IST-2002-507932

ECRYPT

European Network of Excellence in Cryptology

Network of Excellence

Information Society Technologies

D.VAM.9
Report on "eBATS Performance Benchmarks"

Due date of deliverable: 31. December 2006
Actual submission date: 1. March 2007

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)	

Report on "eBATS Performance Benchmarks"

Editor
Daniel Page (BRIS)

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

1. March 2007
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

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 Pentium, PowerPC, etc.? How much network bandwidth do the systems consume? The eBATS (ECRYPT Benchmarking of Asymmetric Systems) project aims to answer these questions.

This report provides a comprehensive description of the eBATS progress to date. This report lists the public-key systems measured so far; lists the computers used for measurements; lists the compilers used for measurements; presents the measurements in graphical form; presents the measurements in tabular form; and describes the complete database of measurements available online. This report also describes the eBATS benchmarking process, explaining how a cryptographic implementor adds a new public-key system to eBATS, how the database of measurements is built, and how tables and graphs are created from the database. This report concludes by looking ahead to the future of eBATS.

Chapter 1

Introduction

eBATS (ECRYPT Benchmarking of Asymmetric Systems), run by the VAMPIRE lab, is a benchmarking project for public-key cryptography. eBATS measures public-key cryptosystems according to several criteria:

- Time to generate a key pair (a secret key and a corresponding public key).
- Length of the secret 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 secret key.
- Time to sign a message using a secret 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 Pentium III 68a, time on a Motorola PowerPC G4 7410, time on an AMD Athlon 64 X2, 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. eBATS goes further, taking into account the speed at which real computers can carry out those arithmetic operations. For example, the Pentium, 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 eBATS results.

Chapters 2 through 7 of this report describe the measurements collected by eBATS so far. Chapter 2 lists the public-key systems measured. Chapter 3 lists the computers used for measurements. Chapter 4 lists the compilers used for measurements. Chapter 5 presents the resulting measurements in graphical form. Chapter 6 presents the resulting measurements in tabular form. Chapter 7 describes the complete database of measurements available online.

Chapters 8 and 9 of this report describe the eBATS benchmarking process. Chapter 8 explains how a cryptographic implementor adds a new public-key system to eBATS. Chapter 9 explains how the database of measurements is created, and how tables and graphs are created from the database. See Figure 1.1 for a summary of the data flow in this process.

Chapter 10 looks ahead to the future of eBATS.

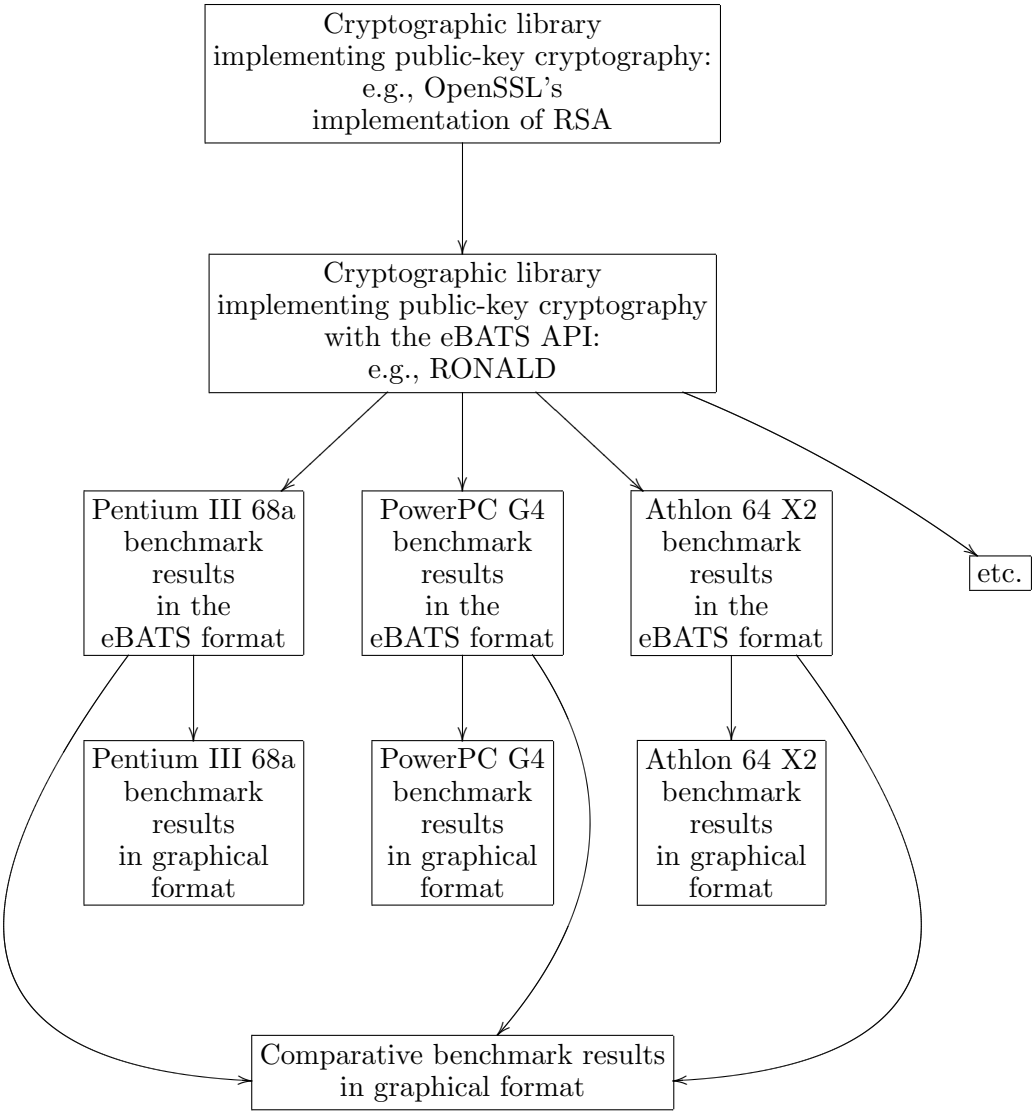


Figure 1.1: Benchmarking a public-key system: data flow.

Chapter 2

Which public-key systems are measured?

2.1 Introduction

This report includes measurements of 15 different BATs (Benchmarkable Asymmetric Tools): 15 software packages providing public-key functions. For example, `DONALD` is a signing BAT; this means that it is a software package providing functions to generate keys, sign messages, and verify signatures. The BATs total 45113 lines of code, not counting the lines of code in underlying libraries such as GMP, NTL, and OpenSSL.

One BAT can provide more than one public-key system. For example, `DONALD` is a parametrized BAT that supports three different signature systems, namely 512-bit DSA, 1024-bit DSA, and 2048-bit DSA, depending on the choice of parameter. Overall this report includes measurements of 116 different public-key systems. The systems are described below.

Some BATs were developed internally as part of the eBATS project, but eBATS is also open to submissions from other parts of VAMPIRE, submissions from other parts of ECRYPT, and submissions from outside ECRYPT. The following list of public-key systems include acknowledgments to authors of BATs.

2.2 List of public-key systems measured

Here are descriptions of the public-key systems measured:

- `bls 1` (only for x86-architecture computers): Pairing-based short signatures. Software written by Michael Scott (Dublin City University).
- `claus 1`: Classic Diffie-Hellman secret sharing modulo a 1024-bit prime. Software written internally on top of OpenSSL.
- `claus++ 1`: Classic Diffie-Hellman secret sharing modulo a 1024-bit prime. Software written internally on top of GMP and NTL.
- `curve25519-gaudry 1`: 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 (Laboratoire Lorrain de Recherche en Informatique et ses Applications).

- `donald 1 512`: DSA signatures using a 512-bit prime. Software written internally on top of OpenSSL.
- `donald 1 1024`: DSA signatures using a 1024-bit prime. Software written internally on top of OpenSSL.
- `donald 1 2048`: DSA signatures using a 2048-bit prime. Software written internally on top of OpenSSL.
- `ecdonald 1 nist-b-163`: 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.
- `ecdonald 1 nist-b-233`: 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.
- `ecdonald 1 nist-b-283`: 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.
- `ecdonald 1 nist-b-409`: 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.
- `ecdonald 1 nist-b-571`: 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.
- `ecdonald 1 nist-k-163`: 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.
- `ecdonald 1 nist-k-233`: 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.
- `ecdonald 1 nist-k-283`: 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.
- `ecdonald 1 nist-k-409`: 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.
- `ecdonald 1 nist-k-571`: 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.
- `ecdonald 1 nist-p-192`: 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.
- `ecdonald 1 nist-p-224`: 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.

- `ecdonald 1 nist-p-256`: 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.
- `ecdonald 1 nist-p-384`: 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.
- `ecdonald 1 nist-p-521`: 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.
- `ecdonald 1 secp160r1`: 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.
- `nistp256-sss-ultrasparc 1` (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).
- `ntru-enc 1 ees787ep1`: NTRU encryption with $N = 787$ and $q = 587$. Software written by Mark Etzel (NTRU Cryptosystems).
- `rainbow 1`: Rainbow multivariate-quadratic signatures. Software written by Jintai Ding and Dieter Schmidt (University of Cincinnati).
- `ronald 1 768`: 768-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 832`: 832-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 896`: 896-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 960`: 960-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 1024`: 1024-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 1088`: 1088-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 1152`: 1152-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 1216`: 1216-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 1280`: 1280-bit RSA encryption and signatures. Software written internally on top of OpenSSL.

- `ronald 1 1344`: 1344-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 1408`: 1408-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 1472`: 1472-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 1536`: 1536-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 1664`: 1664-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 1792`: 1792-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 1920`: 1920-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 2048`: 2048-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 2176`: 2176-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 2304`: 2304-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 2432`: 2432-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 2560`: 2560-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 2688`: 2688-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 2816`: 2816-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 2944`: 2944-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 3072`: 3072-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 3328`: 3328-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 3584`: 3584-bit RSA encryption and signatures. Software written internally on top of OpenSSL.

- `ronald 1 3840`: 3840-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 1 4096`: 4096-bit RSA encryption and signatures. Software written internally on top of OpenSSL.
- `ronald 2 768`: 768-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 832`: 832-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 896`: 896-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 960`: 960-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 1024`: 1024-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 1088`: 1088-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 1152`: 1152-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 1216`: 1216-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 1280`: 1280-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 1344`: 1344-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 1408`: 1408-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 1472`: 1472-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 1536`: 1536-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 1664`: 1664-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 1792`: 1792-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 1920`: 1920-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.

- `ronald 2 2048`: 2048-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 2176`: 2176-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 2304`: 2304-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 2432`: 2432-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 2560`: 2560-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 2688`: 2688-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 2816`: 2816-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 2944`: 2944-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 3072`: 3072-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 3328`: 3328-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 3584`: 3584-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 3840`: 3840-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 2 4096`: 4096-bit RSA encryption (with malleability defense) and signatures. Software written internally on top of OpenSSL.
- `ronald 3 768`: 768-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 832`: 832-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 896`: 896-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 960`: 960-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 1024`: 1024-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.

- `ronald 3 1088`: 1088-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 1152`: 1152-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 1216`: 1216-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 1280`: 1280-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 1344`: 1344-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 1408`: 1408-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 1472`: 1472-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 1536`: 1536-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 1664`: 1664-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 1792`: 1792-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 1920`: 1920-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 2048`: 2048-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 2176`: 2176-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 2304`: 2304-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 2432`: 2432-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 2560`: 2560-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 2688`: 2688-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 2816`: 2816-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.

- `ronald 3 2944`: 2944-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 3072`: 3072-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 3328`: 3328-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 3584`: 3584-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 3840`: 3840-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `ronald 3 4096`: 4096-bit RSA encryption (with malleability defense) and signatures (with message recovery). Software written internally on top of OpenSSL.
- `sflashv2 1`: SFLASHv2 multivariate-quadratic signatures. Software written by Louis Goubin (Université de Versailles), Nicolas Courtois (University College London), and Thomas Icart (École Polytechnique).
- `sflashv2 2`: SFLASHv2 multivariate-quadratic signatures. Improved software written by Louis Goubin (Université de Versailles), Nicolas Courtois (University College London), and Thomas Icart (École Polytechnique).
- `surf127eps 1`: 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).

Chapter 3

Which computers are used for measurements?

3.1 Introduction

Timings depend heavily on the choice of computer. For example, a 2000MHz Athlon 64 will sign a message much more quickly than a 133MHz Pentium 1.

Reporting CPU cycles (microseconds/2000 on a 2000MHz Athlon 64, 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, an Athlon 64 can generally do more in one cycle than a Pentium 1.

To ensure direct comparability of all systems on whichever computers are of interest to the users, eBATS times each system on a wide variety of computers. This report includes measurements for 21 computers with 5 different architectures (amd64, ia64, ppc32, sparcv9, x86) and a broad range of 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 `mace` has one CPU, an AMD Athlon 64 X2 containing two separate 2000MHz 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 BATs 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 500000 cycles on `mace` was observed to take $500000/2000 = 250$ microseconds on a single 2000MHz core of `mace`; this means that a single core can carry out 4 new computations each millisecond, and both cores together can carry out 8 new computations each millisecond.

3.3 List of computers used for measurements

Here are descriptions of the computers used for measurements:

- amd64 architecture, 2000MHz, 2 cores, AMD Athlon 64 X2 (15,75,2), owned by University of Illinois at Chicago, named `mace`.
- amd64 architecture, 2137MHz, 2 cores, Intel Core 2 Duo (6f6), owned by University of Illinois at Chicago, named `katana`.
- amd64 architecture, 2192MHz, 2 cores, AMD Opteron 250 (f58), owned by Hewlett-Packard, named `td189`.
- amd64 architecture, 2390MHz, 2 cores, AMD Opteron 250 (f5a), owned by Hewlett-Packard, named `td159`.
- amd64 architecture, 3000MHz, 1 core, Intel Pentium 4 (f43), owned by Technische Universiteit Eindhoven, named `pclin153`.
- ia64 architecture, 900MHz, 2 cores, HP Itanium II, owned by Hewlett-Packard, named `td156`.
- ia64 architecture, 1500MHz, 16 cores, HP Itanium II, owned by Hewlett-Packard, named `td178`.
- ppc32 architecture, 533MHz, 2 cores, Motorola PowerPC G4 7410, owned by University of Illinois at Chicago, named `gggg`.
- sparcv9 architecture, 1050MHz, 48 cores, Sun UltraSPARC IV, owned by Danmarks Tekniske Universitet, named `hald`.
- x86 architecture, 133MHz, 1 core, Intel Pentium (52c), owned by University of Illinois at Chicago, named `cruncher`. Measurements are in progress but are not yet finished.
- x86 architecture, 800MHz (power-saving mode), 1 core, Intel Pentium M (6d8), owned by D. J. Bernstein, named `atlas`.
- x86 architecture, 900MHz, 1 core, AMD Athlon (622), owned by University of Illinois at Chicago, named `thoth`.
- x86 architecture, 1000MHz, 2 cores, Intel Pentium III (68a), owned by University of Illinois at Chicago, named `neumann`.
- x86 architecture, 1400MHz, 2 cores, Intel Pentium III (6b1), owned by Hewlett-Packard, named `td152`.
- x86 architecture, 1400MHz, 2 cores, Intel Pentium III (6b1), owned by Hewlett-Packard, named `td158`.
- x86 architecture, 1900MHz, 1 core, Intel Pentium 4 (f12), owned by University of Illinois at Chicago, named `fireball`.

- x86 architecture, 2800MHz, 2 cores, Intel Pentium 4 (f29), owned by Technische Universiteit Eindhoven, named `poema`.
- x86 architecture, 2991MHz, 8 cores, Intel Pentium 4 (f26), owned by Hewlett-Packard, named `td185`.
- x86 architecture, 3000MHz, 1 core, Intel Pentium 4 (f41), owned by Technische Universiteit Eindhoven, named `pclin118`.
- x86 architecture, 3066MHz, 4 cores, Intel Xeon (f25), owned by Hewlett-Packard, named `td162`.
- x86 architecture, 3200MHz, 4 cores, Intel Xeon (f25), owned by Hewlett-Packard, named `td186`.
- x86 architecture, 3400MHz, 1 core, Intel Pentium 4 (f29), owned by University of Illinois at Chicago, named `shell`.

Chapter 4

Which compilers are used for measurements?

4.1 Introduction

The choice of compiler, including compiler options, can dramatically affect the speed of a BAT. The eBATS benchmarking toolkit, BATMAN (Benchmarking of Asymmetric Tools on Multiple Architectures, Non-interactively), tries compiling each BAT under each of the compilers listed below, and selects the compiler that produces the highest speeds for the BAT. All speed reports for the BAT use the selected compiler.

The best compiler can vary from one computer to another. Even on one computer, the best compiler can vary from one BAT to another. Even within one BAT, the best compiler can vary from one parameter selection (i.e., one public-key system) to another. Consequently, BATMAN tries each compiler again for each computer/BAT/parameter combination. For example, on the computer `td186`, BATMAN selected `gcc -O -fomit-frame-pointer` for the `ntru-enc 1 ees787ep1` public-key system, and selected `gcc -march=nocona -O2 -fomit-frame-pointer` for the `sflashv2 2` public-key system.

BATMAN does *not* try different compilers for different operations by the same public-key system on the same computer. BATMAN chooses a compiler on the basis of one operation (either a BAT-specified "tune target," or computing a shared secret, or signing a short message, or encrypting a short message) and then uses that compiler to measure all operations. 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 library, switching from one version to another when they switch from one public-key operation to another, but in practice applications link with one compiled version of the library and expect the library to provide good performance for all operations.

Some compilers (for example, `gcc -m64 -maltivec -O3 -fomit-frame-pointer`) are machine-specific. On other machines, BATMAN sees that those compilers are unable to handle some simple test programs, and does not waste further time trying those compilers. BATMAN also skips compilers that are functional but that cannot link programs together with the first functional compiler in the list; in particular, the timings reported for the amd64 architecture do not include x86-architecture compilers. BATMAN also checks whether a compiled BAT passes some simple tests such as being able to decrypt an encrypted message; if the tests fail, BATMAN skips that compiler for that BAT.

4.2 Tuned BATs

Some BATs have multiple "tunings." BATMAN tries each tuning with each compiler and selects the compiler/tuning combination that produces the highest speeds for the BAT. Tunings are used in several ways:

- Trying additional compiler options that could improve performance. For example, `surf127eps 1` has two tunings: an `unroll` tuning that adds `-funroll-loops` to the compiler options, and a `nounroll` tuning that does not. BATMAN ended up selecting `unroll` on most computers, but `nounroll` on `td162`.
- Trying different code that could improve performance. For example, `claus++ 1` has two tunings: a `GMP` tuning with code that uses the GMP library for modular exponentiation, and an `NTL` tuning with code that uses the NTL library for modular exponentiation. BATMAN ended up selecting `GMP` on all computers.
- Trying different code that works on different machines. For example, `sflashv2 2` has two tunings: a `little` tuning with code that works on little-endian computers (amd64, ia64, x86), and a `big` tuning with code that works on big-endian computers (ppc32, sparcv9).

BAT authors who want to use a special compiler for a particular machine can simply include that compiler's assembly-language output as one of their BAT tunings.

4.3 List of compilers used for measurements

Here is the list of 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 -q64 -O2
- xlc -q64 -O
- xlc -q64
- xlc -q64 -qtune=pwr3 -O2
- xlc -q64 -qtune=pwr3 -O
- xlc -q64 -qtune=pwr3
- /opt/SUNWspro/bin/cc -fast -xarch=v9
- /opt/SUNWspro/bin/cc -xarch=v9
- /opt/ansic/bin/cc +DD64 -fast
- /opt/ansic/bin/cc +DD64
- 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`

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

Measurements in graphical form

5.1 Introduction

This chapter presents a series of graphs, one for each computer. The vertical axis on each graph is time, from 2^{16} cycles through 2^{32} cycles. The horizontal labels on the graph are as follows:

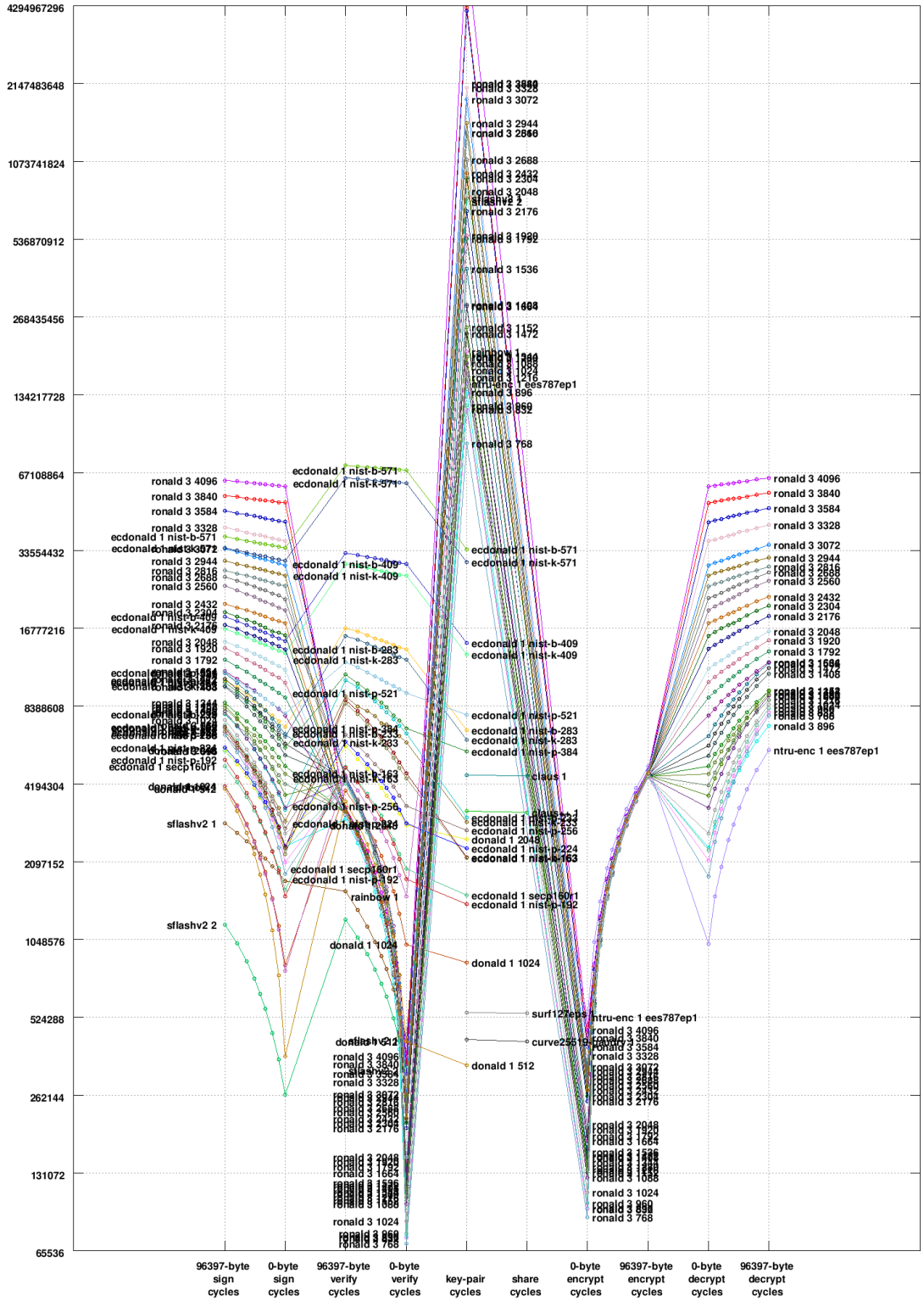
- "Key-pair cycles": Time to generate a secret key and a public key.
- "Share cycles": Time to compute a shared secret.
- "0-byte encrypt cycles": Time to encrypt a 0-byte message.
- "96397-byte encrypt cycles": Time to encrypt a 96397-byte message.
- "0-byte decrypt cycles": Time to decrypt an encrypted 0-byte message.
- "96397-byte decrypt cycles": Time to decrypt an encrypted 96397-byte message.
- "0-byte sign cycles": Time to sign a 0-byte message.
- "96397-byte sign cycles": Time to sign a 96397-byte message.
- "0-byte verify cycles": Time to verify a signed 0-byte message.
- "96397-byte verify cycles": Time to verify a signed 96397-byte message.

Each graph is a superimposition of several curves, one curve for each BAT.

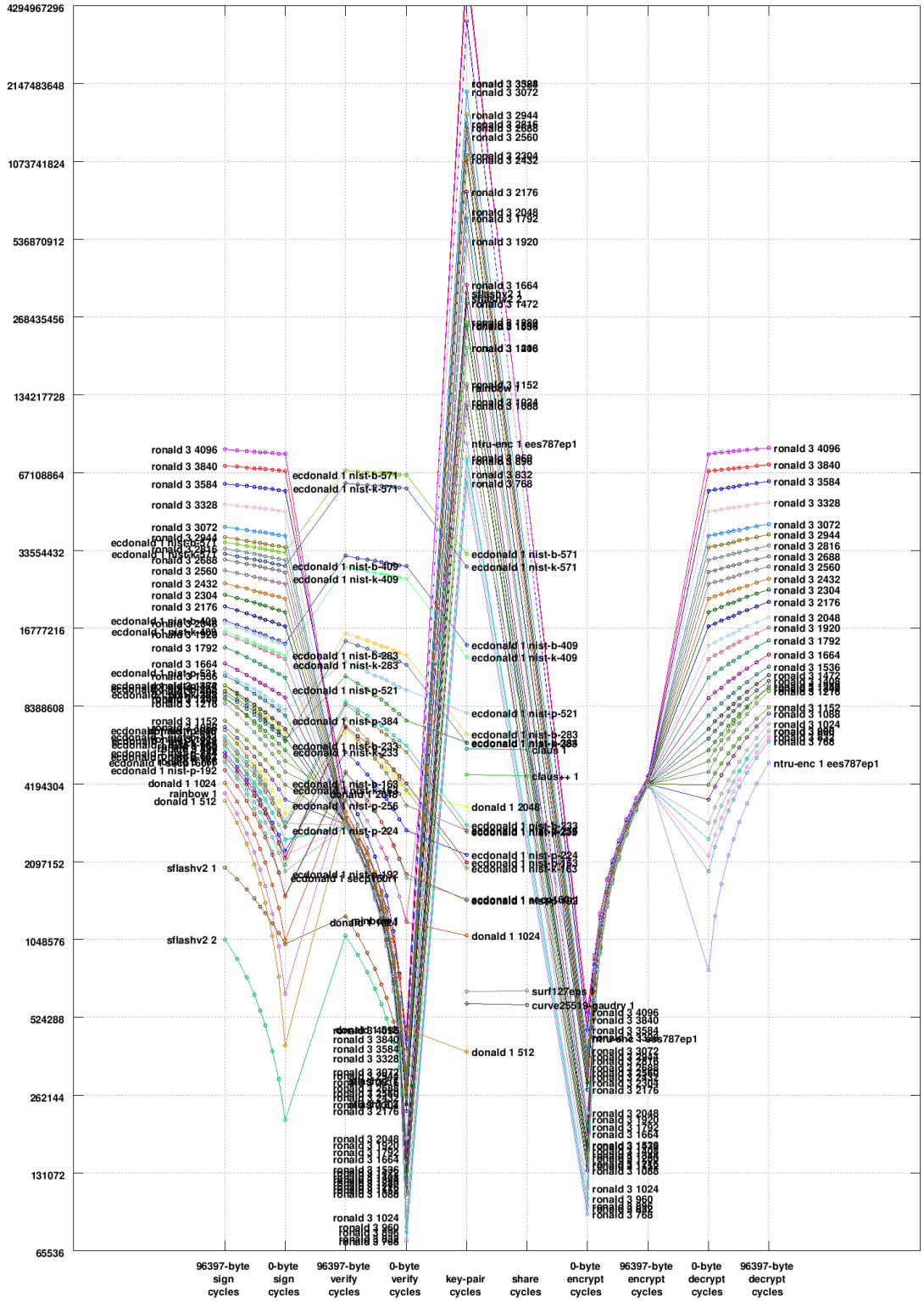
Several intermediate message sizes between 0 bytes and 96397 bytes are also plotted, although not labelled. Secret-key cryptography becomes an increasingly important part of total encryption, decryption, signature, and verification time as message lengths increase.

These graphs show, among other things, that cryptographic performance depends heavily upon implementation techniques. For example, Section 5.10 shows that key generation for `nistp256-sss-ultrasparc 1` is three times faster than key generation for `ecdonald 1 nist-p-256`—even though both of these systems are computing exactly the same function! The `nistp256-sss-ultrasparc 1` BAT decomposes that function into CPU operations much more efficiently than the `ecdonald 1 nist-p-256` BAT does.

