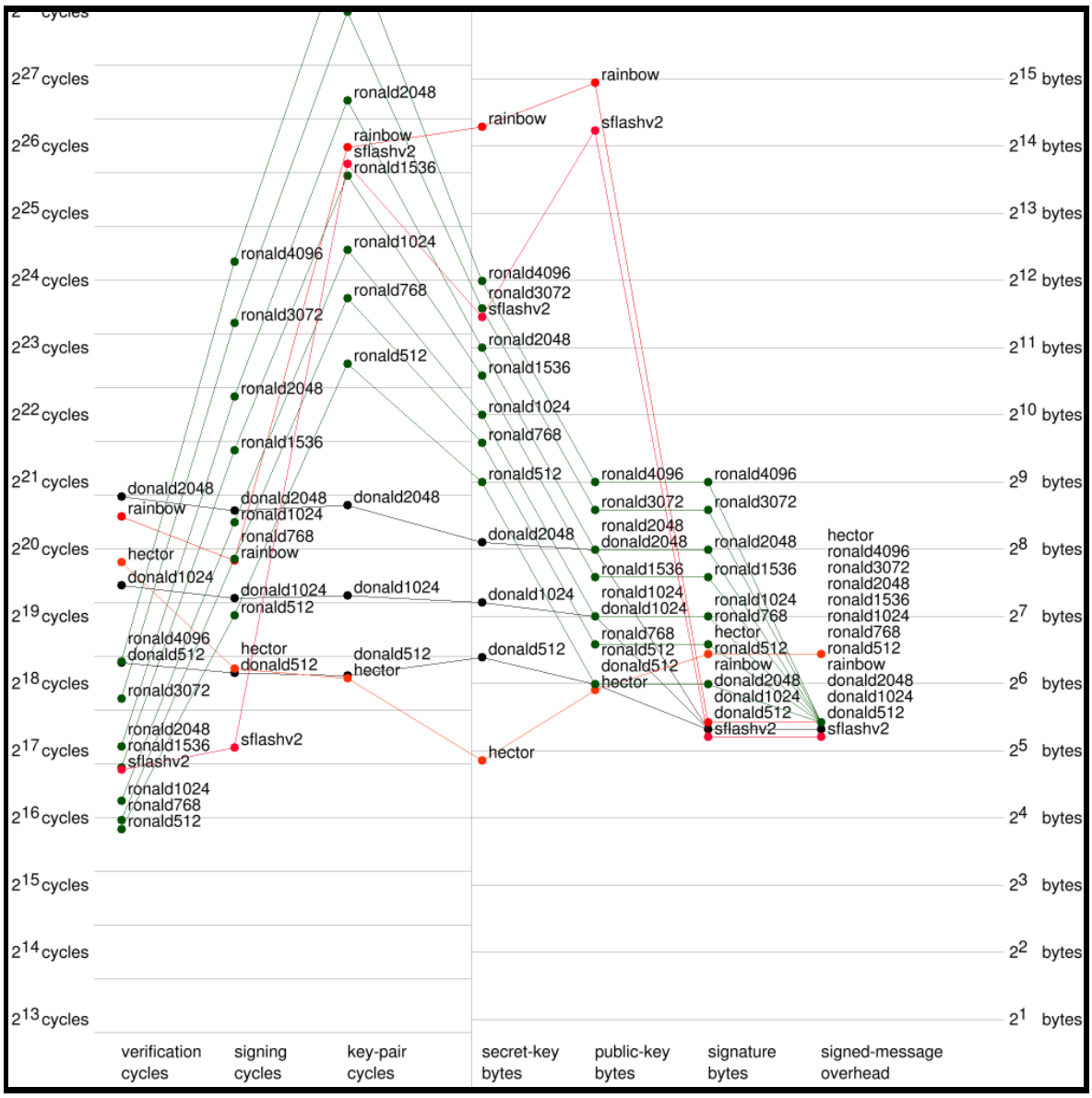
Cycles to verify 59 bytes			
quartile	median	quartile	system
118320	119377	121403	ronald512
124958	127372	132712	ronald768
166237	167985	171105	ronald1024
259642	262095	266018	ronald1536
375210	376350	377535	sflashv2
379162	382088	384517	ronald2048
749902	752288	754642	ronald3072
1072575	1080232	1102178	donald512
1157347	1160497	1163558	ronald4096
3129683	3137085	3204660	donald1024
10351890	10493505	10507162	donald2048

Signing 0 bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
41	`ronald512`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.9 amd64, 3392MHz, Intel Pentium D (f64), nmi0104



Cycles to generate a key pair			
quartile	median	quartile	system
794274	796467	829209	`hector`
821219	825044	828189	`donald512`
2311983	2317644	2324223	`donald1024`
7398434	7413054	7427436	`donald2048`
34308839	46131591	62690662	`ronald512`
74186997	107134680	160729305	`ronald768`
138206634	199851677	294243344	`ronald1024`
308011202	521419359	927070214	`ronald1536`
606320334	606503526	606790520	`sflashv2`
750971838	751456287	752257701	`rainbow`
761807383	1368755731	2204295837	`ronald2048`
2336193176	4319205011	6489504673	`ronald3072`
7364015460	12037323484	19812321390	`ronald4096`

Secret key	
bytes	system
29	`hector`
84	`donald512`
148	`donald1024`
276	`donald2048`
512	`ronald512`
768	`ronald768`
1024	`ronald1024`
1536	`ronald1536`
2048	`ronald2048`
2823	`sflashv2`
3072	`ronald3072`
4096	`ronald4096`
20107	`rainbow`

Cycles to sign 59 bytes			
quartile	median	quartile	system
324190	325822	327114	`sflashv2`
845342	853230	859214	`donald512`
869873	900541	934745	`hector`
1770873	1792055	1808205	`ronald512`
2230264	2245496	2262547	`donald1024`
3617362	3636249	3649050	`rainbow`
3687062	3707241	3742312	`ronald768`
5908282	5948776	5985700	`ronald1024`
6885748	6919391	6975168	`donald2048`
15009708	15080326	15144399	`ronald1536`
30060743	30158850	30266086	`ronald2048`
77649268	77927983	78175163	`ronald3072`
171568726	171926423	172793083	`ronald4096`

Public key	
bytes	system
60	`hector`
64	`donald512`
64	`ronald512`
96	`ronald768`
128	`donald1024`
128	`ronald1024`
192	`ronald1536`
256	`donald2048`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
19266	`sflashv2`
31680	`rainbow`

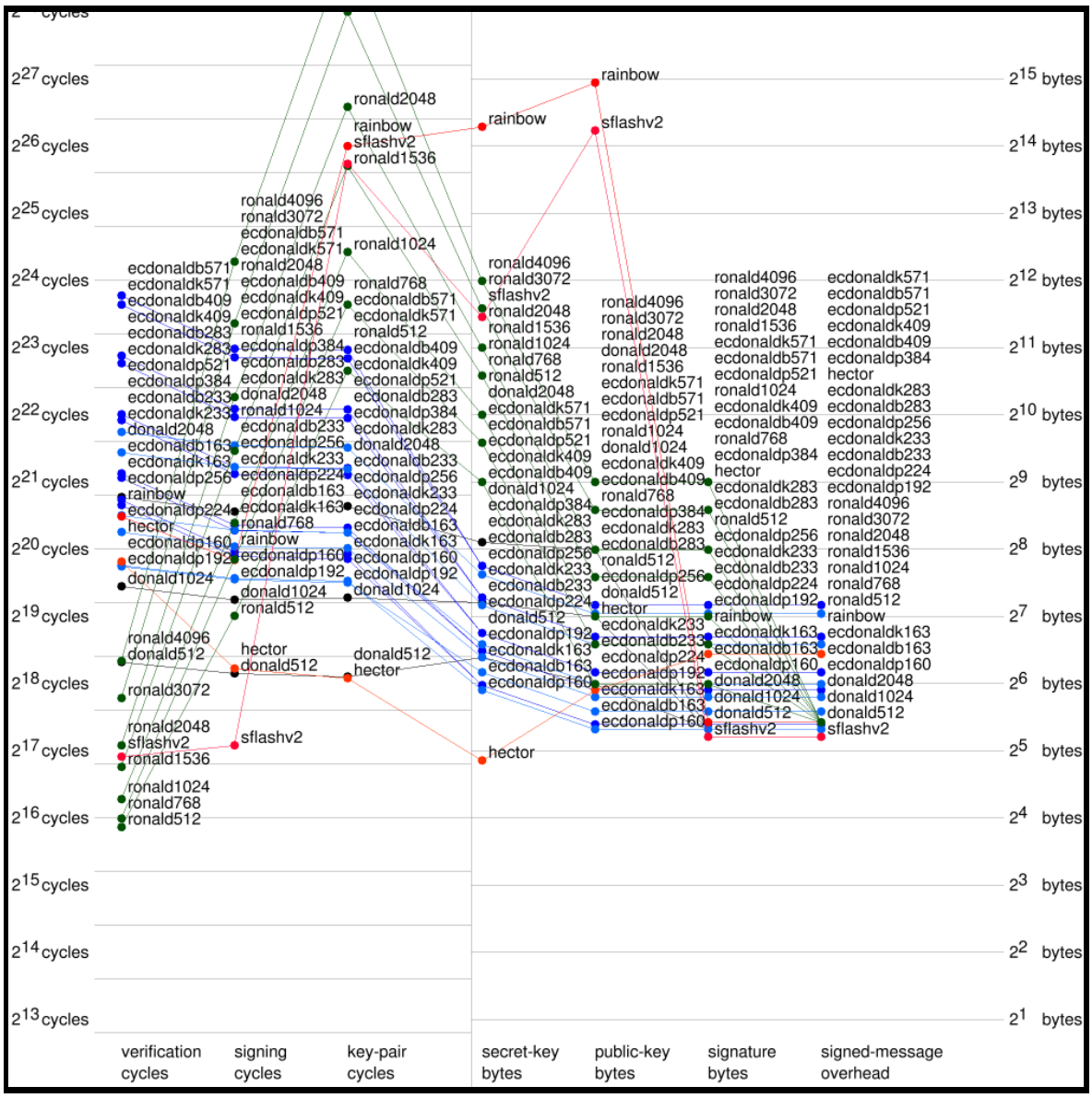
Cycles to verify 59 bytes			
quartile	median	quartile	system
112574	113577	116263	`ronald512`
126939	127789	129183	`ronald768`
163693	164220	164951	`ronald1024`
244766	245412	246534	`sflashv2`
251770	253147	255884	`ronald1536`
328525	330463	336923	`ronald2048`
611218	613088	614822	`ronald3072`
971975	977925	988720	`donald512`
984011	986442	988448	`ronald4096`
2593435	2650436	2662336	`donald1024`
3556553	3559817	3621646	`hector`
6422226	6430981	6440042	`rainbow`
8273526	8298414	8321925	`donald2048`

Signing 0 bytes	
bytes	system
37	sflashv2
40	donald1024
40	donald2048
40	donald512
43	rainbow
64	ronald512
87	hector
96	ronald768
128	ronald1024
192	ronald1536
256	ronald2048
384	ronald3072
512	ronald4096

Signing 23 bytes	
bytes	system
37	sflashv2
40	donald1024
40	donald2048
40	donald512
41	ronald512
43	rainbow
73	ronald768
87	hector
105	ronald1024
169	ronald1536
233	ronald2048
361	ronald3072
489	ronald4096

Signing many bytes	
bytes	system
37	sflashv2
40	donald1024
40	donald2048
40	donald512
43	rainbow
43	ronald1024
43	ronald1536
43	ronald2048
43	ronald3072
43	ronald4096
43	ronald512
43	ronald768
87	hector

10.10 amd64, 3392MHz, Intel Pentium D (f64), `nmi0161`



Cycles to generate a key pair			
quartile	median	quartile	system
793322	796756	838474	hector
810118	812855	818533	donald512
2249474	2257413	2263193	donald1024
2701453	2730710	2750685	ecdonaldp192
2764540	2795157	2824720	ecdonaldp160
3689323	3719532	3742091	ecdonaldk163
3928360	3964944	3991481	ecdonaldb163
4209965	4261441	4329033	ecdonaldp224
5176262	5212880	5251810	ecdonaldk233
5174137	5228486	5273434	ecdonaldp256
5514494	5543989	5572702	ecdonaldb233
7311173	7327867	7343541	donald2048
10879031	10932768	11013620	ecdonaldk283
11720361	11834618	11949096	ecdonaldp384
11909571	12002323	12116155	ecdonaldb283
15471785	15600220	15700010	ecdonaldp521
22811416	22913008	22996597	ecdonaldk409
25459863	25582501	25680081	ecdonaldb409
29353883	42051710	60672014	ronald512
49223092	49400555	49516053	ecdonaldk571
55035154	55146402	55324052	ecdonaldb571
62921760	98254356	155857802	ronald768
122064930	193863274	279344884	ronald1024
344964340	588792841	970523132	ronald1536
604188160	604392568	604640955	sflashv2
759467979	761585142	765891973	rainbow
879376238	1265123935	2019421041	ronald2048
2230576630	4310843000	6672027043	ronald3072
5928946503	10327745973	21416410467	ronald4096

Secret key	
bytes	system
29	`hector`
60	`ecdonaldp160`
63	`ecdonaldb163`
63	`ecdonaldk163`
72	`ecdonaldp192`
84	`donald512`
84	`ecdonaldp224`
90	`ecdonaldb233`
90	`ecdonaldk233`
96	`ecdonaldp256`
108	`ecdonaldb283`
108	`ecdonaldk283`
144	`ecdonaldp384`
148	`donald1024`
156	`ecdonaldb409`
156	`ecdonaldk409`
198	`ecdonaldp521`
216	`ecdonaldb571`
216	`ecdonaldk571`
276	`donald2048`
512	`ronald512`
768	`ronald768`
1024	`ronald1024`
1536	`ronald1536`
2048	`ronald2048`
2823	`sflashv2`
3072	`ronald3072`
4096	`ronald4096`
20107	`rainbow`

Cycles to sign 59 bytes			
quartile	median	quartile	system
332792	334254	335495	`sflashv2`
842231	848300	860149	`donald512`
873086	904961	938315	`hector`
1745441	1776177	1844840	`ronald512`
2177836	2191963	2204407	`donald1024`
2826726	2854895	2876723	`ecdonaldp192`
2860607	2891445	2931344	`ecdonaldp160`
3647469	3664843	3680891	`rainbow`
3677355	3698826	3731925	`ronald768`
3809275	3846233	3889566	`ecdonaldk163`
4017780	4053548	4073081	`ecdonaldb163`
4325072	4354329	4417671	`ecdonaldp224`
5319844	5351702	5389544	`ecdonaldk233`
5350019	5394593	5449214	`ecdonaldp256`
5726467	5752936	5795538	`ecdonaldb233`
5901414	5926795	5952397	`ronald1024`
6799507	6840749	6874936	`donald2048`
11038491	11124766	11211398	`ecdonaldk283`
12017317	12157312	12249826	`ecdonaldp384`
12146976	12190972	12268441	`ecdonaldb283`
14858357	14921648	14988390	`ronald1536`
15986409	16056483	16138168	`ecdonaldp521`
23160222	23231061	23286855	`ecdonaldk409`
25690757	25764843	25866588	`ecdonaldb409`
29869833	29928653	30030517	`ronald2048`
49684693	49872322	50043189	`ecdonaldk571`
55508383	55688175	55840750	`ecdonaldb571`
77294750	77434575	77634019	`ronald3072`
171118600	171470908	171769989	`ronald4096`

Public key	
bytes	system
40	ecdonaldp160
42	ecdonaldb163
42	ecdonaldk163
48	ecdonaldp192
56	ecdonaldp224
60	ecdonaldb233
60	ecdonaldk233
60	hector
64	donald512
64	ecdonaldp256
64	ronald512
72	ecdonaldb283
72	ecdonaldk283
96	ecdonaldp384
96	ronald768
104	ecdonaldb409
104	ecdonaldk409
128	donald1024
128	ronald1024
132	ecdonaldp521
144	ecdonaldb571
144	ecdonaldk571
192	ronald1536
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2
31680	rainbow

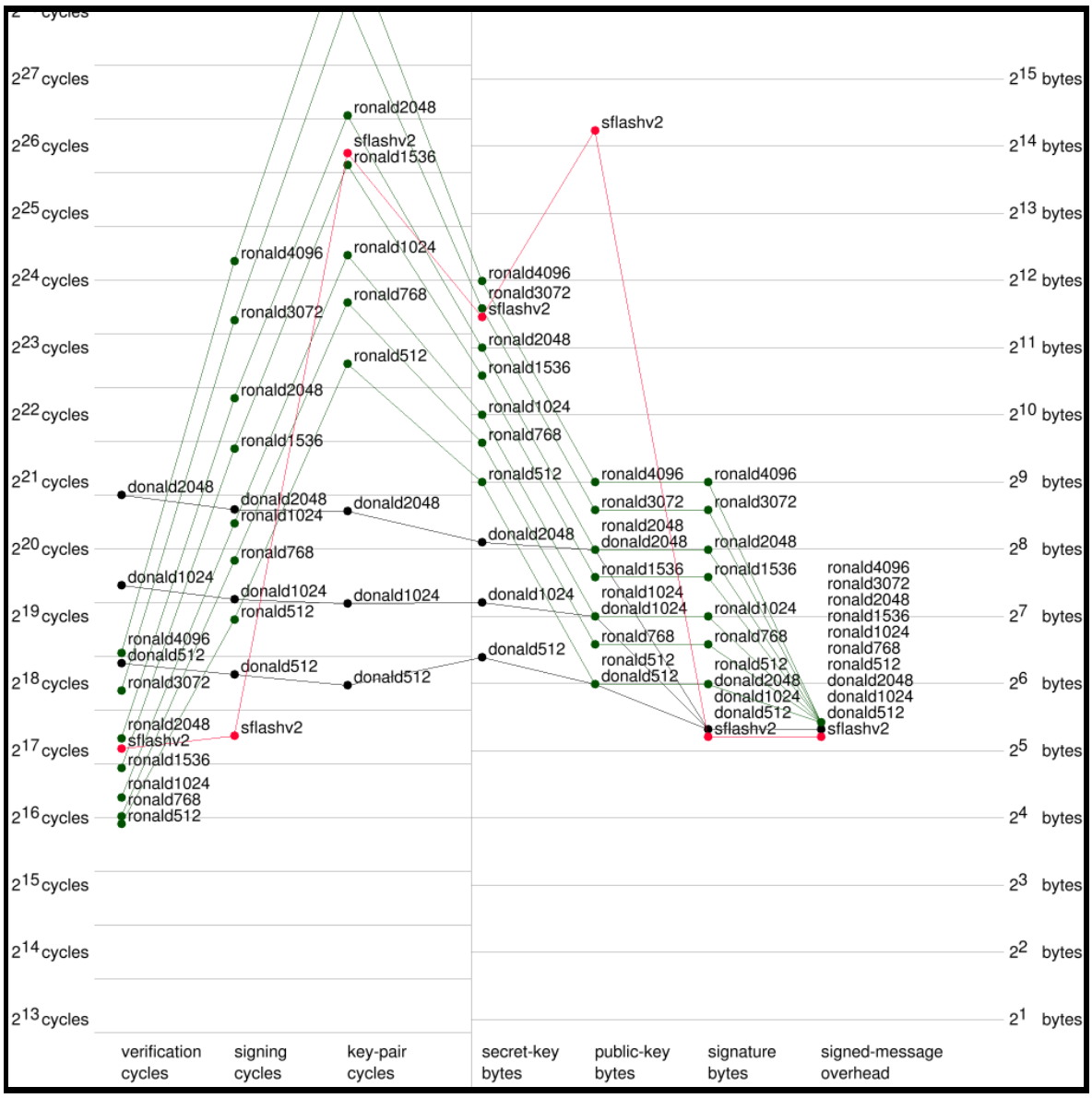
Cycles to verify 59 bytes			
quartile	median	quartile	system
113951	116977	118014	ronald512
127585	130407	131036	ronald768
165580	167620	169745	ronald1024
252297	253810	255578	ronald1536
288796	290258	292604	sflashv2
335257	336226	337688	ronald2048
615060	617508	620007	ronald3072
971329	978673	985252	donald512
997356	998750	1002779	ronald4096
2551700	2600388	2633283	donald1024
3335842	3362345	3412784	ecdonaldp192
3397620	3416932	3444846	ecdonaldp160
3586286	3591777	3653096	hector
5169649	5259800	5370555	ecdonaldp224
6433701	6442847	6446740	rainbow
6450922	6502942	6558532	ecdonaldp256
7366338	7418783	7487565	ecdonaldk163
7928800	7964755	7987467	ecdonaldb163
8098613	8234358	8261167	donald2048
10465591	10551832	10729397	ecdonaldk233
11118459	11190811	11294256	ecdonaldb233
14549654	14612112	14666597	ecdonaldp384
18833926	19021113	19128672	ecdonaldp521
22021426	22154876	22293120	ecdonaldk283
23932600	24014999	24200044	ecdonaldb283
46061109	46195290	46387798	ecdonaldk409
50925081	51087669	51191777	ecdonaldb409
98568975	98841230	99081474	ecdonaldk571
110319698	110558072	110786943	ecdonaldb571

Signing 0 bytes	
bytes	system
37	sflashv2
40	donald1024
40	donald2048
40	donald512
40	ecdonaldp160
42	ecdonaldb163
42	ecdonaldk163
43	rainbow
48	ecdonaldp192
56	ecdonaldp224
60	ecdonaldb233
60	ecdonaldk233
64	ecdonaldp256
64	ronald512
72	ecdonaldb283
72	ecdonaldk283
87	hector
96	ecdonaldp384
96	ronald768
104	ecdonaldb409
104	ecdonaldk409
128	ronald1024
132	ecdonaldp521
144	ecdonaldb571
144	ecdonaldk571
192	ronald1536
256	ronald2048
384	ronald3072
512	ronald4096

Signing 23 bytes	
bytes	system
37	sflashv2
40	donald1024
40	donald2048
40	donald512
40	ecdonaldp160
41	ronald512
42	ecdonaldb163
42	ecdonaldk163
43	rainbow
48	ecdonaldp192
56	ecdonaldp224
60	ecdonaldb233
60	ecdonaldk233
64	ecdonaldp256
72	ecdonaldb283
72	ecdonaldk283
73	ronald768
87	hector
96	ecdonaldp384
104	ecdonaldb409
104	ecdonaldk409
105	ronald1024
132	ecdonaldp521
144	ecdonaldb571
144	ecdonaldk571
169	ronald1536
233	ronald2048
361	ronald3072
489	ronald4096

Signing many bytes	
bytes	system
37	sflashv2
40	donald1024
40	donald2048
40	donald512
40	ecdonaldp160
42	ecdonaldb163
42	ecdonaldk163
43	rainbow
43	ronald1024
43	ronald1536
43	ronald2048
43	ronald3072
43	ronald4096
43	ronald512
43	ronald768
48	ecdonaldp192
56	ecdonaldp224
60	ecdonaldb233
60	ecdonaldk233
64	ecdonaldp256
72	ecdonaldb283
72	ecdonaldk283
87	hector
96	ecdonaldp384
104	ecdonaldb409
104	ecdonaldk409
132	ecdonaldp521
144	ecdonaldb571
144	ecdonaldk571

10.11 amd64, 3392MHz, Intel Pentium D (f64), nmi0241



Cycles to generate a key pair			
quartile	median	quartile	system
723622	727974	733890	`donald512`
2065466	2085475	2102509	`donald1024`
6822797	6902952	6986439	`donald2048`
29183730	46088972	75967696	`ronald512`
61143781	101659184	166003215	`ronald768`
108284390	186434308	300285705	`ronald1024`
397239170	598240659	876239789	`ronald1536`
690522116	695000256	695274670	`sflashv2`
591046497	1133769831	2021749276	`ronald2048`
2090154573	5009855188	8374850726	`ronald3072`
7514337875	12533630307	19141479851	`ronald4096`

Secret key	
bytes	system
84	`donald512`
148	`donald1024`
276	`donald2048`
512	`ronald512`
768	`ronald768`
1024	`ronald1024`
1536	`ronald1536`
2048	`ronald2048`
2823	`sflashv2`
3072	`ronald3072`
4096	`ronald4096`

Cycles to sign 59 bytes			
quartile	median	quartile	system
376244	378675	382092	`sflashv2`
832048	838134	845155	`donald512`
1681147	1697365	1718700	`ronald512`
2180692	2208266	2224960	`donald1024`
3621187	3639343	3669773	`ronald768`
5834774	5860427	5883122	`ronald1024`
6932719	7009882	7088065	`donald2048`
15288236	15370346	15449175	`ronald1536`
29518052	29606673	29679144	`ronald2048`
80510011	80747875	80971051	`ronald3072`
171599700	172609738	173155115	`ronald4096`

Public key	
bytes	system
64	`donald512`
64	`ronald512`
96	`ronald768`
128	`donald1024`
128	`ronald1024`
192	`ronald1536`
256	`donald2048`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
19266	`sflashv2`

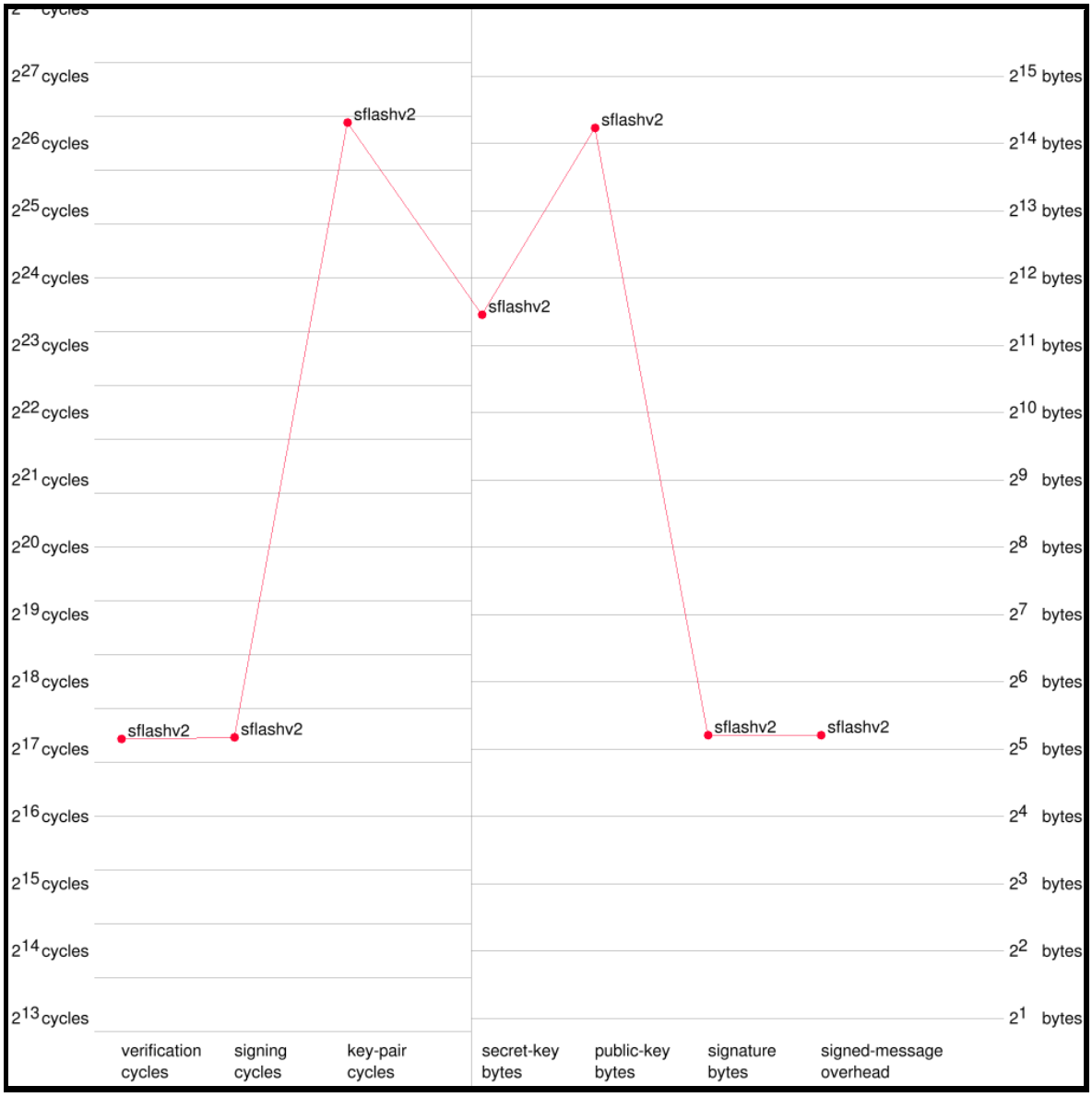
Cycles to verify 59 bytes			
quartile	median	quartile	system
120054	121499	121822	`ronald512`
133586	134215	135677	`ronald768`
169660	171615	173043	`ronald1024`
246109	250308	252994	`ronald1536`
320790	322490	324156	`sflashv2`
363545	366554	369733	`ronald2048`
676957	682142	693158	`ronald3072`
957321	965141	971482	`donald512`
1097775	1103351	1112225	`ronald4096`
2621944	2637856	2668184	`donald1024`
8358441	8489987	8594163	`donald2048`

Signing 0 bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
41	`ronald512`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.12 ia64, 900MHz, HP Itanium II, `nmi0025`



Cycles to generate a key pair			
quartile	median	quartile	system
996617236	997189186	1054306860	`sflashv2`

Secret key	
bytes	system
2823	`sflashv2`

Cycles to sign 59 bytes			
quartile	median	quartile	system
364761	364831	367280	`sflashv2`

Public key	
bytes	system
19266	`sflashv2`

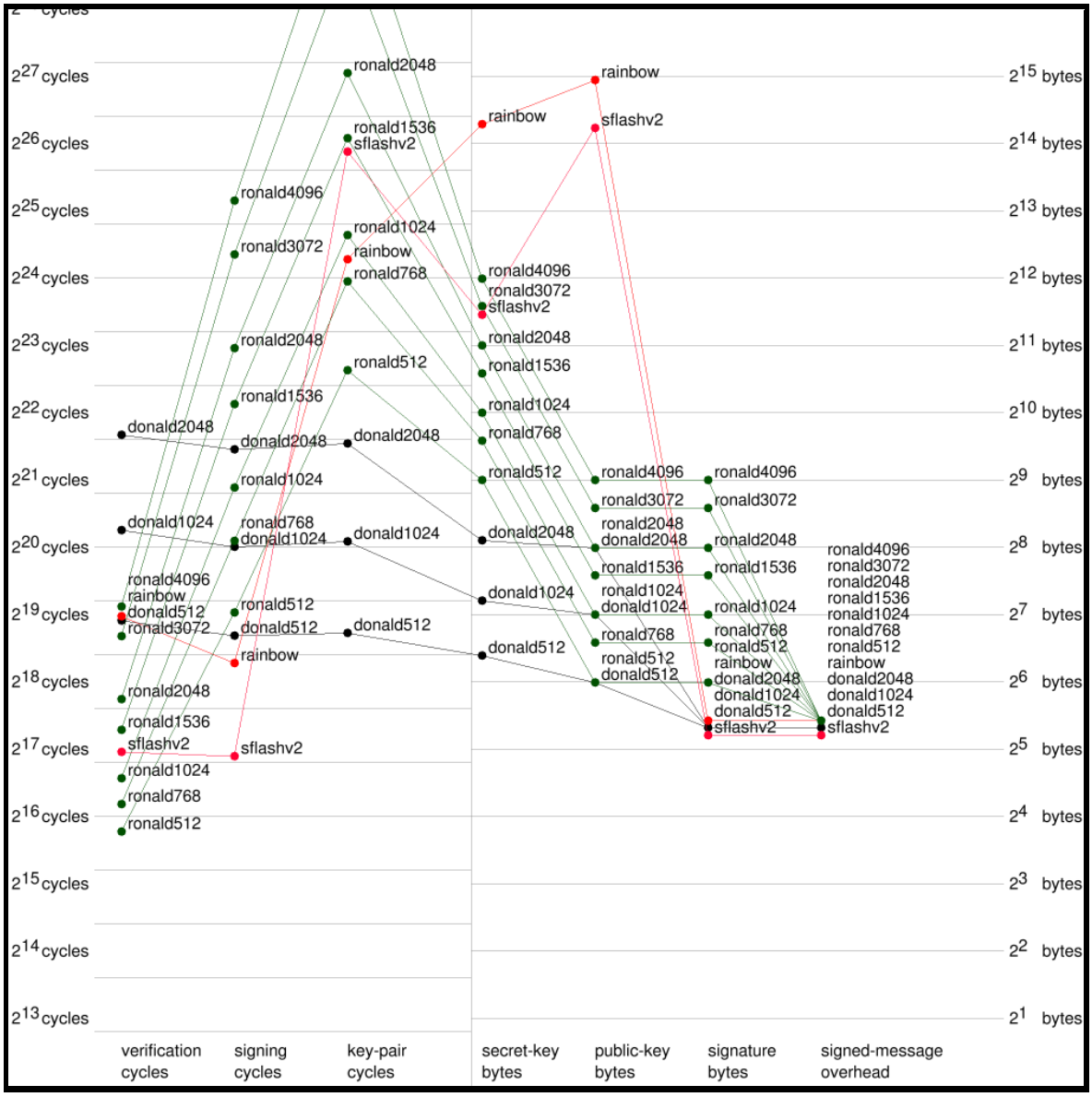
Cycles to verify 59 bytes			
quartile	median	quartile	system
355534	355634	357633	`sflashv2`

Signing 0 bytes	
bytes	system
37	`sflashv2`

Signing 23 bytes	
bytes	system
37	`sflashv2`

Signing many bytes	
bytes	system
37	`sflashv2`

10.13 ia64, 997MHz, HP Itanium II, `nmi0020`



Cycles to generate a key pair			
quartile	median	quartile	system
1392446	1394092	1395951	donald512
4550661	4552780	4554843	donald1024
16038416	16041024	16044384	donald2048
31207819	41044407	54813998	ronald512
78675331	128918617	176777416	ronald768
172042913	172095478	172233061	rainbow
141340659	234674402	322972508	ronald1024
685066389	685291495	690131189	sflashv2
491923157	817032042	1239115592	ronald1536
1253087111	1885008781	3066376545	ronald2048
5119720094	9361215870	16163237036	ronald3072
15837041290	26957980340	40273398870	ronald4096

Secret key	
bytes	system
84	donald512
148	donald1024
276	donald2048
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096
20107	rainbow

Cycles to sign 59 bytes			
quartile	median	quartile	system
286386	286622	289727	sflashv2
950022	950515	952297	rainbow
1341405	1351183	1357557	donald512
1810246	1813767	1818001	ronald512
4220914	4250796	4274154	donald1024
4555324	4560176	4567216	ronald768
9069247	9076659	9088902	ronald1024
14717640	14834975	14928909	donald2048
26607064	26621925	26651577	ronald1536
54707357	54740893	54771261	ronald2048
183022807	183065136	183124187	ronald3072
366394861	366597598	367166475	ronald4096

Public key	
bytes	system
64	donald512
64	ronald512
96	ronald768
128	donald1024
128	ronald1024
192	ronald1536
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2
31680	rainbow

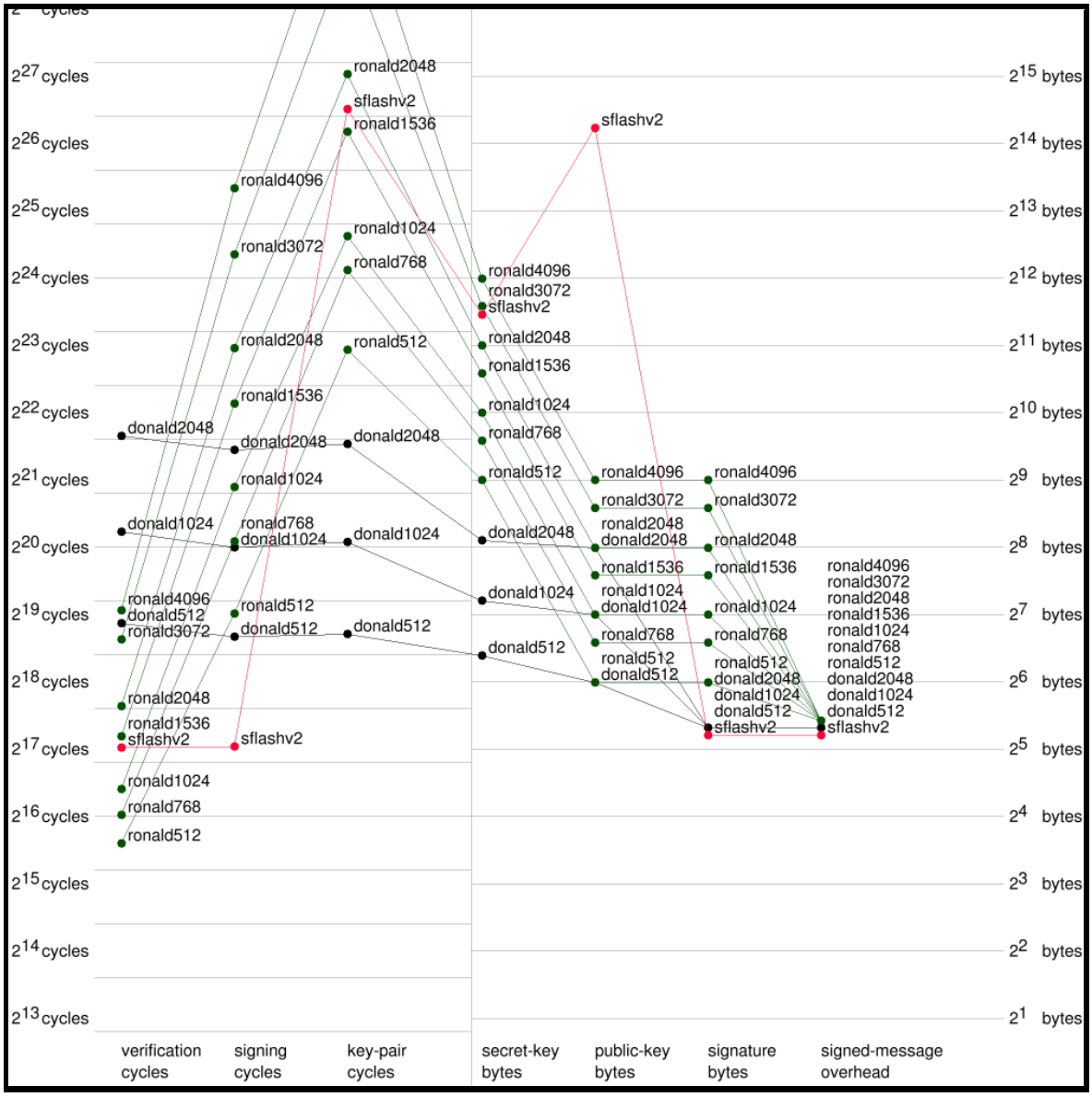
Cycles to verify 59 bytes			
quartile	median	quartile	system
105976	108524	109927	ronald512
151896	154127	154438	ronald768
215096	215824	216803	ronald1024
302588	302891	305903	sflashv2
401716	402073	405023	ronald1536
592798	595351	596199	ronald2048
1341237	1341971	1344819	ronald3072
1637049	1640308	1646006	donald512
1733908	1734073	1734218	rainbow
1958338	1958607	1958859	ronald4096
5196829	5241776	5283992	donald1024
17701769	17962531	18411382	donald2048

Signing 0 bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`rainbow`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
41	`ronald512`
43	`rainbow`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`rainbow`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.14 ia64, 997MHz, HP Itanium II, `nmi0058`



Cycles to generate a key pair			
quartile	median	quartile	system
1377898	1379524	1381408	`donald512`
4520564	4521969	4523611	`donald1024`
15911231	15942192	15949025	`donald2048`
34336011	53523030	91352434	`ronald512`
87896823	149958221	224741297	`ronald768`
131041625	231173782	319721037	`ronald1024`
590710387	887843152	1328933065	`ronald1536`
1023952736	1185400911	1555012089	`sflashv2`
926078587	1863618933	2888820480	`ronald2048`
4751801072	9271876984	15377965954	`ronald3072`
19596078770	30366176850	47228339780	`ronald4096`

Secret key	
bytes	system
84	`donald512`
148	`donald1024`
276	`donald2048`
512	`ronald512`
768	`ronald768`
1024	`ronald1024`
1536	`ronald1536`
2048	`ronald2048`
2823	`sflashv2`
3072	`ronald3072`
4096	`ronald4096`

Cycles to sign 59 bytes			
quartile	median	quartile	system
324601	324871	329060	`sflashv2`
1316192	1328638	1338260	`donald512`
1783233	1791995	1817386	`ronald512`
4170228	4195565	4235764	`donald1024`
4528801	4554358	4673688	`ronald768`
9132960	9155030	9178485	`ronald1024`
14607828	14730695	14852847	`donald2048`
26677910	26726171	26875287	`ronald1536`
54818941	54867570	54926180	`ronald2048`
182450423	182766211	183253576	`ronald3072`
385674800	430043740	507957220	`ronald4096`

Public key	
bytes	system
64	`donald512`
64	`ronald512`
96	`ronald768`
128	`donald1024`
128	`ronald1024`
192	`ronald1536`
256	`donald2048`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
19266	`sflashv2`

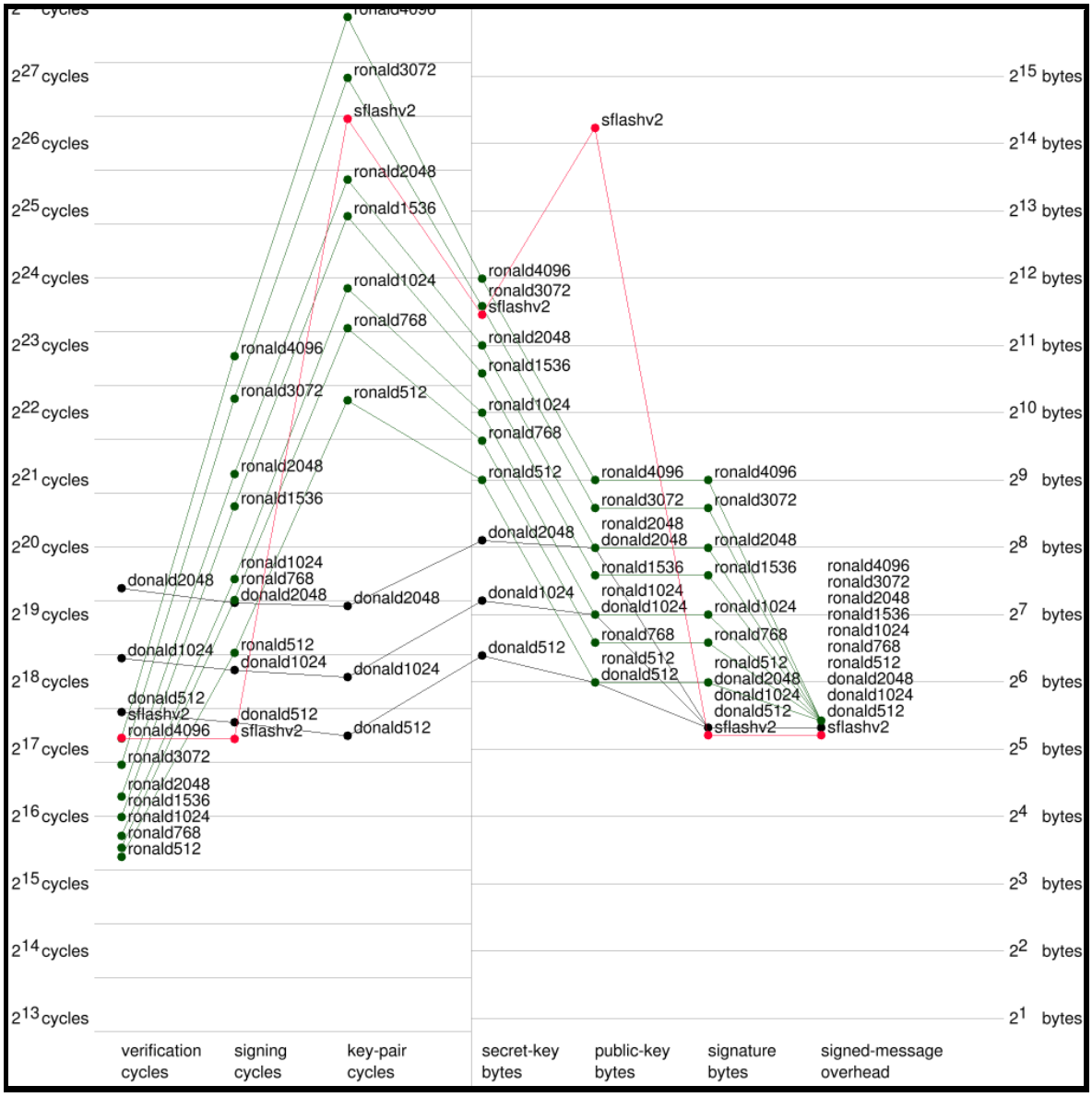
Cycles to verify 59 bytes			
quartile	median	quartile	system
91632	92699	92845	`ronald512`
133400	133946	136567	`ronald768`
184256	187250	187880	`ronald1024`
318669	318792	322299	`sflashv2`
367707	368407	372253	`ronald1536`
543148	544772	546292	`ronald2048`
1279208	1282554	1286236	`ronald3072`
1582642	1587013	1608566	`donald512`
1863389	1866246	1871934	`ronald4096`
5141560	5159304	5183989	`donald1024`
17690072	17717116	18211350	`donald2048`

Signing 0 bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
41	`ronald512`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.15 ia64, 1396MHz, HP Itanium II, `nmi0065`



Cycles to generate a key pair			
quartile	median	quartile	system
367841	370731	373698	donald512
784389	790723	795751	donald1024
1969522	1981954	2006825	donald2048
19387604	27884535	37169258	ronald512
43916156	70772355	99178525	ronald768
55235050	117954676	168150881	ronald1024
189284930	299772095	427954653	ronald1536
331574888	478258821	792427290	ronald2048
1048188529	1048350008	1048481865	sflashv2
1026754479	1778908030	2938962188	ronald3072
1844181220	3875461039	6800039552	ronald4096

Secret key	
bytes	system
84	donald512
148	donald1024
276	donald2048
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096

Cycles to sign 59 bytes			
quartile	median	quartile	system
356975	357086	359238	sflashv2
440928	443429	446486	donald512
860251	865592	872783	donald1024
1079587	1085276	1098762	ronald512
2042382	2059686	2084450	donald2048
2128023	2133132	2141292	ronald768
2783092	2789384	2800363	ronald1024
7118352	7141407	7161346	ronald1536
10797199	10814796	10863321	ronald2048
28499612	28552900	28610717	ronald3072
49121623	49165796	49250187	ronald4096

Public key	
bytes	system
64	donald512
64	ronald512
96	ronald768
128	donald1024
128	ronald1024
192	ronald1536
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2

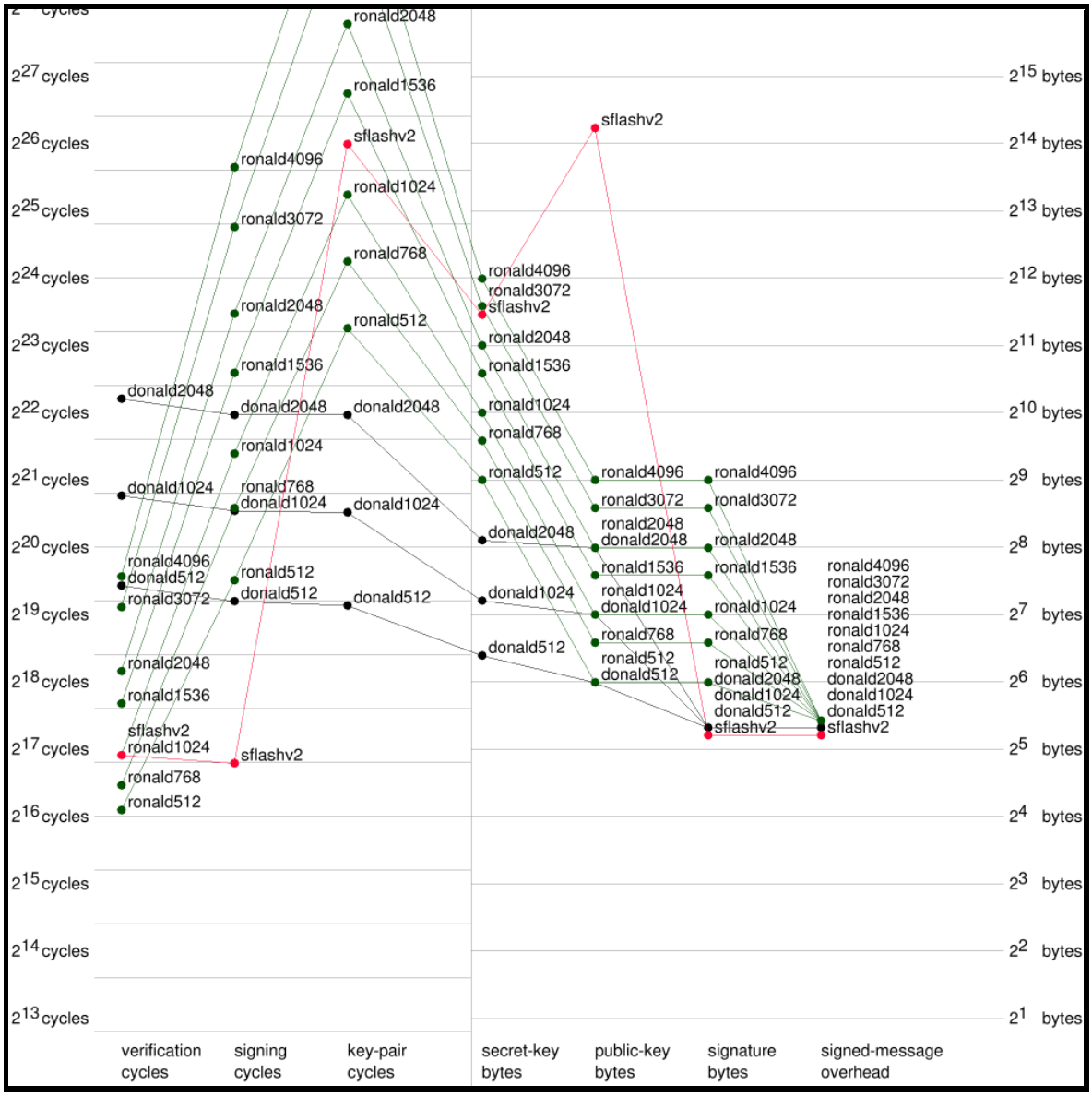
Cycles to verify 59 bytes			
quartile	median	quartile	system
77552	78025	78301	ronald512
87660	87752	88249	ronald768
100958	102774	102938	ronald1024
127789	130316	132869	ronald1536
169914	170270	170778	ronald2048
253567	256494	257477	ronald3072
358077	358581	359970	ronald4096
361602	361736	363890	sflashv2
501452	505260	507896	donald512
1005194	1012712	1027421	donald1024
2460840	2485725	2527974	donald2048

Signing 0 bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
41	`ronald512`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.16 ppc32, 400MHz, Motorola PowerPC G4 7400, nmi0042



Cycles to generate a key pair			
quartile	median	quartile	system
1978416	1993920	2004192	donald512
6548752	6610976	6666448	donald1024
22961072	23143904	23324272	donald2048
50878960	70790640	96844400	ronald512
117034032	167166944	250805296	ronald768
260229552	394739184	567208544	ronald1024
751074160	757883616	810956864	sflashv2
797219632	1454568656	2099686256	ronald1536
2349756432	3556299248	5660071648	ronald2048
9950433840	16131053728	28521894256	ronald3072
22907382640	41674611552	62821583744	ronald4096

Secret key	
bytes	system
84	donald512
148	donald1024
276	donald2048
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096

Cycles to sign 59 bytes			
quartile	median	quartile	system
260720	261008	261040	sflashv2
2095040	2109328	2124528	donald512
2759136	2766800	2774496	ronald512
6675696	6730048	6778080	donald1024
6958128	6981264	6991168	ronald768
14014848	14029632	14041680	ronald1024
23025072	23227872	23460832	donald2048
39679088	39708768	39738496	ronald1536
85212880	85334784	85539952	ronald2048
259516112	260091248	260573328	ronald3072
562707616	563188496	619472272	ronald4096

Public key	
bytes	system
64	donald512
64	ronald512
96	ronald768
128	donald1024
128	ronald1024
192	ronald1536
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2

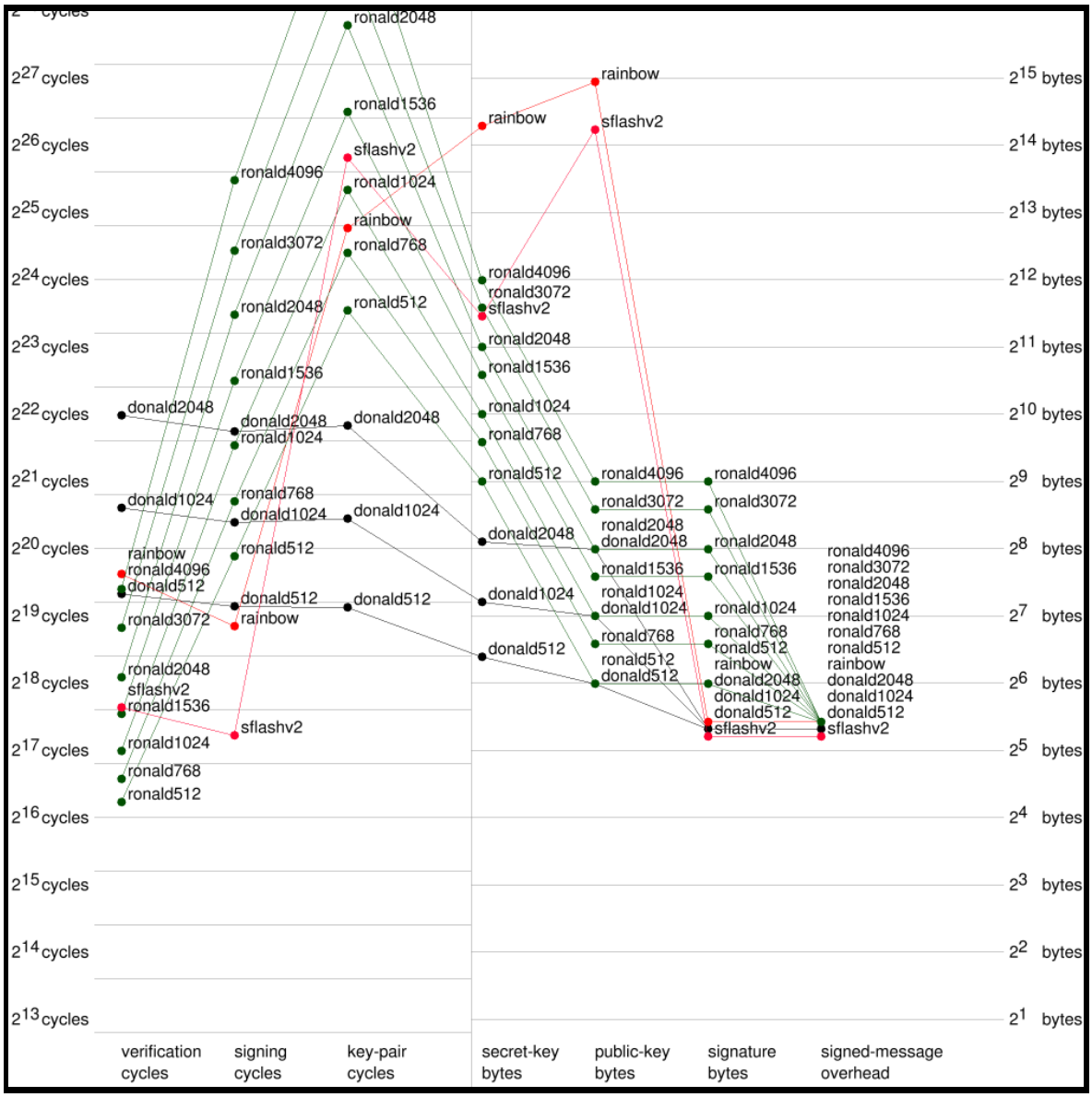
Cycles to verify 59 bytes			
quartile	median	quartile	system
142560	142960	143552	ronald512
195056	196800	199632	ronald768
288944	289008	289184	ronald1024
289328	289472	289504	sflashv2
561584	564192	565456	ronald1536
849904	853072	854224	ronald2048
1942816	1945568	1947088	ronald3072
2515760	2578176	2580736	donald512
2894848	2898288	2903328	ronald4096
8145872	8210400	8232992	donald1024
27674592	28594304	28834640	donald2048

Signing 0 bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
41	`ronald512`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.17 ppc32, 2000MHz, IBM PowerPC G5 970, geespaz



Cycles to generate a key pair			
quartile	median	quartile	system
1968180	1972380	1978680	donald512
6180720	6188160	6207120	donald1024
20469540	20538360	20555160	donald2048
63564120	90472560	124492320	ronald512
123031800	190859460	280169700	ronald768
260991360	261327480	261967980	rainbow
288794520	427897560	609500460	ronald1024
647998920	649147320	650593680	sflashv2
646411560	1171926840	1844777460	ronald1536
2314500000	3578372700	4730867520	ronald2048
6134937480	8733743340	14691004620	ronald3072
19033066440	27596002200	44523097800	ronald4096

Secret key	
bytes	system
84	donald512
148	donald1024
276	donald2048
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096
20107	rainbow

Cycles to sign 59 bytes			
quartile	median	quartile	system
378420	381120	383580	sflashv2
1543920	1556580	1569300	rainbow
1986120	1999140	2010960	donald512
3793560	3807900	3821520	ronald512
5865240	5912760	5954700	donald1024
7746600	7762860	7798500	ronald768
15919500	15949320	15982380	ronald1024
18945120	19053360	19177680	donald2048
36551100	36636780	36813720	ronald1536
85525740	85649940	85979700	ronald2048
196028400	196187820	196483140	ronald3072
483190320	484003380	484761840	ronald4096

Public key	
bytes	system
64	donald512
64	ronald512
96	ronald768
128	donald1024
128	ronald1024
192	ronald1536
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2
31680	rainbow

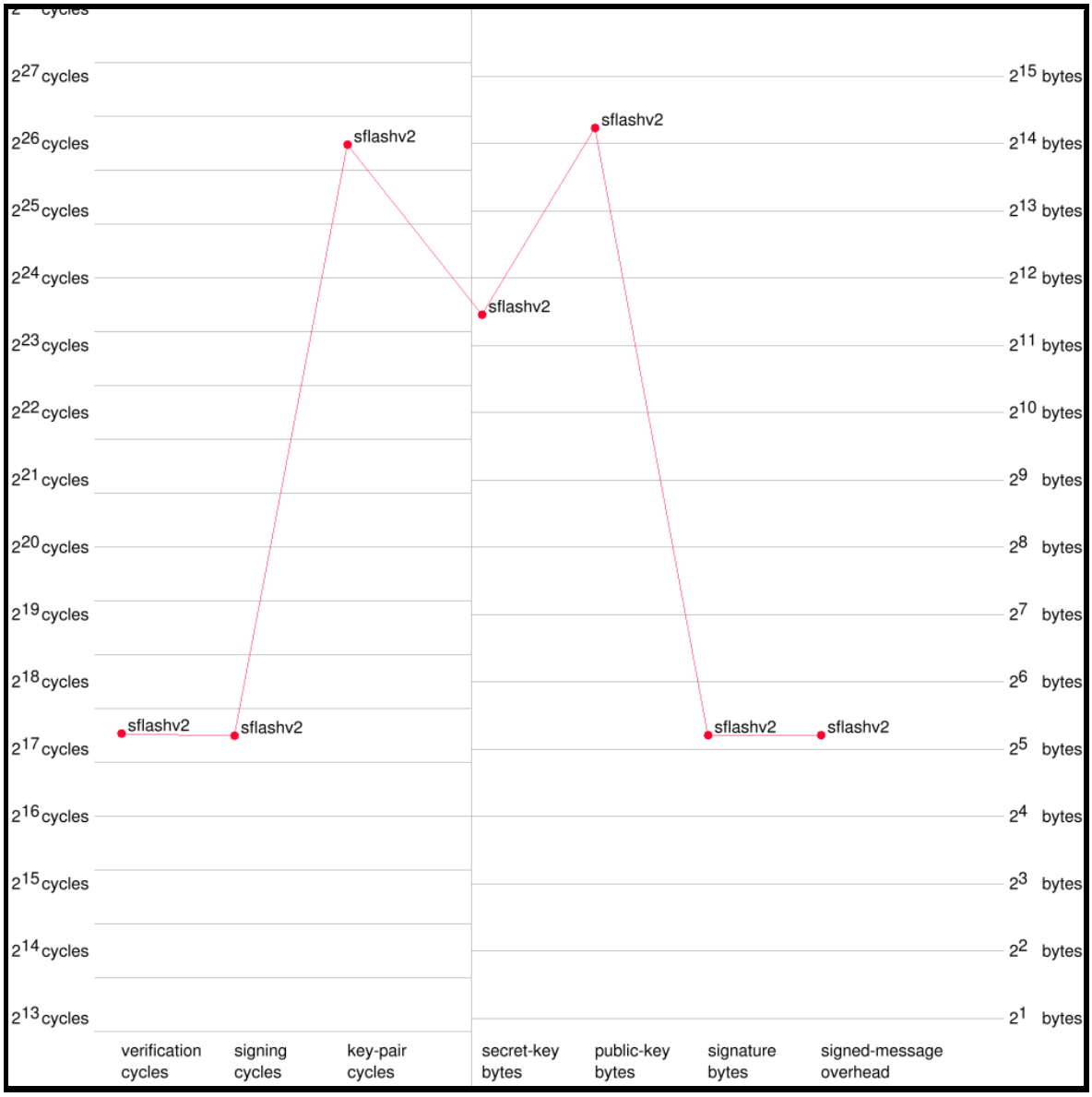
Cycles to verify 59 bytes			
quartile	median	quartile	system
154620	161340	168300	ronald512
215760	216480	216840	ronald768
305340	310560	313680	ronald1024
500580	502440	503340	ronald1536
536400	543720	546780	sflashv2
796860	800880	801840	ronald2048
1520220	1524120	1526400	ronald3072
2343660	2355120	2369520	donald512
2495580	2498640	2505840	ronald4096
2987280	3032100	3054480	rainbow
7076460	7133280	7150560	donald1024
22971300	23472180	23536260	donald2048