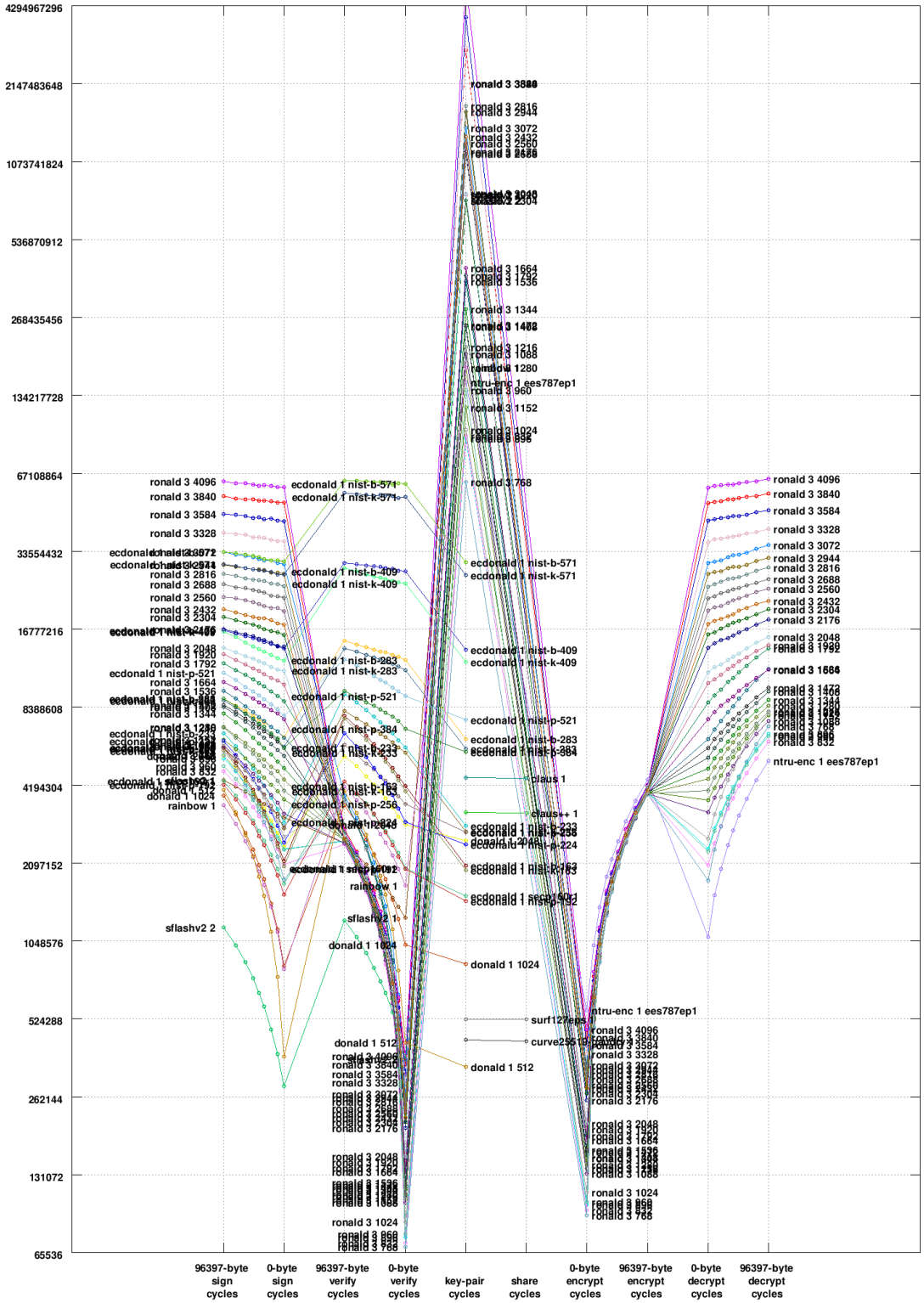
5.2 amd64, 2000MHz, Athlon 64 X2 (15,75,2), mace



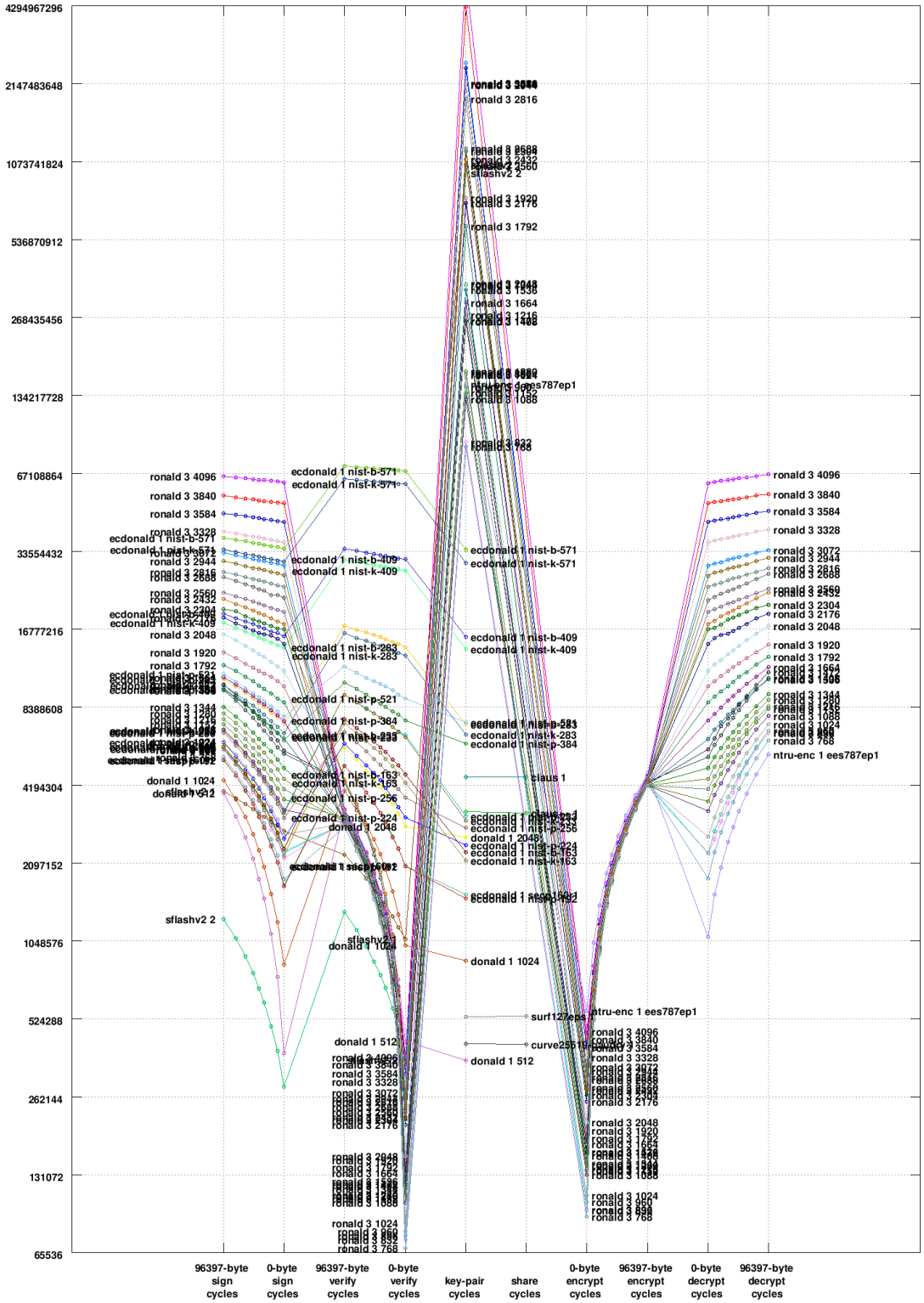
5.3 amd64, 2137MHz, Core 2 Duo (6f6), `katana`



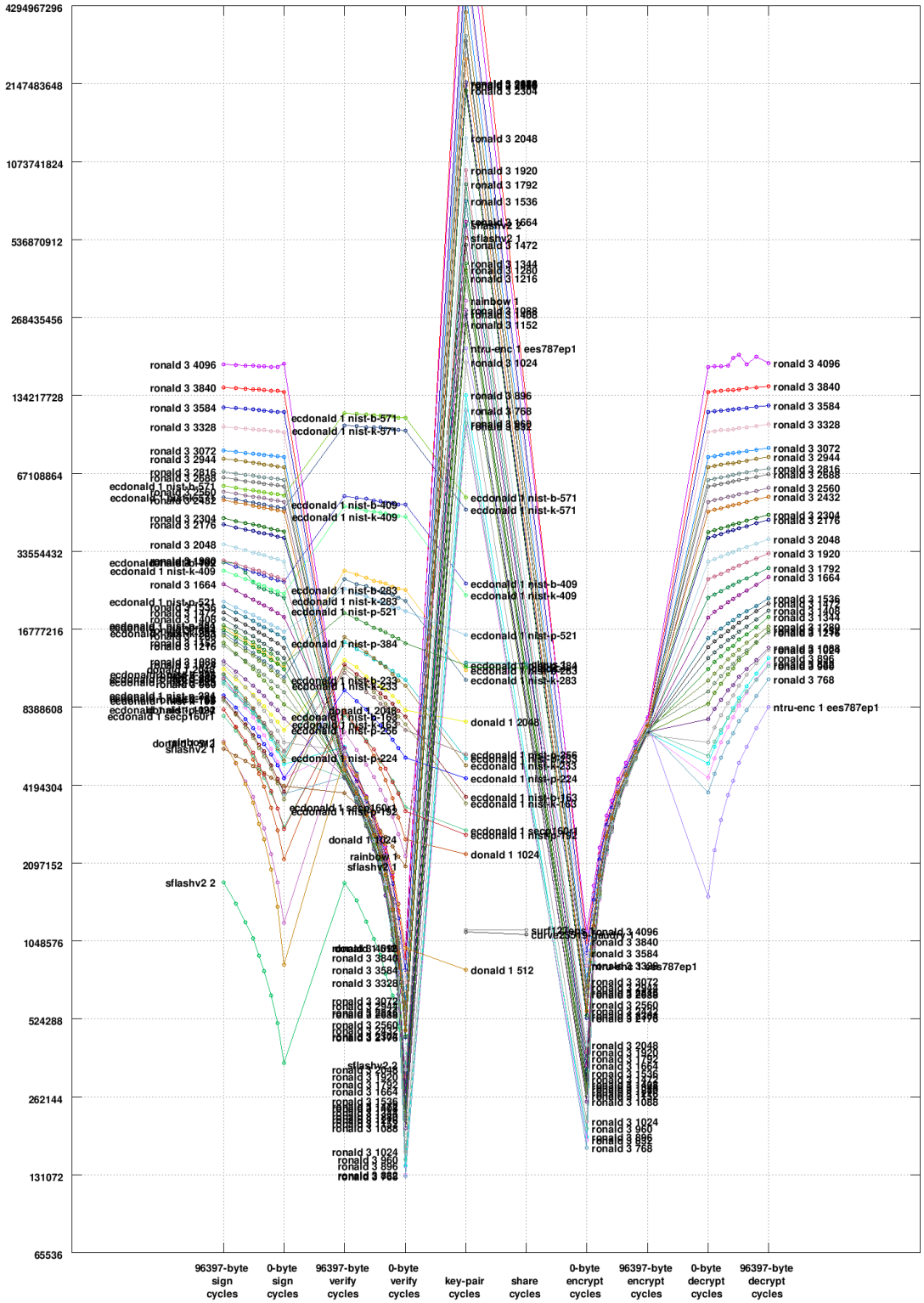
5.4 amd64, 2192MHz, Opteron 250 (f58), `td189`



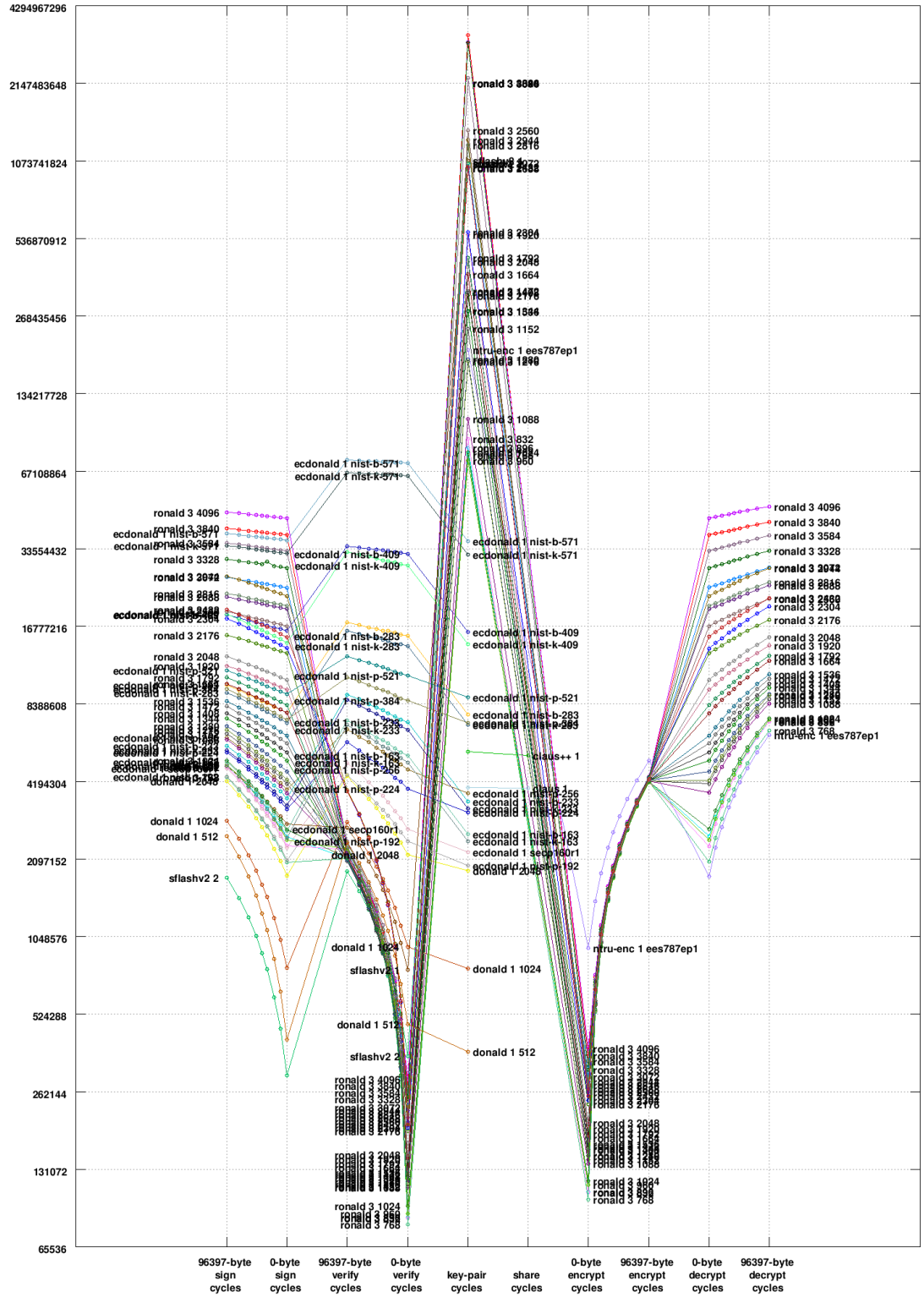
5.5 amd64, 2390MHz, Opteron 250 (f5a), `td159`



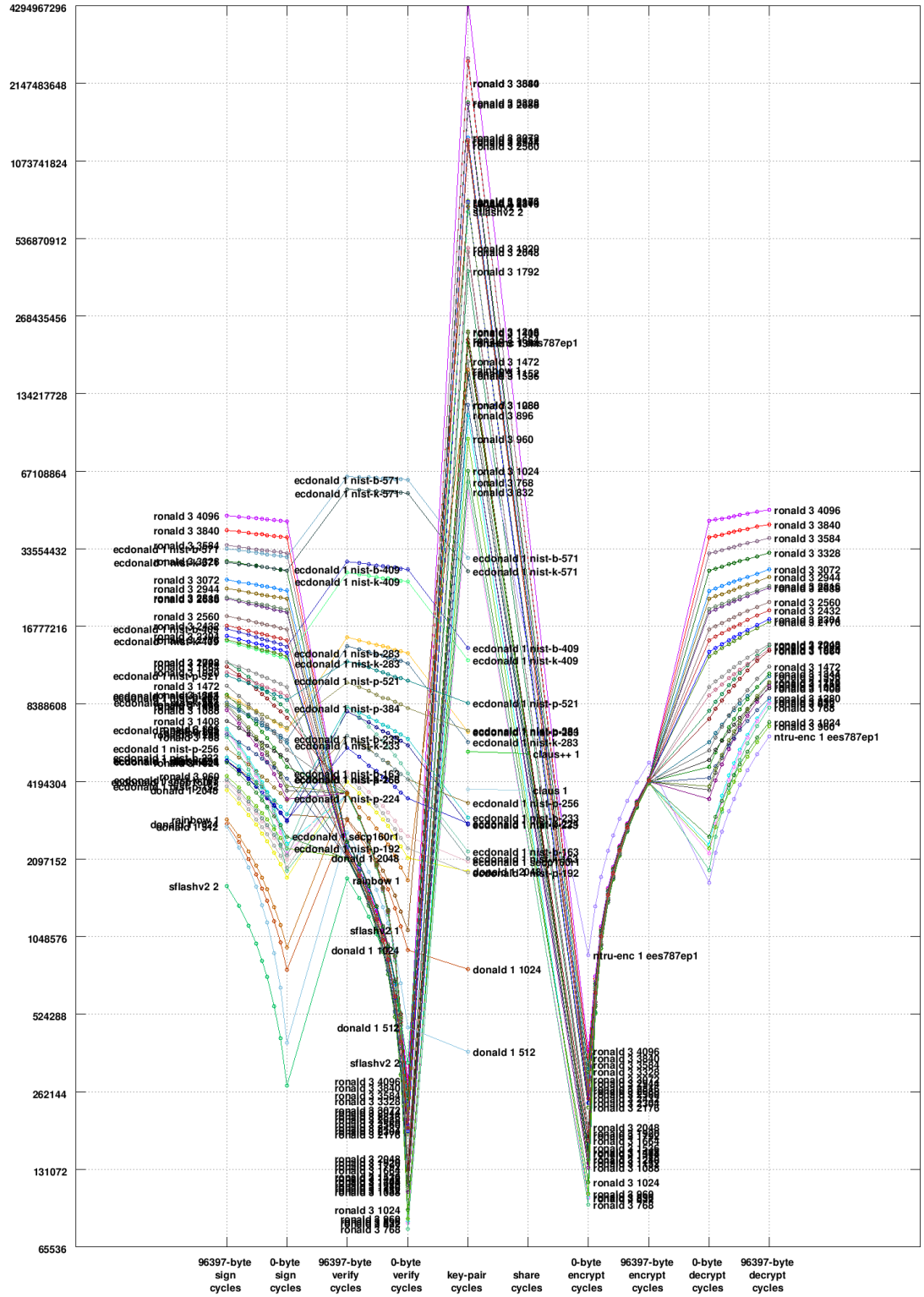
5.6 amd64, 3000MHz, Pentium 4 (f43), `pclin153`



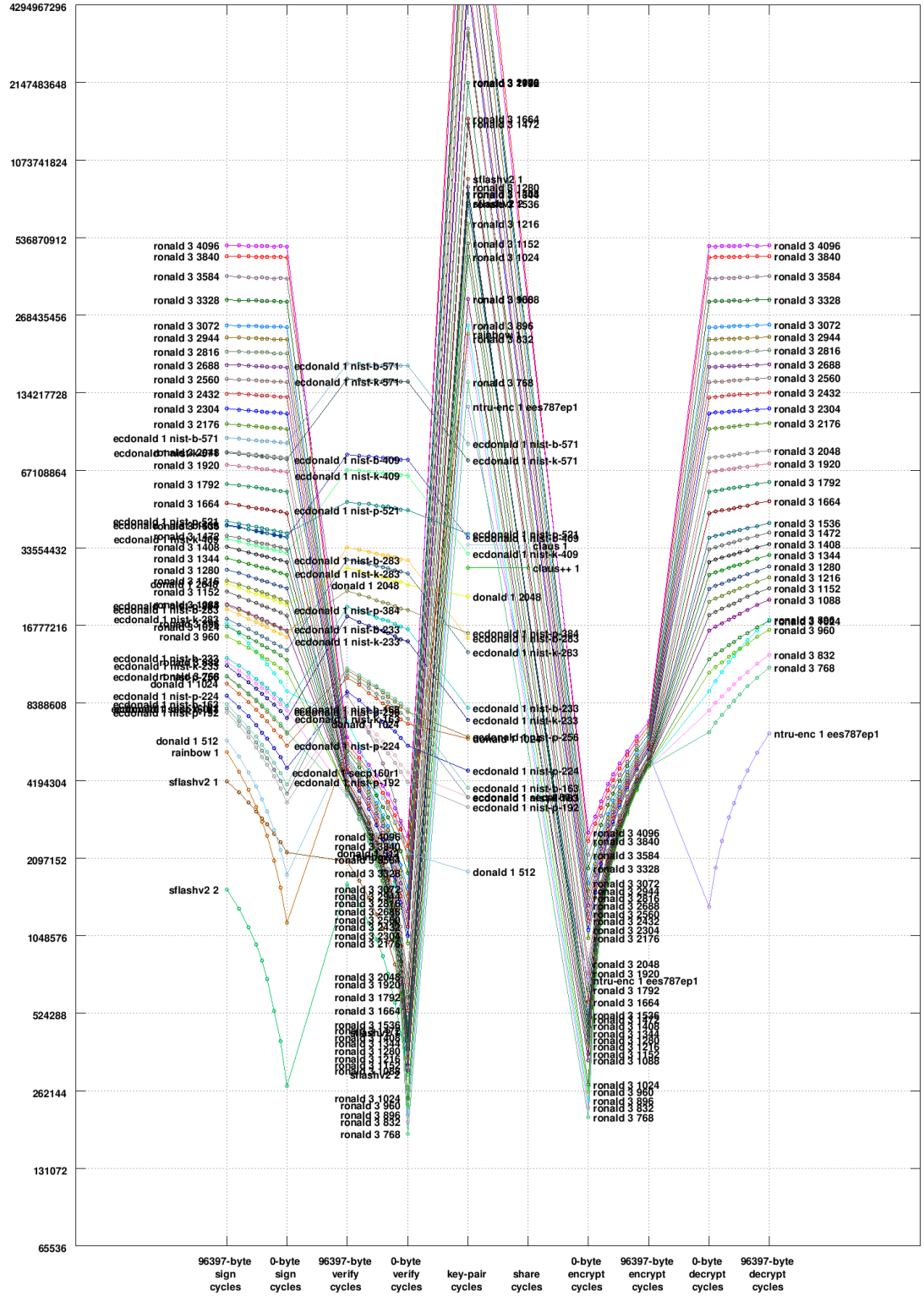
5.7 ia64, 900MHz, Itanium II, `td156`



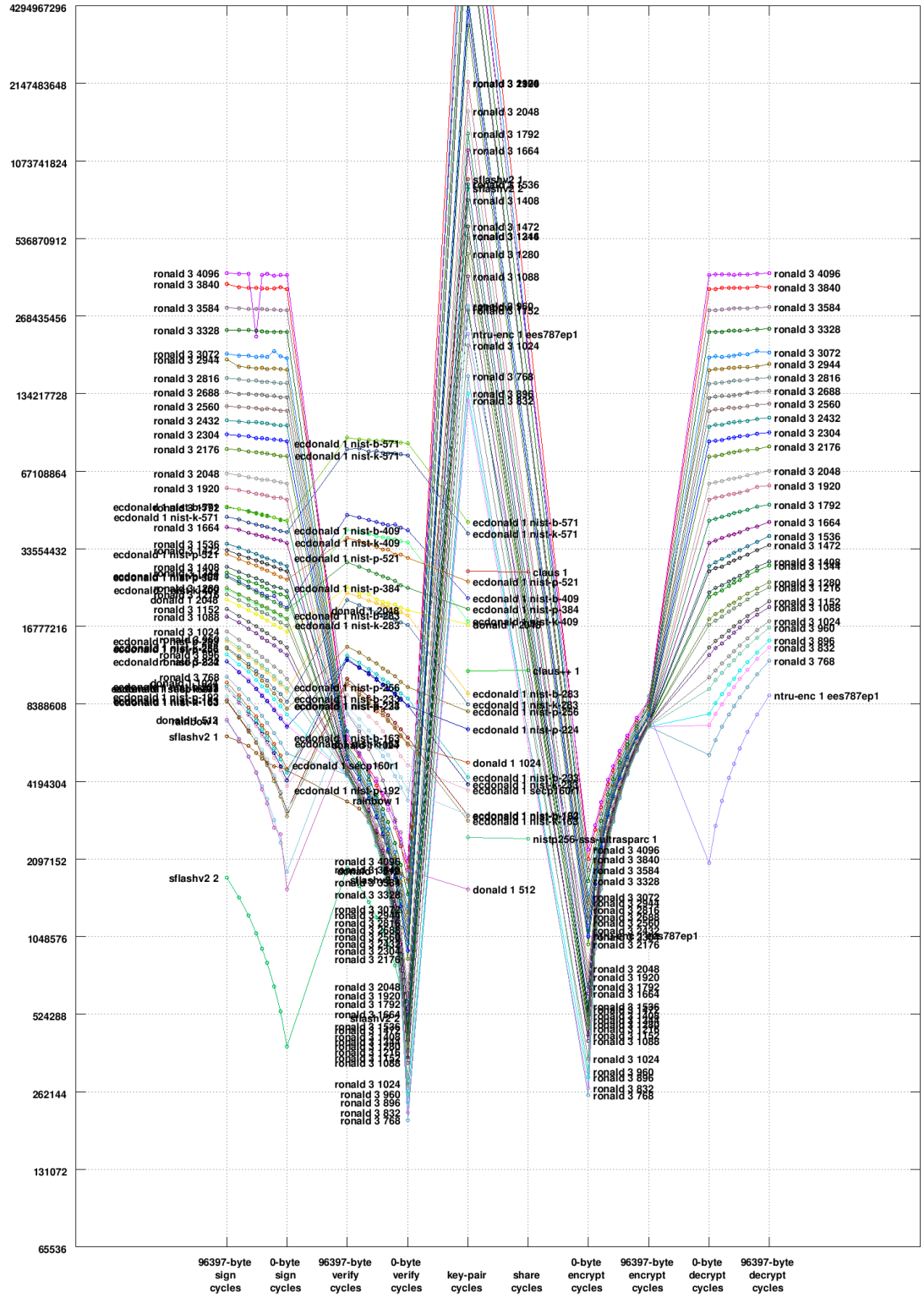
5.8 ia64, 1500MHz, Itanium II, `td178`



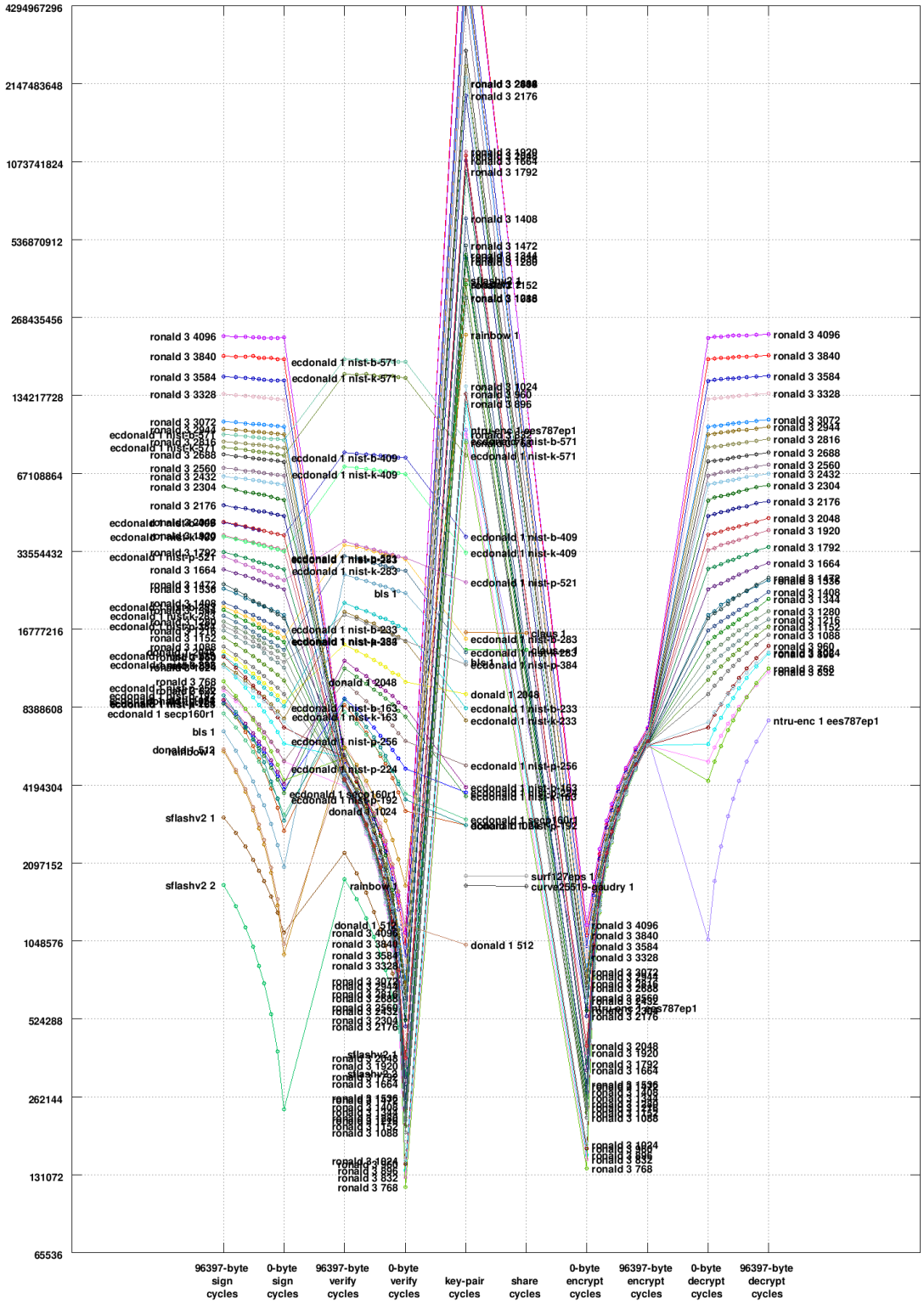
5.9 ppc32, 533MHz, PowerPC G4 7410, gggg