Signing 0 bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`rainbow`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
41	`ronald512`
43	`rainbow`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`rainbow`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.18 ppc32, 2097MHz, IBM POWER5, nmi0154



Cycles to generate a key pair			
quartile	median	quartile	system
751535096	751677592	751878060	`sflashv2`

Secret key	
bytes	system
2823	`sflashv2`

Cycles to sign 59 bytes			
quartile	median	quartile	system
371212	371776	372516	`sflashv2`

Public key	
bytes	system
19266	`sflashv2`

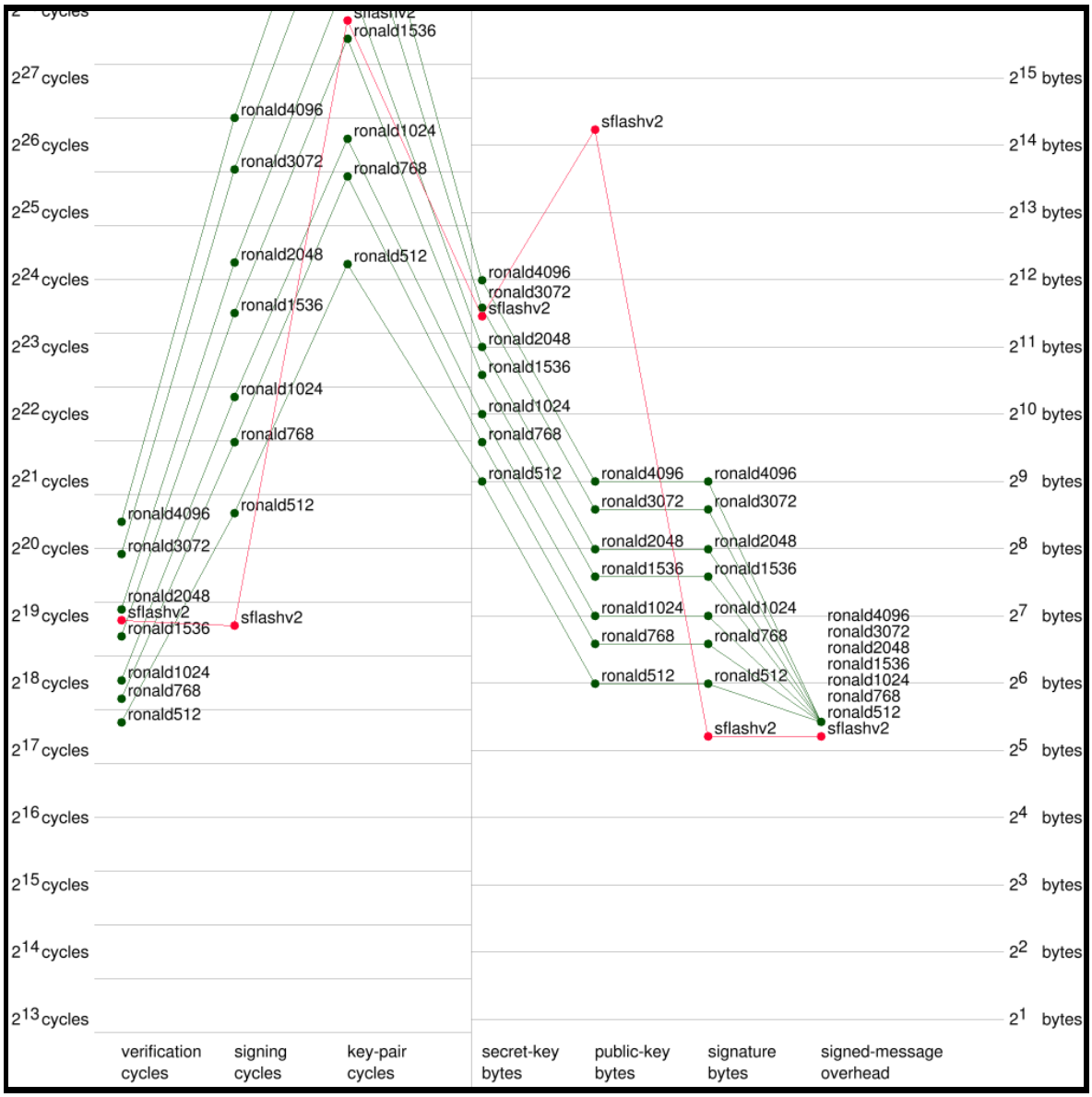
Cycles to verify 59 bytes			
quartile	median	quartile	system
381424	382052	383480	`sflashv2`

Signing 0 bytes	
bytes	system
37	`sflashv2`

Signing 23 bytes	
bytes	system
37	`sflashv2`

Signing many bytes	
bytes	system
37	`sflashv2`

10.19 ppc32, 3192MHz, IBM Cell PPE, `nmips3`



Cycles to generate a key pair			
quartile	median	quartile	system
108269080	164964800	213426680	`ronald512`
328976400	508960880	754239640	`ronald768`
488953360	828124000	1158776920	`ronald1024`
1929924960	3014950400	4687021000	`ronald1536`
3791251200	3793699400	3828413480	`sflashv2`
4044620200	6812872840	9461014960	`ronald2048`
17562541360	26473514320	41529745520	`ronald3072`
41279186040	72006818000	115804393120	`ronald4096`

Secret key	
bytes	system
512	`ronald512`
768	`ronald768`
1024	`ronald1024`
1536	`ronald1536`
2048	`ronald2048`
2823	`sflashv2`
3072	`ronald3072`
4096	`ronald4096`

Cycles to sign 59 bytes			
quartile	median	quartile	system
1564160	1565800	1573360	`sflashv2`
6609960	6646680	6735920	`ronald512`
16413160	16608800	17187760	`ronald768`
29104120	29716560	30161680	`ronald1024`
87215640	87740520	87867680	`ronald1536`
167972800	168163040	168441000	`ronald2048`
554653320	555936120	559464600	`ronald3072`
1080393960	1082798240	1089899040	`ronald4096`

Public key	
bytes	system
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
19266	`sflashv2`

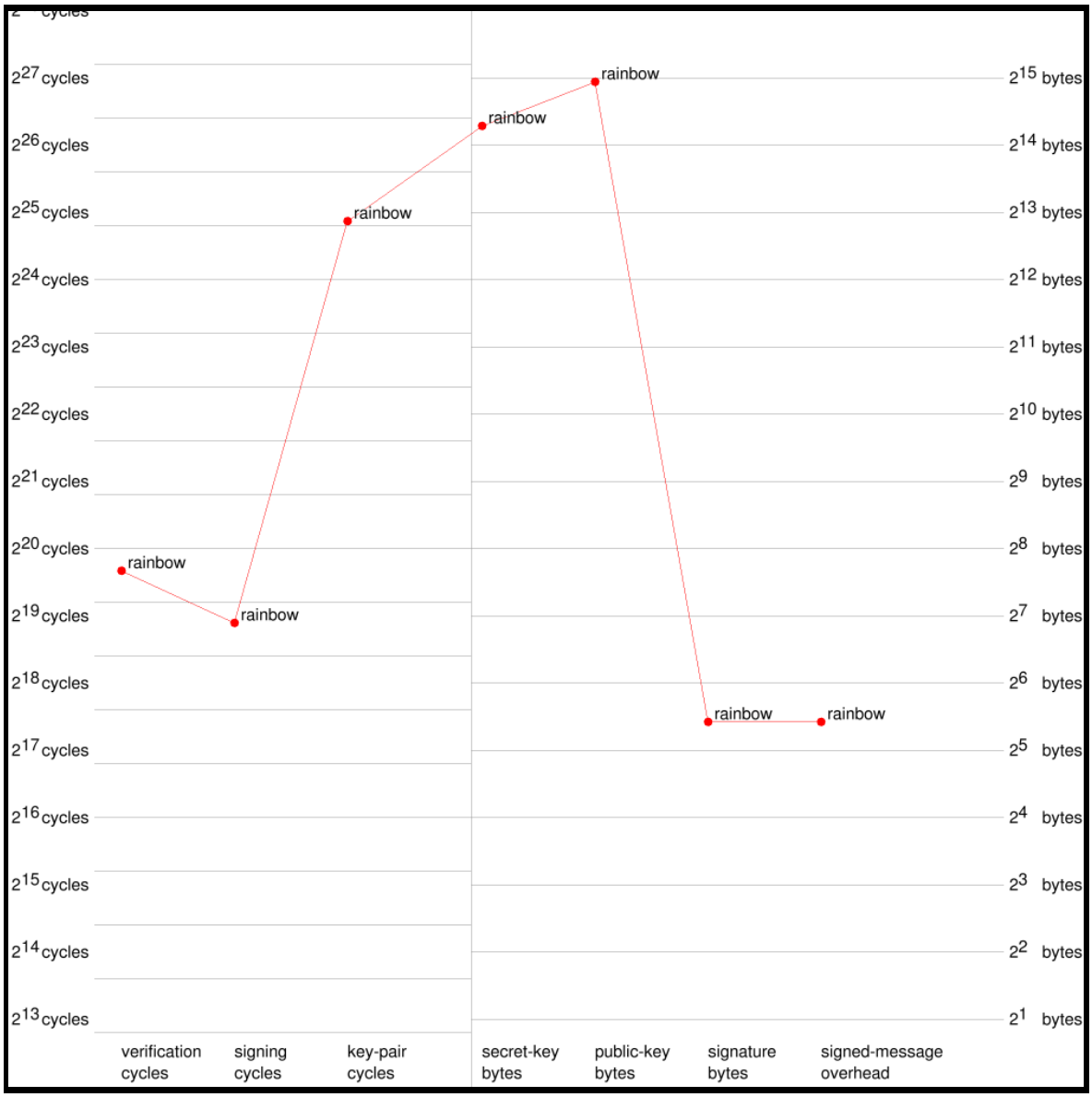
Cycles to verify 59 bytes			
quartile	median	quartile	system
439080	447080	453080	`ronald512`
609000	610360	617240	`ronald768`
765640	768640	772520	`ronald1024`
1354200	1356200	1363200	`ronald1536`
1664080	1670720	2055920	`sflashv2`
1920480	1923720	1931200	`ronald2048`
3902480	3914120	3929840	`ronald3072`
5941080	5946760	5953040	`ronald4096`

Signing 0 bytes	
bytes	system
37	`sflashv2`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
37	`sflashv2`
41	`ronald512`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
37	`sflashv2`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.20 ppc64, 2000MHz, IBM PowerPC G5 970, geespaz



Cycles to generate a key pair			
quartile	median	quartile	system
287217840	287502780	287884560	`rainbow`

Secret key	
bytes	system
20107	`rainbow`

Cycles to sign 59 bytes			
quartile	median	quartile	system
1604460	1616520	1630980	`rainbow`

Public key	
bytes	system
31680	`rainbow`

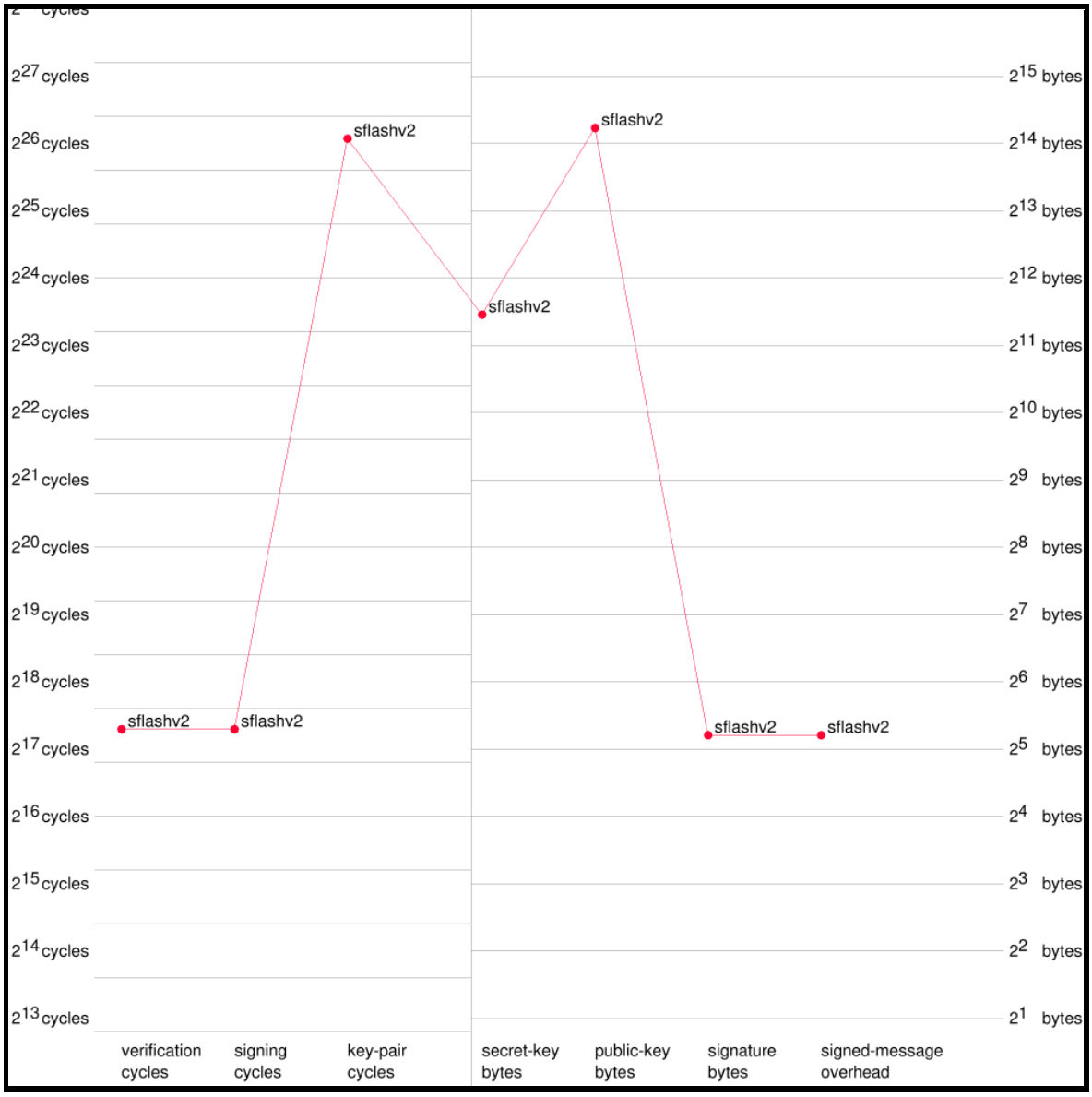
Cycles to verify 59 bytes			
quartile	median	quartile	system
3120300	3166620	3180720	`rainbow`

Signing 0 bytes	
bytes	system
43	`rainbow`

Signing 23 bytes	
bytes	system
43	`rainbow`

Signing many bytes	
bytes	system
43	`rainbow`

10.21 ppc64, 2097MHz, IBM POWER5, `nmi0154`



Cycles to generate a key pair			
quartile	median	quartile	system
808003164	808286860	808568792	`sflashv2`

Secret key	
bytes	system
2823	`sflashv2`

Cycles to sign 59 bytes			
quartile	median	quartile	system
402344	403348	404604	`sflashv2`

Public key	
bytes	system
19266	`sflashv2`

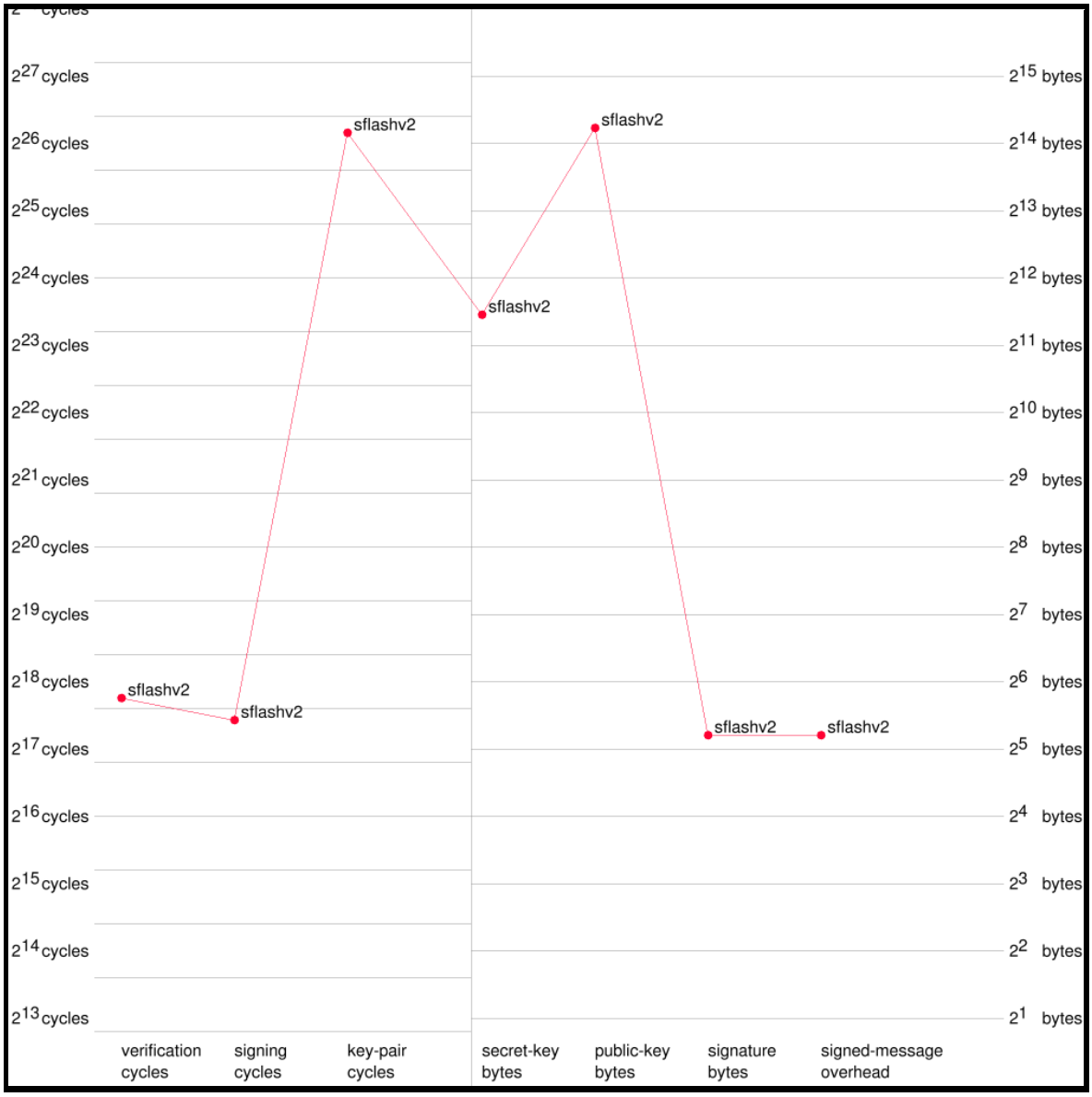
Cycles to verify 59 bytes			
quartile	median	quartile	system
404436	404936	405752	`sflashv2`

Signing 0 bytes	
bytes	system
37	`sflashv2`

Signing 23 bytes	
bytes	system
37	`sflashv2`

Signing many bytes	
bytes	system
37	`sflashv2`

10.22 sparcv9, 300MHz, Sun UltraSPARC IIi, nmi0096



Cycles to generate a key pair			
quartile	median	quartile	system
814579462	872449578	910579114	`sflashv2`

Secret key	
bytes	system
2823	`sflashv2`

Cycles to sign 59 bytes			
quartile	median	quartile	system
454000	455504	457354	`sflashv2`

Public key	
bytes	system
19266	`sflashv2`

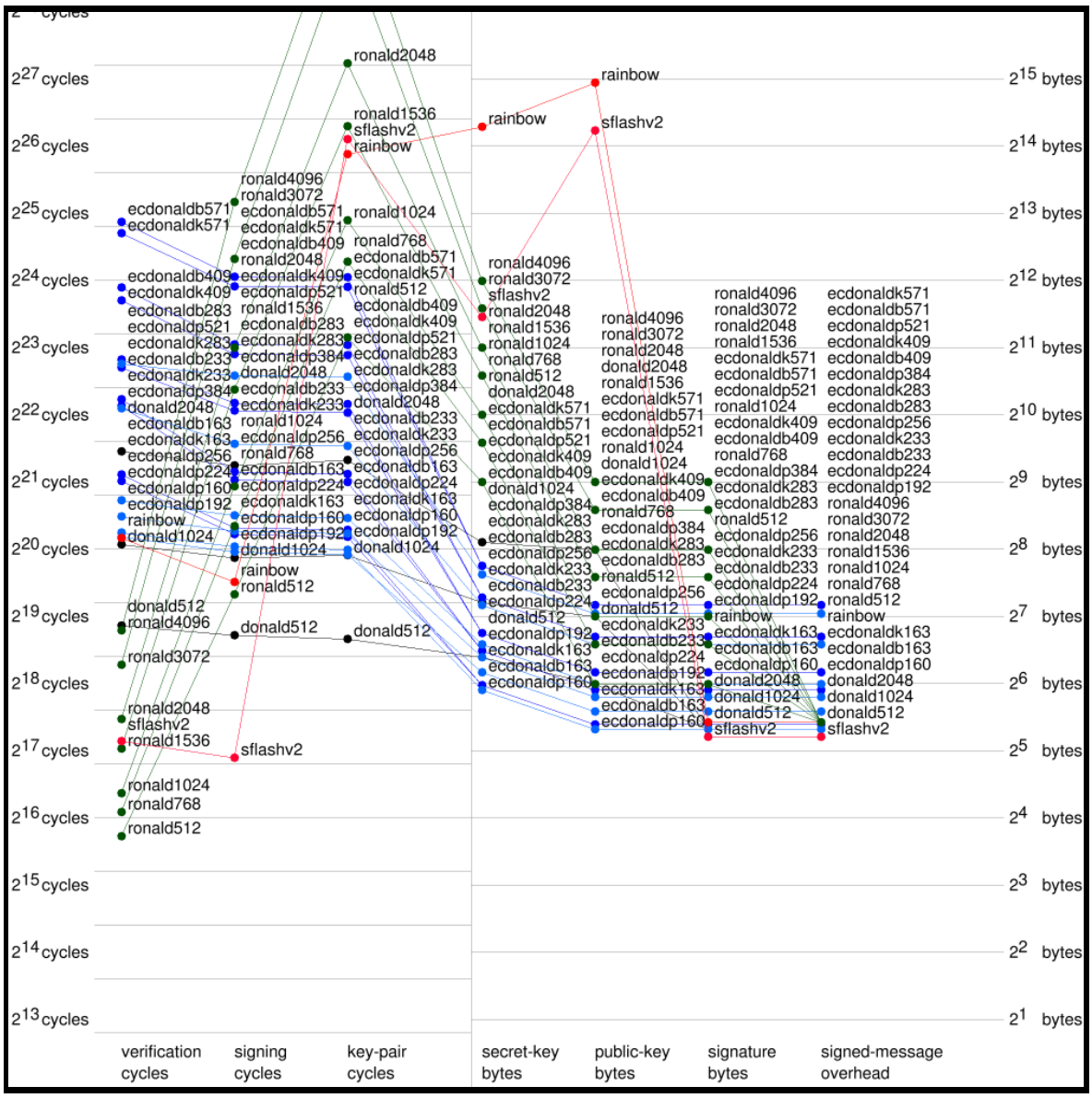
Cycles to verify 59 bytes			
quartile	median	quartile	system
600184	605261	612063	`sflashv2`

Signing 0 bytes	
bytes	system
37	`sflashv2`

Signing 23 bytes	
bytes	system
37	`sflashv2`

Signing many bytes	
bytes	system
37	`sflashv2`

10.23 x86, 1196MHz, Intel Celeron (6b1), `vieux`



Cycles to generate a key pair			
quartile	median	quartile	system
1315577	1318288	1330347	`donald512`
3888707	3895157	4058176	`donald1024`
3866712	3914218	4042348	`ecdonaldp192`
4126422	4169932	4314696	`ecdonaldp160`
4911930	4952480	5059573	`ecdonaldk163`
5085266	5140187	5248784	`ecdonaldp224`
5358282	5415980	5564826	`ecdonaldb163`
6205665	6295519	6454620	`ecdonaldp256`
9908821	9987951	16531462	`ecdonaldk233`
11027590	11135323	17739719	`ecdonaldb233`
13185284	13262601	19961561	`donald2048`
15654624	15937062	22553844	`ecdonaldp384`
18255338	24443254	25079269	`ecdonaldk283`
20720022	27284413	27505548	`ecdonaldb283`
38607770	38844935	39038868	`ecdonaldp521`
51371664	51550224	52640688	`ecdonaldk409`
58259532	58545144	64914996	`ecdonaldb409`
48408792	64734180	87577404	`ronald512`
123342708	123679944	123910176	`ecdonaldk571`
139695576	140134860	146250084	`ecdonaldb571`
112566192	171749700	238474692	`ronald768`
173223120	291759144	445958184	`ronald1024`
687351984	688187760	689153340	`rainbow`
831817620	832715748	838778376	`sflashv2`
661020336	981878784	1359211752	`ronald1536`
1420577532	2222037852	3258565512	`ronald2048`
4996700232	10638374352	14159867448	`ronald3072`
12361629036	22440670944	32867951820	`ronald4096`

Secret key	
bytes	system
60	ecdonaldp160
63	ecdonaldb163
63	ecdonaldk163
72	ecdonaldp192
84	donald512
84	ecdonaldp224
90	ecdonaldb233
90	ecdonaldk233
96	ecdonaldp256
108	ecdonaldb283
108	ecdonaldk283
144	ecdonaldp384
148	donald1024
156	ecdonaldb409
156	ecdonaldk409
198	ecdonaldp521
216	ecdonaldb571
216	ecdonaldk571
276	donald2048
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096
20107	rainbow

Cycles to sign 59 bytes			
quartile	median	quartile	system
285034	285157	285339	sflashv2
1372283	1384697	1407993	donald512
2318820	2345166	2385351	ronald512
2751305	2760174	2834669	rainbow
3725974	3771790	3884494	donald1024
4023780	4056998	4263061	ecdonaldp192
4268717	4342473	4519272	ecdonaldp160
5057001	5112222	5331335	ecdonaldk163
5271460	5339740	5506904	ecdonaldp224
5493752	5553513	5764924	ecdonaldb163
5601502	5672806	5770824	ronald768
6425673	6529786	6735609	ecdonaldp256
9371290	9477944	16152579	ronald1024
10077532	10295097	16933115	ecdonaldk233
11245589	11435302	18079322	ecdonaldb233
12335255	12444483	19224972	donald2048
16103368	16330420	23026958	ecdonaldp384
18690094	25226217	25515180	ecdonaldk283
21066958	27683568	27976058	ecdonaldb283
26433048	32934852	33098496	ronald1536
39333048	39511415	39745836	ecdonaldp521
51989652	52170972	58464516	ecdonaldk409
56517420	56721024	63419988	ronald2048
58762980	59177196	65516628	ecdonaldb409
124360944	124577904	124876968	ecdonaldk571
140686908	141039756	147359856	ecdonaldb571
178010784	178325820	178924679	ronald3072
363173796	369386280	370292208	ronald4096

Public key	
bytes	system
40	ecdonaldp160
42	ecdonaldb163
42	ecdonaldk163
48	ecdonaldp192
56	ecdonaldp224
60	ecdonaldb233
60	ecdonaldk233
64	donald512
64	ecdonaldp256
64	ronald512
72	ecdonaldb283
72	ecdonaldk283
96	ecdonaldp384
96	ronald768
104	ecdonaldb409
104	ecdonaldk409
128	donald1024
128	ronald1024
132	ecdonaldp521
144	ecdonaldb571
144	ecdonaldk571
192	ronald1536
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2
31680	rainbow

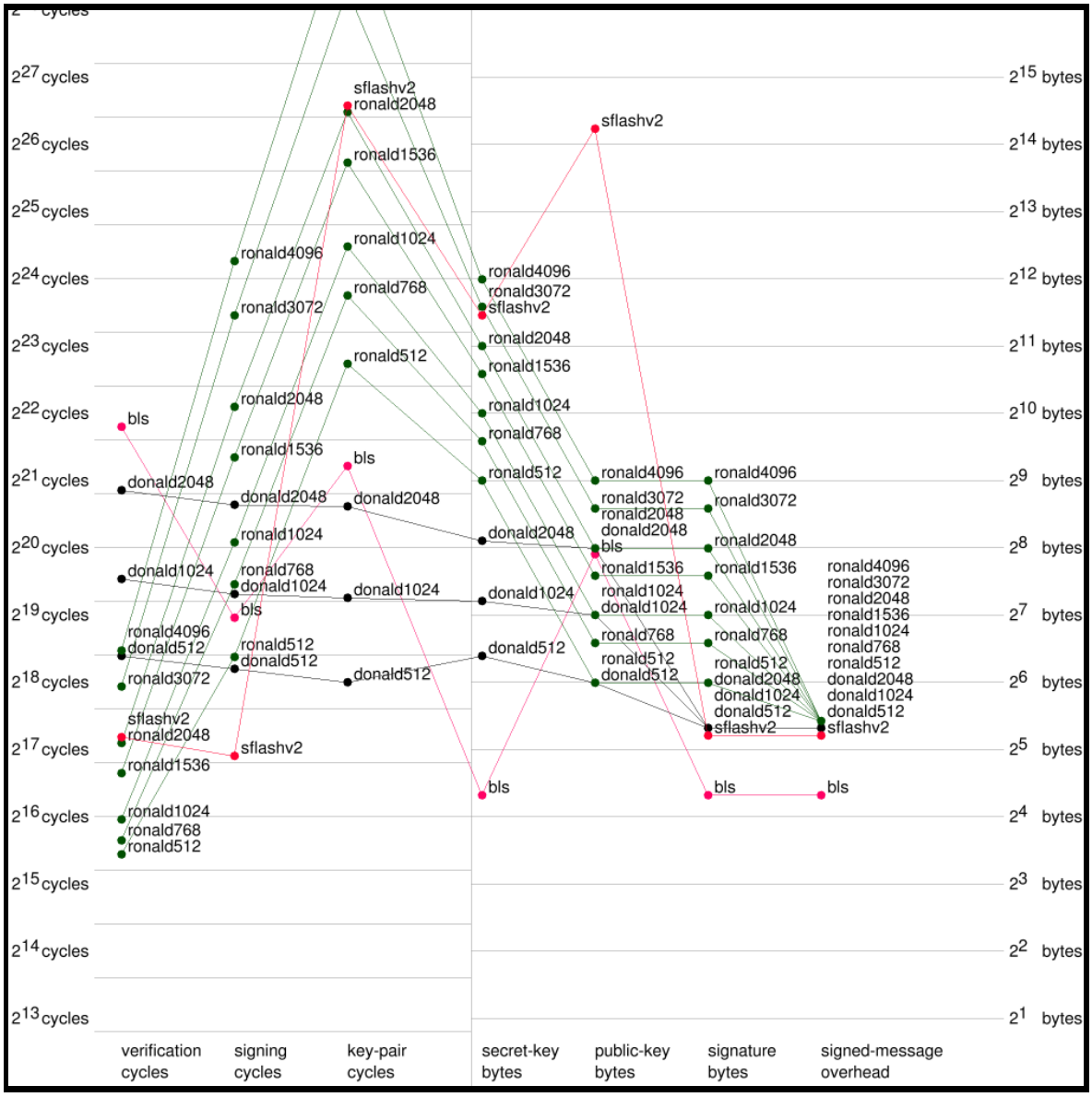
Cycles to verify 59 bytes			
quartile	median	quartile	system
99975	103648	104651	ronald512
140714	141827	142267	ronald768
180710	181065	181308	ronald1024
318884	321947	322512	ronald1536
355179	355244	355290	sflashv2
470794	472081	473139	ronald2048
943451	945869	951147	ronald3072
1471499	1474100	1481776	ronald4096
1569137	1576511	1584815	donald512
4443887	4465118	4601155	donald1024
4871495	4880184	5088118	rainbow
4844484	4922980	5139273	ecdonaldp192
5093448	5225102	5337233	ecdonaldp160
6321052	6417128	6611300	ecdonaldp224
7754309	7915698	8169050	ecdonaldp256
10009599	10127975	16783356	ecdonaldk163
10869842	11000542	17660838	ecdonaldb163
14800620	14858062	21690872	donald2048
19215529	25891282	26161211	ecdonaldp384
20195974	26744961	27037513	ecdonaldk233
22461296	29119464	29285556	ecdonaldb233
43648656	43769076	43885308	ecdonaldk283
45886932	46085280	46308864	ecdonaldp521
48552180	48718200	48919008	ecdonaldb283
103559916	104336520	110446536	ecdonaldk409
122857980	123424896	123818532	ecdonaldb409
243258228	248527632	248916552	ecdonaldk571
281108676	287328612	287806404	ecdonaldb571

Signing 0 bytes	
bytes	system
37	sflashv2
40	donald1024
40	donald2048
40	donald512
40	ecdonaldp160
42	ecdonaldb163
42	ecdonaldk163
43	rainbow
48	ecdonaldp192
56	ecdonaldp224
60	ecdonaldb233
60	ecdonaldk233
64	ecdonaldp256
64	ronald512
72	ecdonaldb283
72	ecdonaldk283
96	ecdonaldp384
96	ronald768
104	ecdonaldb409
104	ecdonaldk409
128	ronald1024
132	ecdonaldp521
144	ecdonaldb571
144	ecdonaldk571
192	ronald1536
256	ronald2048
384	ronald3072
512	ronald4096

Signing 23 bytes	
bytes	system
37	sflashv2
40	donald1024
40	donald2048
40	donald512
40	ecdonaldp160
41	ronald512
42	ecdonaldb163
42	ecdonaldk163
43	rainbow
48	ecdonaldp192
56	ecdonaldp224
60	ecdonaldb233
60	ecdonaldk233
64	ecdonaldp256
72	ecdonaldb283
72	ecdonaldk283
73	ronald768
96	ecdonaldp384
104	ecdonaldb409
104	ecdonaldk409
105	ronald1024
132	ecdonaldp521
144	ecdonaldb571
144	ecdonaldk571
169	ronald1536
233	ronald2048
361	ronald3072
489	ronald4096

Signing many bytes	
bytes	system
37	sflashv2
40	donald1024
40	donald2048
40	donald512
40	ecdonaldp160
42	ecdonaldb163
42	ecdonaldk163
43	rainbow
43	ronald1024
43	ronald1536
43	ronald2048
43	ronald3072
43	ronald4096
43	ronald512
43	ronald768
48	ecdonaldp192
56	ecdonaldp224
60	ecdonaldb233
60	ecdonaldk233
64	ecdonaldp256
72	ecdonaldb283
72	ecdonaldk283
96	ecdonaldp384
104	ecdonaldb409
104	ecdonaldk409
132	ecdonaldp521
144	ecdonaldb571
144	ecdonaldk571

10.24 x86, 1403MHz, AMD Opteron 240 (f58), `nmisles8amd64`



Cycles to generate a key pair			
quartile	median	quartile	system
739267	745148	752018	donald512
2180449	2206392	2233912	donald1024
7144981	7199102	7256029	donald2048
12009893	12112313	12197293	bls
31975256	45171198	63080330	ronald512
69915658	108424749	159627908	ronald768
132959952	203445134	295158340	ronald1024
418007576	603000360	828128504	ronald1536
700871540	1152552145	1958673334	ronald2048
1256690558	1256848012	1257940757	sflashv2
3966100676	5556316865	10930278936	ronald3072
8486988634	15540960656	23135301911	ronald4096

Secret key	
bytes	system
20	bls
84	donald512
148	donald1024
276	donald2048
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096

Cycles to sign 59 bytes			
quartile	median	quartile	system
288287	288292	288457	sflashv2
878175	885102	896872	donald512
1018602	1027145	1043598	ronald512
1691466	1707942	1814564	bls
2305374	2323837	2342443	donald1024
2618562	2622636	2625204	ronald768
4502323	4516224	4526668	ronald1024
7260483	7316654	7371274	donald2048
13454336	13523569	13561676	ronald1536
25781526	25791349	25807200	ronald2048
83874087	83911731	83945079	ronald3072
169074106	169139350	169433709	ronald4096

Public key	
bytes	system
64	donald512
64	ronald512
96	ronald768
128	donald1024
128	ronald1024
192	ronald1536
240	bls
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2

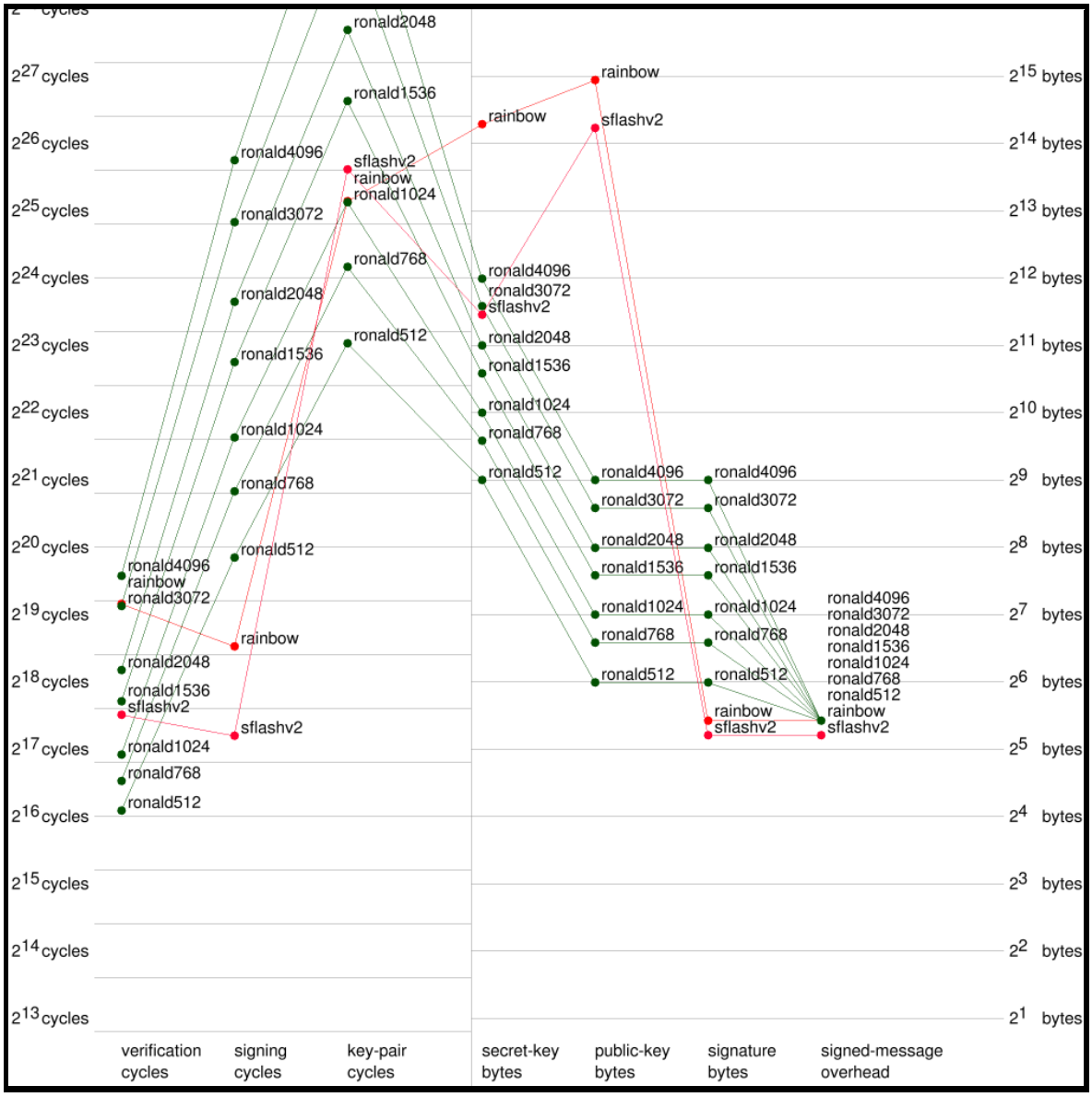
Cycles to verify 59 bytes			
quartile	median	quartile	system
73703	81031	83184	ronald512
94762	96682	97935	ronald768
122486	127168	129897	ronald1024
230607	230869	231314	ronald1536
338683	340182	343587	ronald2048
367279	367718	368003	sflashv2
698391	703822	706191	ronald3072
1015442	1041983	1054044	donald512
1120276	1121639	1127133	ronald4096
2775429	2807051	2848369	donald1024
8779736	8842714	8947546	donald2048
19923964	19955418	20053595	bls

Signing 0 bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
41	`ronald512`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.25 x86, 1833MHz, Intel Core Duo, `nmi0068`



Cycles to generate a key pair			
quartile	median	quartile	system
45829949	58372633	80937175	`ronald512`
109899493	155944811	214727546	`ronald768`
229916819	357946479	479084166	`ronald1024`
363261789	363548086	363765556	`rainbow`
544703555	545320292	545415475	`sflashv2`
837847395	1315412032	2035840906	`ronald1536`
2074070581	3300174625	5432893004	`ronald2048`
7373662934	11839556102	19149236700	`ronald3072`
25966033401	41230080199	71884538572	`ronald4096`

Secret key	
bytes	system
512	`ronald512`
768	`ronald768`
1024	`ronald1024`
1536	`ronald1536`
2048	`ronald2048`
2823	`sflashv2`
3072	`ronald3072`
4096	`ronald4096`
20107	`rainbow`

Cycles to sign 59 bytes			
quartile	median	quartile	system
370832	371327	371789	`sflashv2`
1169861	1176747	1182203	`rainbow`
3671492	3683570	3697837	`ronald512`
8643107	8674864	8700637	`ronald768`
17311360	17341478	17362796	`ronald1024`
45656523	45696244	45773024	`ronald1536`
99487564	99575432	100027719	`ronald2048`
277153426	277393446	277602336	`ronald3072`
612881038	613251155	613976528	`ronald4096`

Public key	
bytes	system
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
19266	`sflashv2`
31680	`rainbow`

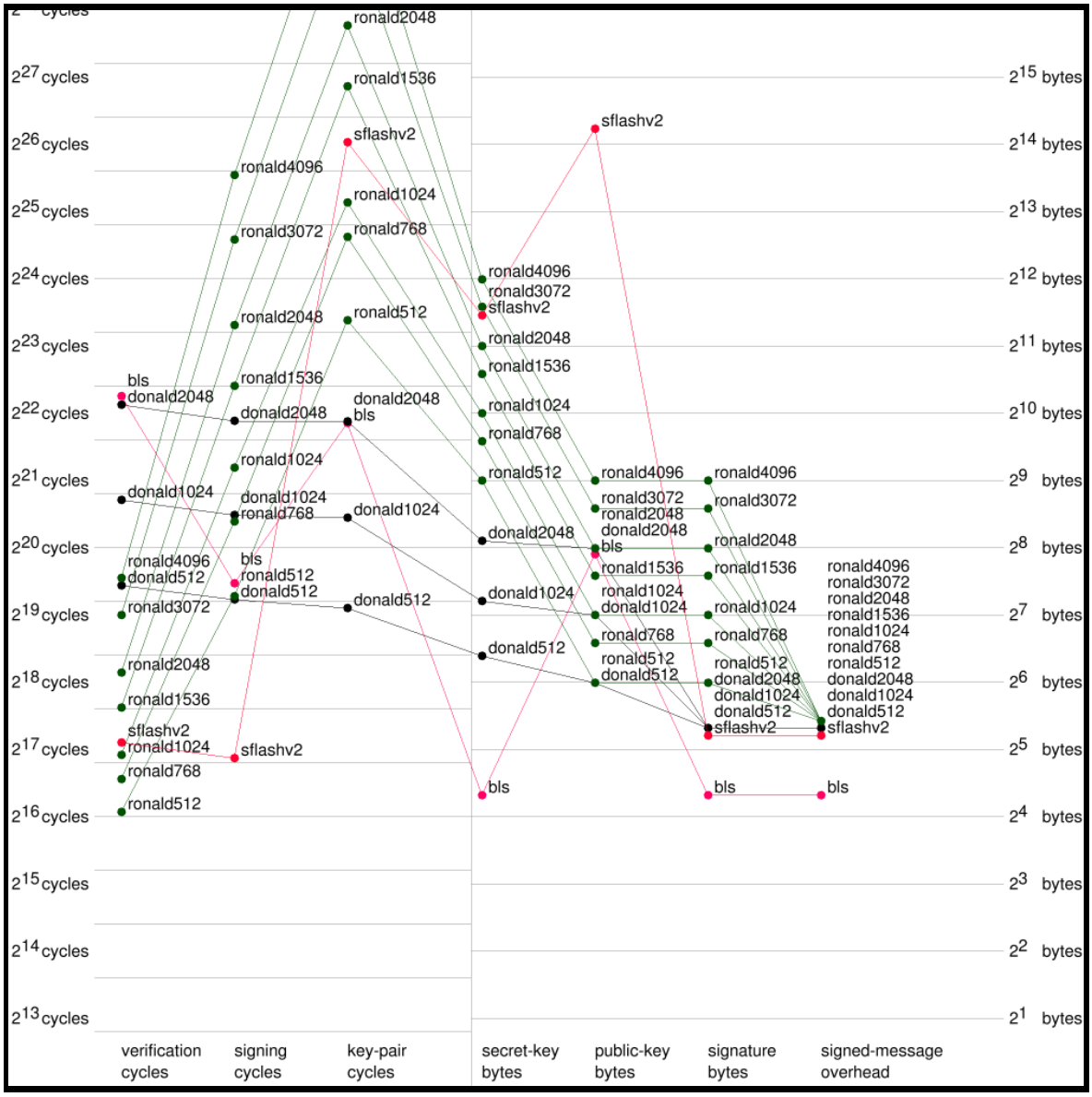
Cycles to verify 59 bytes			
quartile	median	quartile	system
140459	142120	143330	`ronald512`
208120	208439	208879	`ronald768`
287276	291181	291808	`ronald1024`
483736	486244	486684	`sflashv2`
577632	578314	578919	`ronald1536`
863588	864391	865139	`ronald2048`
1979769	1980429	1986468	`ronald3072`
2023450	2030204	2058089	`rainbow`
2902141	2910677	2920731	`ronald4096`

Signing 0 bytes	
bytes	system
37	`sflashv2`
43	`rainbow`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
37	`sflashv2`
41	`ronald512`
43	`rainbow`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
37	`sflashv2`
43	`rainbow`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.26 x86, 2400MHz, Intel Pentium 4 (f24), `nmitest4`



Cycles to generate a key pair			
quartile	median	quartile	system
1926784	1942492	1962196	`donald512`
6141540	6202592	6246600	`donald1024`
20881148	21027916	21176456	`bls`
21215816	21457532	21662116	`donald2048`
61230816	79117120	103595808	`ronald512`
162137388	231099008	298589132	`ronald768`
214779668	359551120	585970440	`ronald1024`
784917616	785416008	797440932	`sflashv2`
972028492	1609420664	2318237480	`ronald1536`
2269485628	3523851468	5592735132	`ronald2048`
7953672024	13791717876	19295783768	`ronald3072`
26344257120	38537292224	58615704308	`ronald4096`

Secret key	
bytes	system
20	`bls`
84	`donald512`
148	`donald1024`
276	`donald2048`
512	`ronald512`
768	`ronald768`
1024	`ronald1024`
1536	`ronald1536`
2048	`ronald2048`
2823	`sflashv2`
3072	`ronald3072`
4096	`ronald4096`

Cycles to sign 59 bytes			
quartile	median	quartile	system
274768	280160	282704	`sflashv2`
2139208	2167064	2186200	`donald512`
2255424	2260204	2267956	`ronald512`
2641552	2663996	2852116	`bls`
5891112	5928144	5954044	`ronald768`
6330140	6416896	6474908	`donald1024`
11765504	11797096	11830380	`ronald1024`
21425088	21635660	21831736	`donald2048`
33696472	33981820	34319608	`ronald1536`
74087052	74198780	74354404	`ronald2048`
222955024	223952812	225879672	`ronald3072`
513038396	513522600	514363244	`ronald4096`

Public key	
bytes	system
64	`donald512`
64	`ronald512`
96	`ronald768`
128	`donald1024`
128	`ronald1024`
192	`ronald1536`
240	`bls`
256	`donald2048`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
19266	`sflashv2`

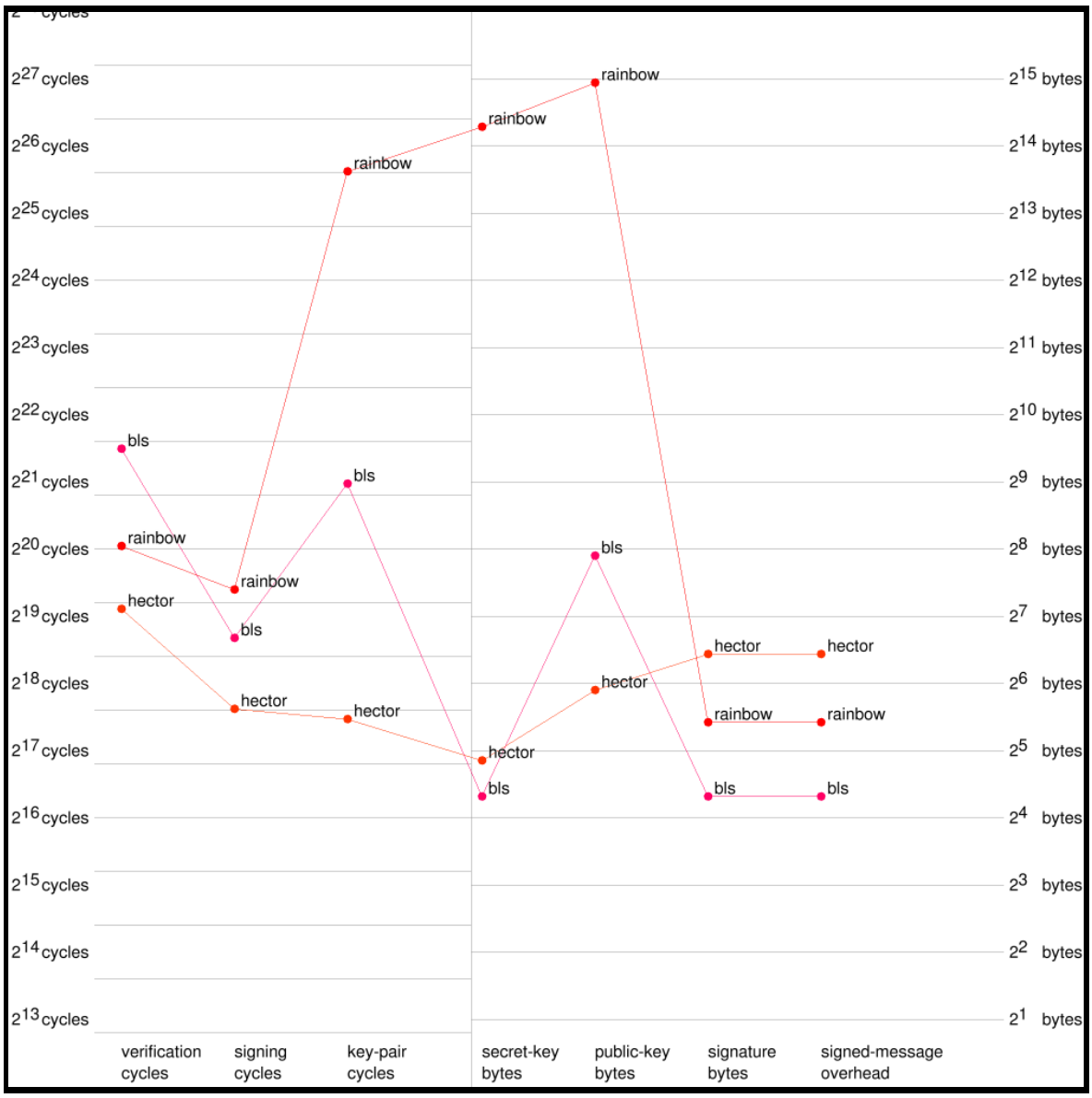
Cycles to verify 59 bytes			
quartile	median	quartile	system
136028	140412	141172	`ronald512`
207136	213548	214080	`ronald768`
289656	292232	296568	`ronald1024`
342444	342716	344256	`sflashv2`
535180	535572	539680	`ronald1536`
840276	842988	849080	`ronald2048`
1766692	1770296	1773448	`ronald3072`
2564828	2597008	2623888	`donald512`
2850972	2863956	2881164	`ronald4096`
7684436	7804280	7982260	`donald1024`
26300316	26680960	26733304	`donald2048`
29566480	29648288	29807536	`bls`

Signing 0 bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
41	`ronald512`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.27 x86, 2400MHz, Intel Core 2 Duo (6fb), `utrecht`



Cycles to generate a key pair			
quartile	median	quartile	system
467442	469935	500013	`hector`
9719334	9783648	9859005	`bls`
550807740	551252394	551513691	`rainbow`

Secret key	
bytes	system
20	`bls`
29	`hector`
20107	`rainbow`

Cycles to sign 59 bytes			
quartile	median	quartile	system
510174	536022	564399	`hector`
1329381	1338102	1423665	`bls`
2497446	2508975	2520288	`rainbow`

Public key	
bytes	system
60	`hector`
240	`bls`
31680	`rainbow`

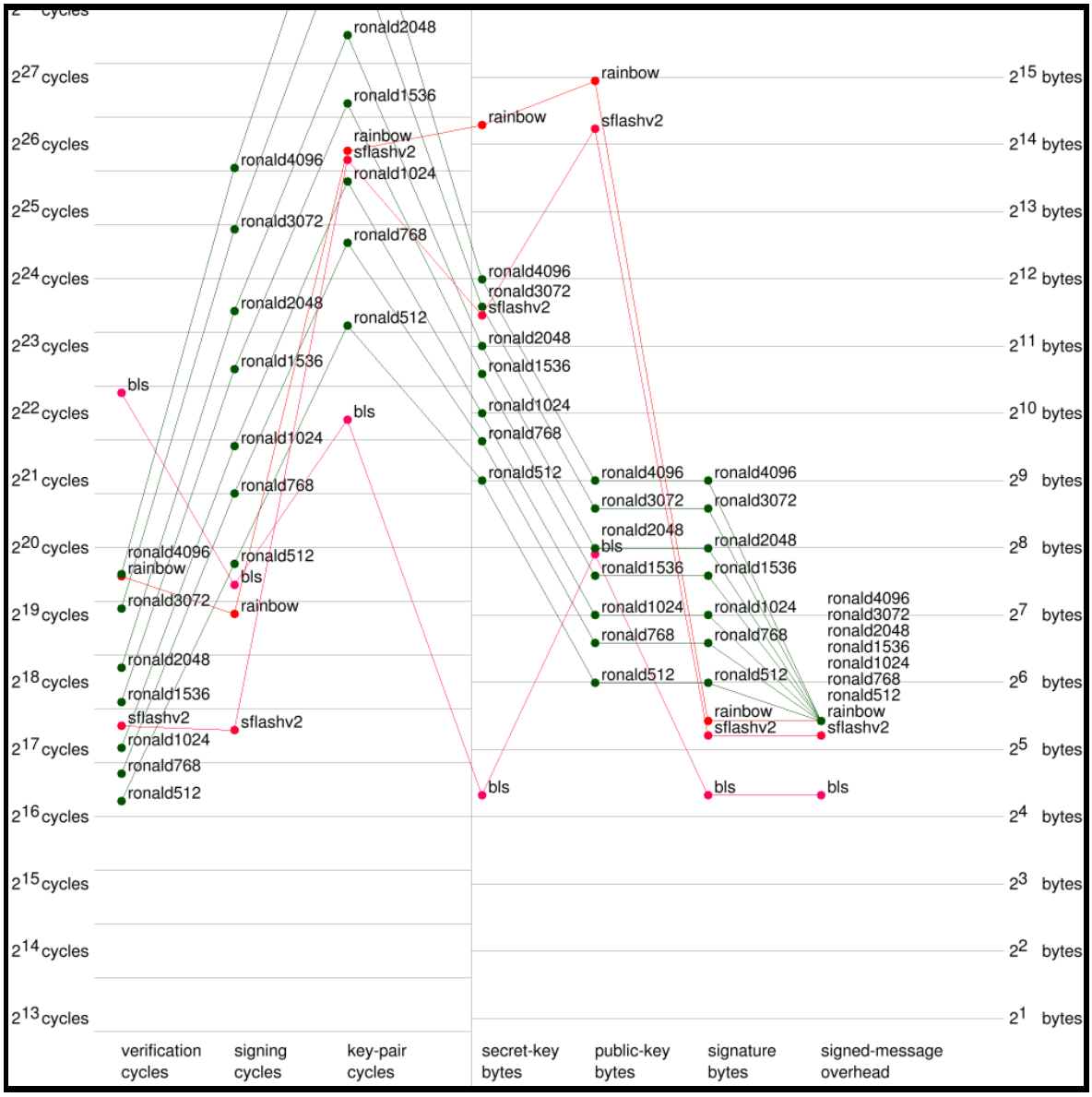
Cycles to verify 59 bytes			
quartile	median	quartile	system
1947645	1949517	1983105	`hector`
4379346	4389615	4413420	`rainbow`
15292962	15333858	15405156	`bls`

Signing 0 bytes	
bytes	system
20	`bls`
43	`rainbow`
87	`hector`

Signing 23 bytes	
bytes	system
20	`bls`
43	`rainbow`
87	`hector`

Signing many bytes	
bytes	system
20	`bls`
43	`rainbow`
87	`hector`

10.28 x86, 2401MHz, Intel Pentium 4 (f24), `nmi0086`



Cycles to generate a key pair			
quartile	median	quartile	system
21804972	21947432	22111980	bls
52228312	73692352	96839056	ronald512
122682828	214949648	325925092	ronald768
271207108	473293452	606975644	ronald1024
618721784	621263632	623909396	sflashv2
695956128	701921536	706481052	rainbow
738286120	1290560976	2017135192	ronald1536
2261460224	3102865324	4494672648	ronald2048
7360399368	12929213664	19048408524	ronald3072
23550877280	42544873132	63476206920	ronald4096

Secret key	
bytes	system
20	bls
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096
20107	rainbow

Cycles to sign 59 bytes			
quartile	median	quartile	system
396972	401948	410536	sflashv2
1786368	1798484	1812296	rainbow
2582992	2609444	2669712	bls
3402096	3423732	3460992	ronald512
8392504	8459424	8587940	ronald768
15477200	15562004	15659400	ronald1024
41927860	42096596	42322076	ronald1536
88864748	89077460	89564520	ronald2048
253576416	254781324	255670756	ronald3072
560629356	561715728	563316836	ronald4096

Public key	
bytes	system
64	ronald512
96	ronald768
128	ronald1024
192	ronald1536
240	bls
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2
31680	rainbow

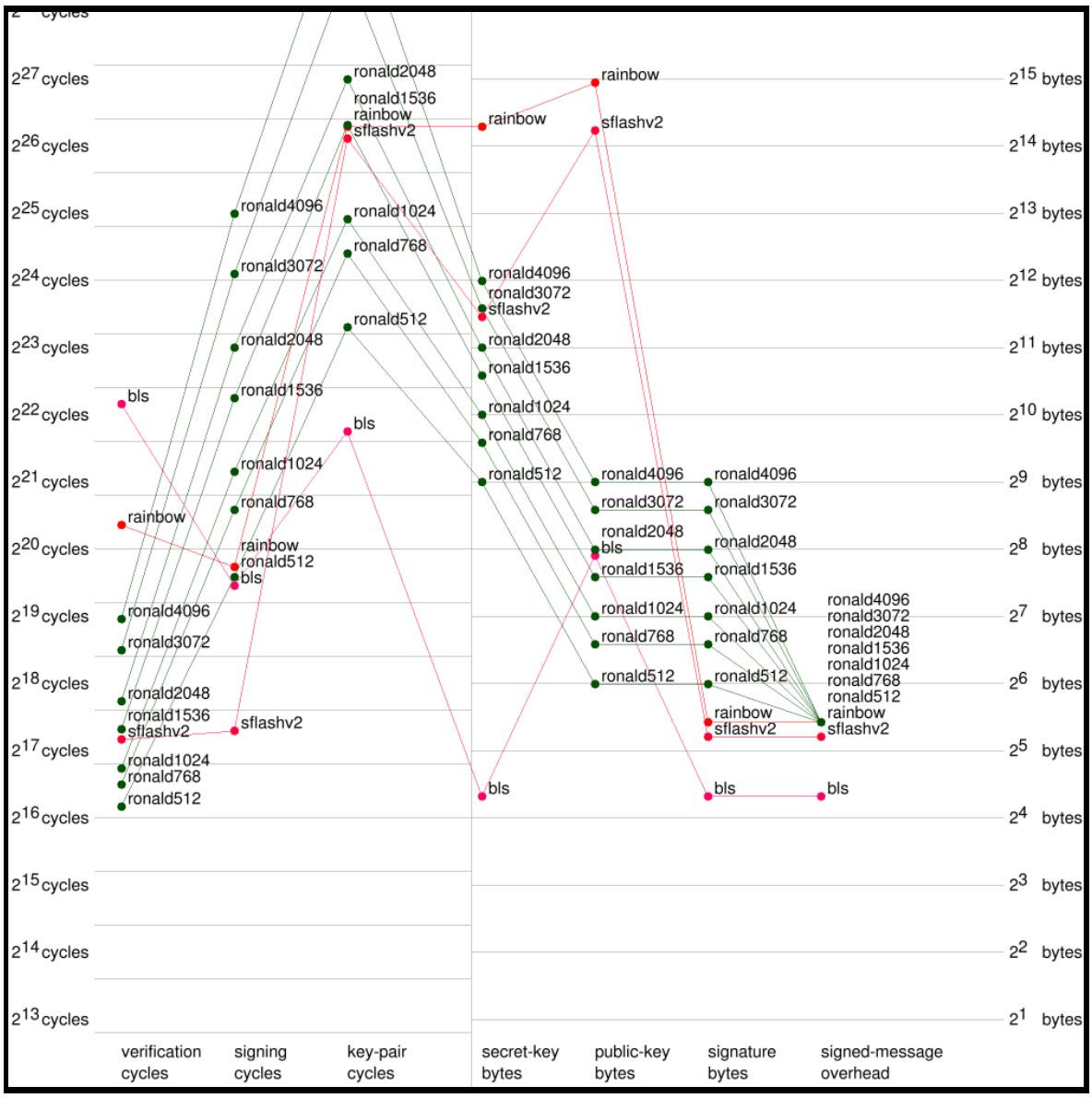
Cycles to verify 59 bytes			
quartile	median	quartile	system
157860	160472	162036	ronald512
216696	229404	237700	ronald768
319380	320492	324564	ronald1024
423240	423752	426964	sflashv2
572628	575712	581756	ronald1536
892456	897564	908592	ronald2048
1924324	1928704	1953020	ronald3072
2889936	2922940	2988632	rainbow
2995736	3003440	3011728	ronald4096
30910988	31056896	31298080	bls