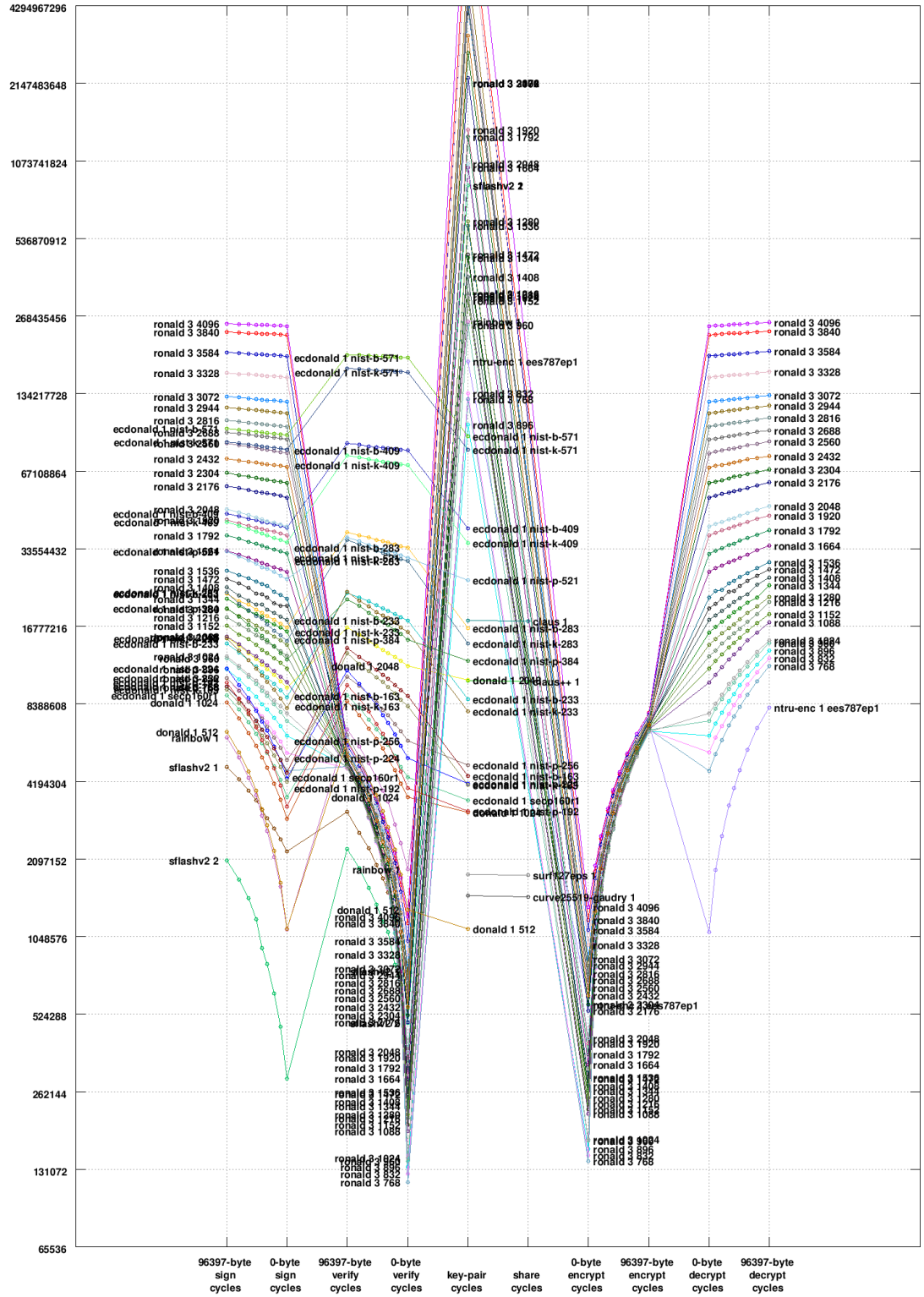
5.10 sparcv9, 1050MHz, UltraSPARC IV, `hald`



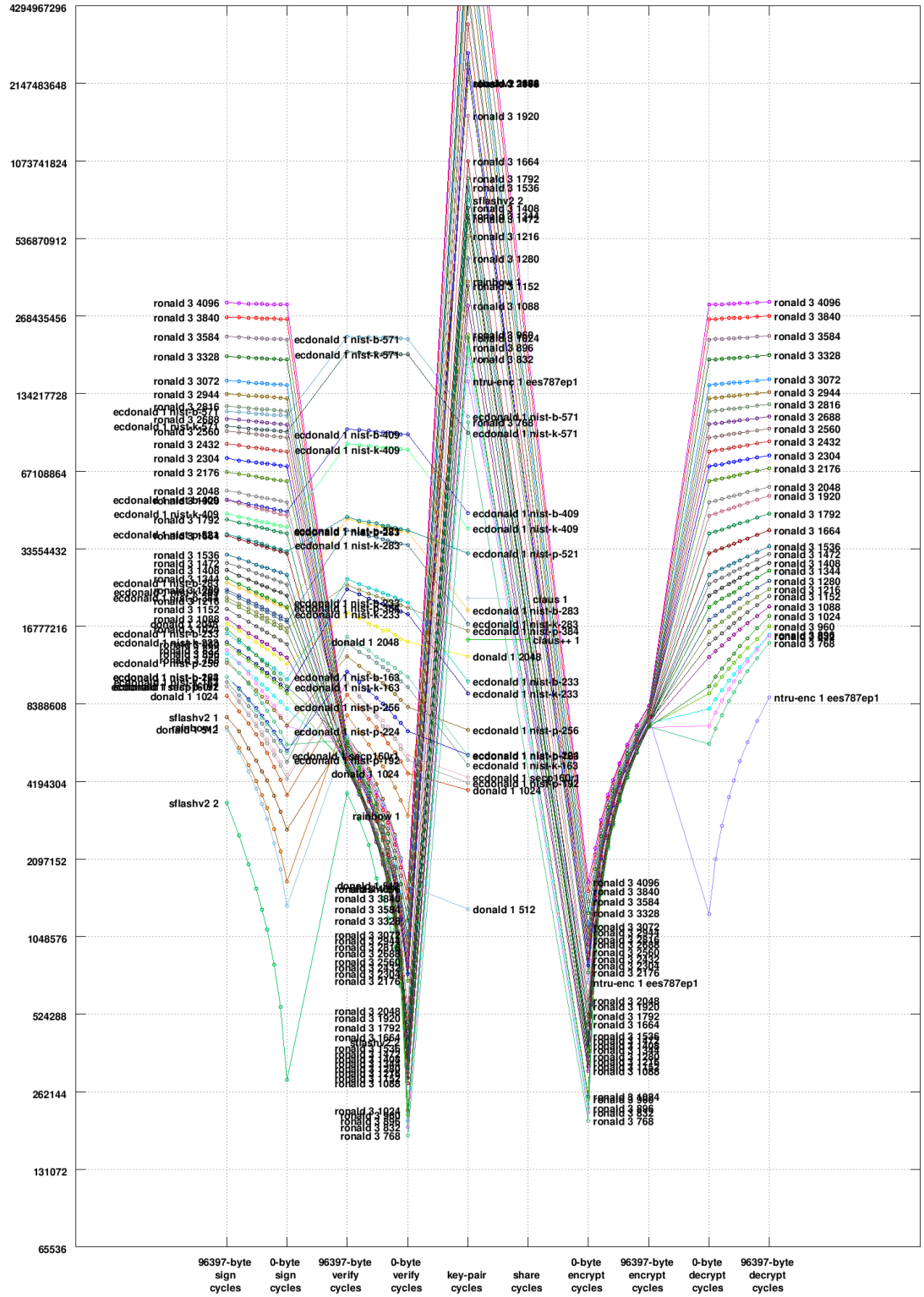
5.11 x86, 800MHz, Pentium M (6d8), `atlas`



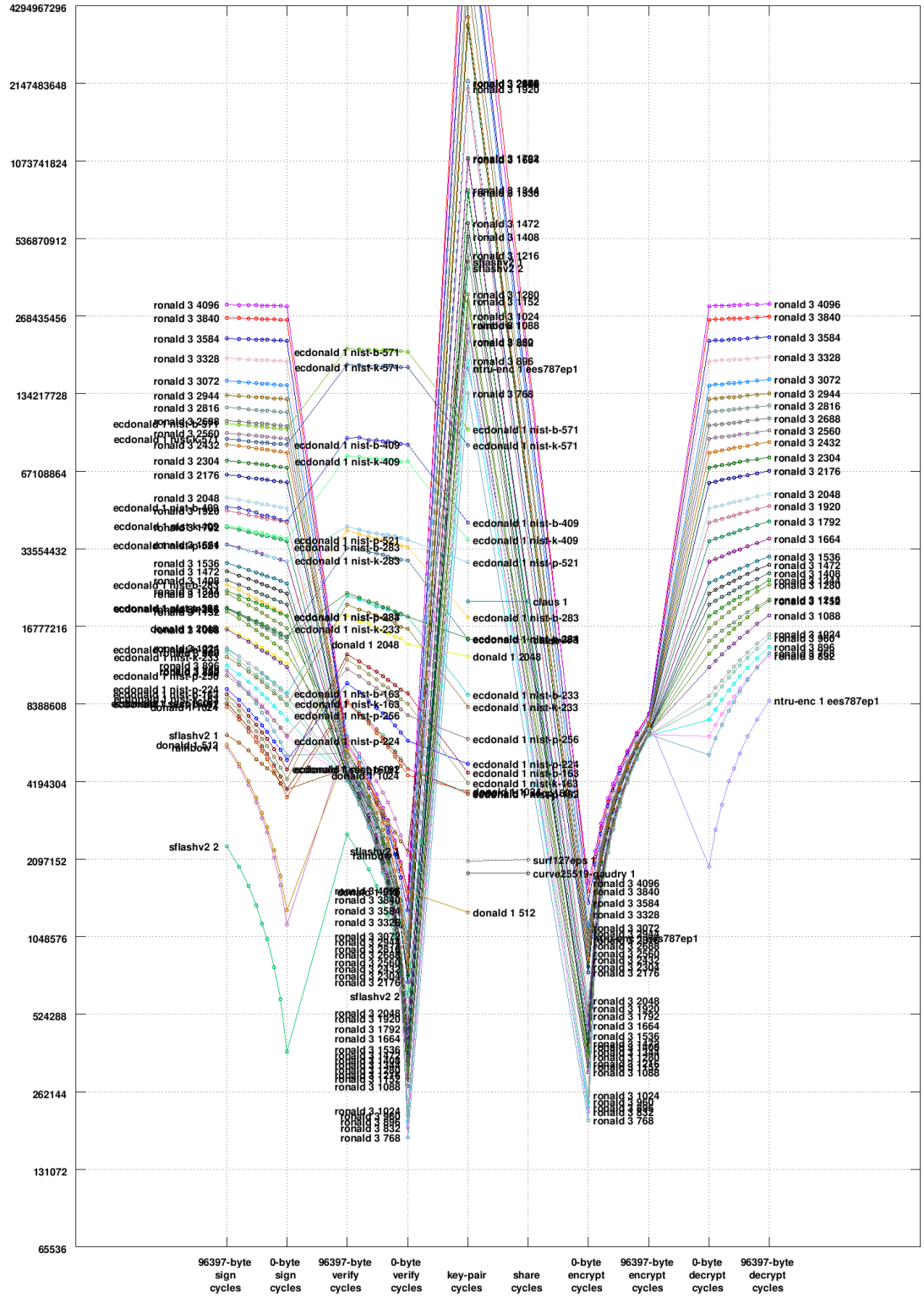
5.12 x86, 900MHz, Athlon (622), `thoth`



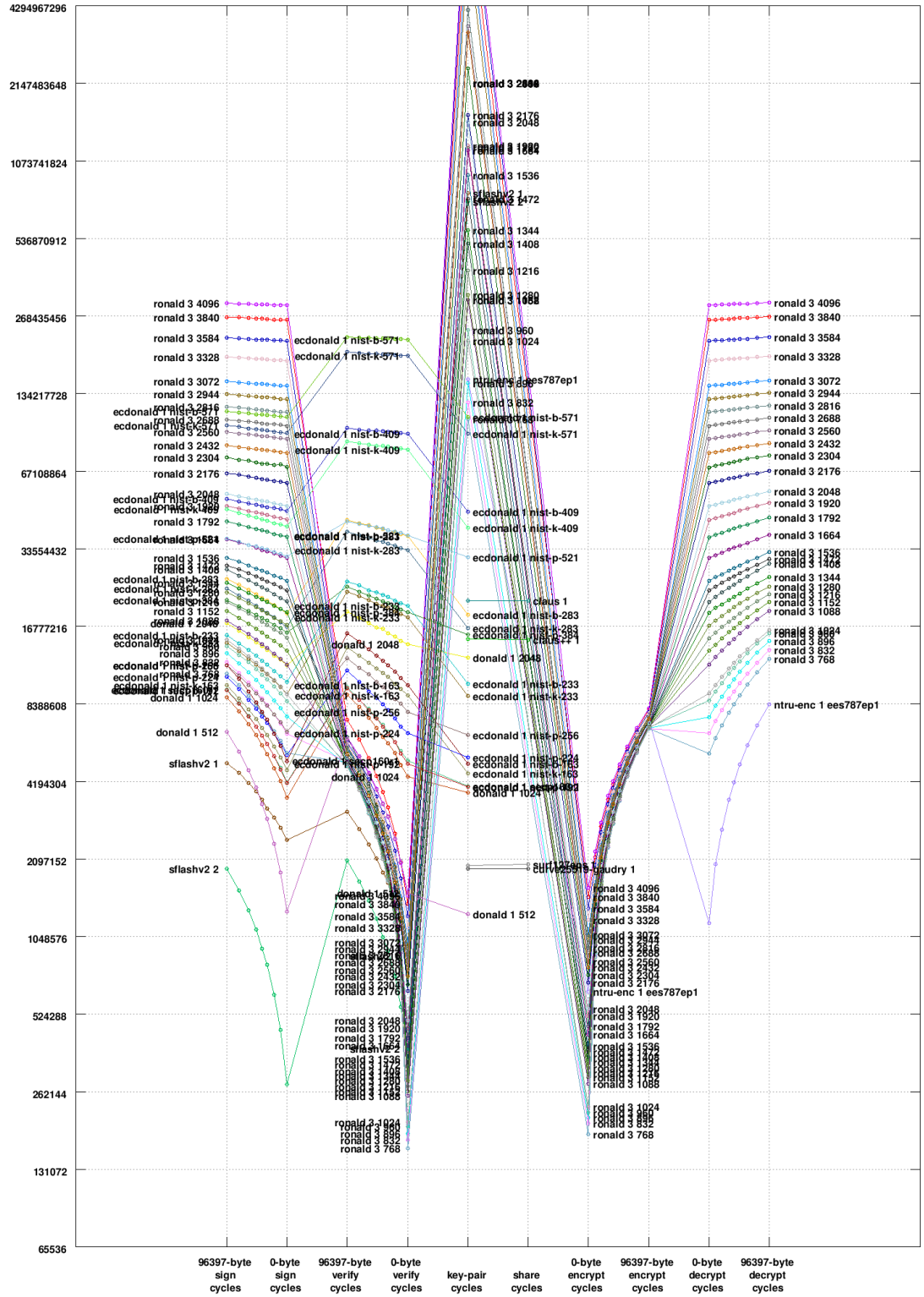
5.13 x86, 1000MHz, Pentium III (68a), `neumann`



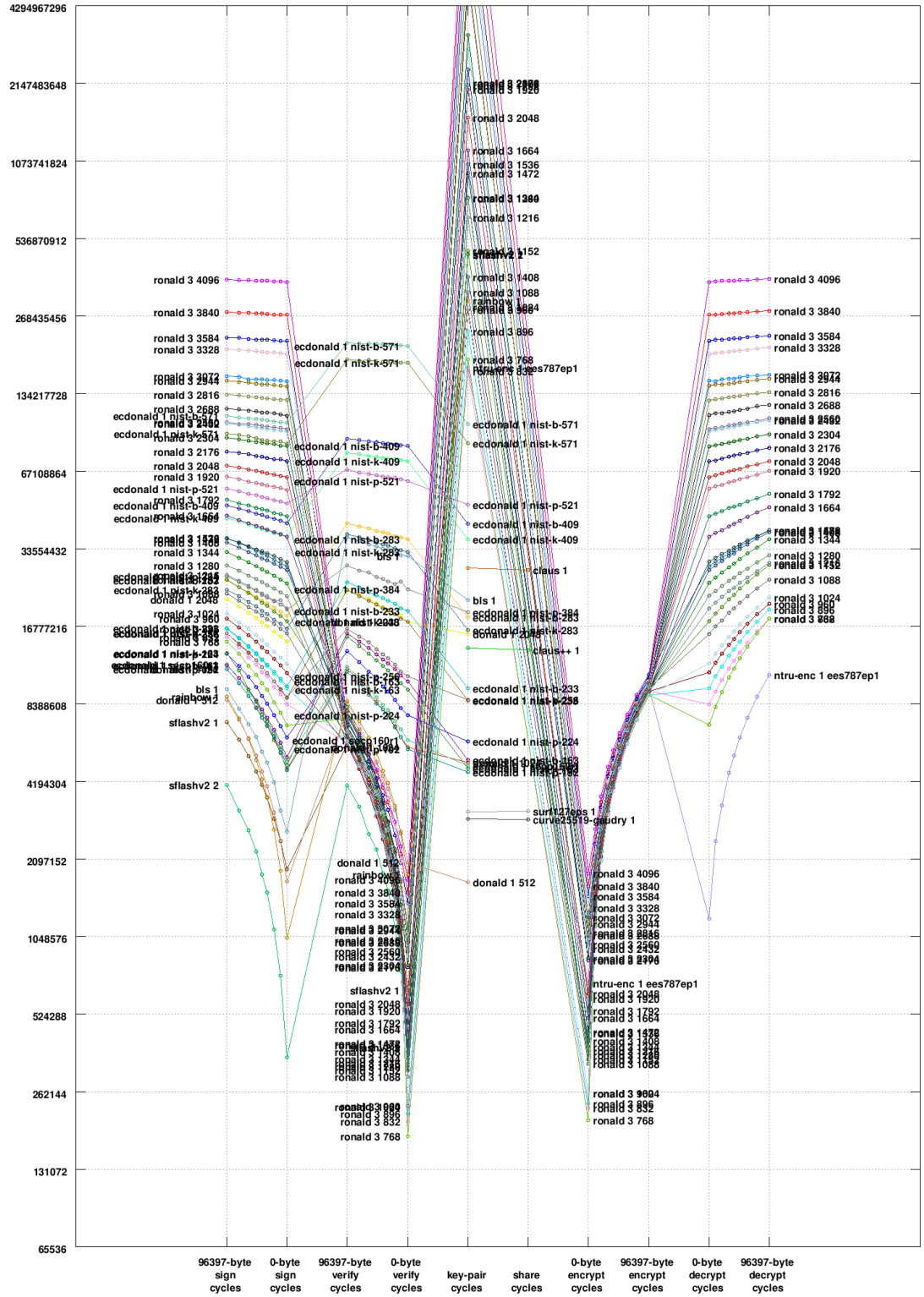
5.14 x86, 1400MHz, Pentium III (6b1), `td152`



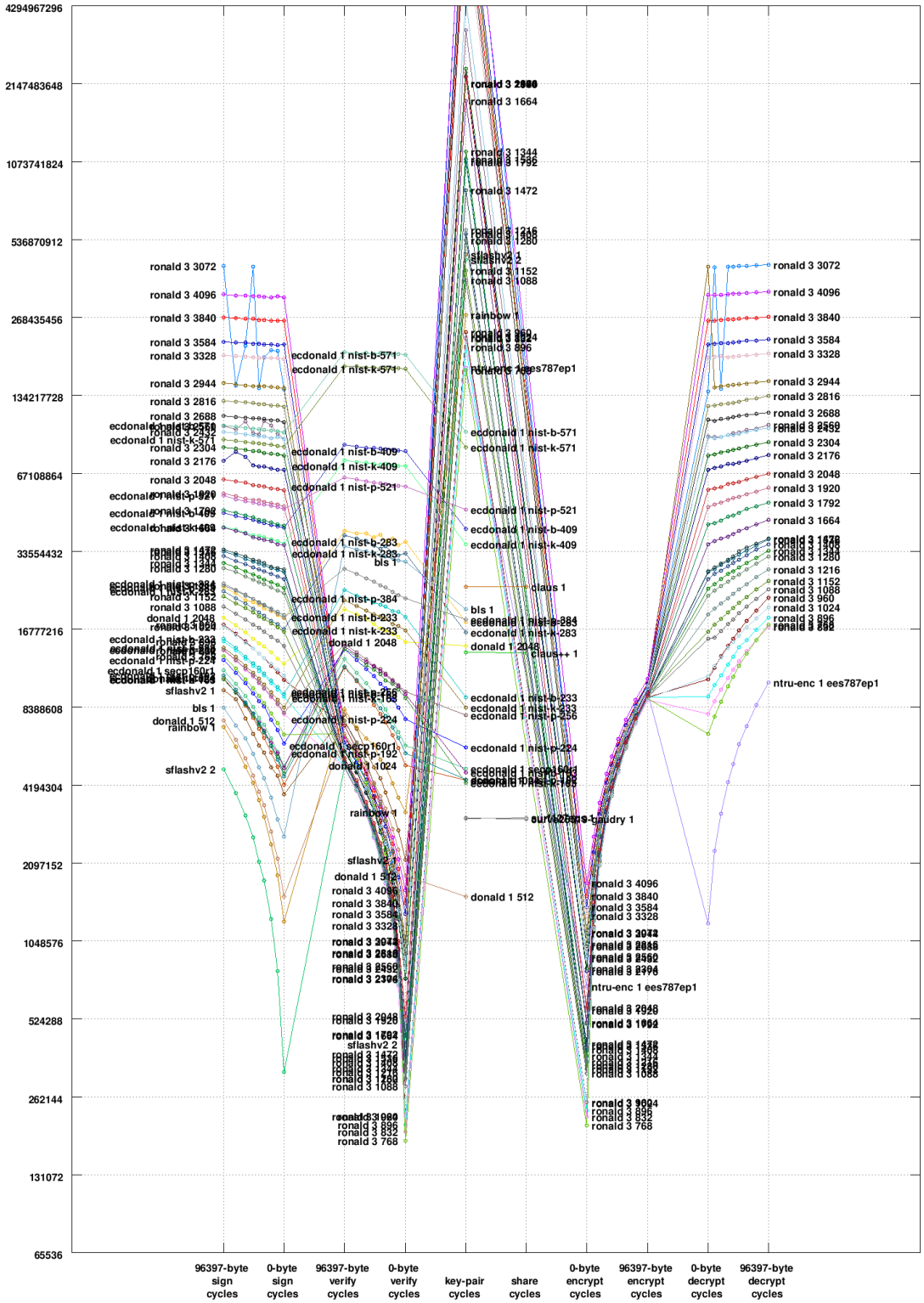
5.15 x86, 1400MHz, Pentium III (6b1), `td158`



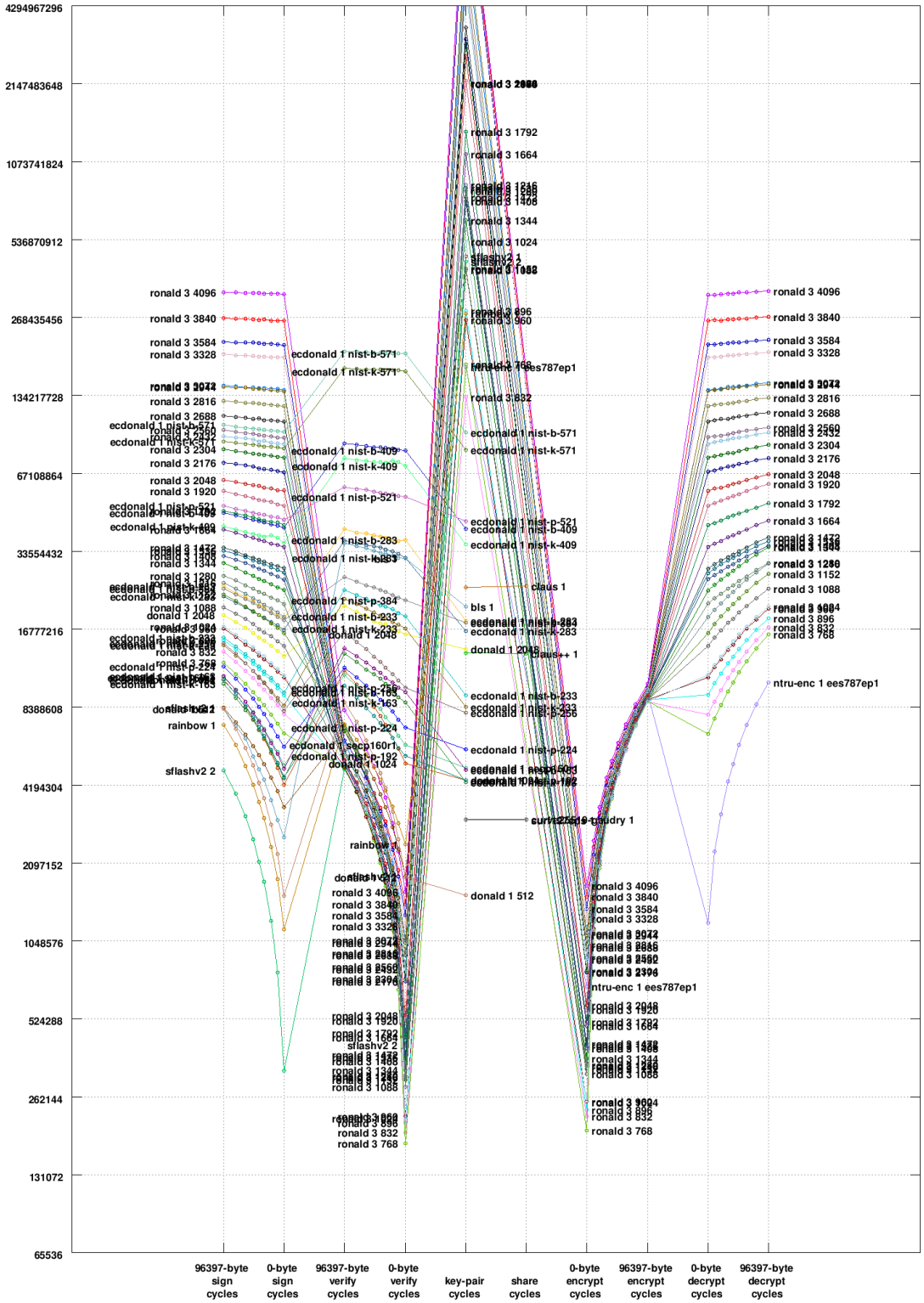
5.16 x86, 1900MHz, Pentium 4 (f12), `fireball`



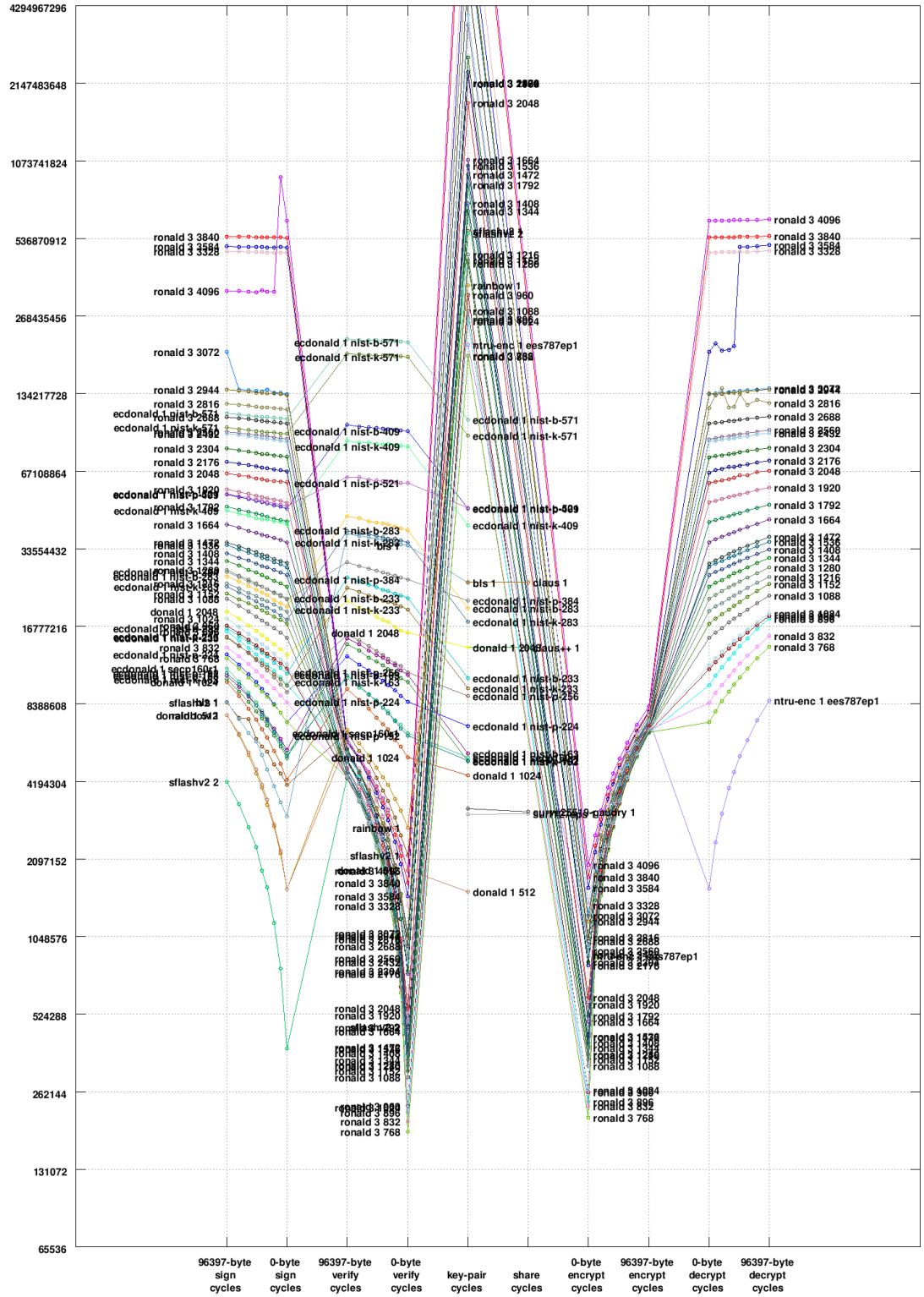
5.17 x86, 2800MHz, Pentium 4 (f29), `poema`