Signing 0 bytes	
bytes	system
20	`bls`
37	`sflashv2`
43	`rainbow`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
20	`bls`
37	`sflashv2`
41	`ronald512`
43	`rainbow`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
20	`bls`
37	`sflashv2`
43	`rainbow`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.29 x86, 2658MHz, Intel Xeon (f25), nmi0013



Cycles to generate a key pair			
quartile	median	quartile	system
19011196	19167524	19317128	`bls`
53729856	73829960	96568216	`ronald512`
110364776	191128364	272077824	`ronald768`
176275812	297432976	440333220	`ronald1024`
836275868	836757548	839840616	`sflashv2`
973492368	974762680	977110700	`rainbow`
533669400	998944988	1449641310	`ronald1536`
1057398372	1805129968	2873439592	`ronald2048`
4494697116	7596521840	10646657540	`ronald3072`
13684713580	22204952460	33402244680	`ronald4096`

Secret key	
bytes	system
20	`bls`
512	`ronald512`
768	`ronald768`
1024	`ronald1024`
1536	`ronald1536`
2048	`ronald2048`
2823	`sflashv2`
3072	`ronald3072`
4096	`ronald4096`
20107	`rainbow`

Cycles to sign 59 bytes			
quartile	median	quartile	system
402512	404272	407172	`sflashv2`
2508268	2634804	2705228	`bls`
2907744	2929360	2973324	`ronald512`
3316844	3355860	3390436	`rainbow`
6941448	6958852	6994440	`ronald768`
11380740	11429748	11473096	`ronald1024`
28492096	29537488	30401288	`ronald1536`
56616428	56786080	57105176	`ronald2048`
144746568	146873184	149052608	`ronald3072`
315928168	318060600	318892992	`ronald4096`

Public key	
bytes	system
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
240	`bls`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
19266	`sflashv2`
31680	`rainbow`

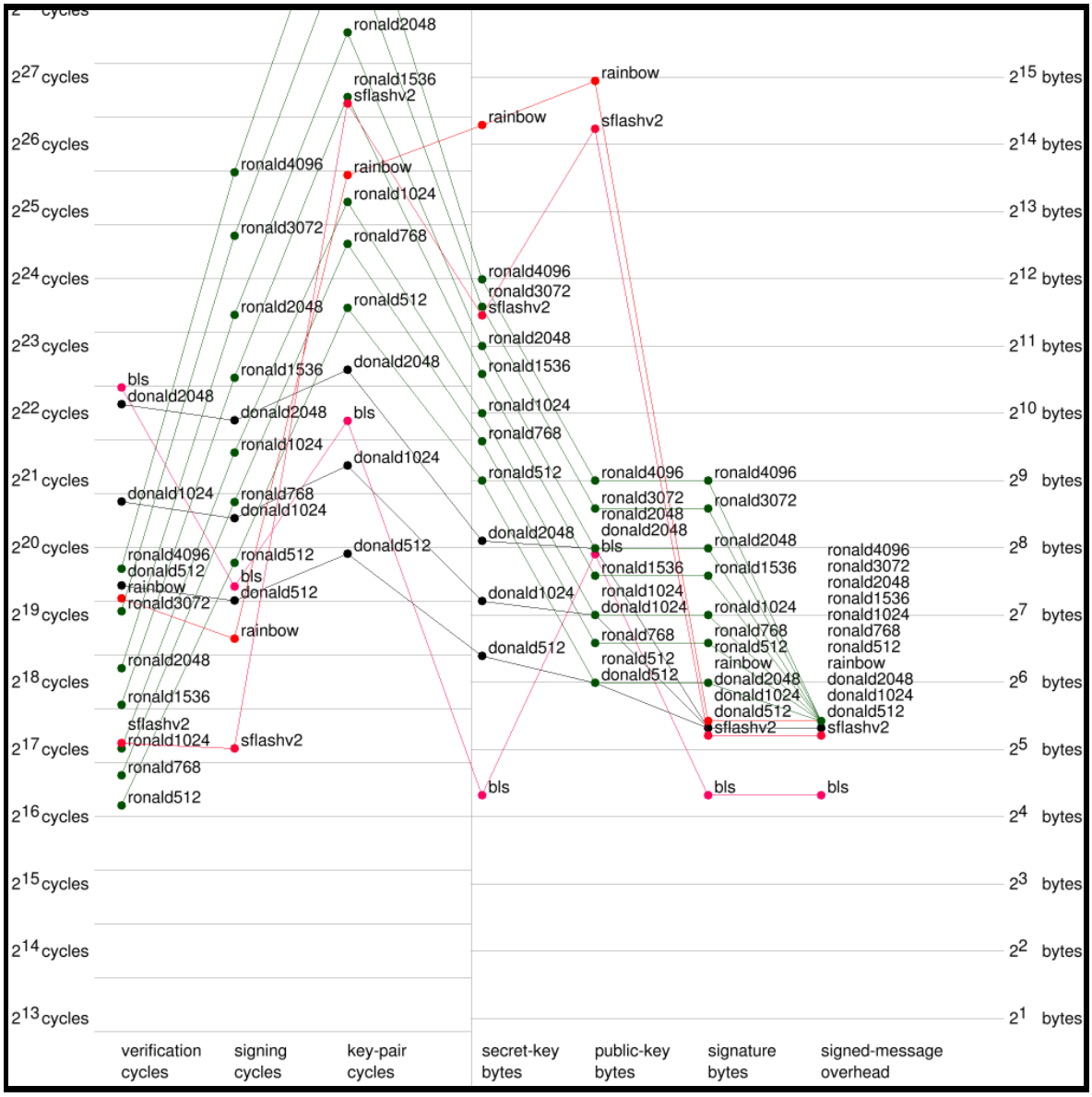
Cycles to verify 59 bytes			
quartile	median	quartile	system
150948	151988	153800	`ronald512`
201148	201864	202684	`ronald768`
245360	248328	251376	`ronald1024`
362512	362768	363132	`sflashv2`
410412	412884	415836	`ronald1536`
584492	591360	613188	`ronald2048`
1132144	1145056	1162720	`ronald3072`
1702324	1715216	1753376	`ronald4096`
5656840	5757172	5774088	`rainbow`
27334092	27410216	27507236	`bls`

Signing 0 bytes	
bytes	system
20	`bls`
37	`sflashv2`
43	`rainbow`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
20	`bls`
37	`sflashv2`
41	`ronald512`
43	`rainbow`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
20	`bls`
37	`sflashv2`
43	`rainbow`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.30 x86, 2658MHz, Intel Xeon (f25), `nmibuild15`



Cycles to generate a key pair			
quartile	median	quartile	system
3850132	3887664	3931200	donald512
12023980	12142172	12274980	donald1024
21345492	21541032	21644548	bls
41276336	41678532	42112104	donald2048
60213652	92437372	135815532	ronald512
141472244	211156008	301518976	ronald768
230902648	362134268	570996200	ronald1024
508883864	511702390	512724220	rainbow
1286943100	1287565300	1288461468	sflashv2
826002008	1401731136	1923573352	ronald1536
2119868808	3223227704	4698495920	ronald2048
7471002986	11161271696	17810136740	ronald3072
21826656700	34852477780	55440670160	ronald4096

Secret key	
bytes	system
20	bls
84	donald512
148	donald1024
276	donald2048
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096
20107	rainbow

Cycles to sign 59 bytes			
quartile	median	quartile	system
313560	316756	320740	sflashv2
1284188	1302024	1334972	rainbow
2118292	2137580	2154816	donald512
2530076	2554604	2716124	bls
3434520	3466500	3506520	ronald512
6108768	6162608	6216384	donald1024
7548040	7591816	7634704	ronald768
14292116	14347624	14394428	ronald1024
21546772	21775376	22043216	donald2048
37450684	37538132	37643728	ronald1536
84521248	84671492	84877828	ronald2048
234641600	235234636	236077404	ronald3072
531132432	532499816	533986568	ronald4096

Public key	
bytes	system
64	donald512
64	ronald512
96	ronald768
128	donald1024
128	ronald1024
192	ronald1536
240	bls
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2
31680	rainbow

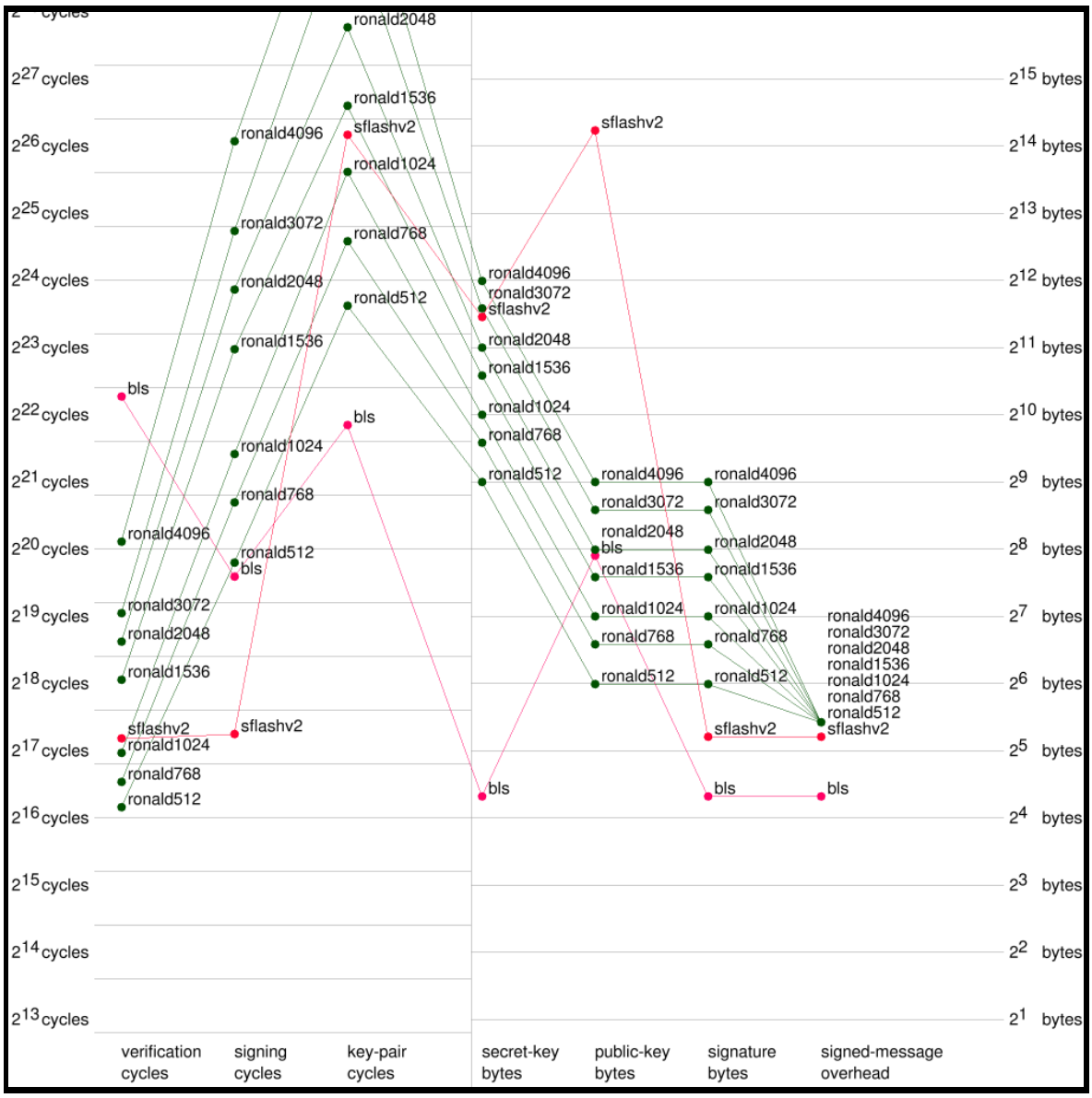
Cycles to verify 59 bytes			
quartile	median	quartile	system
149680	151912	161340	ronald512
222744	224452	232380	ronald768
314616	318036	319724	ronald1024
338172	339600	349084	sflashv2
554804	557444	559348	ronald1536
889464	891000	892204	ronald2048
1846312	1854852	1864048	ronald3072
2193788	2195316	2196472	rainbow
2556976	2596176	2622344	donald512
3190772	3203408	3205492	ronald4096
7446240	7652028	7728584	donald1024
26489868	26730224	26763800	donald2048
33089588	33182888	33339616	bls

Signing 0 bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`rainbow`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
41	`ronald512`
43	`rainbow`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`rainbow`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.31 x86, 2658MHz, Intel Xeon (f25), `nmibuild16`



Cycles to generate a key pair			
quartile	median	quartile	system
20676680	20842588	20969380	`bls`
75158044	97106000	127778412	`ronald512`
162973604	223878156	311134020	`ronald768`
353293992	546778544	831051792	`ronald1024`
870780000	878448684	893839800	`sflashv2`
762802888	1282999020	1903293844	`ronald1536`
2089397292	3522260444	5856464624	`ronald2048`
8272452700	15659323352	24607547780	`ronald3072`
26250070904	49536214142	72187807108	`ronald4096`

Secret key	
bytes	system
20	`bls`
512	`ronald512`
768	`ronald768`
1024	`ronald1024`
1536	`ronald1536`
2048	`ronald2048`
2823	`sflashv2`
3072	`ronald3072`
4096	`ronald4096`

Cycles to sign 59 bytes			
quartile	median	quartile	system
386396	387984	469528	`sflashv2`
2519488	2965252	3130140	`bls`
3527676	3550620	3573004	`ronald512`
7627760	7676312	7721092	`ronald768`
14289948	14348304	14411556	`ronald1024`
38932188	55416064	56061868	`ronald1536`
81119376	119333340	120181844	`ronald2048`
251565544	254812664	364640024	`ronald3072`
545706252	808858292	810169452	`ronald4096`

Public key	
bytes	system
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
240	`bls`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
19266	`sflashv2`

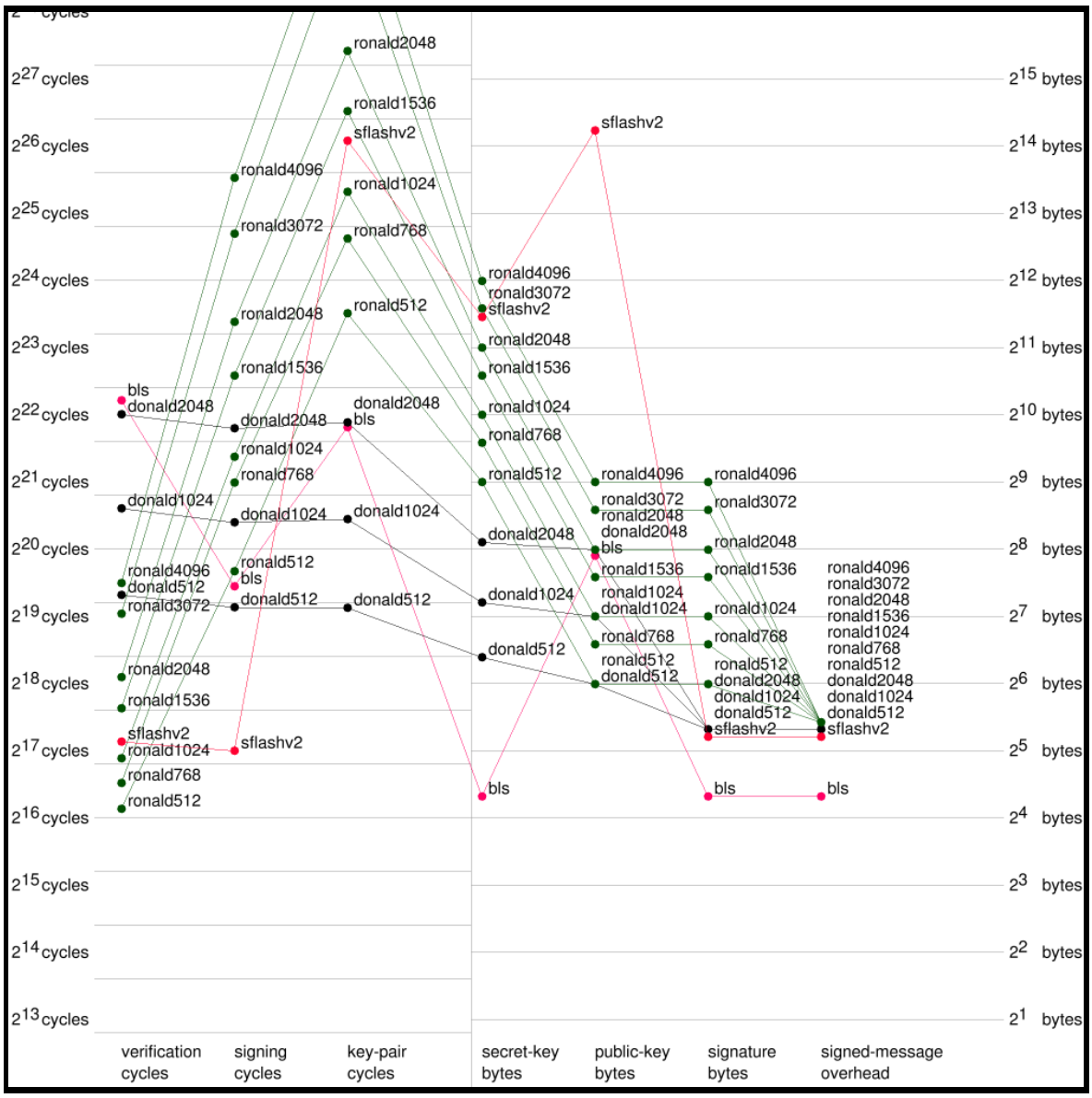
Cycles to verify 59 bytes			
quartile	median	quartile	system
142768	151208	152468	`ronald512`
207896	208636	219384	`ronald768`
303684	304740	463756	`ronald1024`
366032	367308	516056	`sflashv2`
544572	782008	783344	`ronald1536`
892688	1278364	1280112	`ronald2048`
1840288	1843700	1851004	`ronald3072`
3178000	4624180	4632592	`ronald4096`
29923708	30211904	38563540	`bls`

Signing 0 bytes	
bytes	system
20	`bls`
37	`sflashv2`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
20	`bls`
37	`sflashv2`
41	`ronald512`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
20	`bls`
37	`sflashv2`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.32 x86, 2658MHz, Intel Xeon (f25), `nmibuild22`



Cycles to generate a key pair			
quartile	median	quartile	system
1978112	1981880	1986636	donald512
6206724	6215556	6222324	donald1024
20144632	20334152	20472272	bls
21509300	21581872	21750116	donald2048
63574740	88197996	112213632	ronald512
165602740	230503048	337900904	ronald768
271681956	422470804	573485332	ronald1024
813273448	817140364	898533228	sflashv2
750573000	1194379752	1616518404	ronald1536
1534849928	2602041204	4418936916	ronald2048
7528256972	13990251260	22438063840	ronald3072
19417260644	30878128796	53778457324	ronald4096

Secret key	
bytes	system
20	bls
84	donald512
148	donald1024
276	donald2048
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096

Cycles to sign 59 bytes			
quartile	median	quartile	system
312424	313828	315276	sflashv2
1975064	1988640	1998232	donald512
2580472	2609112	2796136	bls
3127304	3158676	3188788	ronald512
5891552	5941568	5993560	donald1024
7737152	9907776	13370580	ronald768
13822088	13900132	13961656	ronald1024
19894076	19982776	20110792	donald2048
39149044	39528796	39949608	ronald1536
78546452	78899620	79135140	ronald2048
245483140	246348456	247089676	ronald3072
504948668	505873024	507873504	ronald4096

Public key	
bytes	system
64	donald512
64	ronald512
96	ronald768
128	donald1024
128	ronald1024
192	ronald1536
240	bls
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2

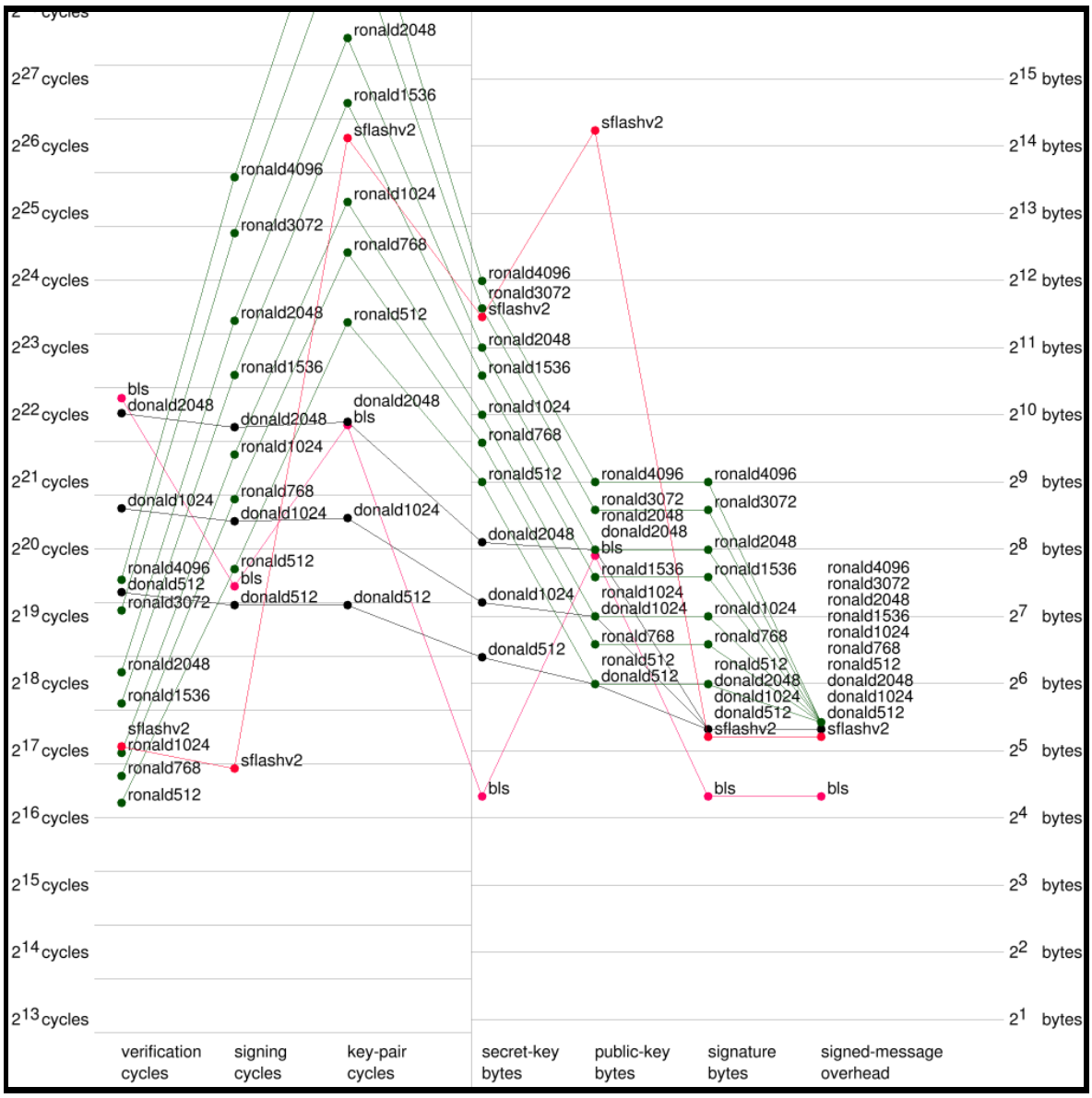
Cycles to verify 59 bytes			
quartile	median	quartile	system
143004	147720	149260	ronald512
205088	206848	342180	ronald768
281880	283880	285188	ronald1024
333772	352016	353320	sflashv2
540364	542520	543740	ronald1536
802116	806220	809584	ronald2048
1833504	1837384	1841436	ronald3072
2316380	2333720	2337664	donald512
2708128	2710308	2712984	ronald4096
7094212	7145140	7184400	donald1024
23791804	23958824	24070296	donald2048
28677608	28802564	28911672	bls

Signing 0 bytes	
bytes	system
20	bls
37	sflashv2
40	donald1024
40	donald2048
40	donald512
64	ronald512
96	ronald768
128	ronald1024
192	ronald1536
256	ronald2048
384	ronald3072
512	ronald4096

Signing 23 bytes	
bytes	system
20	bls
37	sflashv2
40	donald1024
40	donald2048
40	donald512
41	ronald512
73	ronald768
105	ronald1024
169	ronald1536
233	ronald2048
361	ronald3072
489	ronald4096

Signing many bytes	
bytes	system
20	bls
37	sflashv2
40	donald1024
40	donald2048
40	donald512
43	ronald1024
43	ronald1536
43	ronald2048
43	ronald3072
43	ronald4096
43	ronald512
43	ronald768

10.33 x86, 2659MHz, Intel Xeon (f25), `nmibuild21`



Cycles to generate a key pair			
quartile	median	quartile	system
2035100	2046784	2054248	donald512
6276488	6300920	6326160	donald1024
20630804	20806348	20957344	bls
21683528	21720908	21760176	donald2048
61381476	78334376	122254972	ronald512
137576168	192617268	274662668	ronald768
261338256	369887284	641893100	ronald1024
838526748	843067212	847047264	sflashv2
962706012	1324320636	2062747340	ronald1536
1907928256	3073395940	5357449000	ronald2048
6997765800	14174571862	21134092164	ronald3072
22794943996	39712451040	55289766358	ronald4096

Secret key	
bytes	system
20	bls
84	donald512
148	donald1024
276	donald2048
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096

Cycles to sign 59 bytes			
quartile	median	quartile	system
247036	249608	254140	sflashv2
2023876	2040728	2053216	donald512
2587492	2606292	2750760	bls
3225684	3256020	3290084	ronald512
5945632	6017100	6076092	donald1024
7910940	8024284	8165704	ronald768
14195532	14236392	14285020	ronald1024
20119112	20313192	20468916	donald2048
39521060	39737660	40379744	ronald1536
79712236	79983060	80247004	ronald2048
247562036	248299116	249109388	ronald3072
507326148	509665368	510963560	ronald4096

Public key	
bytes	system
64	donald512
64	ronald512
96	ronald768
128	donald1024
128	ronald1024
192	ronald1536
240	bls
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2

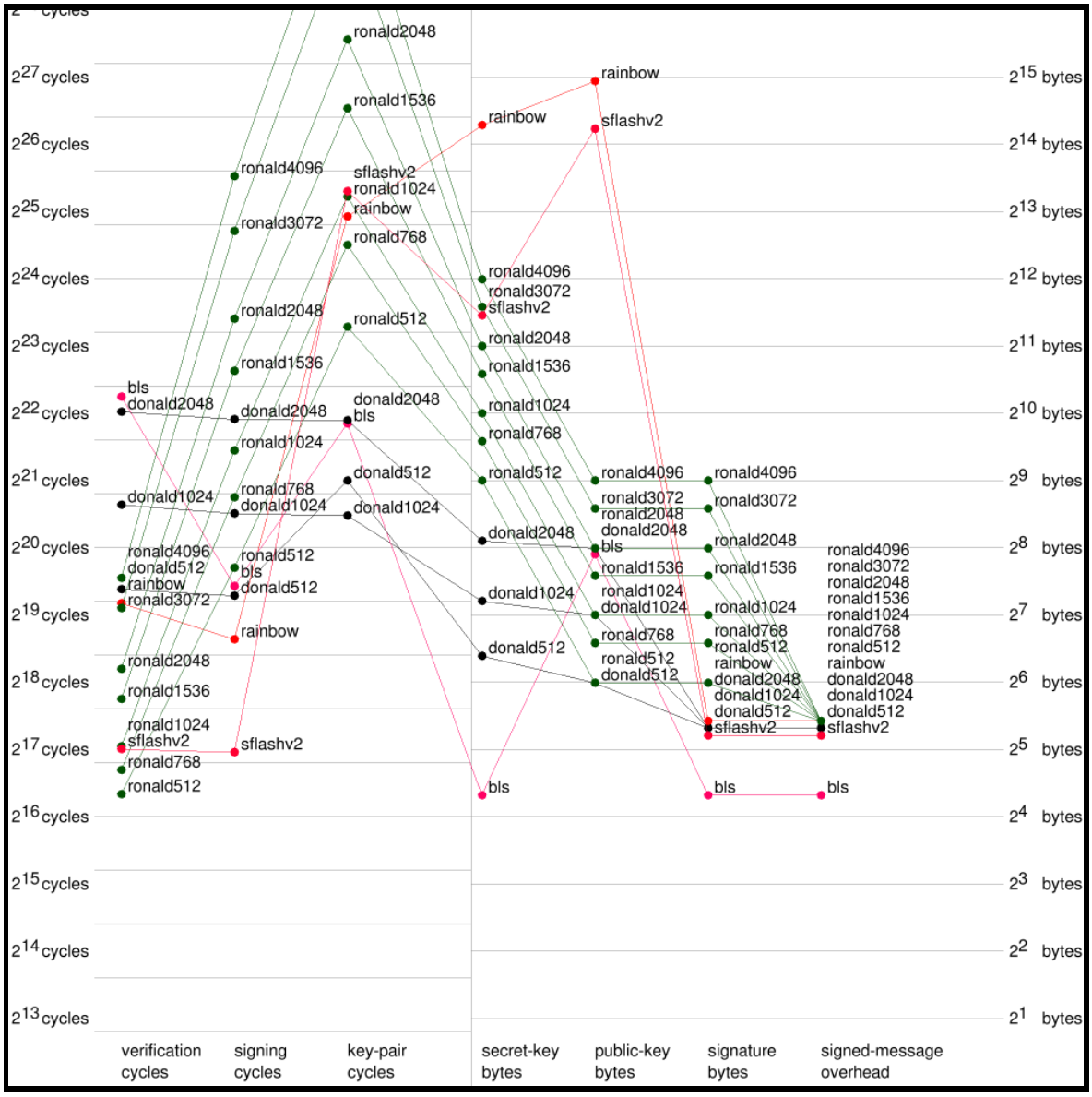
Cycles to verify 59 bytes			
quartile	median	quartile	system
158904	159476	164624	ronald512
218884	225544	233364	ronald768
298984	303276	305952	ronald1024
327488	330632	335840	sflashv2
574568	576800	582476	ronald1536
853592	858664	867144	ronald2048
1902696	1911948	1925268	ronald3072
2396580	2419984	2430688	donald512
2800792	2829800	2841588	ronald4096
7073712	7151808	7193880	donald1024
24281624	24351920	24572948	donald2048
29361172	29459040	29595176	bls

Signing 0 bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
41	`ronald512`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.34 x86, 2659MHz, Intel Xeon (f25), nmibuild26



Cycles to generate a key pair			
quartile	median	quartile	system
6375232	6396376	6420068	donald1024
9888892	10035048	10133644	donald512
20698256	20883836	21016920	bls
21676472	21735940	21778388	donald2048
56178920	72493428	106452768	ronald512
135949432	208285084	302921564	ronald768
300448100	301499856	302840328	rainbow
259451956	390031004	643222568	ronald1024
413222676	415715068	417250968	sflashv2
865956284	1213099128	1792392448	ronald1536
1773464280	2949181700	4167230900	ronald2048
8816952100	13218543800	22665508382	ronald3072
15855570120	31004339780	46717791720	ronald4096

Secret key	
bytes	system
20	bls
84	donald512
148	donald1024
276	donald2048
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096
20107	rainbow

Cycles to sign 59 bytes			
quartile	median	quartile	system
302020	302924	304360	sflashv2
1245868	1291216	1354916	rainbow
2262424	2271788	2278928	donald512
2525528	2574588	2687944	bls
3237976	3267248	3300784	ronald512
6545976	6557076	6575944	donald1024
7906968	8075344	8316260	ronald768
14526940	14785812	15019208	ronald1024
21994632	22045208	22098196	donald2048
40756388	41068064	41444624	ronald1536
80361548	80613824	80950444	ronald2048
248387048	249491104	250663524	ronald3072
506354360	507550444	508692920	ronald4096

Public key	
bytes	system
64	donald512
64	ronald512
96	ronald768
128	donald1024
128	ronald1024
192	ronald1536
240	bls
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2
31680	rainbow

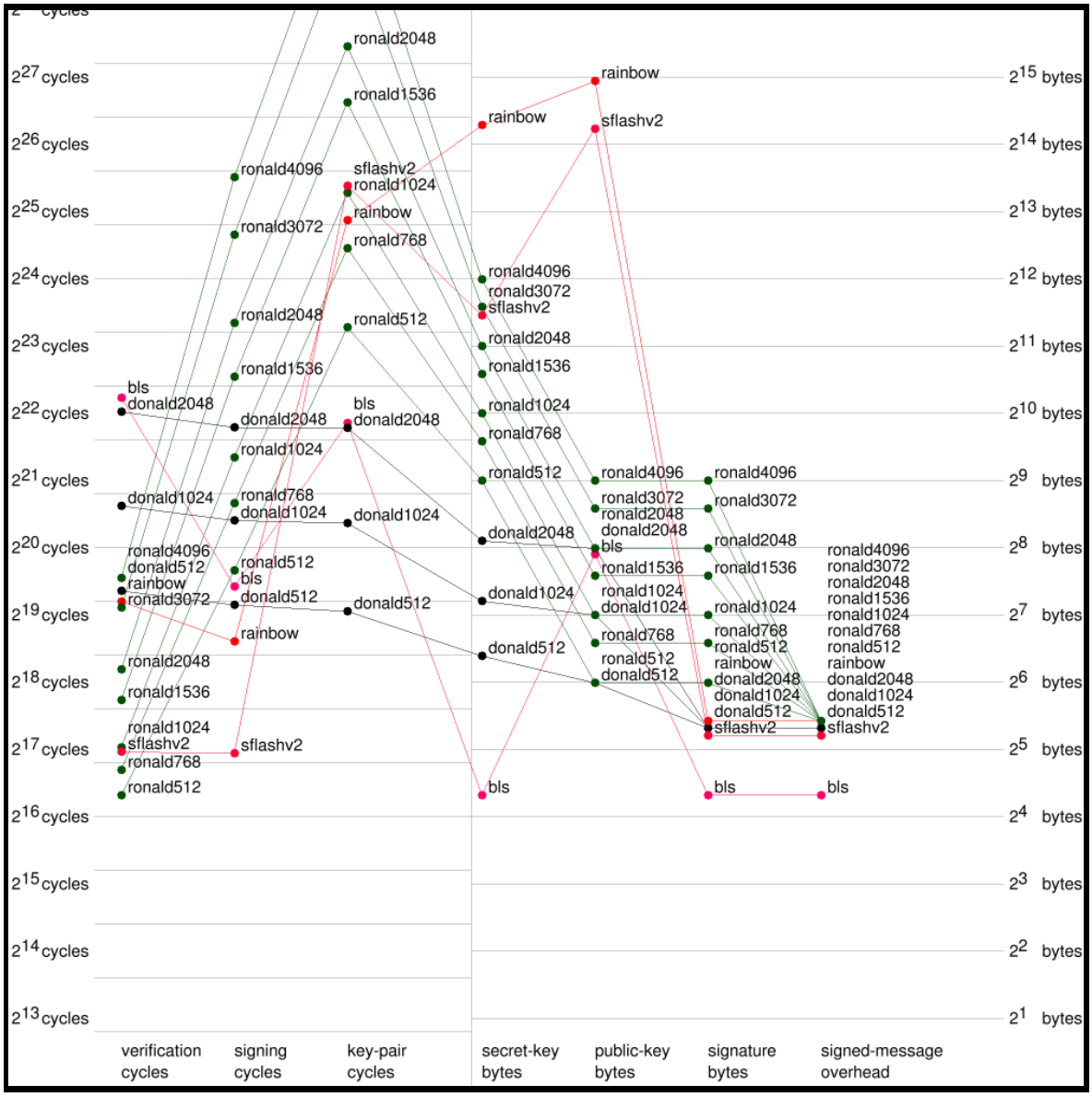
Cycles to verify 59 bytes			
quartile	median	quartile	system
169952	176028	177568	ronald512
238044	240552	243400	ronald768
310020	315112	321784	sflashv2
323348	325280	327924	ronald1024
594280	598612	604720	ronald1536
874216	882024	889192	ronald2048
1931628	1940064	1951956	ronald3072
2053628	2056100	2060324	rainbow
2443208	2475664	2484544	donald512
2852852	2859072	2867024	ronald4096
7153896	7329084	7425320	donald1024
24134928	24239388	24578272	donald2048
29325700	29496480	29639876	bls

Signing 0 bytes	
bytes	system
20	bls
37	sflashv2
40	donald1024
40	donald2048
40	donald512
43	rainbow
64	ronald512
96	ronald768
128	ronald1024
192	ronald1536
256	ronald2048
384	ronald3072
512	ronald4096

Signing 23 bytes	
bytes	system
20	bls
37	sflashv2
40	donald1024
40	donald2048
40	donald512
41	ronald512
43	rainbow
73	ronald768
105	ronald1024
169	ronald1536
233	ronald2048
361	ronald3072
489	ronald4096

Signing many bytes	
bytes	system
20	bls
37	sflashv2
40	donald1024
40	donald2048
40	donald512
43	rainbow
43	ronald1024
43	ronald1536
43	ronald2048
43	ronald3072
43	ronald4096
43	ronald512
43	ronald768

10.35 x86, 2667MHz, Intel Xeon (f25), `nmi0036`



Cycles to generate a key pair			
quartile	median	quartile	system
1836048	1856520	1876484	donald512
5733328	5776780	5817280	donald1024
19473952	19743796	19976208	donald2048
20819872	21006648	21160604	bls
55555796	72417804	94736908	ronald512
123956808	200149736	281714712	ronald768
286219180	287184036	290364680	rainbow
221131216	407445532	591024664	ronald1024
438990440	445787188	452260028	sflashv2
847051008	1306746416	2074758372	ronald1536
1703274616	2691541464	4751881496	ronald2048
7475800820	11727099640	20234187818	ronald3072
17103838662	27490605860	56668850102	ronald4096

Secret key	
bytes	system
20	bls
84	donald512
148	donald1024
276	donald2048
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096
20107	rainbow

Cycles to sign 59 bytes			
quartile	median	quartile	system
296980	298572	300552	sflashv2
1241220	1263460	1288196	rainbow
2000972	2023352	2039984	donald512
2515404	2555624	2688852	bls
3124460	3141384	3169020	ronald512
5930664	5982636	6026456	donald1024
7448664	7505108	7575324	ronald768
13443232	13518296	13605356	ronald1024
19763472	19908392	20102432	donald2048
37768464	38121236	38676736	ronald1536
75967988	76169692	76511532	ronald2048
236148720	238388292	240679760	ronald3072
494392832	498458488	504372280	ronald4096

Public key	
bytes	system
64	donald512
64	ronald512
96	ronald768
128	donald1024
128	ronald1024
192	ronald1536
240	bls
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2
31680	rainbow

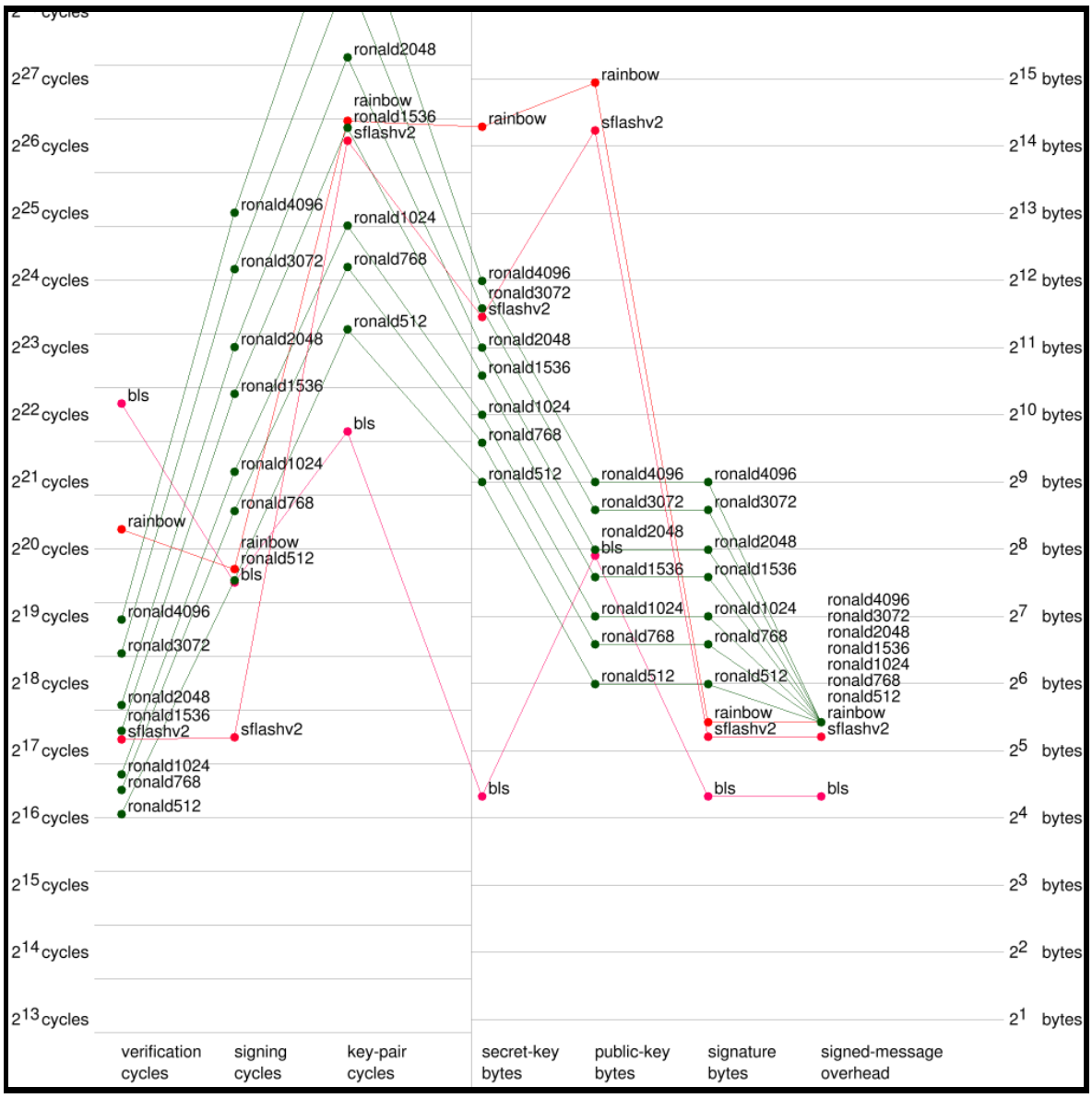
Cycles to verify 59 bytes			
quartile	median	quartile	system
172076	173588	175336	ronald512
239216	240464	242872	ronald768
303572	304972	310088	sflashv2
320716	322544	324660	ronald1024
587884	591004	597136	ronald1536
868664	878036	884724	ronald2048
1935032	1949036	1958404	ronald3072
2095088	2099804	2115864	rainbow
2410004	2424828	2431664	donald512
2853096	2860884	2868552	ronald4096
7114468	7229260	7250944	donald1024
23885272	24279704	24443428	donald2048
28970996	29113992	29301340	bls

Signing 0 bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`rainbow`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
41	`ronald512`
43	`rainbow`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`rainbow`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.36 x86, 2791MHz, Intel Xeon (f27), nmi0024



Cycles to generate a key pair			
quartile	median	quartile	system
19117944	19269780	19386164	`bls`
47251108	71915952	100362180	`ronald512`
109514560	159997504	227001032	`ronald768`
188097048	273181512	460063556	`ronald1024`
818276564	819142808	819719732	`sflashv2`
596645352	963757000	1680046476	`ronald1536`
1046078252	1051753076	1057434272	`rainbow`
1299011056	2387931780	3401881120	`ronald2048`
4192427788	6911003464	14093221966	`ronald3072`
12790370436	21975514450	35468329450	`ronald4096`

Secret key	
bytes	system
20	`bls`
512	`ronald512`
768	`ronald768`
1024	`ronald1024`
1536	`ronald1536`
2048	`ronald2048`
2823	`sflashv2`
3072	`ronald3072`
4096	`ronald4096`
20107	`rainbow`

Cycles to sign 59 bytes			
quartile	median	quartile	system
369584	370800	372556	`sflashv2`
2593092	2739264	2924408	`bls`
2803044	2819088	2832852	`ronald512`
3230900	3248596	3277948	`rainbow`
6834676	6900316	7089556	`ronald768`
11362604	11435836	11488096	`ronald1024`
29833924	31216728	32179200	`ronald1536`
56678944	56896104	57256288	`ronald2048`
154107896	155786168	156940400	`ronald3072`
320064392	321854040	324298584	`ronald4096`

Public key	
bytes	system
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
240	`bls`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
19266	`sflashv2`
31680	`rainbow`

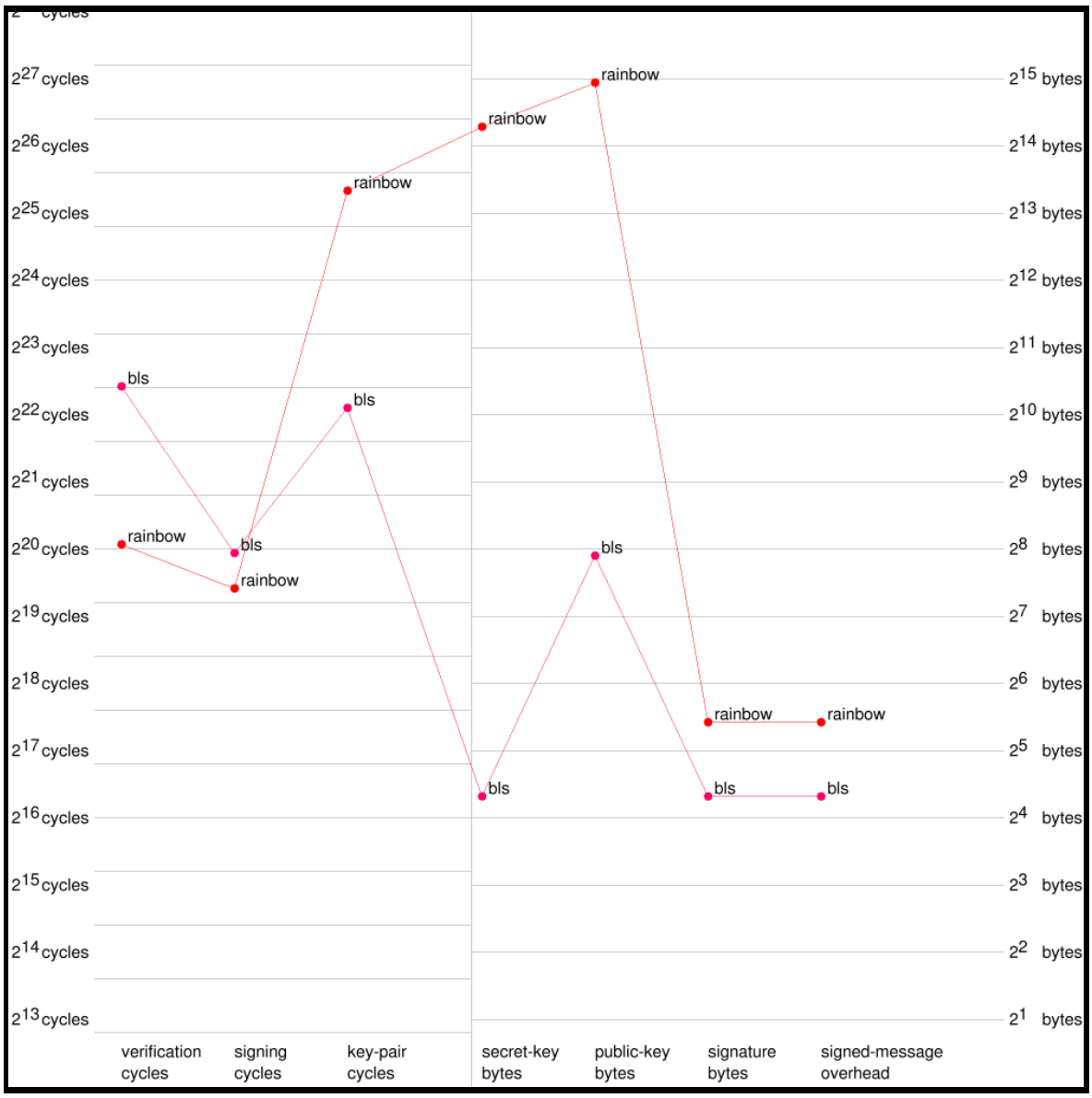
Cycles to verify 59 bytes			
quartile	median	quartile	system
134808	137776	138600	`ronald512`
187144	188296	189292	`ronald768`
229420	230568	231816	`ronald1024`
361788	362148	362560	`sflashv2`
400132	404764	407456	`ronald1536`
557580	563244	576672	`ronald2048`
1086112	1096204	1110292	`ronald3072`
1667208	1700928	1705268	`ronald4096`
5290060	5446944	5514280	`rainbow`
27313372	27483808	27592588	`bls`

Signing 0 bytes	
bytes	system
20	`bls`
37	`sflashv2`
43	`rainbow`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
20	`bls`
37	`sflashv2`
41	`ronald512`
43	`rainbow`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
20	`bls`
37	`sflashv2`
43	`rainbow`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.37 x86, 2800MHz, Intel Xeon (f41), `nmi0057`



Cycles to generate a key pair			
quartile	median	quartile	system
24956526	26130545	37965067	`bls`
364447174	429940700	531878172	`rainbow`

Secret key	
bytes	system
20	`bls`
20107	`rainbow`

Cycles to sign 59 bytes			
quartile	median	quartile	system
2471721	2529065	2581383	`rainbow`
2969505	4017468	4286464	`bls`

Public key	
bytes	system
240	`bls`
31680	`rainbow`

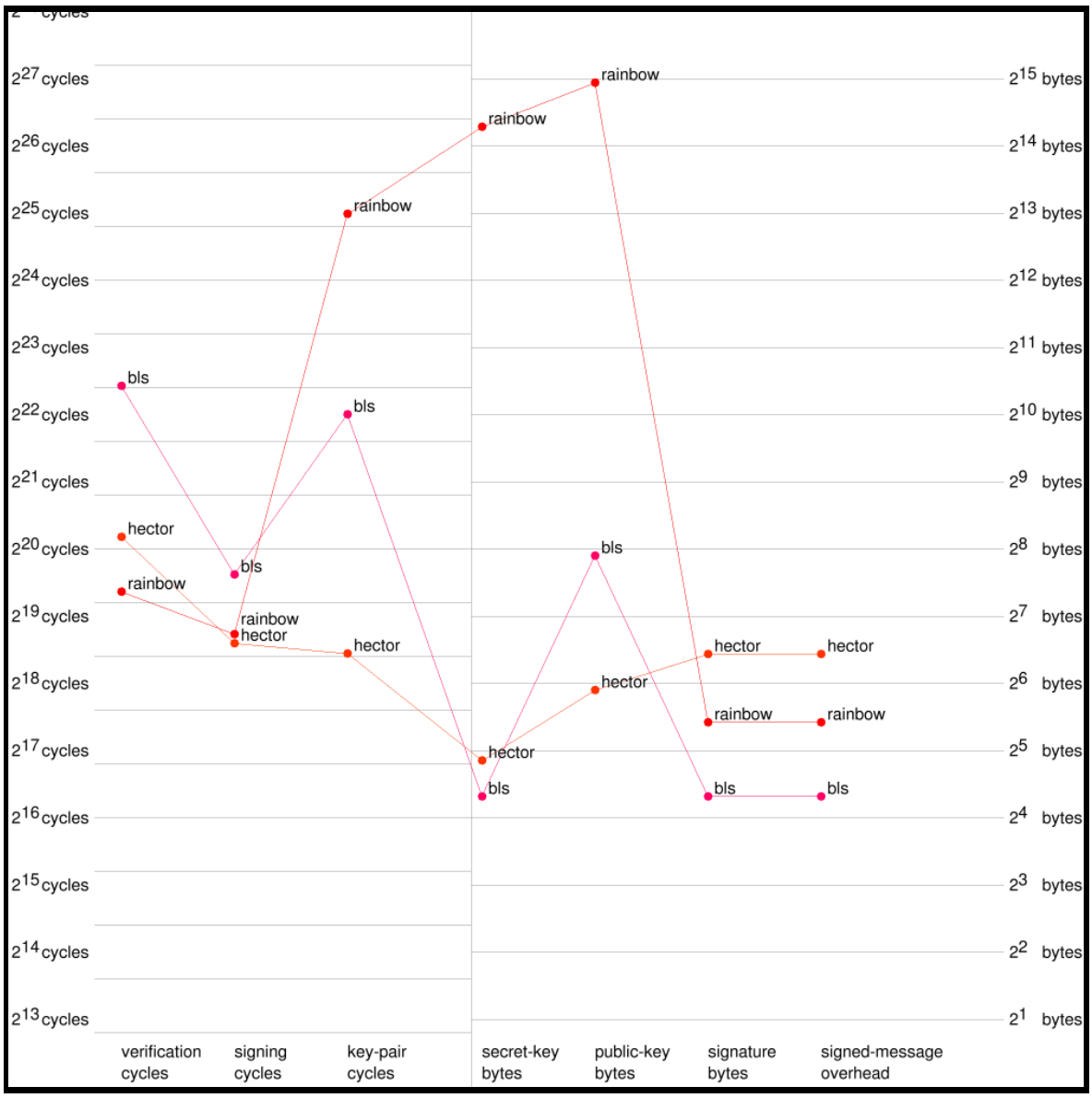
Cycles to verify 59 bytes			
quartile	median	quartile	system
3619735	4475163	4517261	`rainbow`
34332102	34467027	49350469	`bls`

Signing 0 bytes	
bytes	system
20	`bls`
43	`rainbow`

Signing 23 bytes	
bytes	system
20	`bls`
43	`rainbow`

Signing many bytes	
bytes	system
20	`bls`
43	`rainbow`

10.38 x86, 2800MHz, Intel Xeon (f41), `nmi0063`



Cycles to generate a key pair			
quartile	median	quartile	system
1091671	1100372	1155385	`hector`
23739646	23984275	24135636	`bls`
317883727	318938053	321574638	`rainbow`

Secret key	
bytes	system
20	`bls`
29	`hector`
20107	`rainbow`

Cycles to sign 59 bytes			
quartile	median	quartile	system
1204077	1247575	1298066	`hector`
1398145	1402919	1409688	`rainbow`
3004176	3028480	3243989	`bls`

Public key	
bytes	system
60	`hector`
240	`bls`
31680	`rainbow`

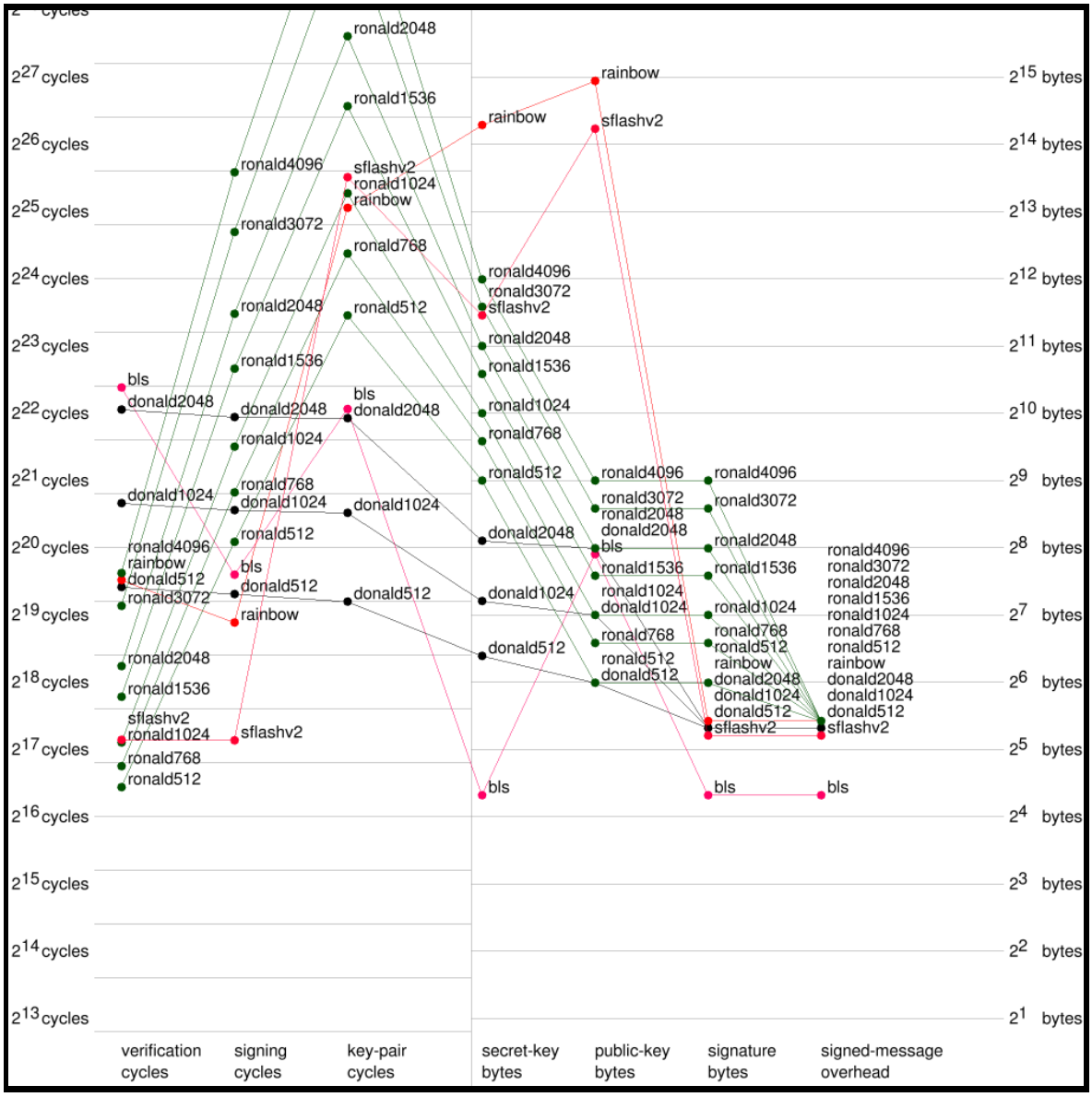
Cycles to verify 59 bytes			
quartile	median	quartile	system
2430064	2431163	2432381	`rainbow`
4926313	4939872	5017040	`hector`
34546673	34616813	34714568	`bls`

Signing 0 bytes	
bytes	system
20	`bls`
43	`rainbow`
87	`hector`

Signing 23 bytes	
bytes	system
20	`bls`
43	`rainbow`
87	`hector`

Signing many bytes	
bytes	system
20	`bls`
43	`rainbow`
87	`hector`

10.39 x86, 2801MHz, Intel Xeon (f41), `nmi0060`



Cycles to generate a key pair			
quartile	median	quartile	system
2098166	2104480	2119432	donald512
6572790	6584648	6632745	donald1024
22391950	22414861	22591436	donald2048
25010097	25186042	25323571	bls
63138278	84305529	132293035	ronald512
117706547	187179265	256842411	ronald768
335998950	336588763	337134441	rainbow
254961917	406672182	642236217	ronald1024
498179696	498451492	499455075	sflashv2
736442945	1245239156	1775048198	ronald1536
1971817771	3063598447	5148872554	ronald2048
9478465843	13731852260	21790357834	ronald3072
27259885233	36914368883	67102479640	ronald4096

Secret key	
bytes	system
20	bls
84	donald512
148	donald1024
276	donald2048
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096
20107	rainbow

Cycles to sign 59 bytes			
quartile	median	quartile	system
350959	352961	355635	sflashv2
1601838	1605807	1613409	rainbow
2317651	2324434	2340366	donald512
2963114	2975546	3189088	bls
3656947	4530239	5242083	ronald512
6813023	6824727	6870801	donald1024
8537802	8579046	8617833	ronald768
15398936	15458555	15515101	ronald1024
22633450	22655465	22809304	donald2048
42358358	42444073	42554022	ronald1536
85539482	85794828	86233539	ronald2048
246064511	246313788	246686167	ronald3072
530409691	531200089	573279329	ronald4096

Public key	
bytes	system
64	donald512
64	ronald512
96	ronald768
128	donald1024
128	ronald1024
192	ronald1536
240	bls
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2
31680	rainbow