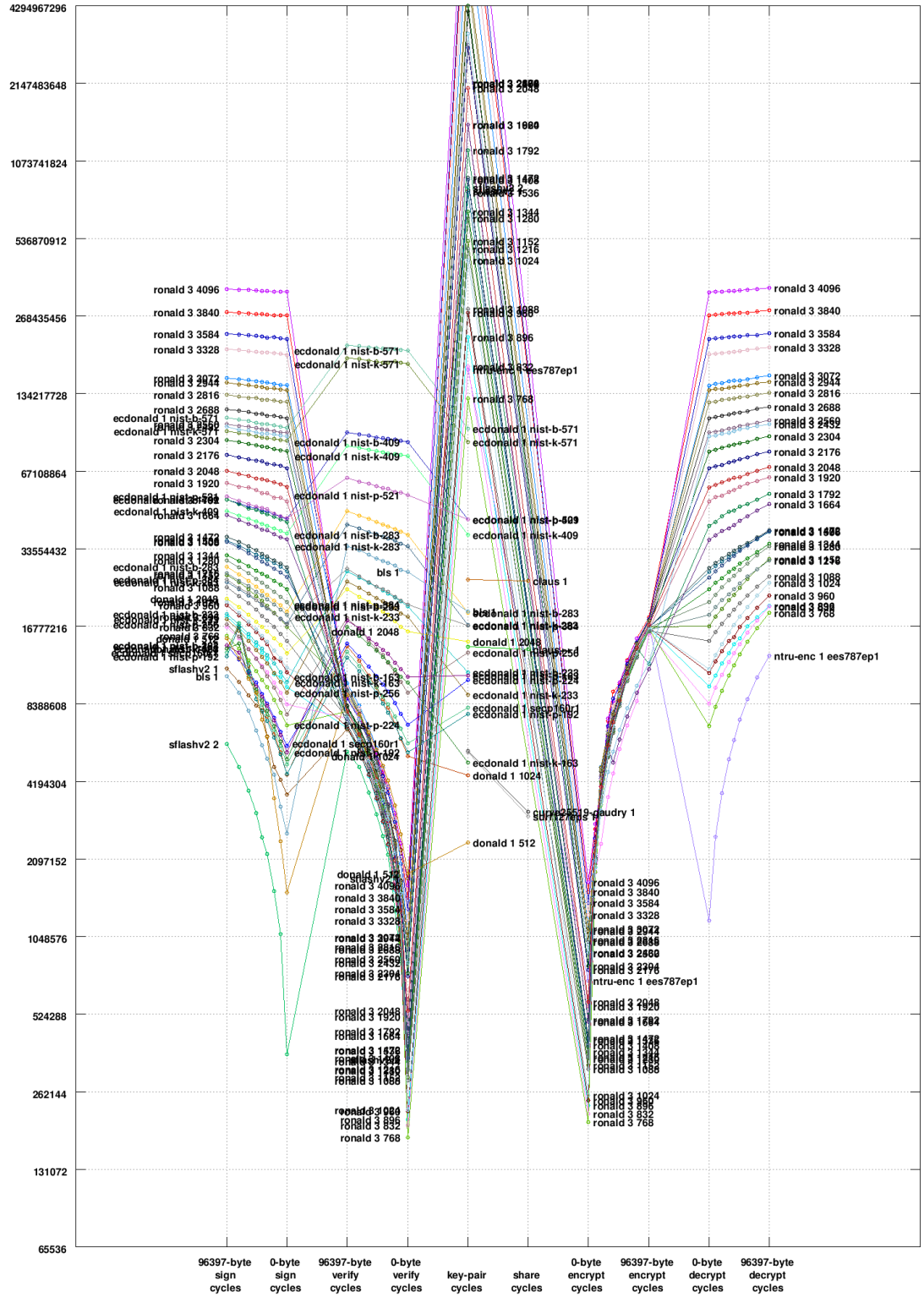
5.18 x86, 2991MHz, Pentium 4 (f26), td185



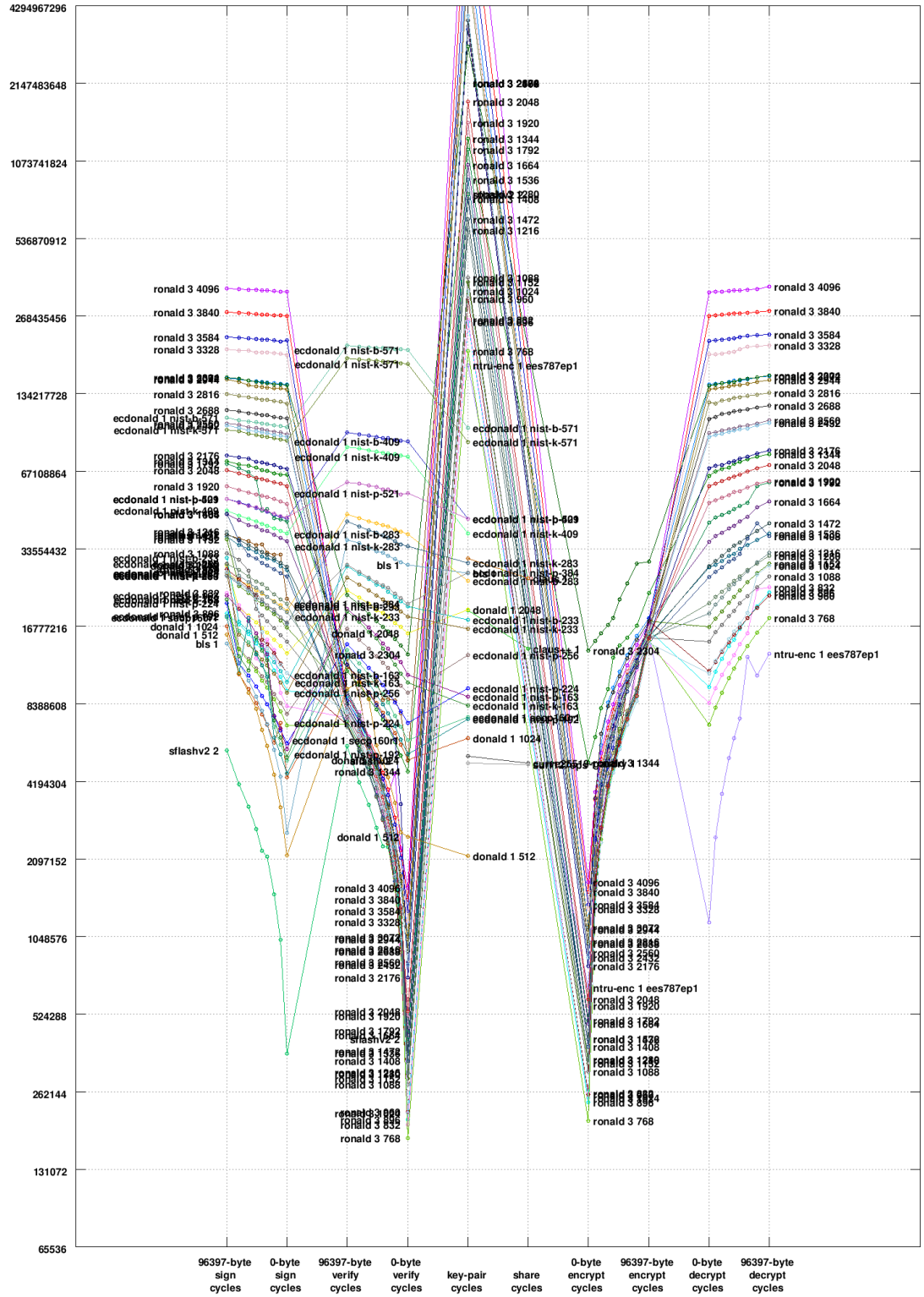
5.19 x86, 3000MHz, Pentium 4 (f41), `pclin118`



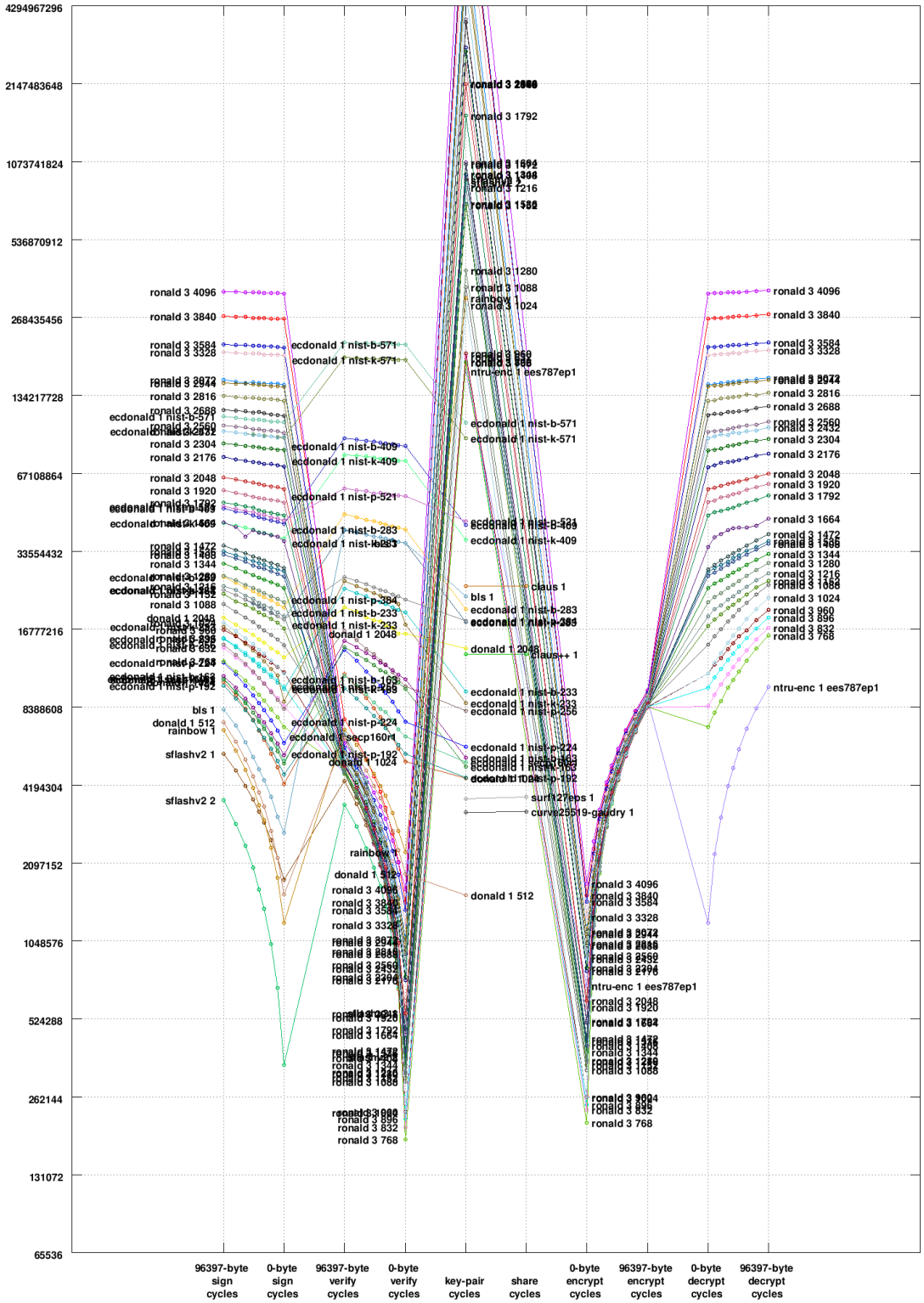
5.20 x86, 3066MHz, Xeon (f25), td162



5.21 x86, 3200MHz, Xeon (f25), `td186`



5.22 x86, 3400MHz, Pentium 4 (f29), `shell`



Chapter 6

Measurements in tabular form

6.1 Introduction

This chapter presents two tables for each computer: one table for time and one table for space. The time table has the following columns:

- "Key-pair cycles": Time to generate a secret key and a public key.
- "Share cycles": Time to compute a shared secret.
- "Encrypt cycles": Time to encrypt a 59-byte message.
- "Decrypt cycles": Time to decrypt an encrypted 59-byte message.
- "Sign cycles": Time to sign a 59-byte message.
- "Verify cycles": Time to verify a signed 59-byte message.

The space table has the following columns:

- "Secret-key bytes": Space for a secret key.
- "Public-key bytes": Space for a public key.
- "Shared-secret bytes": Space for a shared secret.
- "23-byte encrypt bytes": Space for the ciphertext corresponding to a 23-byte plaintext.
- "709-byte encrypt bytes": Space for the ciphertext corresponding to a 709-byte plaintext.
- "23-byte signed bytes": Space for the signed message corresponding to a 23-byte original message.
- "709-byte signed bytes": Space for the signed message corresponding to a 709-byte original message.

Each table has one row for each public-key system.

6.2 amd64, 2000MHz, Athlon 64 X2 (15,75,2), mace

System	key-pair cycles	share cycles	encrypt cycles	decrypt cycles	sign cycles	verify cycles
claus 1	4536790	4494668				
claus++ 1	3280267	3248767				
curve25519-gaudry 1	430518	422188				
donald 1 512	342274				366921	425227
donald 1 1024	855787				842993	1011179
donald 1 2048	2563130				2387880	2854056
ecdonald 1 nist-b-163	2184846				2360083	4670345
ecdonald 1 nist-b-233	3105077				3211478	6334979
ecdonald 1 nist-b-283	6753953				6969027	13857460
ecdonald 1 nist-b-409	14699542				14947490	29771779
ecdonald 1 nist-b-571	33923885				34258091	68336725
ecdonald 1 nist-k-163	2171259				2236050	4385143
ecdonald 1 nist-k-233	2977011				3012920	6131554
ecdonald 1 nist-k-283	6204150				6363819	12662087
ecdonald 1 nist-k-409	13237383				13411110	26698994
ecdonald 1 nist-k-571	30162062				30551621	61016076
ecdonald 1 nist-p-192	1434896				1539854	1814119
ecdonald 1 nist-p-224	2357322				2398450	2926555
ecdonald 1 nist-p-256	2763692				2836660	3440260
ecdonald 1 nist-p-384	5605302				5792665	6862123
ecdonald 1 nist-p-521	7757922				7845615	9372628
ecdonald 1 secp160r1	1552724				1629175	1928938
ntru-enc 1 ees787ep1	148100367		554968	1033530		
rainbow 1	196884729				795225	1507463
ronald 1 768	85871881		93711	1874245	1879367	75354
ronald 1 832	75621929		100445	2120825	2133833	78408
ronald 1 896	108181707		102944	2392804	2372091	79574
ronald 1 960	105836194		107694	2386992	2395228	84627
ronald 1 1024	143771773		115305	2677098	2677900	90883
ronald 1 1088	199043975		132414	3340457	3312448	108495
ronald 1 1152	167403262		138287	3680933	3769182	112100
ronald 1 1216	206675082		142390	4091248	4151053	113527
ronald 1 1280	293483216		146707	4493184	4542148	117872
ronald 1 1344	370203126		153324	4970727	4963227	120487
ronald 1 1408	213491760		159196	5392730	5446640	124124
ronald 1 1472	297614221		160675	5889622	5857116	126696
ronald 1 1536	344843264		166689	6416906	6405975	129615
ronald 1 1664	608207661		178972	7591486	7552938	139506
ronald 1 1792	658848186		188004	8908427	8954020	147864
ronald 1 1920	406740490		200490	10269553	10272785	154121
ronald 1 2048	622108641		208000	11634844	11633210	160486
ronald 1 2176	950203011		254960	14102737	14172090	205888
ronald 1 2304	857717834		264673	15648737	15669777	213507

ronald 1 2432	969901895	278242	17614451	17674447	223633
ronald 1 2560	828228785	292410	19576603	19648600	235840
ronald 1 2688	2250729832	304302	21887738	21850119	246131
ronald 1 2816	2078939891	322253	24477385	24523088	256916
ronald 1 2944	2320736579	332088	27000950	26963122	267933
ronald 1 3072	2849288627	344799	29438612	29541931	278149
ronald 1 3328	1552536040	382188	36373283	36329796	308237
ronald 1 3584	2802475786	408251	43213002	43215240	330237
ronald 1 3840	4457230686	443772	50943501	51018254	357694
ronald 1 4096	5334694741	473576	59466672	59446908	384007
ronald 2 768	66280435	77520	1808187	1852294	75436
ronald 2 832	89385709	83345	2097597	2108953	76637
ronald 2 896	96239259	86804	2355383	2355324	80396
ronald 2 960	116274930	90037	2383330	2403437	81091
ronald 2 1024	138677503	99198	2664771	2665266	89537
ronald 2 1088	117223932	116423	3345138	3380108	104774
ronald 2 1152	227291460	121309	3719951	3731128	112192
ronald 2 1216	201428033	124416	4027760	4048180	110341
ronald 2 1280	194790271	128578	4431124	4447124	112851
ronald 2 1344	208712266	132625	4856912	4828446	119301
ronald 2 1408	310014535	142155	5343032	5316488	122441
ronald 2 1472	286277314	145244	5840742	5821248	126517
ronald 2 1536	240081827	151865	6361856	6341582	128926
ronald 2 1664	451764164	160730	7622277	7610532	135715
ronald 2 1792	489716080	169603	8885531	8928884	143472
ronald 2 1920	779364471	183021	10217402	10332973	151166
ronald 2 2048	630946578	191947	11824205	11867442	157697
ronald 2 2176	739969067	237962	13927345	14066208	200090
ronald 2 2304	749505102	251135	15423505	15458459	211868
ronald 2 2432	1025846418	264123	17234531	17331520	220992
ronald 2 2560	1263194565	277769	19471222	19402247	232371
ronald 2 2688	1519172917	287508	21905436	21856380	240625
ronald 2 2816	1072897753	301043	24196548	24380021	250403
ronald 2 2944	1238886834	314430	26729533	26709609	262196
ronald 2 3072	2449593322	330137	29544508	29590969	274563
ronald 2 3328	2007087428	365851	36347004	36431127	301732
ronald 2 3584	2858304142	397270	43076160	43221198	329380
ronald 2 3840	3123469291	427127	51000963	51357480	353206
ronald 2 4096	5986633472	454274	59252209	59402622	375624
ronald 3 768	86798670	77366	1874157	1872893	71032
ronald 3 832	117854081	85497	2126311	2124043	73145
ronald 3 896	137231174	86121	2378037	2374408	73523
ronald 3 960	122016349	89592	2370671	2361007	77504
ronald 3 1024	166624813	100189	2691080	2681851	86290
ronald 3 1088	177587972	116228	3379586	3376710	99973
ronald 3 1152	245540303	120271	3773203	3774808	102632
ronald 3 1216	156840651	123946	4132841	4175515	104781

ronald 3 1280	187551330		128126	4528827	4554709	108980
ronald 3 1344	188937739		132454	4899183	4892638	110825
ronald 3 1408	299018441		137969	5350542	5411340	116141
ronald 3 1472	231985545		143121	5953709	5930469	119120
ronald 3 1536	411914605		147082	6483689	6511029	122039
ronald 3 1664	295417188		160769	7733002	7715889	130339
ronald 3 1792	539487307		173227	8955057	8951368	137970
ronald 3 1920	553814313		182003	10321830	10298145	145475
ronald 3 2048	822324622		189321	11643484	11672300	151397
ronald 3 2176	689211248		238037	13909318	13977187	195775
ronald 3 2304	924407277		249619	15695393	15660767	204828
ronald 3 2432	965891779		261461	17532965	17514265	213043
ronald 3 2560	1381954964		274520	19638054	19669918	225740
ronald 3 2688	1089040030		288182	21763192	21745566	234690
ronald 3 2816	1382773945		301825	24347824	24312542	246102
ronald 3 2944	1506567189		314776	26673256	26798466	257758
ronald 3 3072	1862675298		325056	29356760	29137355	266082
ronald 3 3328	2066080194		364041	36333912	36404511	296597
ronald 3 3584	4100980140		393309	43162810	43090455	319043
ronald 3 3840	4213536672		428990	51129452	51324737	348472
ronald 3 4096	6998819826		454862	59229843	59197340	370707
sflashv2 1	773573277				1767211	427765
sflashv2 2	750057294				262973	326813
surf127eps 1	545522	544191				

System	secret key bytes	public key bytes	shared secret bytes	23-byte encrypt bytes	709-byte encrypt bytes	23-byte signed bytes	709-byte signed bytes
claus 1	256	128	128				
claus++ 1	256	128	128				
curve25519-gaudry 1	32	32	32				
donald 1 512	84	64				63	749
donald 1 1024	148	128				63	749
donald 1 2048	276	256				63	749
ecdonald 1 nist-b-163	63	42				65	751
ecdonald 1 nist-b-233	90	60				83	769
ecdonald 1 nist-b-283	108	72				95	781
ecdonald 1 nist-b-409	156	104				127	813
ecdonald 1 nist-b-571	216	144				167	853
ecdonald 1 nist-k-163	63	42				65	751
ecdonald 1 nist-k-233	90	60				83	769
ecdonald 1 nist-k-283	108	72				95	781
ecdonald 1 nist-k-409	156	104				127	813
ecdonald 1 nist-k-571	216	144				167	853
ecdonald 1 nist-p-192	72	48				71	757
ecdonald 1 nist-p-224	84	56				79	765
ecdonald 1 nist-p-256	96	64				87	773

`ecdonald 1 nist-p-384`	144	96			119	805
`ecdonald 1 nist-p-521`	198	132			155	841
`ecdonald 1 secp160r1`	60	40			63	749
`ntru-enc 1 ees787ep1`	1854	1574	1574	2282		
`rainbow 1`	20107	31680			66	752
`ronald 1 768`	768	96	119	805	119	805
`ronald 1 832`	832	104	127	813	127	813
`ronald 1 896`	896	112	135	821	135	821
`ronald 1 960`	960	120	143	829	143	829
`ronald 1 1024`	1024	128	151	837	151	837
`ronald 1 1088`	1088	136	159	845	159	845
`ronald 1 1152`	1152	144	167	853	167	853
`ronald 1 1216`	1216	152	175	861	175	861
`ronald 1 1280`	1280	160	183	869	183	869
`ronald 1 1344`	1344	168	191	877	191	877
`ronald 1 1408`	1408	176	199	885	199	885
`ronald 1 1472`	1472	184	207	893	207	893
`ronald 1 1536`	1536	192	215	901	215	901
`ronald 1 1664`	1664	208	231	917	231	917
`ronald 1 1792`	1792	224	247	933	247	933
`ronald 1 1920`	1920	240	263	949	263	949
`ronald 1 2048`	2048	256	279	965	279	965
`ronald 1 2176`	2176	272	295	981	295	981
`ronald 1 2304`	2304	288	311	997	311	997
`ronald 1 2432`	2432	304	327	1013	327	1013
`ronald 1 2560`	2560	320	343	1029	343	1029
`ronald 1 2688`	2688	336	359	1045	359	1045
`ronald 1 2816`	2816	352	375	1061	375	1061
`ronald 1 2944`	2944	368	391	1077	391	1077
`ronald 1 3072`	3072	384	407	1093	407	1093
`ronald 1 3328`	3328	416	439	1125	439	1125
`ronald 1 3584`	3584	448	471	1157	471	1157
`ronald 1 3840`	3840	480	503	1189	503	1189
`ronald 1 4096`	4096	512	535	1221	535	1221
`ronald 2 768`	768	96	96	784	119	805
`ronald 2 832`	832	104	104	784	127	813
`ronald 2 896`	896	112	112	784	135	821
`ronald 2 960`	960	120	120	784	143	829
`ronald 2 1024`	1024	128	128	784	151	837
`ronald 2 1088`	1088	136	136	784	159	845
`ronald 2 1152`	1152	144	144	784	167	853
`ronald 2 1216`	1216	152	152	784	175	861
`ronald 2 1280`	1280	160	160	784	183	869
`ronald 2 1344`	1344	168	168	784	191	877
`ronald 2 1408`	1408	176	176	784	199	885
`ronald 2 1472`	1472	184	184	784	207	893
`ronald 2 1536`	1536	192	192	784	215	901

ronald 2 1664	1664	208	208	784	231	917
ronald 2 1792	1792	224	224	784	247	933
ronald 2 1920	1920	240	240	784	263	949
ronald 2 2048	2048	256	256	784	279	965
ronald 2 2176	2176	272	272	784	295	981
ronald 2 2304	2304	288	288	784	311	997
ronald 2 2432	2432	304	304	784	327	1013
ronald 2 2560	2560	320	320	784	343	1029
ronald 2 2688	2688	336	336	784	359	1045
ronald 2 2816	2816	352	352	784	375	1061
ronald 2 2944	2944	368	368	784	391	1077
ronald 2 3072	3072	384	384	784	407	1093
ronald 2 3328	3328	416	416	784	439	1125
ronald 2 3584	3584	448	448	784	471	1157
ronald 2 3840	3840	480	480	784	503	1189
ronald 2 4096	4096	512	512	784	535	1221
ronald 3 768	768	96	96	784	96	752
ronald 3 832	832	104	104	784	104	752
ronald 3 896	896	112	112	784	112	752
ronald 3 960	960	120	120	784	120	752
ronald 3 1024	1024	128	128	784	128	752
ronald 3 1088	1088	136	136	784	136	752
ronald 3 1152	1152	144	144	784	144	752
ronald 3 1216	1216	152	152	784	152	752
ronald 3 1280	1280	160	160	784	160	752
ronald 3 1344	1344	168	168	784	168	752
ronald 3 1408	1408	176	176	784	176	752
ronald 3 1472	1472	184	184	784	184	752
ronald 3 1536	1536	192	192	784	192	752
ronald 3 1664	1664	208	208	784	208	752
ronald 3 1792	1792	224	224	784	224	752
ronald 3 1920	1920	240	240	784	240	752
ronald 3 2048	2048	256	256	784	256	752
ronald 3 2176	2176	272	272	784	272	752
ronald 3 2304	2304	288	288	784	288	752
ronald 3 2432	2432	304	304	784	304	752
ronald 3 2560	2560	320	320	784	320	752
ronald 3 2688	2688	336	336	784	336	752
ronald 3 2816	2816	352	352	784	352	752
ronald 3 2944	2944	368	368	784	368	752
ronald 3 3072	3072	384	384	784	384	752
ronald 3 3328	3328	416	416	784	416	752
ronald 3 3584	3584	448	448	784	448	752
ronald 3 3840	3840	480	480	784	480	752
ronald 3 4096	4096	512	512	784	512	752
sflashv2 1	2823	19266			60	746
sflashv2 2	2823	19266			60	746

`surf127eps 1`	32	48	48

6.3 amd64, 2137MHz, Core 2 Duo (6f6), `katana`

System	key-pair cycles	share cycles	encrypt cycles	decrypt cycles	sign cycles	verify cycles
`claus 1`	5734944	5709960				
`claus++ 1`	4555240	4509808				
`curve25519-gaudry 1`	591504	584248				
`donald 1 512`	386216				410816	473192
`donald 1 1024`	1084424				1041400	1246312
`donald 1 2048`	3419456				3207200	3864936
`ecdonald 1 nist-b-163`	2080544				2147128	4220480
`ecdonald 1 nist-b-233`	2894120				3002144	5873888
`ecdonald 1 nist-b-283`	6541240				6661744	13217376
`ecdonald 1 nist-b-409`	14471152				14635720	29147336
`ecdonald 1 nist-b-571`	32627448				32909056	65661336
`ecdonald 1 nist-k-163`	1972696				2047768	4002136
`ecdonald 1 nist-k-233`	2740192				2846312	5600816
`ecdonald 1 nist-k-283`	6015248				6129808	12107560
`ecdonald 1 nist-k-409`	12961488				13116088	26091152
`ecdonald 1 nist-k-571`	29016312				29273896	58379424
`ecdonald 1 nist-p-192`	1486648				1564616	1857656
`ecdonald 1 nist-p-224`	2225568				2287384	2736296
`ecdonald 1 nist-p-256`	2765856				2859248	3482696
`ecdonald 1 nist-p-384`	6054880				6199704	7436696
`ecdonald 1 nist-p-521`	7875424				8100856	9601632
`ecdonald 1 secp160r1`	1500328				1529088	1804488
`ntru-enc 1 ees787ep1`	86911928		467536	830784		
`rainbow 1`	142880192				647600	1238776
`ronald 1 768`	61761344		94896	1921080	1923944	81816
`ronald 1 832`	101955776		100880	2206016	2196536	84736
`ronald 1 896`	74680752		105456	2523640	2517736	88912
`ronald 1 960`	88760864		110880	2531520	2534624	92448
`ronald 1 1024`	70595016		119800	2952752	2938632	98712
`ronald 1 1088`	129284736		145104	3622432	3631200	120280
`ronald 1 1152`	151580352		144648	4129808	4149336	123528
`ronald 1 1216`	128703120		151832	4559824	4595232	127376
`ronald 1 1280`	179096528		161336	5143216	5144104	131352
`ronald 1 1344`	224044992		162256	5600608	5613800	135728
`ronald 1 1408`	280668576		166544	6292984	6267672	138696
`ronald 1 1472`	374017400		170480	6843416	6869568	144312
`ronald 1 1536`	235731712		176576	7614672	7611640	147520
`ronald 1 1664`	309548808		193288	9081648	9076384	161048
`ronald 1 1792`	633306144		204912	10806344	10807504	169920
`ronald 1 1920`	730448528		218168	12682344	12675392	180056
`ronald 1 2048`	682127808		230912	14229800	14240704	189728

ronald 1 2176	675318872	284144	17049560	16975320	240368
ronald 1 2304	1376709640	296528	19277944	19253480	253824
ronald 1 2432	1203216184	313432	21754776	21707880	266504
ronald 1 2560	1139087104	329072	24477376	24472608	280128
ronald 1 2688	2052261168	346520	27608664	27516696	292776
ronald 1 2816	1370701608	364456	30799168	30909096	308864
ronald 1 2944	1257267104	375368	34432384	34579360	324024
ronald 1 3072	2067736800	392744	37719440	37752072	336704
ronald 1 3328	2361616968	443336	47166432	47258568	376744
ronald 1 3584	4766342272	477784	56831184	56684608	409896
ronald 1 3840	6405438648	520344	67862320	67822488	446720
ronald 1 4096	6444531160	558840	79237248	79394928	480976
ronald 2 768	39800072	79712	1912312	1925464	76880
ronald 2 832	91269640	86336	2202768	2197952	80136
ronald 2 896	50518712	90880	2559704	2570688	85760
ronald 2 960	119435104	94984	2563816	2555448	87168
ronald 2 1024	120062088	103104	2959528	2947312	95520
ronald 2 1088	122504744	123960	3615664	3627832	114120
ronald 2 1152	163159736	129736	4146824	4153256	118408
ronald 2 1216	127632312	134576	4613824	4641736	123048
ronald 2 1280	121366472	138168	5151408	5153496	126752
ronald 2 1344	248601160	144984	5606984	5611680	129992
ronald 2 1408	270449976	150672	6268208	6263080	134944
ronald 2 1472	252774264	157200	6833712	6840088	138592
ronald 2 1536	494965352	160832	7579080	7619040	142376
ronald 2 1664	474630824	175264	9147432	9080816	154584
ronald 2 1792	362093192	188784	10814768	10831520	163704
ronald 2 1920	667965256	198984	12695400	12681264	173696
ronald 2 2048	759320048	214120	14369336	14393808	184216
ronald 2 2176	750929784	267184	16958760	16972488	234640
ronald 2 2304	1090571800	281368	19334904	19349592	248176
ronald 2 2432	1077571704	301912	21817608	21861896	263336
ronald 2 2560	1722661940	311704	24404904	24478928	271728
ronald 2 2688	1697033288	328856	27705384	27674024	287144
ronald 2 2816	1473256384	346872	30992952	31015272	301944
ronald 2 2944	2338495360	364864	34527672	34491480	316112
ronald 2 3072	2358067912	377504	38079168	38005792	328792
ronald 2 3328	3618237088	427216	47498728	47524128	369072
ronald 2 3584	3935567248	460488	57199824	57037760	401760
ronald 2 3840	4295014520	502720	67740072	67667832	437288
ronald 2 4096	6668515248	548168	79571488	79351824	477496
ronald 3 768	61190368	81928	1919736	1931104	71576
ronald 3 832	66222184	84872	2202544	2210392	72592
ronald 3 896	74385872	89408	2550192	2563296	78032
ronald 3 960	76803560	96248	2558304	2561952	81856
ronald 3 1024	125938800	102496	2956752	2953744	88640
ronald 3 1088	121826976	124272	3639464	3645152	109304

ronald 3 1152	147551744		128896	4154552	4169760	112200
ronald 3 1216	204184248		135448	4673824	4653112	116256
ronald 3 1280	255921864		139624	5146224	5151560	121152
ronald 3 1344	250200608		144280	5652192	5655504	123880
ronald 3 1408	203635664		151312	6283400	6271688	127704
ronald 3 1472	302127912		156960	6850776	6860624	131848
ronald 3 1536	248377400		158992	7699640	7717640	135968
ronald 3 1664	356750280		175216	9025496	9008352	148440
ronald 3 1792	647309288		188760	10789368	10838928	157056
ronald 3 1920	528007520		203488	12738544	12726176	168624
ronald 3 2048	684835224		213488	14316048	14337536	178000
ronald 3 2176	820477320		266816	17028928	17015576	228208
ronald 3 2304	1130800160		282064	19432144	19410064	241208
ronald 3 2432	1091118816		299992	21790168	21804400	255648
ronald 3 2560	1340577184		311944	24818080	24911872	266640
ronald 3 2688	1452895552		326600	27641680	27650672	279208
ronald 3 2816	1502739872		345464	30808608	30810752	294816
ronald 3 2944	1629332704		361192	34454864	34487304	309384
ronald 3 3072	1994216200		377272	38186816	38158832	323264
ronald 3 3328	3916446040		427136	47501992	47416816	363072
ronald 3 3584	3743286952		462176	57091984	57120512	394352
ronald 3 3840	6281430592		505032	68028632	67894768	433464
ronald 3 4096	5848586776		544960	79229128	79455616	467232
sflashv2 1	330734000				1008464	298864
sflashv2 2	317605168				211504	243520
surf127eps 1	658128	665112				

System	secret key bytes	public key bytes	shared secret bytes	23-byte encrypt bytes	709-byte encrypt bytes	23-byte signed bytes	709-byte signed bytes
claus 1	256	128	128				
claus++ 1	256	128	128				
curve25519-gaudry 1	32	32	32				
donald 1 512	84	64				63	749
donald 1 1024	148	128				63	749
donald 1 2048	276	256				63	749
ecdonald 1 nist-b-163	63	42				65	751
ecdonald 1 nist-b-233	90	60				83	769
ecdonald 1 nist-b-283	108	72				95	781
ecdonald 1 nist-b-409	156	104				127	813
ecdonald 1 nist-b-571	216	144				167	853
ecdonald 1 nist-k-163	63	42				65	751
ecdonald 1 nist-k-233	90	60				83	769
ecdonald 1 nist-k-283	108	72				95	781
ecdonald 1 nist-k-409	156	104				127	813
ecdonald 1 nist-k-571	216	144				167	853
ecdonald 1 nist-p-192	72	48				71	757

ecdonald 1 nist-p-224	84	56			79	765
ecdonald 1 nist-p-256	96	64			87	773
ecdonald 1 nist-p-384	144	96			119	805
ecdonald 1 nist-p-521	198	132			155	841
ecdonald 1 secp160r1	60	40			63	749
ntru-enc 1 ees787ep1	1854	1574	1574	2282		
rainbow 1	20107	31680			66	752
ronald 1 768	768	96	119	805	119	805
ronald 1 832	832	104	127	813	127	813
ronald 1 896	896	112	135	821	135	821
ronald 1 960	960	120	143	829	143	829
ronald 1 1024	1024	128	151	837	151	837
ronald 1 1088	1088	136	159	845	159	845
ronald 1 1152	1152	144	167	853	167	853
ronald 1 1216	1216	152	175	861	175	861
ronald 1 1280	1280	160	183	869	183	869
ronald 1 1344	1344	168	191	877	191	877
ronald 1 1408	1408	176	199	885	199	885
ronald 1 1472	1472	184	207	893	207	893
ronald 1 1536	1536	192	215	901	215	901
ronald 1 1664	1664	208	231	917	231	917
ronald 1 1792	1792	224	247	933	247	933
ronald 1 1920	1920	240	263	949	263	949
ronald 1 2048	2048	256	279	965	279	965
ronald 1 2176	2176	272	295	981	295	981
ronald 1 2304	2304	288	311	997	311	997
ronald 1 2432	2432	304	327	1013	327	1013
ronald 1 2560	2560	320	343	1029	343	1029
ronald 1 2688	2688	336	359	1045	359	1045
ronald 1 2816	2816	352	375	1061	375	1061
ronald 1 2944	2944	368	391	1077	391	1077
ronald 1 3072	3072	384	407	1093	407	1093
ronald 1 3328	3328	416	439	1125	439	1125
ronald 1 3584	3584	448	471	1157	471	1157
ronald 1 3840	3840	480	503	1189	503	1189
ronald 1 4096	4096	512	535	1221	535	1221
ronald 2 768	768	96	96	784	119	805
ronald 2 832	832	104	104	784	127	813
ronald 2 896	896	112	112	784	135	821
ronald 2 960	960	120	120	784	143	829
ronald 2 1024	1024	128	128	784	151	837
ronald 2 1088	1088	136	136	784	159	845
ronald 2 1152	1152	144	144	784	167	853
ronald 2 1216	1216	152	152	784	175	861
ronald 2 1280	1280	160	160	784	183	869
ronald 2 1344	1344	168	168	784	191	877
ronald 2 1408	1408	176	176	784	199	885

`ronald 2 1472`	1472	184	184	784	207	893
`ronald 2 1536`	1536	192	192	784	215	901
`ronald 2 1664`	1664	208	208	784	231	917
`ronald 2 1792`	1792	224	224	784	247	933
`ronald 2 1920`	1920	240	240	784	263	949
`ronald 2 2048`	2048	256	256	784	279	965
`ronald 2 2176`	2176	272	272	784	295	981
`ronald 2 2304`	2304	288	288	784	311	997
`ronald 2 2432`	2432	304	304	784	327	1013
`ronald 2 2560`	2560	320	320	784	343	1029
`ronald 2 2688`	2688	336	336	784	359	1045
`ronald 2 2816`	2816	352	352	784	375	1061
`ronald 2 2944`	2944	368	368	784	391	1077
`ronald 2 3072`	3072	384	384	784	407	1093
`ronald 2 3328`	3328	416	416	784	439	1125
`ronald 2 3584`	3584	448	448	784	471	1157
`ronald 2 3840`	3840	480	480	784	503	1189
`ronald 2 4096`	4096	512	512	784	535	1221
`ronald 3 768`	768	96	96	784	96	752
`ronald 3 832`	832	104	104	784	104	752
`ronald 3 896`	896	112	112	784	112	752
`ronald 3 960`	960	120	120	784	120	752
`ronald 3 1024`	1024	128	128	784	128	752
`ronald 3 1088`	1088	136	136	784	136	752
`ronald 3 1152`	1152	144	144	784	144	752
`ronald 3 1216`	1216	152	152	784	152	752
`ronald 3 1280`	1280	160	160	784	160	752
`ronald 3 1344`	1344	168	168	784	168	752
`ronald 3 1408`	1408	176	176	784	176	752
`ronald 3 1472`	1472	184	184	784	184	752
`ronald 3 1536`	1536	192	192	784	192	752
`ronald 3 1664`	1664	208	208	784	208	752
`ronald 3 1792`	1792	224	224	784	224	752
`ronald 3 1920`	1920	240	240	784	240	752
`ronald 3 2048`	2048	256	256	784	256	752
`ronald 3 2176`	2176	272	272	784	272	752
`ronald 3 2304`	2304	288	288	784	288	752
`ronald 3 2432`	2432	304	304	784	304	752
`ronald 3 2560`	2560	320	320	784	320	752
`ronald 3 2688`	2688	336	336	784	336	752
`ronald 3 2816`	2816	352	352	784	352	752
`ronald 3 2944`	2944	368	368	784	368	752
`ronald 3 3072`	3072	384	384	784	384	752
`ronald 3 3328`	3328	416	416	784	416	752
`ronald 3 3584`	3584	448	448	784	448	752
`ronald 3 3840`	3840	480	480	784	480	752
`ronald 3 4096`	4096	512	512	784	512	752

sflashv2 1	2823	19266			60	746
sflashv2 2	2823	19266			60	746
surf127eps 1	32	48	48			

6.4 amd64, 2192MHz, Opteron 250 (f58), td189

System	key-pair cycles	share cycles	encrypt cycles	decrypt cycles	sign cycles	verify cycles
claus 1	4477752	4451520				
claus++ 1	3286230	3274256				
curve25519-gaudry 1	434517	430231				
donald 1 512	341007				374712	428106
donald 1 1024	851413				847562	1003503
donald 1 2048	2563583				2430888	2932983
ecdonald 1 nist-b-163	2047483				2121635	4158327
ecdonald 1 nist-b-233	2911523				2996588	5902398
ecdonald 1 nist-b-283	6313803				6416068	12709509
ecdonald 1 nist-b-409	13942359				13972021	27778227
ecdonald 1 nist-b-571	30442784				30271977	60384407
ecdonald 1 nist-k-163	1960996				2040497	3967165
ecdonald 1 nist-k-233	2772120				2856002	5639743
ecdonald 1 nist-k-283	5782004				5904551	11712061
ecdonald 1 nist-k-409	12500259				12550463	24995882
ecdonald 1 nist-k-571	27076680				26945832	53764410
ecdonald 1 nist-p-192	1493917				1597986	1980779
ecdonald 1 nist-p-224	2472335				2580811	3130773
ecdonald 1 nist-p-256	2760603				2875333	3525899
ecdonald 1 nist-p-384	5624414				5956898	7057335
ecdonald 1 nist-p-521	7510331				7716257	9178334
ecdonald 1 secp160r1	1563109				1753329	2000689
ntru-enc 1 ees787ep1	150991063		596594	1137559		
rainbow 1	171980971				817293	1720107
ronald 1 768	104622561		96825	1842911	1854331	77763
ronald 1 832	75923112		101387	2060117	2083325	80480
ronald 1 896	128417674		105883	2380484	2359728	83386
ronald 1 960	106032960		110706	2288979	2280590	87070
ronald 1 1024	118546757		119253	2634465	2670124	93456
ronald 1 1088	132078405		136760	3243462	3300099	110146
ronald 1 1152	181194157		145492	3618404	3594065	113419
ronald 1 1216	159190921		146369	3991859	3997752	115709
ronald 1 1280	216752334		150331	4392563	4365006	119682
ronald 1 1344	168424946		155649	4883877	4838418	122150
ronald 1 1408	467036725		162177	5365335	5442408	126632
ronald 1 1472	397058060		165247	5802915	5826619	129377
ronald 1 1536	430918498		173761	6435628	6417613	133230
ronald 1 1664	779989029		181928	7444574	7449359	142395
ronald 1 1792	564279408		193792	8858442	8790007	150701

ronald 1 1920	443120081	203878	10163772	10266894	156740
ronald 1 2048	955367095	216707	11491952	11375134	165066
ronald 1 2176	864932524	260067	14056031	14025924	208392
ronald 1 2304	1085355928	272915	15649883	15899881	220276
ronald 1 2432	1093461152	288827	17504686	17487977	229564
ronald 1 2560	1727128536	301743	20033899	20098202	239163
ronald 1 2688	2507982691	312229	21986990	22166233	248499
ronald 1 2816	1024414219	333040	24744880	24411781	260475
ronald 1 2944	1859321212	342106	27207394	27243669	270786
ronald 1 3072	2803901710	352285	30149115	30206640	283282
ronald 1 3328	2272960503	388093	36666829	36356797	310963
ronald 1 3584	2233798324	414821	43651839	43528531	335220
ronald 1 3840	3544288563	452959	51008832	51663315	362867
ronald 1 4096	7414367106	481556	59490859	59472437	387732
ronald 2 768	78154090	80111	1772427	1785380	73715
ronald 2 832	99894448	83307	2046671	2025725	75842
ronald 2 896	73425185	87566	2316568	2346095	80168
ronald 2 960	108942749	90829	2260343	2302525	81519
ronald 2 1024	163512811	102167	2664312	2648355	90432
ronald 2 1088	118440247	120526	3271416	3272634	107949
ronald 2 1152	135821992	126584	3624878	3631094	110748
ronald 2 1216	126287167	129553	3995573	4082164	113408
ronald 2 1280	169477401	131903	4328509	4381492	116583
ronald 2 1344	206946767	136837	4777035	4788714	118666
ronald 2 1408	244012965	142722	5247593	5295418	121466
ronald 2 1472	272240041	150152	5790723	5786109	125436
ronald 2 1536	422856302	154370	6378430	6373351	128839
ronald 2 1664	365549775	167445	7551762	7596849	137300
ronald 2 1792	824027277	175461	8886101	8960528	146134
ronald 2 1920	616568124	184681	10211677	10243760	152622
ronald 2 2048	1041860656	198272	11547295	11478722	160524
ronald 2 2176	848378632	242369	14107394	14065786	203227
ronald 2 2304	1161910201	260235	15922832	15968218	216435
ronald 2 2432	1184673954	272809	17737336	17550651	225371
ronald 2 2560	899972680	282991	19828718	20108316	233981
ronald 2 2688	1609117872	295489	22024735	22045092	243531
ronald 2 2816	1854362583	310075	24364542	24752638	256561
ronald 2 2944	1342105010	321882	26916901	27256973	264341
ronald 2 3072	1660947261	340272	30295044	30001589	275597
ronald 2 3328	2323827209	373430	36872704	36827100	306426
ronald 2 3584	2435345403	402775	43816977	44237512	330176
ronald 2 3840	3875908437	438019	51532645	51710435	355247
ronald 2 4096	5039131054	464575	59217722	59183768	377502
ronald 3 768	62231775	78999	1784091	1781542	69448
ronald 3 832	93974618	83556	2060459	2068824	71704
ronald 3 896	91397993	87073	2367286	2386112	75530
ronald 3 960	140424170	91963	2326566	2342277	77509

ronald 3 1024	98764756		101453	2610375	2648109	85833
ronald 3 1088	193907734		119295	3290217	3249975	101572
ronald 3 1152	120345552		124572	3648394	3636734	103576
ronald 3 1216	206123880		127930	3993510	4008570	108590
ronald 3 1280	172196661		131309	4391284	4410012	109910
ronald 3 1344	289820602		137039	4861322	4903605	114327
ronald 3 1408	248314422		145535	5415802	5448841	117013
ronald 3 1472	250250010		146931	5837135	5889416	119292
ronald 3 1536	370235693		150652	6360870	6315967	123084
ronald 3 1664	417043056		167845	7609172	7597398	133655
ronald 3 1792	390013039		173921	8846965	8750514	138980
ronald 3 1920	798230135		185467	10409883	10427929	147512
ronald 3 2048	808835466		194527	11405458	11524054	155225
ronald 3 2176	1173298420		242283	14257000	14342792	198961
ronald 3 2304	761013420		258222	15896660	16063434	209244
ronald 3 2432	1337956706		270824	17417741	17600256	217696
ronald 3 2560	1266178539		281615	19738829	19784388	227062
ronald 3 2688	1154873561		295899	22200622	22189433	237251
ronald 3 2816	1763606626		310423	24746109	24506374	248414
ronald 3 2944	1675987424		320246	27263633	27203622	258745
ronald 3 3072	1450408236		333130	29885392	29813440	268826
ronald 3 3328	2956113204		369143	36360279	36468717	297233
ronald 3 3584	3873074225		398196	43676856	44066911	321440
ronald 3 3840	2891982673		436000	51482831	51363946	350054
ronald 3 4096	5218931083		467407	59431725	59047231	376256
sflashv2 1	797937873				3161529	1292344
sflashv2 2	761421748				287759	367632
surf127eps 1	523316	522910				

System	secret key bytes	public key bytes	shared secret bytes	23-byte encrypt bytes	709-byte encrypt bytes	23-byte signed bytes	709-byte signed bytes
claus 1	256	128	128				
claus++ 1	256	128	128				
curve25519-gaudry 1	32	32	32				
donald 1 512	84	64				63	749
donald 1 1024	148	128				63	749
donald 1 2048	276	256				63	749
ecdonald 1 nist-b-163	63	42				65	751
ecdonald 1 nist-b-233	90	60				83	769
ecdonald 1 nist-b-283	108	72				95	781
ecdonald 1 nist-b-409	156	104				127	813
ecdonald 1 nist-b-571	216	144				167	853
ecdonald 1 nist-k-163	63	42				65	751
ecdonald 1 nist-k-233	90	60				83	769
ecdonald 1 nist-k-283	108	72				95	781
ecdonald 1 nist-k-409	156	104				127	813

`ecdonald 1 nist-k-571`	216	144			167	853
`ecdonald 1 nist-p-192`	72	48			71	757
`ecdonald 1 nist-p-224`	84	56			79	765
`ecdonald 1 nist-p-256`	96	64			87	773
`ecdonald 1 nist-p-384`	144	96			119	805
`ecdonald 1 nist-p-521`	198	132			155	841
`ecdonald 1 secp160r1`	60	40			63	749
`ntru-enc 1 ees787ep1`	1854	1574	1574	2282		
`rainbow 1`	20107	31680			66	752
`ronald 1 768`	768	96	119	805	119	805
`ronald 1 832`	832	104	127	813	127	813
`ronald 1 896`	896	112	135	821	135	821
`ronald 1 960`	960	120	143	829	143	829
`ronald 1 1024`	1024	128	151	837	151	837
`ronald 1 1088`	1088	136	159	845	159	845
`ronald 1 1152`	1152	144	167	853	167	853
`ronald 1 1216`	1216	152	175	861	175	861
`ronald 1 1280`	1280	160	183	869	183	869
`ronald 1 1344`	1344	168	191	877	191	877
`ronald 1 1408`	1408	176	199	885	199	885
`ronald 1 1472`	1472	184	207	893	207	893
`ronald 1 1536`	1536	192	215	901	215	901
`ronald 1 1664`	1664	208	231	917	231	917
`ronald 1 1792`	1792	224	247	933	247	933
`ronald 1 1920`	1920	240	263	949	263	949
`ronald 1 2048`	2048	256	279	965	279	965
`ronald 1 2176`	2176	272	295	981	295	981
`ronald 1 2304`	2304	288	311	997	311	997
`ronald 1 2432`	2432	304	327	1013	327	1013
`ronald 1 2560`	2560	320	343	1029	343	1029
`ronald 1 2688`	2688	336	359	1045	359	1045
`ronald 1 2816`	2816	352	375	1061	375	1061
`ronald 1 2944`	2944	368	391	1077	391	1077
`ronald 1 3072`	3072	384	407	1093	407	1093
`ronald 1 3328`	3328	416	439	1125	439	1125
`ronald 1 3584`	3584	448	471	1157	471	1157
`ronald 1 3840`	3840	480	503	1189	503	1189
`ronald 1 4096`	4096	512	535	1221	535	1221
`ronald 2 768`	768	96	96	784	119	805
`ronald 2 832`	832	104	104	784	127	813
`ronald 2 896`	896	112	112	784	135	821
`ronald 2 960`	960	120	120	784	143	829
`ronald 2 1024`	1024	128	128	784	151	837
`ronald 2 1088`	1088	136	136	784	159	845
`ronald 2 1152`	1152	144	144	784	167	853
`ronald 2 1216`	1216	152	152	784	175	861
`ronald 2 1280`	1280	160	160	784	183	869

ronald 2 1344	1344	168	168	784	191	877
ronald 2 1408	1408	176	176	784	199	885
ronald 2 1472	1472	184	184	784	207	893
ronald 2 1536	1536	192	192	784	215	901
ronald 2 1664	1664	208	208	784	231	917
ronald 2 1792	1792	224	224	784	247	933
ronald 2 1920	1920	240	240	784	263	949
ronald 2 2048	2048	256	256	784	279	965
ronald 2 2176	2176	272	272	784	295	981
ronald 2 2304	2304	288	288	784	311	997
ronald 2 2432	2432	304	304	784	327	1013
ronald 2 2560	2560	320	320	784	343	1029
ronald 2 2688	2688	336	336	784	359	1045
ronald 2 2816	2816	352	352	784	375	1061
ronald 2 2944	2944	368	368	784	391	1077
ronald 2 3072	3072	384	384	784	407	1093
ronald 2 3328	3328	416	416	784	439	1125
ronald 2 3584	3584	448	448	784	471	1157
ronald 2 3840	3840	480	480	784	503	1189
ronald 2 4096	4096	512	512	784	535	1221
ronald 3 768	768	96	96	784	96	752
ronald 3 832	832	104	104	784	104	752
ronald 3 896	896	112	112	784	112	752
ronald 3 960	960	120	120	784	120	752
ronald 3 1024	1024	128	128	784	128	752
ronald 3 1088	1088	136	136	784	136	752
ronald 3 1152	1152	144	144	784	144	752
ronald 3 1216	1216	152	152	784	152	752
ronald 3 1280	1280	160	160	784	160	752
ronald 3 1344	1344	168	168	784	168	752
ronald 3 1408	1408	176	176	784	176	752
ronald 3 1472	1472	184	184	784	184	752
ronald 3 1536	1536	192	192	784	192	752
ronald 3 1664	1664	208	208	784	208	752
ronald 3 1792	1792	224	224	784	224	752
ronald 3 1920	1920	240	240	784	240	752
ronald 3 2048	2048	256	256	784	256	752
ronald 3 2176	2176	272	272	784	272	752
ronald 3 2304	2304	288	288	784	288	752
ronald 3 2432	2432	304	304	784	304	752
ronald 3 2560	2560	320	320	784	320	752
ronald 3 2688	2688	336	336	784	336	752
ronald 3 2816	2816	352	352	784	352	752
ronald 3 2944	2944	368	368	784	368	752
ronald 3 3072	3072	384	384	784	384	752
ronald 3 3328	3328	416	416	784	416	752
ronald 3 3584	3584	448	448	784	448	752

`ronald 3 3840`	3840	480		480	784	480	752
`ronald 3 4096`	4096	512		512	784	512	752
`sflashv2 1`	2823	19266				60	746
`sflashv2 2`	2823	19266				60	746
`surf127eps 1`	32	48	48				

6.5 amd64, 2390MHz, Opteron 250 (f5a), `td159`

System	key-pair cycles	share cycles	encrypt cycles	decrypt cycles	sign cycles	verify cycles
`claus 1`	4497244	4507934				
`claus++ 1`	3299264	3277480				
`curve25519-gaudry 1`	420844	417783				
`donald 1 512`	361085				388816	434307
`donald 1 1024`	878733				856769	1018285
`donald 1 2048`	2634591				2516500	3032627
`ecdonald 1 nist-b-163`	2303300				2370917	4660172
`ecdonald 1 nist-b-233`	3179738				3280640	6429724
`ecdonald 1 nist-b-283`	7194175				7262904	14350126
`ecdonald 1 nist-b-409`	15642046				15787731	31179223
`ecdonald 1 nist-b-571`	34107008				34371598	68575414
`ecdonald 1 nist-k-163`	2146772				2208698	4327385
`ecdonald 1 nist-k-233`	3049787				3279301	6452517
`ecdonald 1 nist-k-283`	6555617				6648967	13253576
`ecdonald 1 nist-k-409`	14035938				14154276	28153910
`ecdonald 1 nist-k-571`	30288127				30530064	60909163
`ecdonald 1 nist-p-192`	1529169				1704705	2054779
`ecdonald 1 nist-p-224`	2460736				2580370	3133570
`ecdonald 1 nist-p-256`	2867326				3151657	3746802
`ecdonald 1 nist-p-384`	6059073				6262417	7464243
`ecdonald 1 nist-p-521`	7338249				7704571	9112291
`ecdonald 1 secp160r1`	1579753				1730198	2060645
`ntru-enc 1 ees787ep1`	147907491		593972	1115172		
`ronald 1 768`	71960526		96480	1820983	1872569	78244
`ronald 1 832`	86108204		98025	2113985	2121603	79957
`ronald 1 896`	83070259		104618	2290455	2305393	83285
`ronald 1 960`	110474530		115262	2384027	2338470	89746
`ronald 1 1024`	149893397		114303	2635224	2666444	94063
`ronald 1 1088`	145298308		134874	3312570	3305691	110958
`ronald 1 1152`	209942681		137924	3679733	3686379	115375
`ronald 1 1216`	146410677		144430	4009328	3937116	113550
`ronald 1 1280`	331240756		148941	4481640	4496981	121469
`ronald 1 1344`	251215960		146609	4717149	4770924	120335
`ronald 1 1408`	340186818		153276	5402214	5378408	127467
`ronald 1 1472`	367912889		160726	5785986	5729113	125470
`ronald 1 1536`	210320457		165765	6362056	6380621	133295
`ronald 1 1664`	342948605		178231	7529379	7478537	143224

ronald 1 1792	348647404	188150	8792763	8773065	150532
ronald 1 1920	584272831	198748	10253301	10198079	154059
ronald 1 2048	709829745	208509	11448071	11489913	166910
ronald 1 2176	1053701025	253957	14278544	14166726	209863
ronald 1 2304	767159757	265652	15601475	15727381	218245
ronald 1 2432	1600347476	279107	17616510	17655621	227285
ronald 1 2560	1633108874	295092	19596263	19602311	239973
ronald 1 2688	1741287644	309765	21875527	21952680	243625
ronald 1 2816	1254366662	310546	24211338	24261933	260644
ronald 1 2944	1829294764	331355	27073155	26958458	270531
ronald 1 3072	1079534993	348758	31056889	29715850	287603
ronald 1 3328	2501240543	378457	36306605	36310452	312255
ronald 1 3584	2463181383	402637	43350991	43500311	337304
ronald 1 3840	3951338479	444943	51126511	51133842	365254
ronald 1 4096	5194555985	470463	60432290	60367867	387136
ronald 2 768	71709193	80559	1907257	1800168	74854
ronald 2 832	71148320	84533	2163142	2034335	78577
ronald 2 896	75725662	88321	2372812	2381664	82701
ronald 2 960	124490334	91520	2286169	2289188	84566
ronald 2 1024	115089127	99854	2608129	2653329	92014
ronald 2 1088	191266843	119422	3526437	3562671	109689
ronald 2 1152	226771498	123942	3632356	3642638	113227
ronald 2 1216	232064361	126914	3941048	3961177	115273
ronald 2 1280	137941312	131359	4361047	4373276	116361
ronald 2 1344	244824118	133805	4753770	4750822	118202
ronald 2 1408	237181858	139495	5240022	5317981	124970
ronald 2 1472	227946516	146342	5890454	5880214	129031
ronald 2 1536	426066831	151312	6322085	6293791	129264
ronald 2 1664	513425886	162278	7421965	7385630	138910
ronald 2 1792	521674058	170861	9216673	9236912	146375
ronald 2 1920	672485136	182709	10445432	10462789	158623
ronald 2 2048	484432651	196642	12127283	11470872	165846
ronald 2 2176	940616801	231072	14552189	14465180	206343
ronald 2 2304	863494221	250366	15689142	15818730	215948
ronald 2 2432	1168332089	260222	18393033	18406067	224177
ronald 2 2560	1681684369	278299	19812222	19653610	237986
ronald 2 2688	1298028685	292159	21939478	21984196	242708
ronald 2 2816	1041354721	302802	24643391	24679616	258269
ronald 2 2944	1786267786	316226	27304481	27299665	268502
ronald 2 3072	1516513591	331543	29546144	29661290	278021
ronald 2 3328	2692816276	365188	36506417	36689907	308575
ronald 2 3584	2633450525	393241	43493568	43597872	331921
ronald 2 3840	3642382081	423495	53395811	53210324	360991
ronald 2 4096	5266692356	456836	63445882	60545897	382333
ronald 3 768	85104252	80002	1824544	1825077	68768
ronald 3 832	88666184	88203	2186977	2037611	73248
ronald 3 896	163277433	88001	2311872	2295025	75095

ronald 3 960	145033096		92099	2283646	2318334	79324
ronald 3 1024	161705200		99982	2696812	2660199	85223
ronald 3 1088	129703810		119534	3350032	3361679	103811
ronald 3 1152	137303897		124004	3665618	3680846	106204
ronald 3 1216	274172599		128263	4059703	4047120	108471
ronald 3 1280	166408205		129726	4391198	4410932	109537
ronald 3 1344	358696088		135941	4876685	4878256	114853
ronald 3 1408	259810134		146638	5378831	5354173	118328
ronald 3 1472	260656163		146924	5747255	5755295	122149
ronald 3 1536	343481911		149234	6315013	6265178	122988
ronald 3 1664	305522575		160932	7428464	7428805	133029
ronald 3 1792	604749381		172998	8705245	8726223	140785
ronald 3 1920	778854734		183861	10085814	10091098	148928
ronald 3 2048	363574839		199186	11501430	11579627	156275
ronald 3 2176	741193084		240644	15074163	15010650	204327
ronald 3 2304	1177000314		257199	16802340	16813799	215338
ronald 3 2432	1098364285		266219	17470954	17511849	218107
ronald 3 2560	1034736727		277149	19520648	19554354	230537
ronald 3 2688	1209923819		296162	21725394	22231279	241990
ronald 3 2816	1875856221		304979	24405987	24444775	250789
ronald 3 2944	2122662092		317996	27029646	27185078	260668
ronald 3 3072	2575953199		332712	29575866	29587804	272197
ronald 3 3328	2174101647		363505	36396652	36400596	300810
ronald 3 3584	2473092073		393459	43480139	43499089	321163
ronald 3 3840	4240623540		426677	51401640	51446660	352369
ronald 3 4096	5621596564		459081	61583060	61820773	372239
sflashv2 1	1044188365				2800776	1065647
sflashv2 2	970389590				287768	365760
surf127eps 1	535269	535757				