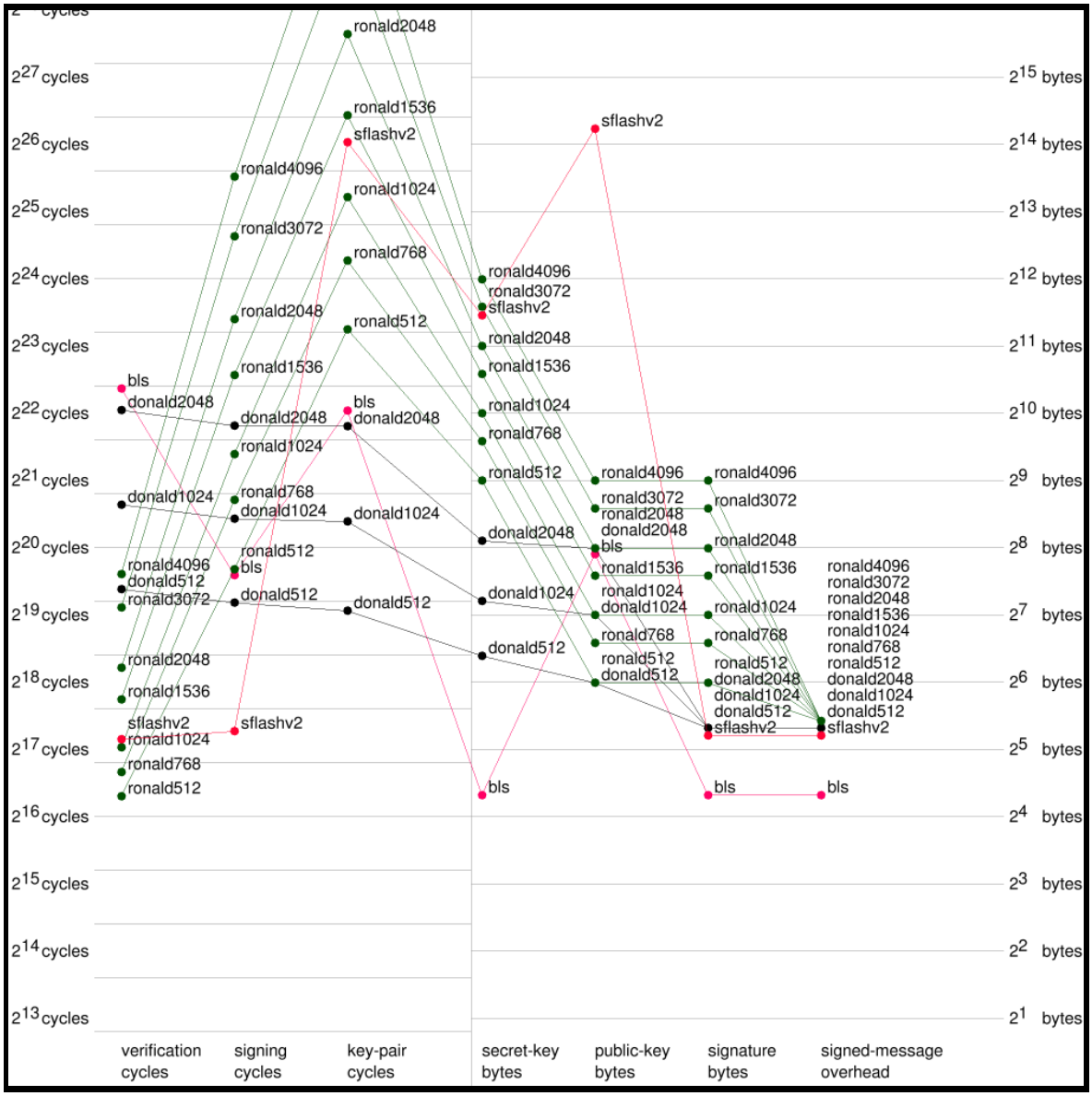
Cycles to verify 59 bytes			
quartile	median	quartile	system
188552	192353	209909	ronald512
249382	253064	256452	ronald768
339458	341173	344239	ronald1024
349510	354501	357651	sflashv2
610456	616623	631225	ronald1536
912716	917819	926436	ronald2048
1979320	1984262	1988532	ronald3072
2530367	2539012	2563785	donald512
2768927	2770082	2777957	rainbow
3025778	3040975	3050117	ronald4096
7386288	7507892	7621586	donald1024
24909374	24945466	25358648	donald2048
33055547	33290635	33492494	bls

Signing 0 bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`rainbow`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
41	`ronald512`
43	`rainbow`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`rainbow`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.40 x86, 2801MHz, Intel Xeon (f41), `nmi0061`



Cycles to generate a key pair			
quartile	median	quartile	system
1854468	1870092	1886990	`donald512`
5858097	5924989	5981360	`donald1024`
20009836	20126029	20395396	`donald2048`
24536736	24726296	24861599	`bls`
51831409	70009996	93203810	`ronald512`
107955757	170084523	255886904	`ronald768`
254960363	385448581	566374438	`ronald1024`
784950068	785285074	785615467	`sflashv2`
637454944	1110499887	1867841304	`ronald1536`
1892848006	3150969815	4644112634	`ronald2048`
7821146403	11499070954	19978732984	`ronald3072`
19538977493	33192958337	50179811206	`ronald4096`

Secret key	
bytes	system
20	`bls`
84	`donald512`
148	`donald1024`
276	`donald2048`
512	`ronald512`
768	`ronald768`
1024	`ronald1024`
1536	`ronald1536`
2048	`ronald2048`
2823	`sflashv2`
3072	`ronald3072`
4096	`ronald4096`

Cycles to sign 59 bytes			
quartile	median	quartile	system
394779	396088	401198	`sflashv2`
2048466	2072098	2087043	`donald512`
2941841	2962764	3158890	`bls`
3167255	3189165	3206770	`ronald512`
6068867	6106408	6149766	`donald1024`
7762412	7795095	7808157	`ronald768`
14040579	14103460	14148680	`ronald1024`
20139364	20326229	20549032	`donald2048`
38900484	38979731	39075946	`ronald1536`
80037538	80126046	80223780	`ronald2048`
233018898	233453269	234866457	`ronald3072`
500453079	500939474	501585469	`ronald4096`

Public key	
bytes	system
64	`donald512`
64	`ronald512`
96	`ronald768`
128	`donald1024`
128	`ronald1024`
192	`ronald1536`
240	`bls`
256	`donald2048`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
19266	`sflashv2`

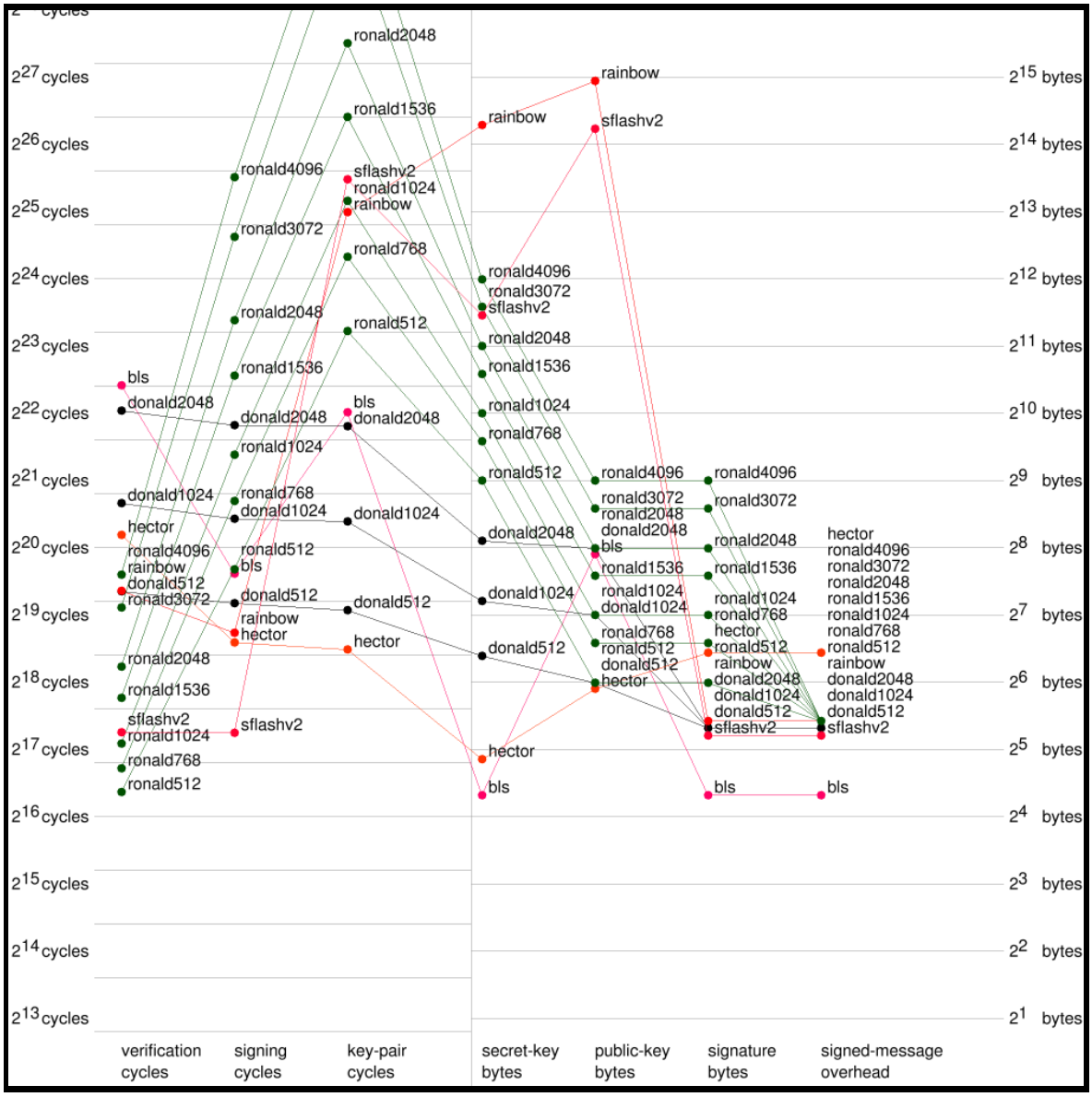
Cycles to verify 59 bytes			
quartile	median	quartile	system
162834	171626	172564	`ronald512`
232351	233457	236782	`ronald768`
314993	320684	323876	`ronald1024`
354823	357882	363237	`sflashv2`
592606	594846	599515	`ronald1536`
895664	898415	903700	`ronald2048`
1948177	1955485	1966860	`ronald3072`
2439332	2463118	2470146	`donald512`
2995965	3002552	3007865	`ronald4096`
7277753	7343224	7527142	`donald1024`
24066217	24800531	24885105	`donald2048`
32653446	32752237	32935315	`bls`

Signing 0 bytes	
bytes	system
20	bls
37	sflashv2
40	donald1024
40	donald2048
40	donald512
64	ronald512
96	ronald768
128	ronald1024
192	ronald1536
256	ronald2048
384	ronald3072
512	ronald4096

Signing 23 bytes	
bytes	system
20	bls
37	sflashv2
40	donald1024
40	donald2048
40	donald512
41	ronald512
73	ronald768
105	ronald1024
169	ronald1536
233	ronald2048
361	ronald3072
489	ronald4096

Signing many bytes	
bytes	system
20	bls
37	sflashv2
40	donald1024
40	donald2048
40	donald512
43	ronald1024
43	ronald1536
43	ronald2048
43	ronald3072
43	ronald4096
43	ronald512
43	ronald768

10.41 x86, 2801MHz, Intel Xeon (f41), `nmi0062`



Cycles to generate a key pair			
quartile	median	quartile	system
1127448	1136807	1196804	`hector`
1870141	1884848	1898456	`donald512`
5877137	5918444	5963069	`donald1024`
20081180	20193075	20331073	`donald2048`
23991849	24177860	24354330	`bls`
52108189	68678911	98830193	`ronald512`
131075518	179342674	258994820	`ronald768`
312965114	318238865	335388907	`rainbow`
262577112	367310279	523617633	`ronald1024`
484174313	484345568	484553692	`sflashv2`
706837264	1084235838	1610758394	`ronald1536`
1896639528	2797233019	4786404868	`ronald2048`
9009107268	14898226784	20076445662	`ronald3072`
19938992976	34645796878	56876971515	`ronald4096`

Secret key	
bytes	system
20	`bls`
29	`hector`
84	`donald512`
148	`donald1024`
276	`donald2048`
512	`ronald512`
768	`ronald768`
1024	`ronald1024`
1536	`ronald1536`
2048	`ronald2048`
2823	`sflashv2`
3072	`ronald3072`
4096	`ronald4096`
20107	`rainbow`

Cycles to sign 59 bytes			
quartile	median	quartile	system
386673	388661	390425	`sflashv2`
1203580	1245195	1288938	`hector`
1401043	1404760	1413923	`rainbow`
2053884	2063264	2079574	`donald512`
3003252	3023216	3260082	`bls`
3180408	3198825	3216283	`ronald512`
6050254	6116488	6168764	`donald1024`
7672161	7709583	7741167	`ronald768`
13958084	14001820	14042861	`ronald1024`
20272406	20457556	20593524	`donald2048`
38570539	38664920	38737377	`ronald1536`
78838249	78934394	79031246	`ronald2048`
231462462	231848603	232235990	`ronald3072`
499602761	500193568	500682889	`ronald4096`

Public key	
bytes	system
60	hector
64	donald512
64	ronald512
96	ronald768
128	donald1024
128	ronald1024
192	ronald1536
240	bls
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2
31680	rainbow

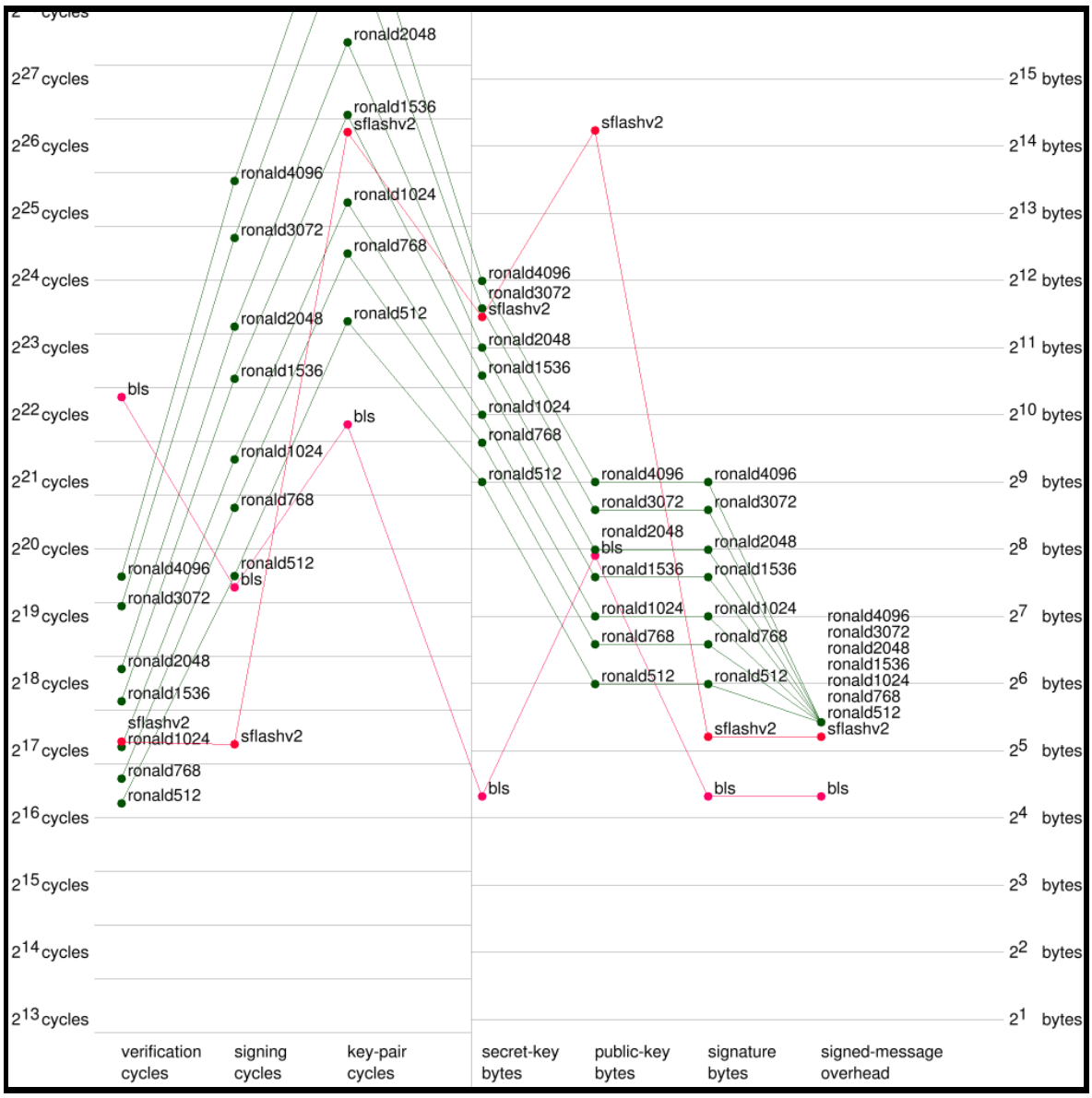
Cycles to verify 59 bytes			
quartile	median	quartile	system
175371	180810	185227	ronald512
245105	245784	246645	ronald768
333403	338170	339801	ronald1024
389501	391629	393246	sflashv2
602182	609791	611184	ronald1536
903021	906661	910448	ronald2048
1946861	1953504	1957914	ronald3072
2380567	2406222	2414027	donald512
2422287	2423260	2430393	rainbow
2956233	2967377	2977184	ronald4096
4968964	4978666	5044235	hector
7308238	7466102	7589001	donald1024
24433857	24629626	25169599	donald2048
33956531	34066844	34246464	bls

Signing 0 bytes	
bytes	system
20	bls
37	sflashv2
40	donald1024
40	donald2048
40	donald512
43	rainbow
64	ronald512
87	hector
96	ronald768
128	ronald1024
192	ronald1536
256	ronald2048
384	ronald3072
512	ronald4096

Signing 23 bytes	
bytes	system
20	bls
37	sflashv2
40	donald1024
40	donald2048
40	donald512
41	ronald512
43	rainbow
73	ronald768
87	hector
105	ronald1024
169	ronald1536
233	ronald2048
361	ronald3072
489	ronald4096

Signing many bytes	
bytes	system
20	bls
37	sflashv2
40	donald1024
40	donald2048
40	donald512
43	rainbow
43	ronald1024
43	ronald1536
43	ronald2048
43	ronald3072
43	ronald4096
43	ronald512
43	ronald768
87	hector

10.42 x86, 2802MHz, Intel Xeon (f29), `nmibuild40`



Cycles to generate a key pair			
quartile	median	quartile	system
20832748	20974916	21101452	`bls`
55402980	79371528	106082840	`ronald512`
122771552	189919672	272779516	`ronald768`
241012056	366826040	556942572	`ronald1024`
911337544	911906008	913420332	`sflashv2`
667364232	1142707944	1863476376	`ronald1536`
1634032488	2901537872	4877682916	`ronald2048`
7309902724	12591050788	22835310392	`ronald3072`
20261740780	32532255864	51662583696	`ronald4096`

Secret key	
bytes	system
20	`bls`
512	`ronald512`
768	`ronald768`
1024	`ronald1024`
1536	`ronald1536`
2048	`ronald2048`
2823	`sflashv2`
3072	`ronald3072`
4096	`ronald4096`

Cycles to sign 59 bytes			
quartile	median	quartile	system
338584	340324	342660	`sflashv2`
2529788	2574148	2589440	`bls`
2956684	2975880	3012088	`ronald512`
7136948	7182380	7211972	`ronald768`
13151888	13358912	13561264	`ronald1024`
36907212	37852544	38286832	`ronald1536`
74079900	74366004	74738368	`ronald2048`
231566016	233676916	235724972	`ronald3072`
484845536	485835204	486799700	`ronald4096`

Public key	
bytes	system
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
240	`bls`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
19266	`sflashv2`

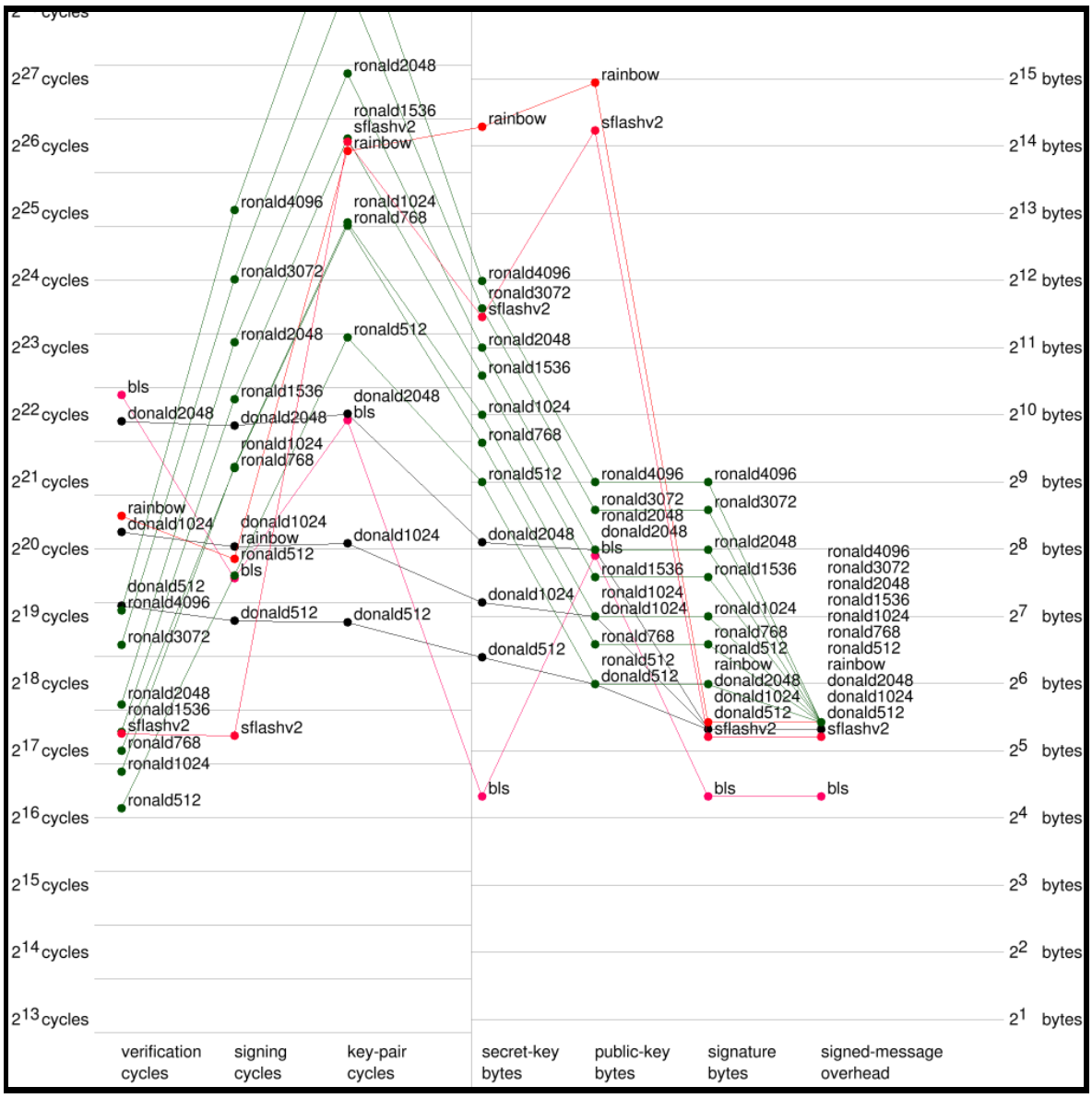
Cycles to verify 59 bytes			
quartile	median	quartile	system
155848	158304	160828	`ronald512`
216852	218088	220164	`ronald768`
325012	327540	330544	`ronald1024`
350920	351308	352752	`sflashv2`
588308	592356	597132	`ronald1536`
887840	894348	902516	`ronald2048`
1995584	2017236	2039876	`ronald3072`
2938932	2964728	2979084	`ronald4096`
29888140	29988456	30118988	`bls`

Signing 0 bytes	
bytes	system
20	`bls`
37	`sflashv2`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
20	`bls`
37	`sflashv2`
41	`ronald512`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
20	`bls`
37	`sflashv2`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.43 x86, 2995MHz, Intel Xeon (f41), nmi0079



Cycles to generate a key pair			
quartile	median	quartile	system
1623015	1644037	2678423	donald512
4535820	4558013	4578578	donald1024
21966780	22146720	22304445	bls
23802450	24219975	24376365	donald2048
48047670	64806975	97461758	ronald512
159014918	273220320	432828068	ronald768
199999627	283866060	422939895	ronald1024
713523375	714521497	725709143	rainbow
800430270	806564527	921143542	sflashv2
561061095	838286070	1275902460	ronald1536
1244420220	1944193575	2963318265	ronald2048
3719472420	6255840202	11861142645	ronald3072
11238903060	19789691220	34486359480	ronald4096

Secret key	
bytes	system
20	bls
84	donald512
148	donald1024
276	donald2048
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096
20107	rainbow

Cycles to sign 59 bytes			
quartile	median	quartile	system
376050	378930	561022	sflashv2
1649970	1671915	2708505	donald512
2873220	2895480	3105900	bls
2967795	2992245	3017580	ronald512
3688178	3710632	3727620	rainbow
4330837	4356915	4392127	donald1024
11861918	11945940	12017445	ronald768
12078022	12133650	12190298	ronald1024
16357800	20677132	22749038	donald2048
29004952	29130757	29265713	ronald1536
60522885	60625133	60748808	ronald2048
136371120	136561275	136914000	ronald3072
332452725	332911260	333494775	ronald4096

Public key	
bytes	system
64	donald512
64	ronald512
96	ronald768
128	donald1024
128	ronald1024
192	ronald1536
240	bls
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2
31680	rainbow

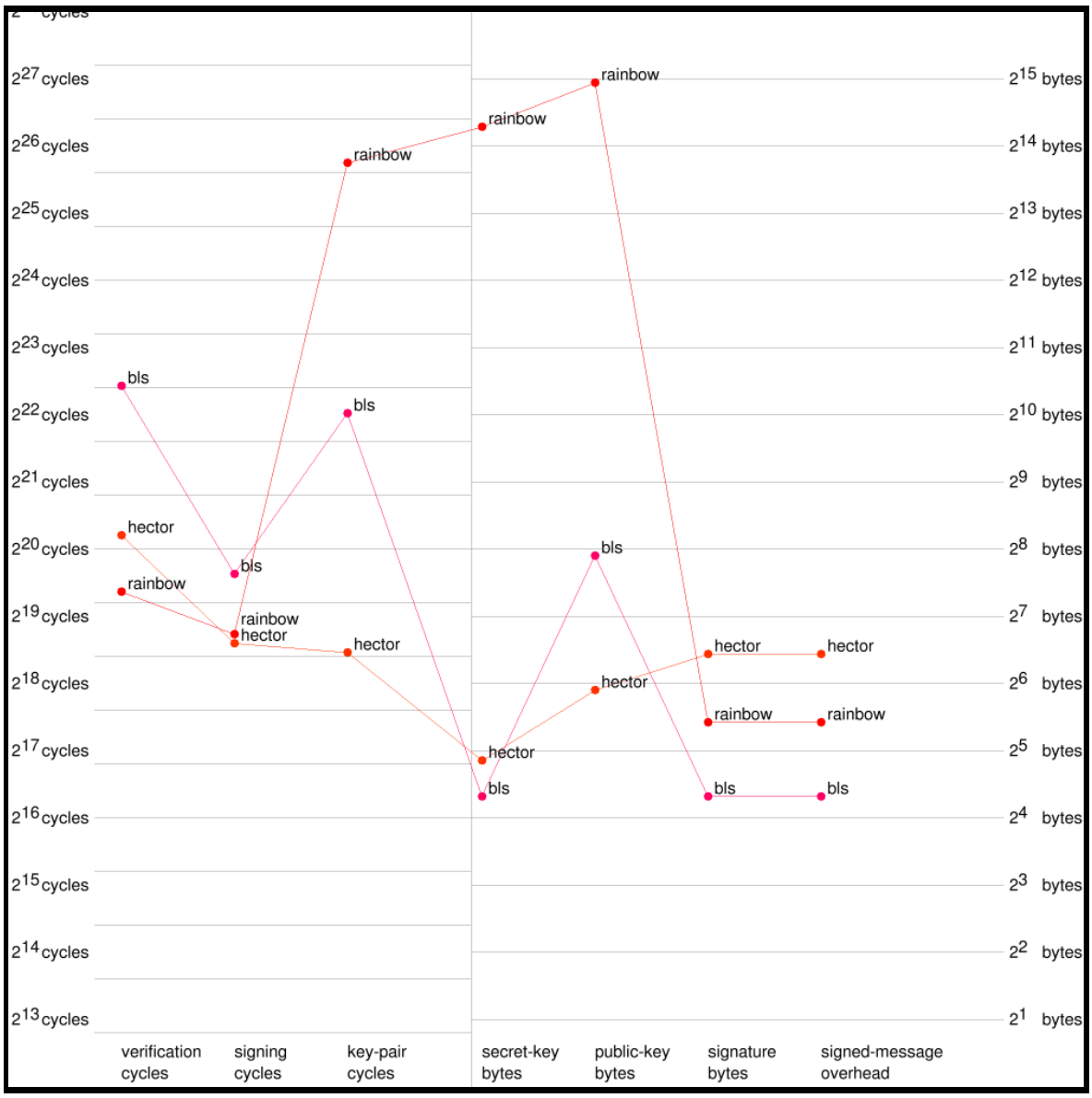
Cycles to verify 59 bytes			
quartile	median	quartile	system
147120	148508	149190	ronald512
238080	239265	241417	ronald1024
306578	313357	319402	ronald768
384690	389242	701152	sflashv2
397598	399188	404040	ronald1536
563205	566737	571298	ronald2048
1222793	1228995	1242150	ronald3072
1900897	1911832	1917637	ronald4096
1975402	2037270	3348397	donald512
5168520	5250060	5300115	donald1024
6436425	6462908	6481942	rainbow
19462462	21874365	27264285	donald2048
30641753	30719453	30856350	bls

Signing 0 bytes	
bytes	system
20	bls
37	sflashv2
40	donald1024
40	donald2048
40	donald512
43	rainbow
64	ronald512
96	ronald768
128	ronald1024
192	ronald1536
256	ronald2048
384	ronald3072
512	ronald4096

Signing 23 bytes	
bytes	system
20	bls
37	sflashv2
40	donald1024
40	donald2048
40	donald512
41	ronald512
43	rainbow
73	ronald768
105	ronald1024
169	ronald1536
233	ronald2048
361	ronald3072
489	ronald4096

Signing many bytes	
bytes	system
20	bls
37	sflashv2
40	donald1024
40	donald2048
40	donald512
43	rainbow
43	ronald1024
43	ronald1536
43	ronald2048
43	ronald3072
43	ronald4096
43	ronald512
43	ronald768

10.44 x86, 2996MHz, Intel Xeon (f41), `nmi0076`



Cycles to generate a key pair			
quartile	median	quartile	system
1098990	1114425	1161780	`hector`
24120172	24282248	24476505	`bls`
460660853	613365847	618836520	`rainbow`

Secret key	
bytes	system
20	`bls`
29	`hector`
20107	`rainbow`

Cycles to sign 59 bytes			
quartile	median	quartile	system
1219395	1250970	1304730	`hector`
1398720	1412580	1416600	`rainbow`
3029775	3067770	3256072	`bls`