System	secret key bytes	public key bytes	shared secret bytes	23-byte encrypt bytes	709-byte encrypt bytes	23-byte signed bytes	709-byte signed bytes
claus 1	256	128	128				
claus++ 1	256	128	128				
curve25519-gaudry 1	32	32	32				
donald 1 512	84	64				63	749
donald 1 1024	148	128				63	749
donald 1 2048	276	256				63	749
ecdonald 1 nist-b-163	63	42				65	751
ecdonald 1 nist-b-233	90	60				83	769
ecdonald 1 nist-b-283	108	72				95	781
ecdonald 1 nist-b-409	156	104				127	813
ecdonald 1 nist-b-571	216	144				167	853
ecdonald 1 nist-k-163	63	42				65	751
ecdonald 1 nist-k-233	90	60				83	769
ecdonald 1 nist-k-283	108	72				95	781

ecdonald 1 nist-k-409	156	104			127	813
ecdonald 1 nist-k-571	216	144			167	853
ecdonald 1 nist-p-192	72	48			71	757
ecdonald 1 nist-p-224	84	56			79	765
ecdonald 1 nist-p-256	96	64			87	773
ecdonald 1 nist-p-384	144	96			119	805
ecdonald 1 nist-p-521	198	132			155	841
ecdonald 1 secp160r1	60	40			63	749
ntru-enc 1 ees787ep1	1854	1574	1574	2282		
ronald 1 768	768	96	119	805	119	805
ronald 1 832	832	104	127	813	127	813
ronald 1 896	896	112	135	821	135	821
ronald 1 960	960	120	143	829	143	829
ronald 1 1024	1024	128	151	837	151	837
ronald 1 1088	1088	136	159	845	159	845
ronald 1 1152	1152	144	167	853	167	853
ronald 1 1216	1216	152	175	861	175	861
ronald 1 1280	1280	160	183	869	183	869
ronald 1 1344	1344	168	191	877	191	877
ronald 1 1408	1408	176	199	885	199	885
ronald 1 1472	1472	184	207	893	207	893
ronald 1 1536	1536	192	215	901	215	901
ronald 1 1664	1664	208	231	917	231	917
ronald 1 1792	1792	224	247	933	247	933
ronald 1 1920	1920	240	263	949	263	949
ronald 1 2048	2048	256	279	965	279	965
ronald 1 2176	2176	272	295	981	295	981
ronald 1 2304	2304	288	311	997	311	997
ronald 1 2432	2432	304	327	1013	327	1013
ronald 1 2560	2560	320	343	1029	343	1029
ronald 1 2688	2688	336	359	1045	359	1045
ronald 1 2816	2816	352	375	1061	375	1061
ronald 1 2944	2944	368	391	1077	391	1077
ronald 1 3072	3072	384	407	1093	407	1093
ronald 1 3328	3328	416	439	1125	439	1125
ronald 1 3584	3584	448	471	1157	471	1157
ronald 1 3840	3840	480	503	1189	503	1189
ronald 1 4096	4096	512	535	1221	535	1221
ronald 2 768	768	96	96	784	119	805
ronald 2 832	832	104	104	784	127	813
ronald 2 896	896	112	112	784	135	821
ronald 2 960	960	120	120	784	143	829
ronald 2 1024	1024	128	128	784	151	837
ronald 2 1088	1088	136	136	784	159	845
ronald 2 1152	1152	144	144	784	167	853
ronald 2 1216	1216	152	152	784	175	861
ronald 2 1280	1280	160	160	784	183	869

`ronald 2 1344`	1344	168	168	784	191	877
`ronald 2 1408`	1408	176	176	784	199	885
`ronald 2 1472`	1472	184	184	784	207	893
`ronald 2 1536`	1536	192	192	784	215	901
`ronald 2 1664`	1664	208	208	784	231	917
`ronald 2 1792`	1792	224	224	784	247	933
`ronald 2 1920`	1920	240	240	784	263	949
`ronald 2 2048`	2048	256	256	784	279	965
`ronald 2 2176`	2176	272	272	784	295	981
`ronald 2 2304`	2304	288	288	784	311	997
`ronald 2 2432`	2432	304	304	784	327	1013
`ronald 2 2560`	2560	320	320	784	343	1029
`ronald 2 2688`	2688	336	336	784	359	1045
`ronald 2 2816`	2816	352	352	784	375	1061
`ronald 2 2944`	2944	368	368	784	391	1077
`ronald 2 3072`	3072	384	384	784	407	1093
`ronald 2 3328`	3328	416	416	784	439	1125
`ronald 2 3584`	3584	448	448	784	471	1157
`ronald 2 3840`	3840	480	480	784	503	1189
`ronald 2 4096`	4096	512	512	784	535	1221
`ronald 3 768`	768	96	96	784	96	752
`ronald 3 832`	832	104	104	784	104	752
`ronald 3 896`	896	112	112	784	112	752
`ronald 3 960`	960	120	120	784	120	752
`ronald 3 1024`	1024	128	128	784	128	752
`ronald 3 1088`	1088	136	136	784	136	752
`ronald 3 1152`	1152	144	144	784	144	752
`ronald 3 1216`	1216	152	152	784	152	752
`ronald 3 1280`	1280	160	160	784	160	752
`ronald 3 1344`	1344	168	168	784	168	752
`ronald 3 1408`	1408	176	176	784	176	752
`ronald 3 1472`	1472	184	184	784	184	752
`ronald 3 1536`	1536	192	192	784	192	752
`ronald 3 1664`	1664	208	208	784	208	752
`ronald 3 1792`	1792	224	224	784	224	752
`ronald 3 1920`	1920	240	240	784	240	752
`ronald 3 2048`	2048	256	256	784	256	752
`ronald 3 2176`	2176	272	272	784	272	752
`ronald 3 2304`	2304	288	288	784	288	752
`ronald 3 2432`	2432	304	304	784	304	752
`ronald 3 2560`	2560	320	320	784	320	752
`ronald 3 2688`	2688	336	336	784	336	752
`ronald 3 2816`	2816	352	352	784	352	752
`ronald 3 2944`	2944	368	368	784	368	752
`ronald 3 3072`	3072	384	384	784	384	752
`ronald 3 3328`	3328	416	416	784	416	752
`ronald 3 3584`	3584	448	448	784	448	752

ronald 3 3840	3840	480		480	784	480	752
ronald 3 4096	4096	512		512	784	512	752
sflashv2 1	2823	19266				60	746
sflashv2 2	2823	19266				60	746
surf127eps 1	32	48	48				

6.6 amd64, 3000MHz, Pentium 4 (f43), pclin153

System	key-pair cycles	share cycles	encrypt cycles	decrypt cycles	sign cycles	verify cycles
claus 1	12488333	12304725				
claus++ 1	11941515	11925165				
curve25519-gaudry 1	1134555	1108672				
donald 1 512	810293				852060	987390
donald 1 1024	2270843				2176845	2562877
donald 1 2048	7362105				6861675	8290658
ecdonald 1 nist-b-163	3779483				3915967	7691227
ecdonald 1 nist-b-233	5321355				5458402	10785240
ecdonald 1 nist-b-283	11628855				11860485	23632612
ecdonald 1 nist-b-409	25197548				25395233	50524755
ecdonald 1 nist-b-571	54297893				55076595	109855185
ecdonald 1 nist-k-163	3560925				3685335	7209195
ecdonald 1 nist-k-233	5004112				5182170	10112475
ecdonald 1 nist-k-283	10705590				10934228	21707543
ecdonald 1 nist-k-409	22708598				22823647	45315975
ecdonald 1 nist-k-571	48595500				49171290	98285055
ecdonald 1 nist-p-192	2686890				2843992	3350850
ecdonald 1 nist-p-224	4451078				4448933	5382960
ecdonald 1 nist-p-256	5511202				5655712	6697223
ecdonald 1 nist-p-384	12213322				12384322	14875522
ecdonald 1 nist-p-521	15967207				16318628	19580257
ecdonald 1 secp160r1	2805990				2942408	3511928
ntru-enc 1 ees787ep1	203983313		894427	1617090		
rainbow 1	311852347				1233427	2237692
ronald 1 768	130187543		178395	3816803	3786225	152760
ronald 1 832	187135515		190208	4432867	4419270	161175
ronald 1 896	153617273		203887	5015948	4985213	168510
ronald 1 960	140006948		209842	5431830	5437155	172883
ronald 1 1024	188582730		225593	6240622	6250567	187335
ronald 1 1088	236368238		266947	7536848	7524352	222383
ronald 1 1152	243538455		268177	8361232	8348197	232178
ronald 1 1216	359158478		277657	9599753	9539722	235635
ronald 1 1280	426903337		289463	10543365	10686780	241103
ronald 1 1344	644414468		298507	11864760	11874030	252292
ronald 1 1408	534806610		314925	12948450	13082310	260175
ronald 1 1472	509000753		318352	14329762	14355210	268815
ronald 1 1536	511151948		328920	15599062	16757595	273690

ronald 1 1664	736256220	355283	18625620	18710647	303555
ronald 1 1792	1209457455	380160	22257285	22152817	318750
ronald 1 1920	1012889602	406342	26103368	26194957	337155
ronald 1 2048	1147314285	431452	30819975	30853230	360698
ronald 1 2176	1813237155	534533	35365710	35266103	452340
ronald 1 2304	2463126030	552893	39928042	39986213	471870
ronald 1 2432	2563949400	585727	45174517	45374588	500265
ronald 1 2560	3794173432	615930	50845995	50608298	521985
ronald 1 2688	2871943462	648210	56855663	56920628	552953
ronald 1 2816	3119872995	675727	63669983	63788873	581700
ronald 1 2944	7868391375	722828	70907085	71085322	612585
ronald 1 3072	5802235170	739538	88387140	77609857	640065
ronald 1 3328	5960058030	853193	111009300	97625910	737633
ronald 1 3584	8372373660	952485	115975560	115756253	831202
ronald 1 3840	6523832910	1048440	138296070	137885310	921773
ronald 1 4096	16434259635	1151903	172602818	173019038	1011173
ronald 2 768	97686788	150007	3845250	3820058	144660
ronald 2 832	118859737	162675	4384170	4390627	150517
ronald 2 896	124574212	170768	5072340	5042010	160665
ronald 2 960	253095180	180735	5435685	5483775	165360
ronald 2 1024	190663380	195172	6155468	6130822	176910
ronald 2 1088	251825025	236123	7489042	7438627	211680
ronald 2 1152	290672228	253485	8372962	8544510	220785
ronald 2 1216	369889388	250372	9547260	9551108	226200
ronald 2 1280	255894203	260715	10470300	10421760	231998
ronald 2 1344	306704287	274522	11670862	11638260	240255
ronald 2 1408	501973808	283117	12835192	12796980	250117
ronald 2 1472	484720943	292830	14253742	14185635	256823
ronald 2 1536	430233975	302835	15443332	15451725	269385
ronald 2 1664	578834580	329977	18494970	18592193	290640
ronald 2 1792	610409152	353280	22077090	21972683	306600
ronald 2 1920	824070337	379455	26032680	25835445	328320
ronald 2 2048	1179499485	403327	30703080	30631395	348570
ronald 2 2176	1740476265	498533	35241600	35202885	439680
ronald 2 2304	2521358730	525173	39843060	39951300	464393
ronald 2 2432	2333183040	555638	45150293	45281925	488625
ronald 2 2560	2170966380	583890	50603108	50511112	512512
ronald 2 2688	3514993793	617760	56767530	56654692	546458
ronald 2 2816	4239614505	644333	63002385	62990160	568860
ronald 2 2944	3581607165	685935	70492005	70684448	600232
ronald 2 3072	4349174415	719468	77673158	77599912	629235
ronald 2 3328	8110575540	830048	96806130	96378885	723158
ronald 2 3584	6243121853	922387	115592700	115397535	817853
ronald 2 3840	12469420935	1024492	138136823	137682878	909420
ronald 2 4096	12262817152	1122435	173272590	172689323	995513
ronald 3 768	117131430	151703	3911370	3882158	131002
ronald 3 832	101923027	161010	4477612	4479982	136942

ronald 3 896	134744340		166252	5068590	5023725	143242
ronald 3 960	104737635		177720	5439922	5435467	151260
ronald 3 1024	179895953		194813	6135630	6155475	162990
ronald 3 1088	285633157		232425	7537283	7584990	198270
ronald 3 1152	252609787		245558	8649727	8602477	207833
ronald 3 1216	380328818		253515	9612997	9562582	213930
ronald 3 1280	409429162		259942	10603462	10543268	222202
ronald 3 1344	432782692		265897	11761245	11746672	228150
ronald 3 1408	275947627		275280	12892283	12955530	237472
ronald 3 1472	513360705		290955	14248823	14250495	244215
ronald 3 1536	753411442		297870	15455055	15550208	255622
ronald 3 1664	627752145		327683	18686760	18752812	276705
ronald 3 1792	875406653		351285	22135305	22267875	295028
ronald 3 1920	996241822		370890	26147880	26111948	313425
ronald 3 2048	1320049762		400560	30550740	30683107	332565
ronald 3 2176	2172633570		511305	37807320	37732733	441637
ronald 3 2304	2021843970		522705	39751050	39906832	453353
ronald 3 2432	2674049715		551047	47785245	47747738	476670
ronald 3 2560	2115841897		581978	52204447	52099425	501855
ronald 3 2688	3134399085		632445	59733247	59584868	544050
ronald 3 2816	3290446395		645915	63376485	63148387	557363
ronald 3 2944	4062394395		679928	70937647	71020605	588337
ronald 3 3072	5060955780		710093	77474152	77406735	615495
ronald 3 3328	6303433965		830287	97073693	96667237	722070
ronald 3 3584	6796688490		922770	115742647	115549950	809183
ronald 3 3840	15255355365		1027020	138552210	138521752	898755
ronald 3 4096	10897082415		1116570	172408418	172254188	983753
sflashv2 1	546840968				4212345	2021978
sflashv2 2	611867145				349867	349388
surf127eps 1	1152922	1157122				

System	secret key bytes	public key bytes	shared secret bytes	23-byte encrypt bytes	709-byte encrypt bytes	23-byte signed bytes	709-byte signed bytes
claus 1	256	128	128				
claus++ 1	256	128	128				
curve25519-gaudry 1	32	32	32				
donald 1 512	84	64				63	749
donald 1 1024	148	128				63	749
donald 1 2048	276	256				63	749
ecdonald 1 nist-b-163	63	42				65	751
ecdonald 1 nist-b-233	90	60				83	769
ecdonald 1 nist-b-283	108	72				95	781
ecdonald 1 nist-b-409	156	104				127	813
ecdonald 1 nist-b-571	216	144				167	853
ecdonald 1 nist-k-163	63	42				65	751
ecdonald 1 nist-k-233	90	60				83	769

`ecdonald 1 nist-k-283`	108	72			95	781
`ecdonald 1 nist-k-409`	156	104			127	813
`ecdonald 1 nist-k-571`	216	144			167	853
`ecdonald 1 nist-p-192`	72	48			71	757
`ecdonald 1 nist-p-224`	84	56			79	765
`ecdonald 1 nist-p-256`	96	64			87	773
`ecdonald 1 nist-p-384`	144	96			119	805
`ecdonald 1 nist-p-521`	198	132			155	841
`ecdonald 1 secp160r1`	60	40			63	749
`ntru-enc 1 ees787ep1`	1854	1574	1574	2282		
`rainbow 1`	20107	31680			66	752
`ronald 1 768`	768	96	119	805	119	805
`ronald 1 832`	832	104	127	813	127	813
`ronald 1 896`	896	112	135	821	135	821
`ronald 1 960`	960	120	143	829	143	829
`ronald 1 1024`	1024	128	151	837	151	837
`ronald 1 1088`	1088	136	159	845	159	845
`ronald 1 1152`	1152	144	167	853	167	853
`ronald 1 1216`	1216	152	175	861	175	861
`ronald 1 1280`	1280	160	183	869	183	869
`ronald 1 1344`	1344	168	191	877	191	877
`ronald 1 1408`	1408	176	199	885	199	885
`ronald 1 1472`	1472	184	207	893	207	893
`ronald 1 1536`	1536	192	215	901	215	901
`ronald 1 1664`	1664	208	231	917	231	917
`ronald 1 1792`	1792	224	247	933	247	933
`ronald 1 1920`	1920	240	263	949	263	949
`ronald 1 2048`	2048	256	279	965	279	965
`ronald 1 2176`	2176	272	295	981	295	981
`ronald 1 2304`	2304	288	311	997	311	997
`ronald 1 2432`	2432	304	327	1013	327	1013
`ronald 1 2560`	2560	320	343	1029	343	1029
`ronald 1 2688`	2688	336	359	1045	359	1045
`ronald 1 2816`	2816	352	375	1061	375	1061
`ronald 1 2944`	2944	368	391	1077	391	1077
`ronald 1 3072`	3072	384	407	1093	407	1093
`ronald 1 3328`	3328	416	439	1125	439	1125
`ronald 1 3584`	3584	448	471	1157	471	1157
`ronald 1 3840`	3840	480	503	1189	503	1189
`ronald 1 4096`	4096	512	535	1221	535	1221
`ronald 2 768`	768	96	96	784	119	805
`ronald 2 832`	832	104	104	784	127	813
`ronald 2 896`	896	112	112	784	135	821
`ronald 2 960`	960	120	120	784	143	829
`ronald 2 1024`	1024	128	128	784	151	837
`ronald 2 1088`	1088	136	136	784	159	845
`ronald 2 1152`	1152	144	144	784	167	853

ronald 2 1216	1216	152	152	784	175	861
ronald 2 1280	1280	160	160	784	183	869
ronald 2 1344	1344	168	168	784	191	877
ronald 2 1408	1408	176	176	784	199	885
ronald 2 1472	1472	184	184	784	207	893
ronald 2 1536	1536	192	192	784	215	901
ronald 2 1664	1664	208	208	784	231	917
ronald 2 1792	1792	224	224	784	247	933
ronald 2 1920	1920	240	240	784	263	949
ronald 2 2048	2048	256	256	784	279	965
ronald 2 2176	2176	272	272	784	295	981
ronald 2 2304	2304	288	288	784	311	997
ronald 2 2432	2432	304	304	784	327	1013
ronald 2 2560	2560	320	320	784	343	1029
ronald 2 2688	2688	336	336	784	359	1045
ronald 2 2816	2816	352	352	784	375	1061
ronald 2 2944	2944	368	368	784	391	1077
ronald 2 3072	3072	384	384	784	407	1093
ronald 2 3328	3328	416	416	784	439	1125
ronald 2 3584	3584	448	448	784	471	1157
ronald 2 3840	3840	480	480	784	503	1189
ronald 2 4096	4096	512	512	784	535	1221
ronald 3 768	768	96	96	784	96	752
ronald 3 832	832	104	104	784	104	752
ronald 3 896	896	112	112	784	112	752
ronald 3 960	960	120	120	784	120	752
ronald 3 1024	1024	128	128	784	128	752
ronald 3 1088	1088	136	136	784	136	752
ronald 3 1152	1152	144	144	784	144	752
ronald 3 1216	1216	152	152	784	152	752
ronald 3 1280	1280	160	160	784	160	752
ronald 3 1344	1344	168	168	784	168	752
ronald 3 1408	1408	176	176	784	176	752
ronald 3 1472	1472	184	184	784	184	752
ronald 3 1536	1536	192	192	784	192	752
ronald 3 1664	1664	208	208	784	208	752
ronald 3 1792	1792	224	224	784	224	752
ronald 3 1920	1920	240	240	784	240	752
ronald 3 2048	2048	256	256	784	256	752
ronald 3 2176	2176	272	272	784	272	752
ronald 3 2304	2304	288	288	784	288	752
ronald 3 2432	2432	304	304	784	304	752
ronald 3 2560	2560	320	320	784	320	752
ronald 3 2688	2688	336	336	784	336	752
ronald 3 2816	2816	352	352	784	352	752
ronald 3 2944	2944	368	368	784	368	752
ronald 3 3072	3072	384	384	784	384	752

`ronald 3 3328`	3328	416		416	784	416	752
`ronald 3 3584`	3584	448		448	784	448	752
`ronald 3 3840`	3840	480		480	784	480	752
`ronald 3 4096`	4096	512		512	784	512	752
`sflashv2 1`	2823	19266				60	746
`sflashv2 2`	2823	19266				60	746
`surf127eps 1`	32	48	48				

6.7 ia64, 900MHz, Itanium II, `td156`

System	key-pair cycles	share cycles	encrypt cycles	decrypt cycles	sign cycles	verify cycles
`claus 1`	3975982	3951073				
`claus++ 1`	5463008	5296783				
`donald 1 512`	374400				419508	484890
`donald 1 1024`	789709				793647	948961
`donald 1 2048`	1884655				1805770	2141860
`ecdonald 1 nist-b-163`	2614549				2691331	5308182
`ecdonald 1 nist-b-233`	3506361				3603710	7110832
`ecdonald 1 nist-b-283`	7606013				7751549	15405009
`ecdonald 1 nist-b-409`	15956840				16126671	32006628
`ecdonald 1 nist-b-571`	35890822				36189523	72268123
`ecdonald 1 nist-k-163`	2458305				2530313	4958130
`ecdonald 1 nist-k-233`	3286334				3388480	6678855
`ecdonald 1 nist-k-283`	6963153				7090451	13984972
`ecdonald 1 nist-k-409`	14312113				14505134	28889252
`ecdonald 1 nist-k-571`	31882631				32174085	64250869
`ecdonald 1 nist-p-192`	1979182				2078855	2426720
`ecdonald 1 nist-p-224`	3181050				3290107	3877596
`ecdonald 1 nist-p-256`	3768235				3895501	4690638
`ecdonald 1 nist-p-384`	7062546				7256332	8595377
`ecdonald 1 nist-p-521`	8890160				9122528	10764039
`ecdonald 1 secp160r1`	2232560				2309701	2768596
`ntru-enc 1 ees787ep1`	197993171		991523	1841309		
`ronald 1 768`	55759145		108409	2018042	2021112	90583
`ronald 1 832`	92980530		115033	2346179	2343007	94610
`ronald 1 896`	103496051		117385	2536412	2543710	95276
`ronald 1 960`	104701406		121732	2470170	2470466	98975
`ronald 1 1024`	99247596		129217	2716529	2724740	105075
`ronald 1 1088`	126496626		149755	3776819	3770301	122175
`ronald 1 1152`	106503776		150042	4073456	4074717	123796
`ronald 1 1216`	149761336		154093	4229712	4220020	126179
`ronald 1 1280`	132701477		159637	4540566	4534091	127817
`ronald 1 1344`	259929943		166526	5033419	5047903	131461
`ronald 1 1408`	343687021		166607	5353544	5384614	133304
`ronald 1 1472`	245148832		172273	5845889	5837027	136058
`ronald 1 1536`	185341674		175693	6259692	6249181	137093

ronald 1 1664	490725051	184438	7692544	7663756	144728
ronald 1 1792	335118123	193473	8239807	8264285	149794
ronald 1 1920	325392974	203609	9465655	9444559	155941
ronald 1 2048	462332834	207292	10227197	10188227	160788
ronald 1 2176	480295419	246800	13215508	13212176	195370
ronald 1 2304	1060594768	255706	13796849	13774730	201549
ronald 1 2432	963112176	263421	15278387	15287463	207641
ronald 1 2560	1141907507	271794	16773287	16773230	214043
ronald 1 2688	955481332	282417	19509148	19498597	220759
ronald 1 2816	1049291070	290100	20045178	20066872	227815
ronald 1 2944	1103874717	300909	21998375	21997612	234324
ronald 1 3072	1402505550	313239	23712568	23686836	240630
ronald 1 3328	2926394464	335613	28250761	28279929	259047
ronald 1 3584	2209159949	354418	32878059	32884223	272497
ronald 1 3840	2791119497	379841	37958338	37943875	290147
ronald 1 4096	4039478680	396070	43786715	43749719	307572
ronald 2 768	53582151	91602	2024341	2031744	84032
ronald 2 832	52678814	97663	2342428	2345219	86530
ronald 2 896	81161497	98334	2539090	2555954	90195
ronald 2 960	76247167	101615	2465455	2469840	92071
ronald 2 1024	124347710	109197	2737952	2737431	99820
ronald 2 1088	150287755	129832	3778334	3797048	115707
ronald 2 1152	106134205	132062	4075602	4074280	116441
ronald 2 1216	196962885	134716	4210643	4225376	119097
ronald 2 1280	171683306	137908	4534602	4536841	121826
ronald 2 1344	174738568	146651	5036420	5033221	125832
ronald 2 1408	265527575	147447	5394319	5407435	126284
ronald 2 1472	211891701	151934	5867540	5876524	128969
ronald 2 1536	309026845	154719	6265916	6281044	130392
ronald 2 1664	439664158	167432	7683611	7684138	137422
ronald 2 1792	548051588	172307	8255013	8258654	142965
ronald 2 1920	431741621	182149	9478692	9478762	147514
ronald 2 2048	467671873	190964	10392032	10387986	152584
ronald 2 2176	738031053	226975	13151615	13160270	187981
ronald 2 2304	523210118	235837	13753521	13748354	193616
ronald 2 2432	589421508	245322	15220645	15235928	199481
ronald 2 2560	924383211	253808	16765120	16784815	206137
ronald 2 2688	1154599757	262283	19421202	19445556	210027
ronald 2 2816	1865178820	271152	20057793	20100207	219006
ronald 2 2944	1611924696	281903	21941150	21944858	226166
ronald 2 3072	1168608742	293779	23672111	23582356	230990
ronald 2 3328	1594324277	313415	28225763	28173804	249643
ronald 2 3584	2484458454	335528	32809091	32813540	263937
ronald 2 3840	2900785251	355868	37865455	37843341	280604
ronald 2 4096	4191097617	378852	44236587	44155080	297373
ronald 3 768	77634593	90862	2046626	2044659	80687
ronald 3 832	89741871	97040	2350680	2358373	84194

`ronald 3 896`	82782971	97886	2562093	2555424	86029
`ronald 3 960`	73772788	101748	2484853	2483228	88702
`ronald 3 1024`	79653191	108893	2752999	2733387	94880
`ronald 3 1088`	106666810	129455	3796190	3782043	111860
`ronald 3 1152`	239774741	131405	4108973	4099170	110060
`ronald 3 1216`	178849343	134606	4231801	4248052	114983
`ronald 3 1280`	182166540	137930	4570912	4566780	117682
`ronald 3 1344`	280893226	143390	5063295	5062274	121498
`ronald 3 1408`	331805809	145444	5432314	5416699	122164
`ronald 3 1472`	335581946	149720	5882829	5890075	125576
`ronald 3 1536`	279855950	153499	6312912	6304674	126971
`ronald 3 1664`	389005263	161870	7729004	7732028	134413
`ronald 3 1792`	451676122	171282	8312209	8285847	138489
`ronald 3 1920`	556312699	178695	9521953	9501988	144545
`ronald 3 2048`	436489991	189084	10373476	10399389	149110
`ronald 3 2176`	321436427	224195	13169428	13190133	183348
`ronald 3 2304`	568736230	234002	13756153	13794076	190187
`ronald 3 2432`	1014115144	243107	15250071	15250295	195518
`ronald 3 2560`	1406027042	250254	16814130	16797914	201423
`ronald 3 2688`	1007938660	258906	19504440	19525907	207462
`ronald 3 2816`	1238105617	271064	20100052	20069967	215269
`ronald 3 2944`	1295644420	279296	21976735	21952087	222341
`ronald 3 3072`	1050211005	289779	23716669	23662169	226755
`ronald 3 3328`	3074976356	309900	28282948	28256478	246232
`ronald 3 3584`	2251959479	334753	32991185	32871526	261177
`ronald 3 3840`	3298263665	354200	37931294	37909159	276779
`ronald 3 4096`	3094353102	374078	44231970	44159441	293109
`sflashv2 1`	1079594622			2864661	782220
`sflashv2 2`	1044980562			303802	360885

System	secret key bytes	public key bytes	shared secret bytes	23-byte encrypt bytes	709-byte encrypt bytes	23-byte signed bytes	709-byte signed bytes
`claus 1`	256	128	128				
`claus++ 1`	256	128	128				
`donald 1 512`	84	64				63	749
`donald 1 1024`	148	128				63	749
`donald 1 2048`	276	256				63	749
`ecdonald 1 nist-b-163`	63	42				65	751
`ecdonald 1 nist-b-233`	90	60				83	769
`ecdonald 1 nist-b-283`	108	72				95	781
`ecdonald 1 nist-b-409`	156	104				127	813
`ecdonald 1 nist-b-571`	216	144				167	853
`ecdonald 1 nist-k-163`	63	42				65	751
`ecdonald 1 nist-k-233`	90	60				83	769
`ecdonald 1 nist-k-283`	108	72				95	781
`ecdonald 1 nist-k-409`	156	104				127	813

ecdonald 1 nist-k-571	216	144			167	853
ecdonald 1 nist-p-192	72	48			71	757
ecdonald 1 nist-p-224	84	56			79	765
ecdonald 1 nist-p-256	96	64			87	773
ecdonald 1 nist-p-384	144	96			119	805
ecdonald 1 nist-p-521	198	132			155	841
ecdonald 1 secp160r1	60	40			63	749
ntru-enc 1 ees787ep1	1854	1574	1574	2282		
ronald 1 768	768	96	119	805	119	805
ronald 1 832	832	104	127	813	127	813
ronald 1 896	896	112	135	821	135	821
ronald 1 960	960	120	143	829	143	829
ronald 1 1024	1024	128	151	837	151	837
ronald 1 1088	1088	136	159	845	159	845
ronald 1 1152	1152	144	167	853	167	853
ronald 1 1216	1216	152	175	861	175	861
ronald 1 1280	1280	160	183	869	183	869
ronald 1 1344	1344	168	191	877	191	877
ronald 1 1408	1408	176	199	885	199	885
ronald 1 1472	1472	184	207	893	207	893
ronald 1 1536	1536	192	215	901	215	901
ronald 1 1664	1664	208	231	917	231	917
ronald 1 1792	1792	224	247	933	247	933
ronald 1 1920	1920	240	263	949	263	949
ronald 1 2048	2048	256	279	965	279	965
ronald 1 2176	2176	272	295	981	295	981
ronald 1 2304	2304	288	311	997	311	997
ronald 1 2432	2432	304	327	1013	327	1013
ronald 1 2560	2560	320	343	1029	343	1029
ronald 1 2688	2688	336	359	1045	359	1045
ronald 1 2816	2816	352	375	1061	375	1061
ronald 1 2944	2944	368	391	1077	391	1077
ronald 1 3072	3072	384	407	1093	407	1093
ronald 1 3328	3328	416	439	1125	439	1125
ronald 1 3584	3584	448	471	1157	471	1157
ronald 1 3840	3840	480	503	1189	503	1189
ronald 1 4096	4096	512	535	1221	535	1221
ronald 2 768	768	96	96	784	119	805
ronald 2 832	832	104	104	784	127	813
ronald 2 896	896	112	112	784	135	821
ronald 2 960	960	120	120	784	143	829
ronald 2 1024	1024	128	128	784	151	837
ronald 2 1088	1088	136	136	784	159	845
ronald 2 1152	1152	144	144	784	167	853
ronald 2 1216	1216	152	152	784	175	861
ronald 2 1280	1280	160	160	784	183	869
ronald 2 1344	1344	168	168	784	191	877

`ronald 2 1408`	1408	176	176	784	199	885
`ronald 2 1472`	1472	184	184	784	207	893
`ronald 2 1536`	1536	192	192	784	215	901
`ronald 2 1664`	1664	208	208	784	231	917
`ronald 2 1792`	1792	224	224	784	247	933
`ronald 2 1920`	1920	240	240	784	263	949
`ronald 2 2048`	2048	256	256	784	279	965
`ronald 2 2176`	2176	272	272	784	295	981
`ronald 2 2304`	2304	288	288	784	311	997
`ronald 2 2432`	2432	304	304	784	327	1013
`ronald 2 2560`	2560	320	320	784	343	1029
`ronald 2 2688`	2688	336	336	784	359	1045
`ronald 2 2816`	2816	352	352	784	375	1061
`ronald 2 2944`	2944	368	368	784	391	1077
`ronald 2 3072`	3072	384	384	784	407	1093
`ronald 2 3328`	3328	416	416	784	439	1125
`ronald 2 3584`	3584	448	448	784	471	1157
`ronald 2 3840`	3840	480	480	784	503	1189
`ronald 2 4096`	4096	512	512	784	535	1221
`ronald 3 768`	768	96	96	784	96	752
`ronald 3 832`	832	104	104	784	104	752
`ronald 3 896`	896	112	112	784	112	752
`ronald 3 960`	960	120	120	784	120	752
`ronald 3 1024`	1024	128	128	784	128	752
`ronald 3 1088`	1088	136	136	784	136	752
`ronald 3 1152`	1152	144	144	784	144	752
`ronald 3 1216`	1216	152	152	784	152	752
`ronald 3 1280`	1280	160	160	784	160	752
`ronald 3 1344`	1344	168	168	784	168	752
`ronald 3 1408`	1408	176	176	784	176	752
`ronald 3 1472`	1472	184	184	784	184	752
`ronald 3 1536`	1536	192	192	784	192	752
`ronald 3 1664`	1664	208	208	784	208	752
`ronald 3 1792`	1792	224	224	784	224	752
`ronald 3 1920`	1920	240	240	784	240	752
`ronald 3 2048`	2048	256	256	784	256	752
`ronald 3 2176`	2176	272	272	784	272	752
`ronald 3 2304`	2304	288	288	784	288	752
`ronald 3 2432`	2432	304	304	784	304	752
`ronald 3 2560`	2560	320	320	784	320	752
`ronald 3 2688`	2688	336	336	784	336	752
`ronald 3 2816`	2816	352	352	784	352	752
`ronald 3 2944`	2944	368	368	784	368	752
`ronald 3 3072`	3072	384	384	784	384	752
`ronald 3 3328`	3328	416	416	784	416	752
`ronald 3 3584`	3584	448	448	784	448	752
`ronald 3 3840`	3840	480	480	784	480	752

ronald 3 4096	4096	512	512	784	512	752
sflashv2 1	2823	19266			60	746
sflashv2 2	2823	19266			60	746

6.8 ia64, 1500MHz, Itanium II, td178

System	key-pair cycles	share cycles	encrypt cycles	decrypt cycles	sign cycles	verify cycles
claus 1	3903761	3876515				
claus++ 1	5476207	5392450				
donald 1 512	375281				407040	463514
donald 1 1024	783135				782172	923724
donald 1 2048	1876547				1776801	2145335
ecdonald 1 nist-b-163	2238709				2304622	4531268
ecdonald 1 nist-b-233	3035195				3125669	6148721
ecdonald 1 nist-b-283	6536599				6649844	13215588
ecdonald 1 nist-b-409	13830141				14005987	27799936
ecdonald 1 nist-b-571	30876041				31127114	62152411
ecdonald 1 nist-k-163	2104863				2179318	4228884
ecdonald 1 nist-k-233	2850488				2943401	5747532
ecdonald 1 nist-k-283	5968460				6065187	12070211
ecdonald 1 nist-k-409	12424209				12552577	24915938
ecdonald 1 nist-k-571	27419829				27655101	55193421
ecdonald 1 nist-p-192	1855563				1947346	2314156
ecdonald 1 nist-p-224	2887812				2972990	3571221
ecdonald 1 nist-p-256	3472454				3547625	4297259
ecdonald 1 nist-p-384	6611183				6781512	8145988
ecdonald 1 nist-p-521	8453837				8696343	10303643
ecdonald 1 secp160r1	2049696				2096546	2541437
ntru-enc 1 ees787ep1	211756610		930160	1743372		
rainbow 1	166039642				951132	1733096
ronald 1 768	81498445		102994	1898586	1899079	87167
ronald 1 832	83574624		108339	2201039	2214417	90494
ronald 1 896	88569419		111096	2404190	2390890	92012
ronald 1 960	81999456		114601	2292272	2304766	95251
ronald 1 1024	118091808		121043	2535010	2545718	99556
ronald 1 1088	143706781		141630	3600062	3572529	117936
ronald 1 1152	116526199		143025	3875694	3870619	116740
ronald 1 1216	163252571		150266	3997263	4010928	122216
ronald 1 1280	175474547		149721	4302860	4310745	124048
ronald 1 1344	183574268		156283	4773921	4796245	129134
ronald 1 1408	124935381		155895	5089236	5090235	129498
ronald 1 1472	248699848		162834	5546199	5548232	131006
ronald 1 1536	244439793		164373	5941093	5949903	134663
ronald 1 1664	485347780		176539	7380311	7347555	141792
ronald 1 1792	449928391		182203	7889626	7874696	145848
ronald 1 1920	465654510		191587	9040625	9052463	151947

ronald 1 2048	555951193	198101	9660485	9682564	156687
ronald 1 2176	672014197	236453	12778027	12755201	190935
ronald 1 2304	793939750	242426	13330580	13324294	197283
ronald 1 2432	1097202517	250234	14803100	14811956	203988
ronald 1 2560	1102697775	260073	16243928	16282424	209860
ronald 1 2688	794535864	268193	18949524	18940122	216244
ronald 1 2816	1296302420	280664	19538343	19572276	222039
ronald 1 2944	1765490490	285726	21393007	21384620	229141
ronald 1 3072	1659627970	299821	23025836	23079641	236562
ronald 1 3328	1773533678	320317	27517584	27501633	253271
ronald 1 3584	2336055981	338882	32055191	32119283	268576
ronald 1 3840	2951624142	358185	37063062	37058109	284957
ronald 1 4096	3507884425	383929	42744417	42721679	302436
ronald 2 768	83312864	86306	1921099	1917583	80222
ronald 2 832	62197344	92276	2217371	2205909	85315
ronald 2 896	74226408	94259	2402440	2401322	87176
ronald 2 960	82057683	97170	2321169	2321254	88787
ronald 2 1024	70838884	103592	2581776	2563806	92082
ronald 2 1088	84938352	124642	3593996	3581947	111158
ronald 2 1152	227911319	126598	3879229	3883159	112745
ronald 2 1216	138838719	129518	4034015	4019291	115159
ronald 2 1280	206859319	132880	4346553	4333731	115153
ronald 2 1344	121311001	139442	4788452	4784442	121719
ronald 2 1408	169690793	140896	5099187	5123080	122752
ronald 2 1472	186275889	145056	5580189	5568634	125260
ronald 2 1536	332079792	148021	5980559	5948567	126229
ronald 2 1664	207820663	161033	7381686	7354094	133833
ronald 2 1792	263446844	167630	7893361	7886206	135704
ronald 2 1920	286124012	174594	9076486	9058544	143765
ronald 2 2048	474471843	181790	9735972	9747334	148955
ronald 2 2176	474489831	218707	12887076	12847509	182919
ronald 2 2304	860383880	227799	13406818	13399716	189136
ronald 2 2432	919843712	236914	14853753	14836428	195300
ronald 2 2560	837080436	244305	16365243	16327408	202935
ronald 2 2688	1140682553	254885	19088556	19060004	206877
ronald 2 2816	1450229885	260745	19600707	19547603	213453
ronald 2 2944	1077733750	271669	21470462	21509803	220818
ronald 2 3072	1066829755	283418	23095452	23139887	227517
ronald 2 3328	1407604920	303758	27665024	27579688	245347
ronald 2 3584	2611603775	325941	32197305	32203577	258314
ronald 2 3840	3638100069	344899	37179382	37137808	274924
ronald 2 4096	4162745366	366877	42986267	42945850	293560
ronald 3 768	60801104	86810	1901589	1891516	77473
ronald 3 832	55828319	92270	2211767	2197299	81664
ronald 3 896	110711682	93834	2384613	2392717	83199
ronald 3 960	89779777	97205	2304132	2312550	84667
ronald 3 1024	67125700	104970	2562523	2560964	90546

ronald 3 1088	121064027	123820	3576257	3580635	108752
ronald 3 1152	161304705	126268	3877080	3881983	110382
ronald 3 1216	233426256	129150	4026004	4016148	112851
ronald 3 1280	121593817	132273	4317322	4295786	112479
ronald 3 1344	211523477	139614	4775202	4762526	119026
ronald 3 1408	230977950	142088	5080414	5089127	115665
ronald 3 1472	179169133	145394	5551202	5549711	122919
ronald 3 1536	157888004	147192	5955484	5956052	121196
ronald 3 1664	217878701	157906	7337376	7368012	130315
ronald 3 1792	400930190	164960	7902633	7874900	135681
ronald 3 1920	491197533	173494	9032554	9023979	140187
ronald 3 2048	474118012	180007	9761860	9768923	144645
ronald 3 2176	753103878	217493	12829098	12808389	179239
ronald 3 2304	742940371	226418	13353562	13302803	184951
ronald 3 2432	1296414977	236388	14832389	14823030	191539
ronald 3 2560	1224960768	242790	16288739	16290809	197442
ronald 3 2688	1784515270	251925	19000776	19012593	203549
ronald 3 2816	734066856	261299	19543871	19520283	210315
ronald 3 2944	1268593636	270141	21391619	21427682	217197
ronald 3 3072	1324867427	278961	23009954	23073548	223505
ronald 3 3328	1808942367	302270	27563323	27522267	241618
ronald 3 3584	2685658653	322207	32159660	32199405	255215
ronald 3 3840	2611086130	343479	37082863	37071050	271524
ronald 3 4096	4639325622	367326	42924182	43023787	287988
sflashv2 1	714834367			3133882	1109978
sflashv2 2	682710964			278304	342275

System	secret key bytes	public key bytes	shared secret bytes	23-byte encrypt bytes	709-byte encrypt bytes	23-byte signed bytes	709-byte signed bytes
claus 1	256	128	128				
claus++ 1	256	128	128				
donald 1 512	84	64				63	749
donald 1 1024	148	128				63	749
donald 1 2048	276	256				63	749
ecdonald 1 nist-b-163	63	42				65	751
ecdonald 1 nist-b-233	90	60				83	769
ecdonald 1 nist-b-283	108	72				95	781
ecdonald 1 nist-b-409	156	104				127	813
ecdonald 1 nist-b-571	216	144				167	853
ecdonald 1 nist-k-163	63	42				65	751
ecdonald 1 nist-k-233	90	60				83	769
ecdonald 1 nist-k-283	108	72				95	781
ecdonald 1 nist-k-409	156	104				127	813
ecdonald 1 nist-k-571	216	144				167	853
ecdonald 1 nist-p-192	72	48				71	757
ecdonald 1 nist-p-224	84	56				79	765

`ecdonald 1 nist-p-256`	96	64			87	773
`ecdonald 1 nist-p-384`	144	96			119	805
`ecdonald 1 nist-p-521`	198	132			155	841
`ecdonald 1 secp160r1`	60	40			63	749
`ntru-enc 1 ees787ep1`	1854	1574	1574	2282		
`rainbow 1`	20107	31680			66	752
`ronald 1 768`	768	96	119	805	119	805
`ronald 1 832`	832	104	127	813	127	813
`ronald 1 896`	896	112	135	821	135	821
`ronald 1 960`	960	120	143	829	143	829
`ronald 1 1024`	1024	128	151	837	151	837
`ronald 1 1088`	1088	136	159	845	159	845
`ronald 1 1152`	1152	144	167	853	167	853
`ronald 1 1216`	1216	152	175	861	175	861
`ronald 1 1280`	1280	160	183	869	183	869
`ronald 1 1344`	1344	168	191	877	191	877
`ronald 1 1408`	1408	176	199	885	199	885
`ronald 1 1472`	1472	184	207	893	207	893
`ronald 1 1536`	1536	192	215	901	215	901
`ronald 1 1664`	1664	208	231	917	231	917
`ronald 1 1792`	1792	224	247	933	247	933
`ronald 1 1920`	1920	240	263	949	263	949
`ronald 1 2048`	2048	256	279	965	279	965
`ronald 1 2176`	2176	272	295	981	295	981
`ronald 1 2304`	2304	288	311	997	311	997
`ronald 1 2432`	2432	304	327	1013	327	1013
`ronald 1 2560`	2560	320	343	1029	343	1029
`ronald 1 2688`	2688	336	359	1045	359	1045
`ronald 1 2816`	2816	352	375	1061	375	1061
`ronald 1 2944`	2944	368	391	1077	391	1077
`ronald 1 3072`	3072	384	407	1093	407	1093
`ronald 1 3328`	3328	416	439	1125	439	1125
`ronald 1 3584`	3584	448	471	1157	471	1157
`ronald 1 3840`	3840	480	503	1189	503	1189
`ronald 1 4096`	4096	512	535	1221	535	1221
`ronald 2 768`	768	96	96	784	119	805
`ronald 2 832`	832	104	104	784	127	813
`ronald 2 896`	896	112	112	784	135	821
`ronald 2 960`	960	120	120	784	143	829
`ronald 2 1024`	1024	128	128	784	151	837
`ronald 2 1088`	1088	136	136	784	159	845
`ronald 2 1152`	1152	144	144	784	167	853
`ronald 2 1216`	1216	152	152	784	175	861
`ronald 2 1280`	1280	160	160	784	183	869
`ronald 2 1344`	1344	168	168	784	191	877
`ronald 2 1408`	1408	176	176	784	199	885
`ronald 2 1472`	1472	184	184	784	207	893

ronald 2 1536	1536	192	192	784	215	901
ronald 2 1664	1664	208	208	784	231	917
ronald 2 1792	1792	224	224	784	247	933
ronald 2 1920	1920	240	240	784	263	949
ronald 2 2048	2048	256	256	784	279	965
ronald 2 2176	2176	272	272	784	295	981
ronald 2 2304	2304	288	288	784	311	997
ronald 2 2432	2432	304	304	784	327	1013
ronald 2 2560	2560	320	320	784	343	1029
ronald 2 2688	2688	336	336	784	359	1045
ronald 2 2816	2816	352	352	784	375	1061
ronald 2 2944	2944	368	368	784	391	1077
ronald 2 3072	3072	384	384	784	407	1093
ronald 2 3328	3328	416	416	784	439	1125
ronald 2 3584	3584	448	448	784	471	1157
ronald 2 3840	3840	480	480	784	503	1189
ronald 2 4096	4096	512	512	784	535	1221
ronald 3 768	768	96	96	784	96	752
ronald 3 832	832	104	104	784	104	752
ronald 3 896	896	112	112	784	112	752
ronald 3 960	960	120	120	784	120	752
ronald 3 1024	1024	128	128	784	128	752
ronald 3 1088	1088	136	136	784	136	752
ronald 3 1152	1152	144	144	784	144	752
ronald 3 1216	1216	152	152	784	152	752
ronald 3 1280	1280	160	160	784	160	752
ronald 3 1344	1344	168	168	784	168	752
ronald 3 1408	1408	176	176	784	176	752
ronald 3 1472	1472	184	184	784	184	752
ronald 3 1536	1536	192	192	784	192	752
ronald 3 1664	1664	208	208	784	208	752
ronald 3 1792	1792	224	224	784	224	752
ronald 3 1920	1920	240	240	784	240	752
ronald 3 2048	2048	256	256	784	256	752
ronald 3 2176	2176	272	272	784	272	752
ronald 3 2304	2304	288	288	784	288	752
ronald 3 2432	2432	304	304	784	304	752
ronald 3 2560	2560	320	320	784	320	752
ronald 3 2688	2688	336	336	784	336	752
ronald 3 2816	2816	352	352	784	352	752
ronald 3 2944	2944	368	368	784	368	752
ronald 3 3072	3072	384	384	784	384	752
ronald 3 3328	3328	416	416	784	416	752
ronald 3 3584	3584	448	448	784	448	752
ronald 3 3840	3840	480	480	784	480	752
ronald 3 4096	4096	512	512	784	512	752
sflashv2 1	2823	19266			60	746

sflashv2 2	2823	19266			60	746

6.9 ppc32, 533MHz, PowerPC G4 7410, gggg

System	key-pair cycles	share cycles	encrypt cycles	decrypt cycles	sign cycles	verify cycles
claus 1	34383808	34355888				
claus++ 1	28144752	28048848				
donald 1 512	1851984				1817392	2179648
donald 1 1024	6090400				5732928	6935776
donald 1 2048	21657648				20117584	24250080
ecdonald 1 nist-b-163	3916656				4030816	7974816
ecdonald 1 nist-b-233	8038432				8174240	16174560
ecdonald 1 nist-b-283	14936240				15117520	30052960
ecdonald 1 nist-b-409	36666288				36839424	73667760
ecdonald 1 nist-b-571	84946480				85382544	170881440
ecdonald 1 nist-k-163	3610000				3744640	7307536
ecdonald 1 nist-k-233	7212224				7336528	14471216
ecdonald 1 nist-k-283	13230576				13401888	26566128
ecdonald 1 nist-k-409	31743056				32012688	63932448
ecdonald 1 nist-k-571	73425456				73959152	147856752
ecdonald 1 nist-p-192	3308480				3444960	4217824
ecdonald 1 nist-p-224	4590288				4700784	5674112
ecdonald 1 nist-p-256	6213040				6393088	7695792
ecdonald 1 nist-p-384	15676240				15808720	19131744
ecdonald 1 nist-p-521	37895920				38288848	47233040
ecdonald 1 secp160r1	3634064				3723472	4552000
ntru-enc 1 ees787ep1	118737024		746208	1391824		
rainbow 1	225503280				1175824	2128976
ronald 1 768	151813488		213616	6472816	6480432	197664
ronald 1 832	183578480		231328	7833792	7842624	218368
ronald 1 896	289884288		249136	9340512	9322880	232272
ronald 1 960	303187792		269744	10982080	10999200	253424
ronald 1 1024	253478016		285328	12395424	12371008	263808
ronald 1 1088	378953584		349792	16006368	16047280	333776
ronald 1 1152	543648672		371536	18352432	18375344	349616
ronald 1 1216	545725152		395040	20759296	20790880	372832
ronald 1 1280	812688096		423712	23328112	23384224	393744
ronald 1 1344	716787968		450592	26331072	26329504	416560
ronald 1 1408	677693840		470304	29577488	29528256	442608
ronald 1 1472	1050244624		499664	33168928	33207168	483904
ronald 1 1536	905619488		524704	36733392	36746272	494048
ronald 1 1664	1279753120		595280	45771104	45745536	558256
ronald 1 1792	1445629920		663424	55274128	55293776	632192
ronald 1 1920	2192373872		731680	66202432	66238800	717200
ronald 1 2048	2266584336		825264	75131472	74948816	792560
ronald 1 2176	3698978736		1036720	96825888	96981344	998304

ronald 1 2304	4085190320	1113344	111582928	111753856	1069856
ronald 1 2432	4418637376	1193488	129220096	129066544	1151872
ronald 1 2560	5252295696	1277328	147648832	147260288	1237552
ronald 1 2688	8460205344	1387808	168288992	168277072	1334608
ronald 1 2816	8131569792	1485712	190945328	190249808	1420960
ronald 1 2944	10417785472	1572528	215486816	215835168	1519392
ronald 1 3072	9708291520	1668496	240460544	241276224	1613136
ronald 1 3328	20823028224	1919632	302760592	303310544	1858896
ronald 1 3584	24956402176	2165040	371940464	371209072	2106528
ronald 1 3840	18850022944	2439184	450985200	449277264	2372320
ronald 1 4096	27882594064	2643312	494909696	496175600	2570496
ronald 2 768	191537248	194864	6435376	6446816	189856
ronald 2 832	149798160	215456	7847024	7859168	208384
ronald 2 896	160130000	231264	9315696	9318256	221904
ronald 2 960	366640704	250432	11022928	11012304	238416
ronald 2 1024	309060512	267296	12354752	12396480	254896
ronald 2 1088	442992976	334512	16005184	16031376	320144
ronald 2 1152	489582144	355520	18393104	18395152	341344
ronald 2 1216	425612928	377776	20797536	20780368	364016
ronald 2 1280	760912336	402256	23358560	23335200	384384
ronald 2 1344	626706448	426016	26317504	26351760	407392
ronald 2 1408	995275856	455920	29527136	29564640	430880
ronald 2 1472	1069800960	481648	33085728	33216432	460752
ronald 2 1536	1372077472	510816	36782272	36817984	484000
ronald 2 1664	1643356912	581088	45691392	45685872	559184
ronald 2 1792	1328196352	642768	55222288	55133392	614800
ronald 2 1920	3719287232	716032	66043648	66080512	697216
ronald 2 2048	2189674624	774720	74564064	74758704	775264
ronald 2 2176	3402607296	1014752	97207600	97084944	986368
ronald 2 2304	4480592752	1098080	111638608	111795888	1059840
ronald 2 2432	5197759696	1178400	129037600	129003360	1141104
ronald 2 2560	4580775968	1260000	147696640	147738448	1219296
ronald 2 2688	6661248112	1364048	167880976	168470832	1320880
ronald 2 2816	9513547360	1452240	190169040	190446208	1409728
ronald 2 2944	12451683728	1551152	215611104	215111552	1509040
ronald 2 3072	14140723440	1649968	240738960	240635680	1599152
ronald 2 3328	23234713152	1912688	303544080	303370816	1848736
ronald 2 3584	28742781280	2133264	371067936	370842352	2070464
ronald 2 3840	22197670224	2429808	450509040	450346224	2362352
ronald 2 4096	23126736672	2612160	496472192	495695600	2545024
ronald 3 768	146991520	193808	6469632	6468464	180688
ronald 3 832	217382224	215504	7813536	7837248	199664
ronald 3 896	245544096	229504	9316080	9322912	216368
ronald 3 960	310005760	248560	11015376	11002304	230560
ronald 3 1024	451669472	267952	12328576	12380128	247424
ronald 3 1088	309312912	333888	16022704	15982336	311376
ronald 3 1152	510607136	358112	18305360	18353728	332240

`ronald 3 1216`	608588736	380160	20786352	20765728	353888
`ronald 3 1280`	840229168	402624	23304496	23331360	379104
`ronald 3 1344`	791559488	428416	26333824	26356240	399904
`ronald 3 1408`	794919536	450656	29558176	29502096	424592
`ronald 3 1472`	1480269584	481952	33166544	33215984	450336
`ronald 3 1536`	723792080	507248	36773552	36773648	475344
`ronald 3 1664`	1548196768	577520	45719328	45734944	540592
`ronald 3 1792`	2139862576	641792	55274672	55409776	607760
`ronald 3 1920`	3270580192	717232	66133024	66160224	712896
`ronald 3 2048`	3468572016	781952	75017776	74865360	750288
`ronald 3 2176`	3344566288	1010064	96997152	97007136	974224
`ronald 3 2304`	5055063504	1096544	111161280	111680512	1053568
`ronald 3 2432`	5596296272	1185616	129019568	128982624	1128560
`ronald 3 2560`	7784705728	1268064	147664480	147958624	1210944
`ronald 3 2688`	9458014560	1364112	167983568	168677968	1312800
`ronald 3 2816`	10181847840	1454752	190621984	190770960	1395344
`ronald 3 2944`	14410439616	1556176	215518864	215779552	1496384
`ronald 3 3072`	17880770864	1659872	241039008	240782464	1591184
`ronald 3 3328`	19927430272	1908720	303264288	302924688	1833456
`ronald 3 3584`	17041745136	2144208	370596304	371806416	2083360
`ronald 3 3840`	38816021552	2421792	450613904	449990464	2334736
`ronald 3 4096`	31546186160	2616880	496743456	496233920	2536448
`sflashv2 1`	905677280			2199248	445424
`sflashv2 2`	727987712			273616	303776

System	secret key bytes	public key bytes	shared secret bytes	23-byte encrypt bytes	709-byte encrypt bytes	23-byte signed bytes	709-byte signed bytes
`claus 1`	256	128	128				
`claus++ 1`	256	128	128				
`donald 1 512`	84	64				63	749
`donald 1 1024`	148	128				63	749
`donald 1 2048`	276	256				63	749
`ecdonald 1 nist-b-163`	63	42				65	751
`ecdonald 1 nist-b-233`	90	60				83	769
`ecdonald 1 nist-b-283`	108	72				95	781
`ecdonald 1 nist-b-409`	156	104				127	813
`ecdonald 1 nist-b-571`	216	144				167	853
`ecdonald 1 nist-k-163`	63	42				65	751
`ecdonald 1 nist-k-233`	90	60				83	769
`ecdonald 1 nist-k-283`	108	72				95	781
`ecdonald 1 nist-k-409`	156	104				127	813
`ecdonald 1 nist-k-571`	216	144				167	853
`ecdonald 1 nist-p-192`	72	48				71	757
`ecdonald 1 nist-p-224`	84	56				79	765
`ecdonald 1 nist-p-256`	96	64				87	773
`ecdonald 1 nist-p-384`	144	96				119	805

ecdonald 1 nist-p-521	198	132			155	841
ecdonald 1 secp160r1	60	40			63	749
ntru-enc 1 ees787ep1	1854	1574	1574	2282		
rainbow 1	20107	31680			66	752
ronald 1 768	768	96	119	805	119	805
ronald 1 832	832	104	127	813	127	813
ronald 1 896	896	112	135	821	135	821
ronald 1 960	960	120	143	829	143	829
ronald 1 1024	1024	128	151	837	151	837
ronald 1 1088	1088	136	159	845	159	845
ronald 1 1152	1152	144	167	853	167	853
ronald 1 1216	1216	152	175	861	175	861
ronald 1 1280	1280	160	183	869	183	869
ronald 1 1344	1344	168	191	877	191	877
ronald 1 1408	1408	176	199	885	199	885
ronald 1 1472	1472	184	207	893	207	893
ronald 1 1536	1536	192	215	901	215	901
ronald 1 1664	1664	208	231	917	231	917
ronald 1 1792	1792	224	247	933	247	933
ronald 1 1920	1920	240	263	949	263	949
ronald 1 2048	2048	256	279	965	279	965
ronald 1 2176	2176	272	295	981	295	981
ronald 1 2304	2304	288	311	997	311	997
ronald 1 2432	2432	304	327	1013	327	1013
ronald 1 2560	2560	320	343	1029	343	1029
ronald 1 2688	2688	336	359	1045	359	1045
ronald 1 2816	2816	352	375	1061	375	1061
ronald 1 2944	2944	368	391	1077	391	1077
ronald 1 3072	3072	384	407	1093	407	1093
ronald 1 3328	3328	416	439	1125	439	1125
ronald 1 3584	3584	448	471	1157	471	1157
ronald 1 3840	3840	480	503	1189	503	1189
ronald 1 4096	4096	512	535	1221	535	1221
ronald 2 768	768	96	96	784	119	805
ronald 2 832	832	104	104	784	127	813
ronald 2 896	896	112	112	784	135	821
ronald 2 960	960	120	120	784	143	829
ronald 2 1024	1024	128	128	784	151	837
ronald 2 1088	1088	136	136	784	159	845
ronald 2 1152	1152	144	144	784	167	853
ronald 2 1216	1216	152	152	784	175	861
ronald 2 1280	1280	160	160	784	183	869
ronald 2 1344	1344	168	168	784	191	877
ronald 2 1408	1408	176	176	784	199	885
ronald 2 1472	1472	184	184	784	207	893
ronald 2 1536	1536	192	192	784	215	901
ronald 2 1664	1664	208	208	784	231	917