Public key	
bytes	system
60	`hector`
240	`bls`
31680	`rainbow`

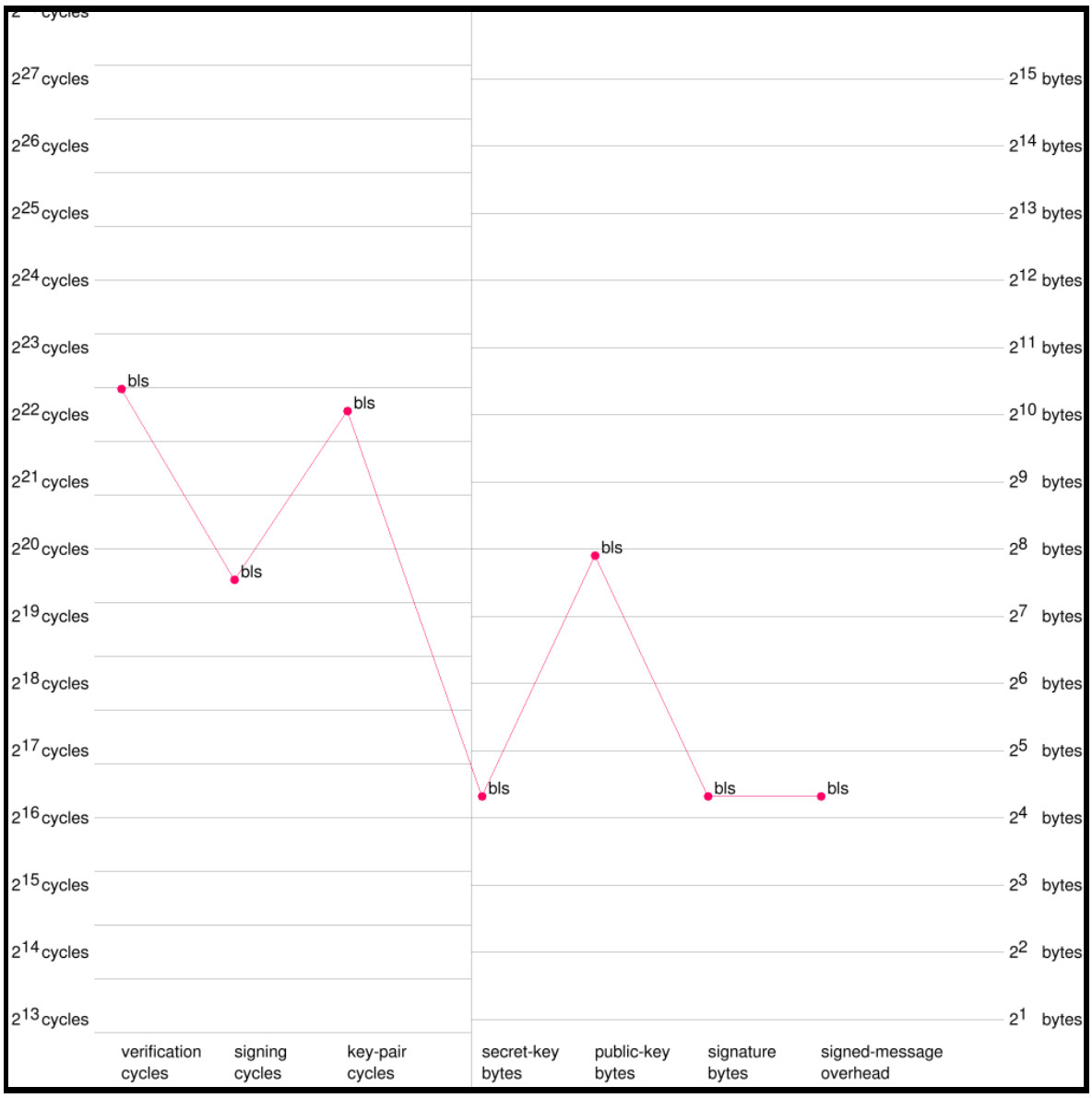
Cycles to verify 59 bytes			
quartile	median	quartile	system
2439780	2442233	2443912	`rainbow`
5030730	5039145	5118540	`hector`
34543770	34716847	34899090	`bls`

Signing 0 bytes	
bytes	system
20	`bls`
43	`rainbow`
87	`hector`

Signing 23 bytes	
bytes	system
20	`bls`
43	`rainbow`
87	`hector`

Signing many bytes	
bytes	system
20	`bls`
43	`rainbow`
87	`hector`

10.45 x86, 3000MHz, Intel Xeon (f4a), `nmi0090`



Cycles to generate a key pair			
quartile	median	quartile	system
24919515	25071795	25240687	`bls`

Secret key	
bytes	system
20	`bls`

Cycles to sign 59 bytes			
quartile	median	quartile	system
2812725	2841915	3277028	`bls`

Public key	
bytes	system
240	`bls`

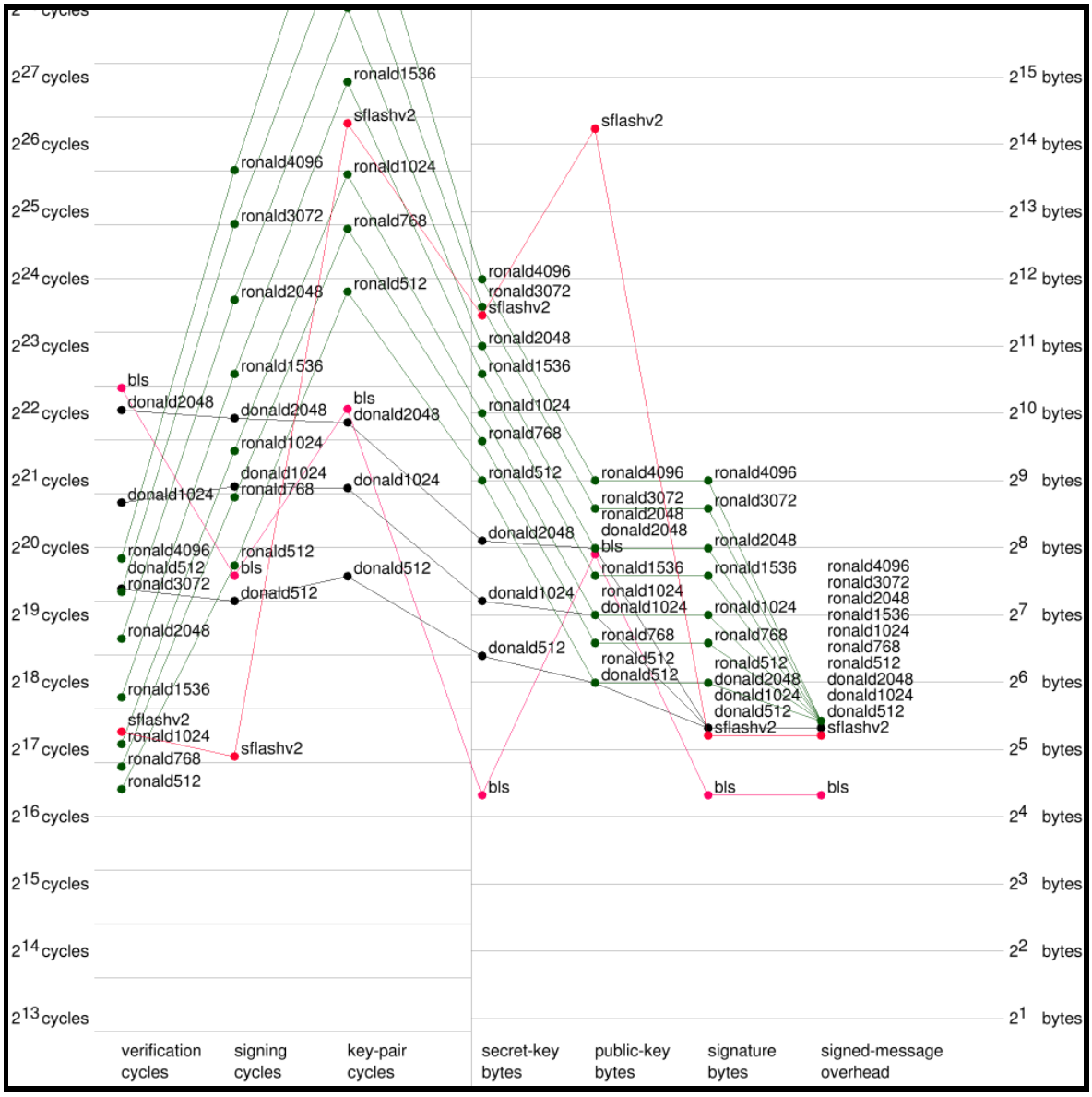
Cycles to verify 59 bytes			
quartile	median	quartile	system
33245760	33287475	33738270	`bls`

Signing 0 bytes	
bytes	system
20	`bls`

Signing 23 bytes	
bytes	system
20	`bls`

Signing many bytes	
bytes	system
20	`bls`

10.46 x86, 3000MHz, Intel Xeon (f4a), `nmi0102`



Cycles to generate a key pair			
quartile	median	quartile	system
1927808	2920755	2963025	donald512
8852048	9055072	9165540	donald1024
20338658	21102780	27207495	donald2048
24966600	25194427	25381500	bls
77974313	114022027	165896482	ronald512
148915065	257060887	379561575	ronald768
355747920	518465655	711557332	ronald1024
847634325	997420957	1315997895	sflashv2
1016928877	1706542680	2716289280	ronald1536
2404484955	4428239798	6881091420	ronald2048
7047485205	12954383633	24900832650	ronald3072
27936908310	42679217490	66111754410	ronald4096

Secret key	
bytes	system
20	bls
84	donald512
148	donald1024
276	donald2048
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096

Cycles to sign 59 bytes			
quartile	median	quartile	system
278700	284902	495000	sflashv2
2103847	2123865	3343485	donald512
2902035	2930227	3146490	bls
3326873	3358125	3387195	ronald512
7999785	8073345	12764783	ronald768
6207555	9257865	9455242	donald1024
14572575	14668830	15315052	ronald1024
20564572	22364992	29771085	donald2048
39296760	39510143	60033893	ronald1536
93956932	102971182	121666935	ronald2048
233918347	272215560	295159455	ronald3072
503529390	544892175	637431390	ronald4096

Public key	
bytes	system
64	donald512
64	ronald512
96	ronald768
128	donald1024
128	ronald1024
192	ronald1536
240	bls
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2

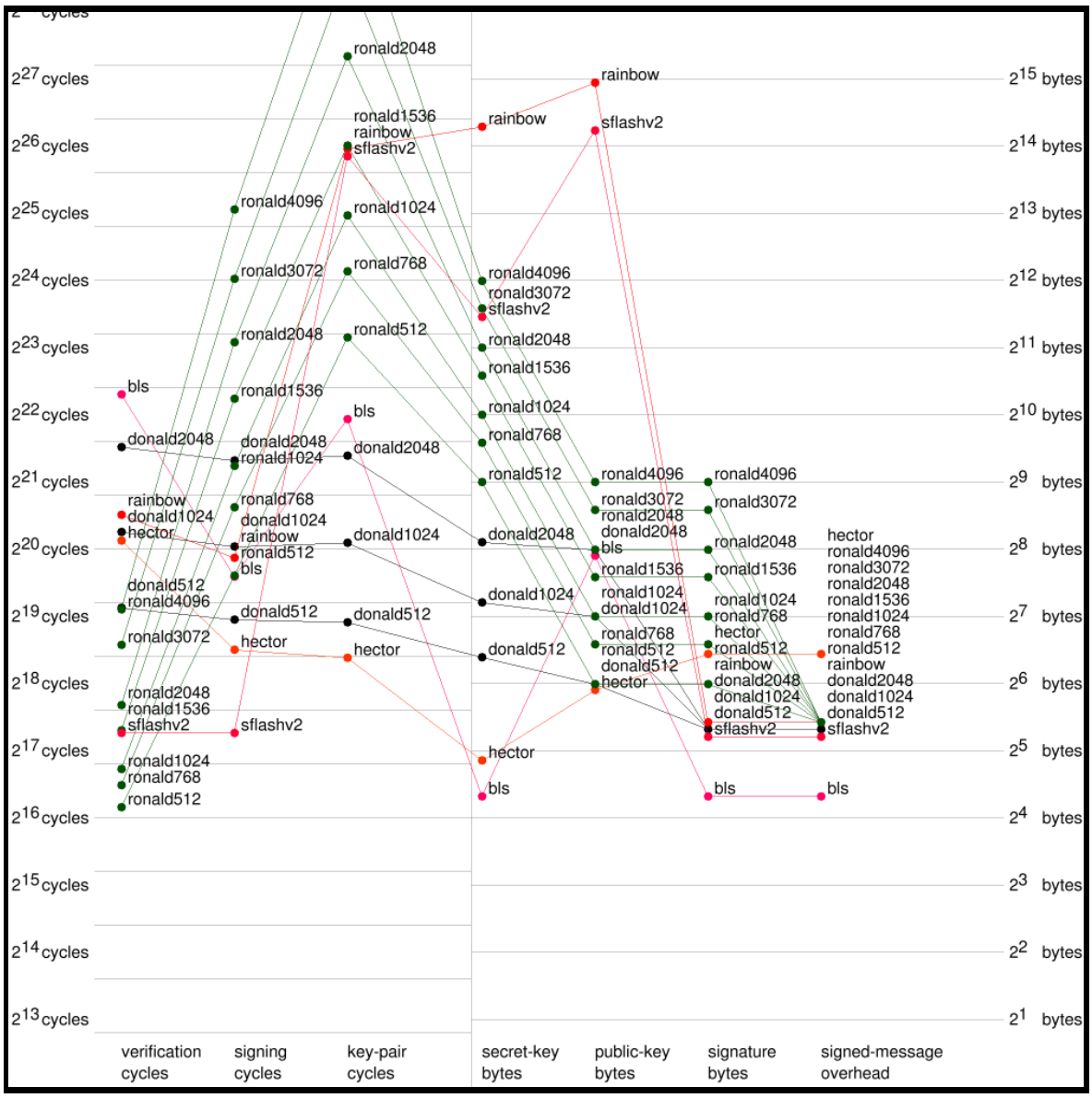
Cycles to verify 59 bytes			
quartile	median	quartile	system
184155	187380	279053	ronald512
245190	249758	393225	ronald768
335100	336188	337575	ronald1024
386400	392265	677085	sflashv2
611700	614287	900203	ronald1536
910605	1301865	1330785	ronald2048
1976783	2376757	2757097	ronald3072
2449567	2492692	4034070	donald512
3002370	3660720	4226648	ronald4096
7384815	7524938	11395260	donald1024
24450053	24860588	30971108	donald2048
32923867	33004665	55239525	bls

Signing 0 bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
41	`ronald512`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.47 x86, 3391MHz, Intel Pentium D (f64), `nmi0099`



Cycles to generate a key pair			
quartile	median	quartile	system
1036439	1041080	1082084	`hector`
1629994	1637423	1647606	`donald512`
4556221	4564874	4574122	`donald1024`
14071665	14101976	14124110	`donald2048`
22303116	22482517	22627374	`bls`
45724305	64457727	95529868	`ronald512`
110023711	151372998	227363338	`ronald768`
179614129	311072698	498750012	`ronald1024`
666799347	669610246	673996348	`sflashv2`
734317397	737872556	739694956	`rainbow`
487144724	764582854	1270566655	`ronald1536`
1313910382	2429477820	3183898244	`ronald2048`
4607221731	7544344354	11688239466	`ronald3072`
13592309693	23098160440	40194217903	`ronald4096`

Secret key	
bytes	system
20	`bls`
29	`hector`
84	`donald512`
148	`donald1024`
276	`donald2048`
512	`ronald512`
768	`ronald768`
1024	`ronald1024`
1536	`ronald1536`
2048	`ronald2048`
2823	`sflashv2`
3072	`ronald3072`
4096	`ronald4096`
20107	`rainbow`

Cycles to sign 59 bytes			
quartile	median	quartile	system
392156	393839	396984	`sflashv2`
1116016	1151512	1190765	`hector`
1690361	1699898	1710336	`donald512`
2933537	2948497	3153670	`bls`
2964205	2990810	3053302	`ronald512`
3748670	3770787	3795828	`rainbow`
4340678	4369935	4394483	`donald1024`
7200588	7239059	7271631	`ronald768`
12244080	12296185	12366310	`ronald1024`
13085563	13173130	13268364	`donald2048`
29161154	29230225	29348188	`ronald1536`
60700455	60825983	60921591	`ronald2048`
136868377	137252084	137656310	`ronald3072`
334862243	336166347	338531217	`ronald4096`

Public key	
bytes	system
60	hector
64	donald512
64	ronald512
96	ronald768
128	donald1024
128	ronald1024
192	ronald1536
240	bls
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2
31680	rainbow

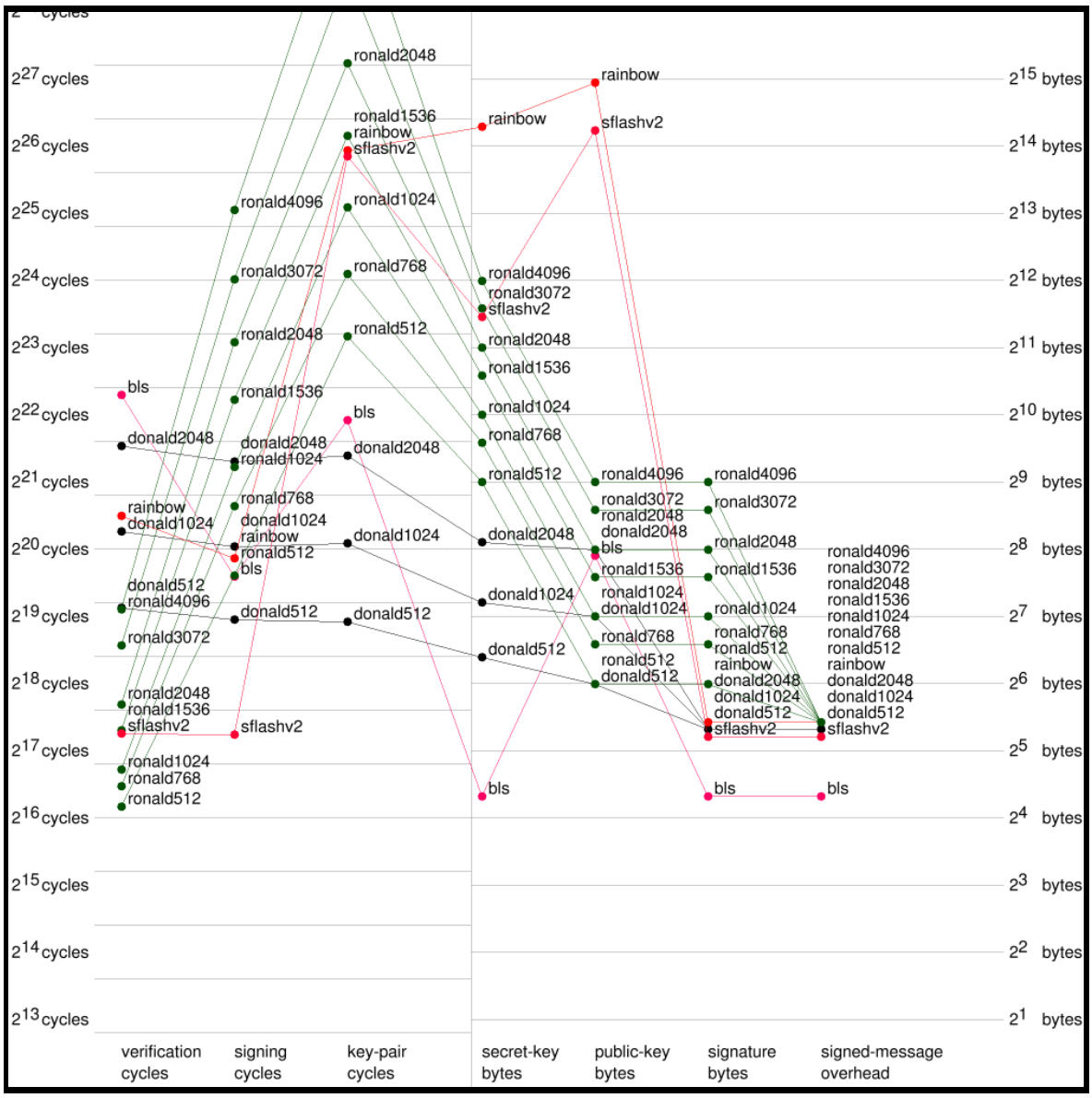
Cycles to verify 59 bytes			
quartile	median	quartile	system
147458	150790	154173	ronald512
198934	200277	201331	ronald768
244834	247163	248914	ronald1024
386835	393057	400503	sflashv2
403342	407745	412947	ronald1536
562530	564400	567528	ronald2048
1218186	1223184	1227094	ronald3072
1935603	1941468	1950954	ronald4096
1942556	1979599	1989867	donald512
4679709	4710972	4755869	hector
5244687	5262231	5304017	donald1024
6550763	6565536	6604228	rainbow
15462418	15698718	16007149	donald2048
30802351	30945695	31070135	bls

Signing 0 bytes	
bytes	system
20	bls
37	sflashv2
40	donald1024
40	donald2048
40	donald512
43	rainbow
64	ronald512
87	hector
96	ronald768
128	ronald1024
192	ronald1536
256	ronald2048
384	ronald3072
512	ronald4096

Signing 23 bytes	
bytes	system
20	bls
37	sflashv2
40	donald1024
40	donald2048
40	donald512
41	ronald512
43	rainbow
73	ronald768
87	hector
105	ronald1024
169	ronald1536
233	ronald2048
361	ronald3072
489	ronald4096

Signing many bytes	
bytes	system
20	bls
37	sflashv2
40	donald1024
40	donald2048
40	donald512
43	rainbow
43	ronald1024
43	ronald1536
43	ronald2048
43	ronald3072
43	ronald4096
43	ronald512
43	ronald768
87	hector

10.48 x86, 3392MHz, Intel Pentium D (f64), `nmi0104`



Cycles to generate a key pair			
quartile	median	quartile	system
1645328	1650649	1655341	donald512
4541176	4551495	4561746	donald1024
13983231	14018234	14055311	donald2048
22012552	22176636	22306941	bls
48925201	65461135	92741052	ronald512
100275843	146307015	211133166	ronald768
209731091	345950867	532700559	ronald1024
664991720	665613274	667175965	sflashv2
719844532	720203793	721027800	rainbow
468451949	869812616	1399760076	ronald1536
1248863673	2222472101	3314071035	ronald2048
4611194937	7183259917	12607715525	ronald3072
15725022355	23806696045	34264536864	ronald4096

Secret key	
bytes	system
20	bls
84	donald512
148	donald1024
276	donald2048
512	ronald512
768	ronald768
1024	ronald1024
1536	ronald1536
2048	ronald2048
2823	sflashv2
3072	ronald3072
4096	ronald4096
20107	rainbow

Cycles to sign 59 bytes			
quartile	median	quartile	system
383333	384880	386750	sflashv2
1684785	1695597	1706426	donald512
2929491	2949653	3151953	bls
2981426	3004036	3027224	ronald512
3738011	3753175	3775207	rainbow
4343993	4364716	4392902	donald1024
7263675	7311632	7348726	ronald768
12095109	12151753	12218716	ronald1024
12960154	13038779	13131871	donald2048
28940001	29008256	29075831	ronald1536
60633016	60739929	60856821	ronald2048
136096424	136382330	136591515	ronald3072
332523825	333391811	334533480	ronald4096

Public key	
bytes	system
64	donald512
64	ronald512
96	ronald768
128	donald1024
128	ronald1024
192	ronald1536
240	bls
256	donald2048
256	ronald2048
384	ronald3072
512	ronald4096
19266	sflashv2
31680	rainbow

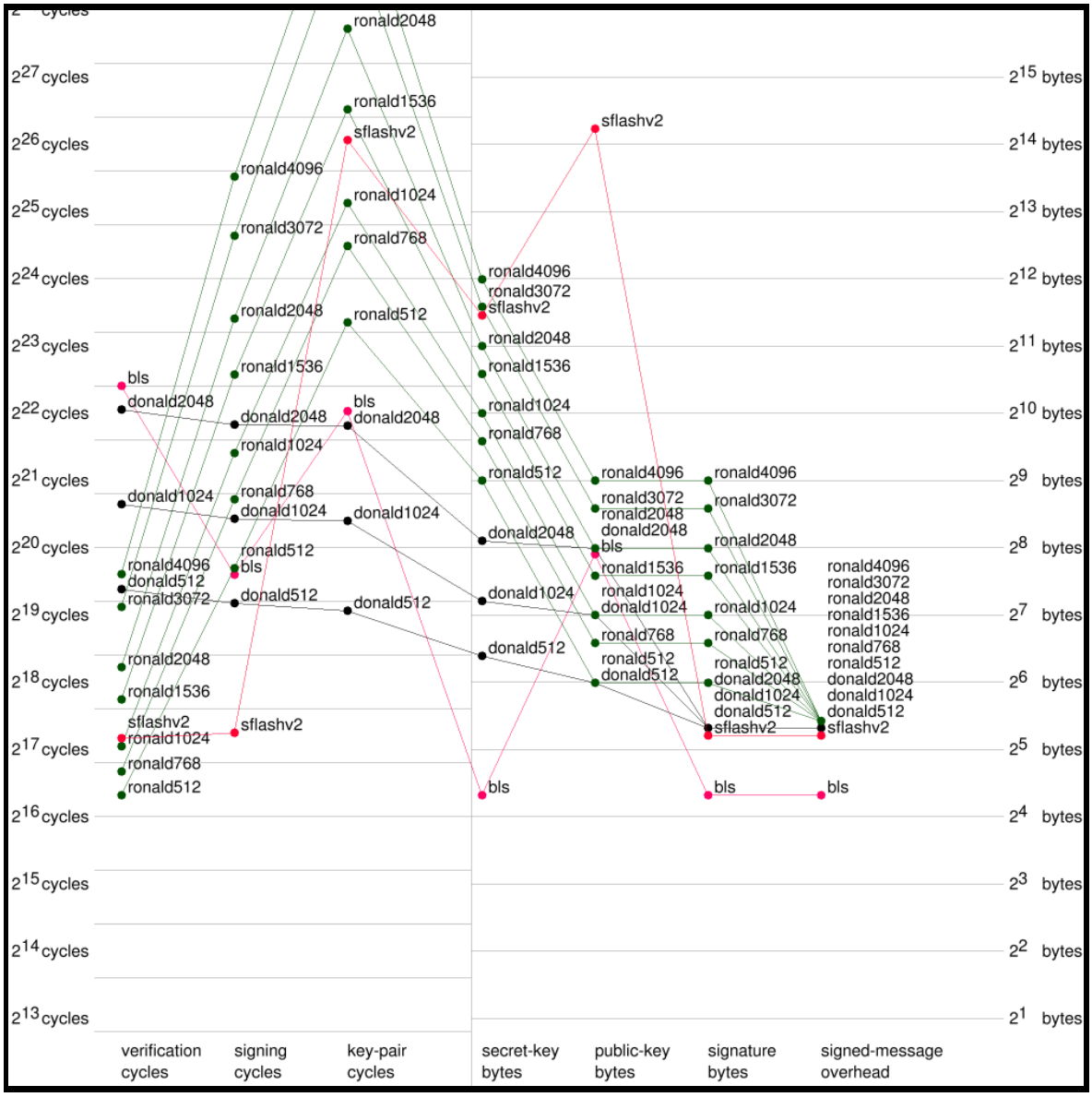
Cycles to verify 59 bytes			
quartile	median	quartile	system
151283	151810	152881	ronald512
189465	198390	199376	ronald768
244120	245191	246449	ronald1024
380919	390898	391680	sflashv2
404923	406045	409292	ronald1536
567120	568429	569415	ronald2048
1215177	1217880	1219495	ronald3072
1932016	1934719	1940210	ronald4096
1971915	1977814	1983968	donald512
5289448	5303609	5319300	donald1024
6446978	6460068	6480417	rainbow
15859708	15889492	16024336	donald2048
30568822	30683096	30834362	bls

Signing 0 bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`rainbow`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
41	`ronald512`
43	`rainbow`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`rainbow`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`

10.49 x86, 3392MHz, Intel Pentium D (f64), `nmi0241`



Cycles to generate a key pair			
quartile	median	quartile	system
1854564	1870697	1887884	`donald512`
5870049	5933731	5981722	`donald1024`
20034551	20236987	20357449	`donald2048`
24306311	24481802	24648504	`bls`
58044358	76603292	111913924	`ronald512`
114788012	206068441	284793758	`ronald768`
229982256	357273802	457739161	`ronald1024`
802127014	802639190	807898973	`sflashv2`
791227566	1199668886	1802122893	`ronald1536`
1710331342	3374473939	4819859975	`ronald2048`
8193369776	13679878954	19101521708	`ronald3072`
20227707346	31673914191	52975352026	`ronald4096`

Secret key	
bytes	system
20	`bls`
84	`donald512`
148	`donald1024`
276	`donald2048`
512	`ronald512`
768	`ronald768`
1024	`ronald1024`
1536	`ronald1536`
2048	`ronald2048`
2823	`sflashv2`
3072	`ronald3072`
4096	`ronald4096`

Cycles to sign 59 bytes			
quartile	median	quartile	system
386767	387923	390456	`sflashv2`
2040272	2059533	2083316	`donald512`
2970784	2985217	3173798	`bls`
3208325	3232703	3247986	`ronald512`
6056250	6107726	6153014	`donald1024`
7855547	7867889	7902807	`ronald768`
14250029	14304480	14363266	`ronald1024`
20366731	20516569	20733183	`donald2048`
39097875	39207202	39284637	`ronald1536`
80360734	80491583	80713433	`ronald2048`
233808327	234232613	234588389	`ronald3072`
501231298	502606564	503926478	`ronald4096`

Public key	
bytes	system
64	`donald512`
64	`ronald512`
96	`ronald768`
128	`donald1024`
128	`ronald1024`
192	`ronald1536`
240	`bls`
256	`donald2048`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`
19266	`sflashv2`

Cycles to verify 59 bytes			
quartile	median	quartile	system
171275	173213	175576	`ronald512`
233087	235416	237507	`ronald768`
323204	326604	330310	`ronald1024`
360519	361692	363477	`sflashv2`
595527	597941	603432	`ronald1536`
898365	901357	907545	`ronald2048`
1960287	1968175	1986603	`ronald3072`
2438956	2463895	2481031	`donald512`
2992323	3000449	3018265	`ronald4096`
7290824	7396819	7566105	`donald1024`
24852861	24994233	25023456	`donald2048`
33763700	33801814	33830578	`bls`

Signing 0 bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
64	`ronald512`
96	`ronald768`
128	`ronald1024`
192	`ronald1536`
256	`ronald2048`
384	`ronald3072`
512	`ronald4096`

Signing 23 bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
41	`ronald512`
73	`ronald768`
105	`ronald1024`
169	`ronald1536`
233	`ronald2048`
361	`ronald3072`
489	`ronald4096`

Signing many bytes	
bytes	system
20	`bls`
37	`sflashv2`
40	`donald1024`
40	`donald2048`
40	`donald512`
43	`ronald1024`
43	`ronald1536`
43	`ronald2048`
43	`ronald3072`
43	`ronald4096`
43	`ronald512`
43	`ronald768`