`ronald 2 1792`	1792	224	224	784	247	933
`ronald 2 1920`	1920	240	240	784	263	949
`ronald 2 2048`	2048	256	256	784	279	965
`ronald 2 2176`	2176	272	272	784	295	981
`ronald 2 2304`	2304	288	288	784	311	997
`ronald 2 2432`	2432	304	304	784	327	1013
`ronald 2 2560`	2560	320	320	784	343	1029
`ronald 2 2688`	2688	336	336	784	359	1045
`ronald 2 2816`	2816	352	352	784	375	1061
`ronald 2 2944`	2944	368	368	784	391	1077
`ronald 2 3072`	3072	384	384	784	407	1093
`ronald 2 3328`	3328	416	416	784	439	1125
`ronald 2 3584`	3584	448	448	784	471	1157
`ronald 2 3840`	3840	480	480	784	503	1189
`ronald 2 4096`	4096	512	512	784	535	1221
`ronald 3 768`	768	96	96	784	96	752
`ronald 3 832`	832	104	104	784	104	752
`ronald 3 896`	896	112	112	784	112	752
`ronald 3 960`	960	120	120	784	120	752
`ronald 3 1024`	1024	128	128	784	128	752
`ronald 3 1088`	1088	136	136	784	136	752
`ronald 3 1152`	1152	144	144	784	144	752
`ronald 3 1216`	1216	152	152	784	152	752
`ronald 3 1280`	1280	160	160	784	160	752
`ronald 3 1344`	1344	168	168	784	168	752
`ronald 3 1408`	1408	176	176	784	176	752
`ronald 3 1472`	1472	184	184	784	184	752
`ronald 3 1536`	1536	192	192	784	192	752
`ronald 3 1664`	1664	208	208	784	208	752
`ronald 3 1792`	1792	224	224	784	224	752
`ronald 3 1920`	1920	240	240	784	240	752
`ronald 3 2048`	2048	256	256	784	256	752
`ronald 3 2176`	2176	272	272	784	272	752
`ronald 3 2304`	2304	288	288	784	288	752
`ronald 3 2432`	2432	304	304	784	304	752
`ronald 3 2560`	2560	320	320	784	320	752
`ronald 3 2688`	2688	336	336	784	336	752
`ronald 3 2816`	2816	352	352	784	352	752
`ronald 3 2944`	2944	368	368	784	368	752
`ronald 3 3072`	3072	384	384	784	384	752
`ronald 3 3328`	3328	416	416	784	416	752
`ronald 3 3584`	3584	448	448	784	448	752
`ronald 3 3840`	3840	480	480	784	480	752
`ronald 3 4096`	4096	512	512	784	512	752
`sflashv2 1`	2823	19266			60	746
`sflashv2 2`	2823	19266			60	746

6.10 sparcv9, 1050MHz, UltraSPARC IV, hald

System	key-pair cycles	share cycles	encrypt cycles	decrypt cycles	sign cycles	verify cycles
claus 1	27377275	27351694				
claus++ 1	11237085	11290135				
donald 1 512	1597191				1606245	1919475
donald 1 1024	4953655				4727730	5712645
donald 1 2048	17074485				15906325	18997845
ecdonald 1 nist-b-163	3097410				3220915	6269315
ecdonald 1 nist-b-233	4347740				4502480	8715065
ecdonald 1 nist-b-283	9184550				9407270	18470770
ecdonald 1 nist-b-409	21551370				20018515	39530110
ecdonald 1 nist-b-571	42706122				43122775	85976315
ecdonald 1 nist-k-163	2948680				3086695	5936125
ecdonald 1 nist-k-233	4089112				4270695	8237687
ecdonald 1 nist-k-283	8329028				8567028	16911277
ecdonald 1 nist-k-409	17545770				17883665	35496598
ecdonald 1 nist-k-571	38353255				38945255	77726680
ecdonald 1 nist-p-192	3102970				3235785	3890480
ecdonald 1 nist-p-224	6685121				6834310	8273255
ecdonald 1 nist-p-256	7825300				8008415	9829140
ecdonald 1 nist-p-384	19546105				19419785	23784000
ecdonald 1 nist-p-521	25049305				25493885	30856230
ecdonald 1 secp160r1	3888792				4017225	4834285
nistp256-sss-ultrasparc 1	2537798	2508656				
ntru-enc 1 ees787ep1	228165134		1112753	2077547		
rainbow 1	290051669				1869590	3541974
ronald 1 768	127351190		265287	5368945	5403770	231295
ronald 1 832	228669710		285383	6946490	7076635	246348
ronald 1 896	201386195		305215	7541920	7582345	264127
ronald 1 960	206794525		325238	9658295	9659065	279292
ronald 1 1024	160994960		365075	10555710	10521160	314945
ronald 1 1088	366382314		430420	12979820	13146145	374307
ronald 1 1152	392264835		443450	13987680	14011450	390625
ronald 1 1216	371566154		463525	16950710	16926620	406060
ronald 1 1280	922591519		496309	18044617	18088720	424660
ronald 1 1344	453683014		508795	21627655	21726870	445480
ronald 1 1408	397234940		530320	22896900	22985480	465527
ronald 1 1472	1187468046		559068	27221775	27294480	484165
ronald 1 1536	674162729		586813	28595650	28586510	502860
ronald 1 1664	1072243855		639340	35215145	35393800	561870
ronald 1 1792	919567944		686955	43116075	42897420	602330
ronald 1 1920	2187864660		745130	51752450	51928285	658361
ronald 1 2048	2472010304		805427	59999760	60096795	707085
ronald 1 2176	2507926780		1002160	76248270	76724539	888955
ronald 1 2304	2669440884		1055885	87414785	86991459	948280

ronald 1 2432	3955742816	1125955	99752135	100309655	1013800
ronald 1 2560	4398641725	1202475	114268130	114380730	1080562
ronald 1 2688	5610626515	1267515	129243409	128687640	1146630
ronald 1 2816	8620413635	1346890	146560804	146170940	1225195
ronald 1 2944	8817263126	1435171	164542120	164803420	1301766
ronald 1 3072	9817537250	1509723	183293660	184288355	1373837
ronald 1 3328	13381631439	1712046	231755265	230796120	1575050
ronald 1 3584	25443046271	1900300	284508135	282217634	1748845
ronald 1 3840	24930095865	2090458	338299130	342940984	1931960
ronald 1 4096	31320074945	2272850	385920135	383028819	2102770
ronald 2 768	101501695	236562	5430630	5414070	218390
ronald 2 832	153784175	260830	7035090	7036290	238447
ronald 2 896	121440094	278525	7630415	7651310	256130
ronald 2 960	186257400	298437	9591105	9635410	271780
ronald 2 1024	297855340	332760	10492965	10490810	298920
ronald 2 1088	400291029	395805	13004480	13089160	356682
ronald 2 1152	330591305	415075	13977745	13987735	373945
ronald 2 1216	416480880	437963	17054165	16934500	396475
ronald 2 1280	652043009	457123	18005863	18120200	408296
ronald 2 1344	403162689	480975	21710410	21774135	428418
ronald 2 1408	614450369	499968	22758600	22860145	454100
ronald 2 1472	756130425	527050	27355865	27233410	467550
ronald 2 1536	575225434	552425	28602585	32225835	584352
ronald 2 1664	1130440330	608682	35768765	35512370	540630
ronald 2 1792	1723036885	652230	42778475	42906610	585509
ronald 2 1920	1504125480	716154	52010450	51654440	640133
ronald 2 2048	1501296785	774320	60846320	60867745	691242
ronald 2 2176	2712461475	1000520	77580205	76729680	875528
ronald 2 2304	2292215800	1033667	87817040	88011034	929535
ronald 2 2432	5363890885	1091975	100650320	100867300	997587
ronald 2 2560	6850556575	1173158	115004900	115484820	1061553
ronald 2 2688	3077862635	1242127	129442425	130514690	1128700
ronald 2 2816	8536246540	1319867	146575925	145867185	1200648
ronald 2 2944	7021680040	1403493	165427370	165848995	1281293
ronald 2 3072	10837980680	1487040	185213555	185332330	1352090
ronald 2 3328	12476445930	1682270	231398775	232292674	1566682
ronald 2 3584	19885462365	1874220	297269014	288877474	1736960
ronald 2 3840	27598424445	2087100	341591849	340562714	1926560
ronald 2 4096	20530325425	2245710	387585354	390761959	2078590
ronald 3 768	156640115	235462	5369721	5346580	204015
ronald 3 832	126564175	254216	6915965	6909200	219695
ronald 3 896	134750350	275180	7671875	7698847	241870
ronald 3 960	294601070	295145	9611880	9599850	256390
ronald 3 1024	206882471	330033	10560765	10594210	280698
ronald 3 1088	381551745	392960	12968030	12956205	340030
ronald 3 1152	282079055	413215	13921985	13921240	357219
ronald 3 1216	549912605	434515	16925650	16970035	375035

ronald 3 1280	468684125	456180	17875707	17886730	395945
ronald 3 1344	547686250	474995	21695200	21811385	412180
ronald 3 1408	754684649	493290	22830987	22765485	430279
ronald 3 1472	599177799	525227	27429267	27332560	454965
ronald 3 1536	871415425	545709	28724150	28651460	470575
ronald 3 1664	1182346141	600580	35275260	35215333	524420
ronald 3 1792	1369716645	655487	43052330	43013815	573090
ronald 3 1920	2179604080	710990	51969916	52041369	618955
ronald 3 2048	1675234930	770920	59961745	59888920	671245
ronald 3 2176	3587450540	963320	76210925	76218885	856182
ronald 3 2304	4086324815	1032852	87381407	87550093	922537
ronald 3 2432	4808535855	1099790	100036545	100541530	979838
ronald 3 2560	4491678500	1165190	114918069	115408139	1043875
ronald 3 2688	8972287950	1244038	129689280	130780214	1118355
ronald 3 2816	9770840010	1319200	147719580	146509369	1201627
ronald 3 2944	8941877795	1402737	165820352	166035254	1271410
ronald 3 3072	26062228620	1483240	184802945	186416509	1347117
ronald 3 3328	12647448560	1681232	231140305	231290245	1530470
ronald 3 3584	18916691151	1858496	281165575	281777979	1704840
ronald 3 3840	31643534335	2085970	341388084	341248270	1903090
ronald 3 4096	17124916569	2310165	387511810	385519935	2059532
sflashv2 1	913592370			4803585	1496065
sflashv2 2	843947315			398823	511195

System	secret key bytes	public key bytes	shared secret bytes	23-byte encrypt bytes	709-byte encrypt bytes	23-byte signed bytes	709-byte signed bytes
claus 1	256	128	128				
claus++ 1	256	128	128				
donald 1 512	84	64				63	749
donald 1 1024	148	128				63	749
donald 1 2048	276	256				63	749
ecdonald 1 nist-b-163	63	42				65	751
ecdonald 1 nist-b-233	90	60				83	769
ecdonald 1 nist-b-283	108	72				95	781
ecdonald 1 nist-b-409	156	104				127	813
ecdonald 1 nist-b-571	216	144				167	853
ecdonald 1 nist-k-163	63	42				65	751
ecdonald 1 nist-k-233	90	60				83	769
ecdonald 1 nist-k-283	108	72				95	781
ecdonald 1 nist-k-409	156	104				127	813
ecdonald 1 nist-k-571	216	144				167	853
ecdonald 1 nist-p-192	72	48				71	757
ecdonald 1 nist-p-224	84	56				79	765
ecdonald 1 nist-p-256	96	64				87	773
ecdonald 1 nist-p-384	144	96				119	805
ecdonald 1 nist-p-521	198	132				155	841

ecdonald 1 secp160r1	60	40				63	749
nistp256-sss-ultrasparc 1	32	64	32				
ntru-enc 1 ees787ep1	1854	1574		1574	2282		
rainbow 1	20107	31680				66	752
ronald 1 768	768	96		119	805	119	805
ronald 1 832	832	104		127	813	127	813
ronald 1 896	896	112		135	821	135	821
ronald 1 960	960	120		143	829	143	829
ronald 1 1024	1024	128		151	837	151	837
ronald 1 1088	1088	136		159	845	159	845
ronald 1 1152	1152	144		167	853	167	853
ronald 1 1216	1216	152		175	861	175	861
ronald 1 1280	1280	160		183	869	183	869
ronald 1 1344	1344	168		191	877	191	877
ronald 1 1408	1408	176		199	885	199	885
ronald 1 1472	1472	184		207	893	207	893
ronald 1 1536	1536	192		215	901	215	901
ronald 1 1664	1664	208		231	917	231	917
ronald 1 1792	1792	224		247	933	247	933
ronald 1 1920	1920	240		263	949	263	949
ronald 1 2048	2048	256		279	965	279	965
ronald 1 2176	2176	272		295	981	295	981
ronald 1 2304	2304	288		311	997	311	997
ronald 1 2432	2432	304		327	1013	327	1013
ronald 1 2560	2560	320		343	1029	343	1029
ronald 1 2688	2688	336		359	1045	359	1045
ronald 1 2816	2816	352		375	1061	375	1061
ronald 1 2944	2944	368		391	1077	391	1077
ronald 1 3072	3072	384		407	1093	407	1093
ronald 1 3328	3328	416		439	1125	439	1125
ronald 1 3584	3584	448		471	1157	471	1157
ronald 1 3840	3840	480		503	1189	503	1189
ronald 1 4096	4096	512		535	1221	535	1221
ronald 2 768	768	96		96	784	119	805
ronald 2 832	832	104		104	784	127	813
ronald 2 896	896	112		112	784	135	821
ronald 2 960	960	120		120	784	143	829
ronald 2 1024	1024	128		128	784	151	837
ronald 2 1088	1088	136		136	784	159	845
ronald 2 1152	1152	144		144	784	167	853
ronald 2 1216	1216	152		152	784	175	861
ronald 2 1280	1280	160		160	784	183	869
ronald 2 1344	1344	168		168	784	191	877
ronald 2 1408	1408	176		176	784	199	885
ronald 2 1472	1472	184		184	784	207	893
ronald 2 1536	1536	192		192	784	215	901
ronald 2 1664	1664	208		208	784	231	917

ronald 2 1792	1792	224	224	784	247	933
ronald 2 1920	1920	240	240	784	263	949
ronald 2 2048	2048	256	256	784	279	965
ronald 2 2176	2176	272	272	784	295	981
ronald 2 2304	2304	288	288	784	311	997
ronald 2 2432	2432	304	304	784	327	1013
ronald 2 2560	2560	320	320	784	343	1029
ronald 2 2688	2688	336	336	784	359	1045
ronald 2 2816	2816	352	352	784	375	1061
ronald 2 2944	2944	368	368	784	391	1077
ronald 2 3072	3072	384	384	784	407	1093
ronald 2 3328	3328	416	416	784	439	1125
ronald 2 3584	3584	448	448	784	471	1157
ronald 2 3840	3840	480	480	784	503	1189
ronald 2 4096	4096	512	512	784	535	1221
ronald 3 768	768	96	96	784	96	752
ronald 3 832	832	104	104	784	104	752
ronald 3 896	896	112	112	784	112	752
ronald 3 960	960	120	120	784	120	752
ronald 3 1024	1024	128	128	784	128	752
ronald 3 1088	1088	136	136	784	136	752
ronald 3 1152	1152	144	144	784	144	752
ronald 3 1216	1216	152	152	784	152	752
ronald 3 1280	1280	160	160	784	160	752
ronald 3 1344	1344	168	168	784	168	752
ronald 3 1408	1408	176	176	784	176	752
ronald 3 1472	1472	184	184	784	184	752
ronald 3 1536	1536	192	192	784	192	752
ronald 3 1664	1664	208	208	784	208	752
ronald 3 1792	1792	224	224	784	224	752
ronald 3 1920	1920	240	240	784	240	752
ronald 3 2048	2048	256	256	784	256	752
ronald 3 2176	2176	272	272	784	272	752
ronald 3 2304	2304	288	288	784	288	752
ronald 3 2432	2432	304	304	784	304	752
ronald 3 2560	2560	320	320	784	320	752
ronald 3 2688	2688	336	336	784	336	752
ronald 3 2816	2816	352	352	784	352	752
ronald 3 2944	2944	368	368	784	368	752
ronald 3 3072	3072	384	384	784	384	752
ronald 3 3328	3328	416	416	784	416	752
ronald 3 3584	3584	448	448	784	448	752
ronald 3 3840	3840	480	480	784	480	752
ronald 3 4096	4096	512	512	784	512	752
sflashv2 1	2823	19266			60	746
sflashv2 2	2823	19266			60	746

6.11 x86, 800MHz, Pentium M (6d8), `atlas`

System	key-pair cycles	share cycles	encrypt cycles	decrypt cycles	sign cycles	verify cycles
`bls 1`	12519873				1935029	23016571
`claus 1`	16298564	16234910				
`claus++ 1`	13979950	13951590				
`curve25519-gaudry 1`	1711061	1707794				
`donald 1 512`	1014277				1018063	1210083
`donald 1 1024`	2939180				2778564	3329580
`donald 1 2048`	9432502				8775306	10720888
`ecdonald 1 nist-b-163`	4118919				4236064	8349757
`ecdonald 1 nist-b-233`	8319792				8475611	16828310
`ecdonald 1 nist-b-283`	15419969				15523294	31278269
`ecdonald 1 nist-b-409`	38253748				38461687	76779995
`ecdonald 1 nist-b-571`	89763862				90295982	180116802
`ecdonald 1 nist-k-163`	3799334				3892188	7675487
`ecdonald 1 nist-k-233`	7442523				7605857	15108644
`ecdonald 1 nist-k-283`	13671257				13987845	28054792
`ecdonald 1 nist-k-409`	33055564				33542401	66897838
`ecdonald 1 nist-k-571`	78346819				78754343	157249846
`ecdonald 1 nist-p-192`	2926741				3075466	3642745
`ecdonald 1 nist-p-224`	3917547				4030191	4880548
`ecdonald 1 nist-p-256`	4998833				5198116	6219906
`ecdonald 1 nist-p-384`	12239286				12540679	15065482
`ecdonald 1 nist-p-521`	25527384				25799137	31252932
`ecdonald 1 secp160r1`	3096625				3223032	3874206
`ntru-enc 1 ees787ep1`	98915423		626870	1109490		
`rainbow 1`	229929237				931871	1713957
`ronald 1 768`	79950803		144158	4381958	4401624	129074
`ronald 1 832`	154306691		156103	5175536	5215413	139248
`ronald 1 896`	135396688		164564	6066473	6098099	149082
`ronald 1 960`	209745996		177064	7061011	7074299	156759
`ronald 1 1024`	115036205		179649	7372331	7354424	161502
`ronald 1 1088`	219322030		226278	9486016	9464790	203014
`ronald 1 1152`	359131740		235997	10680627	10765500	214625
`ronald 1 1216`	452283186		249489	12050637	12067707	224527
`ronald 1 1280`	308491312		256486	13427423	13393799	230698
`ronald 1 1344`	340491304		267562	15000338	14979851	241964
`ronald 1 1408`	514101705		280588	16740407	16781662	254405
`ronald 1 1472`	587402603		296956	18624134	18565529	267874
`ronald 1 1536`	654013129		303031	19077545	19018457	272899
`ronald 1 1664`	694255148		340031	23955648	23968399	308243
`ronald 1 1792`	1170709845		362861	28680760	28640203	326954
`ronald 1 1920`	1174568560		396294	33883498	33878472	360000
`ronald 1 2048`	1533417588		422563	38446696	38521844	384119
`ronald 1 2176`	1838673692		547424	45707206	45825631	505781

ronald 1 2304	1209162149	577256	52390808	52456397	530122
ronald 1 2432	3045475640	614884	60270848	60310170	570282
ronald 1 2560	2888933969	646853	65898371	65972839	595057
ronald 1 2688	4112131017	698426	74364480	74462697	647142
ronald 1 2816	3888640861	727024	84276083	84099061	678203
ronald 1 2944	3326817560	775112	95066025	95321046	721054
ronald 1 3072	5782076023	810171	101313659	101445823	750584
ronald 1 3328	6749432015	916903	129546898	129329522	858128
ronald 1 3584	12519493308	1009731	152733034	152224338	942042
ronald 1 3840	10944118560	1114041	185169544	185451480	1042404
ronald 1 4096	12194809923	1219000	224384732	222472983	1143458
ronald 2 768	136658562	126347	4391749	4401081	123998
ronald 2 832	171776833	139439	5193514	5181777	135696
ronald 2 896	146702645	146945	6109578	6073832	143447
ronald 2 960	157644535	158480	7038106	7028096	152646
ronald 2 1024	123995525	163353	7350951	7341823	156924
ronald 2 1088	179215477	208093	9438110	9488085	199216
ronald 2 1152	235174753	218113	10700551	10678637	208779
ronald 2 1216	267548279	229433	12023849	12048468	220066
ronald 2 1280	370074998	236303	13376323	13336651	225594
ronald 2 1344	456422844	252383	14964348	15072448	237236
ronald 2 1408	442953941	264240	16612470	16604141	250543
ronald 2 1472	454919152	280713	18617010	18632161	262877
ronald 2 1536	683089245	285442	19123698	19559071	268464
ronald 2 1664	831460908	321649	23949879	23996148	303614
ronald 2 1792	734381991	344720	28727108	28604478	322093
ronald 2 1920	1277469199	380550	33979961	33798272	355304
ronald 2 2048	1186369493	404591	38640944	38546909	377749
ronald 2 2176	1767827286	530352	46078433	46201118	500781
ronald 2 2304	1395510566	562856	52744726	52543708	530265
ronald 2 2432	2878810643	600634	60923829	60648131	563726
ronald 2 2560	1782128088	627325	66408351	66101618	590480
ronald 2 2688	4280519916	675573	74884637	74938156	640184
ronald 2 2816	5917407360	707184	84699613	84272302	668028
ronald 2 2944	4120258969	757127	95798295	95941974	715551
ronald 2 3072	4869463356	789350	103012738	102803677	745852
ronald 2 3328	6636352968	898423	130756137	130921146	849785
ronald 2 3584	7142884206	993428	152859700	152756407	938088
ronald 2 3840	13217415727	1094138	185292563	185606039	1038898
ronald 2 4096	11738663936	1200855	222739616	222053393	1136079
ronald 3 768	87823175	127076	4366444	4374049	118226
ronald 3 832	95063051	138820	5171750	5163582	126609
ronald 3 896	124481323	147582	6057209	6047707	137310
ronald 3 960	136109520	157932	7023353	7022120	145806
ronald 3 1024	145988655	161340	7335460	7323515	148659
ronald 3 1088	319276087	207902	9427170	9425119	192135
ronald 3 1152	358742118	220170	10664166	10666384	201731

`ronald 3 1216`	320170227		229240	11955320	11942787	212427
`ronald 3 1280`	440351130		237286	13286659	13313601	218584
`ronald 3 1344`	466712946		250943	14907614	14891107	229539
`ronald 3 1408`	646356214		262929	16544949	16557012	240467
`ronald 3 1472`	507982732		279913	18434169	18525197	254531
`ronald 3 1536`	453731142		285473	19007671	19014224	261441
`ronald 3 1664`	1079978006		323150	23959794	23991940	294178
`ronald 3 1792`	982068250		344968	28586539	28646853	314241
`ronald 3 1920`	1174842162		378343	34064494	33913624	346838
`ronald 3 2048`	1133014758		403880	38656853	38658742	370911
`ronald 3 2176`	1934341374		528229	45963716	45845049	491561
`ronald 3 2304`	2504517280		557651	52850296	52783086	518121
`ronald 3 2432`	2267262054		602934	60633864	60820726	561846
`ronald 3 2560`	4541864082		628371	66618613	65720299	582279
`ronald 3 2688`	2873627880		678472	74426645	74427280	630521
`ronald 3 2816`	2506246539		707058	84364802	84370145	659027
`ronald 3 2944`	6320131388		754889	94710513	94682793	707179
`ronald 3 3072`	5824950261		789248	101548945	102003206	737278
`ronald 3 3328`	6052125389		898038	129393472	129536005	843966
`ronald 3 3584`	6839192234		991838	152279714	153044108	928481
`ronald 3 3840`	15312871344		1095012	185747170	185491926	1026652
`ronald 3 4096`	14563958694		1201643	223824666	222797417	1129497
`sflashv2 1`	373680415				1131395	384894
`sflashv2 2`	360827591				236302	324485
`surf127eps 1`	1865400	1869713				

System	secret key bytes	public key bytes	shared secret bytes	23-byte encrypt bytes	709-byte encrypt bytes	23-byte signed bytes	709-byte signed bytes
`bls 1`	20	120				43	729
`claus 1`	256	128	128				
`claus++ 1`	256	128	128				
`curve25519-gaudry 1`	32	32	32				
`donald 1 512`	84	64				63	749
`donald 1 1024`	148	128				63	749
`donald 1 2048`	276	256				63	749
`ecdonald 1 nist-b-163`	63	42				65	751
`ecdonald 1 nist-b-233`	90	60				83	769
`ecdonald 1 nist-b-283`	108	72				95	781
`ecdonald 1 nist-b-409`	156	104				127	813
`ecdonald 1 nist-b-571`	216	144				167	853
`ecdonald 1 nist-k-163`	63	42				65	751
`ecdonald 1 nist-k-233`	90	60				83	769
`ecdonald 1 nist-k-283`	108	72				95	781
`ecdonald 1 nist-k-409`	156	104				127	813
`ecdonald 1 nist-k-571`	216	144				167	853
`ecdonald 1 nist-p-192`	72	48				71	757

ecdonald 1 nist-p-224	84	56			79	765
ecdonald 1 nist-p-256	96	64			87	773
ecdonald 1 nist-p-384	144	96			119	805
ecdonald 1 nist-p-521	198	132			155	841
ecdonald 1 secp160r1	60	40			63	749
ntru-enc 1 ees787ep1	1854	1574	1574	2282		
rainbow 1	20107	31680			66	752
ronald 1 768	768	96	119	805	119	805
ronald 1 832	832	104	127	813	127	813
ronald 1 896	896	112	135	821	135	821
ronald 1 960	960	120	143	829	143	829
ronald 1 1024	1024	128	151	837	151	837
ronald 1 1088	1088	136	159	845	159	845
ronald 1 1152	1152	144	167	853	167	853
ronald 1 1216	1216	152	175	861	175	861
ronald 1 1280	1280	160	183	869	183	869
ronald 1 1344	1344	168	191	877	191	877
ronald 1 1408	1408	176	199	885	199	885
ronald 1 1472	1472	184	207	893	207	893
ronald 1 1536	1536	192	215	901	215	901
ronald 1 1664	1664	208	231	917	231	917
ronald 1 1792	1792	224	247	933	247	933
ronald 1 1920	1920	240	263	949	263	949
ronald 1 2048	2048	256	279	965	279	965
ronald 1 2176	2176	272	295	981	295	981
ronald 1 2304	2304	288	311	997	311	997
ronald 1 2432	2432	304	327	1013	327	1013
ronald 1 2560	2560	320	343	1029	343	1029
ronald 1 2688	2688	336	359	1045	359	1045
ronald 1 2816	2816	352	375	1061	375	1061
ronald 1 2944	2944	368	391	1077	391	1077
ronald 1 3072	3072	384	407	1093	407	1093
ronald 1 3328	3328	416	439	1125	439	1125
ronald 1 3584	3584	448	471	1157	471	1157
ronald 1 3840	3840	480	503	1189	503	1189
ronald 1 4096	4096	512	535	1221	535	1221
ronald 2 768	768	96	96	784	119	805
ronald 2 832	832	104	104	784	127	813
ronald 2 896	896	112	112	784	135	821
ronald 2 960	960	120	120	784	143	829
ronald 2 1024	1024	128	128	784	151	837
ronald 2 1088	1088	136	136	784	159	845
ronald 2 1152	1152	144	144	784	167	853
ronald 2 1216	1216	152	152	784	175	861
ronald 2 1280	1280	160	160	784	183	869
ronald 2 1344	1344	168	168	784	191	877
ronald 2 1408	1408	176	176	784	199	885

`ronald 2 1472`	1472	184	184	784	207	893
`ronald 2 1536`	1536	192	192	784	215	901
`ronald 2 1664`	1664	208	208	784	231	917
`ronald 2 1792`	1792	224	224	784	247	933
`ronald 2 1920`	1920	240	240	784	263	949
`ronald 2 2048`	2048	256	256	784	279	965
`ronald 2 2176`	2176	272	272	784	295	981
`ronald 2 2304`	2304	288	288	784	311	997
`ronald 2 2432`	2432	304	304	784	327	1013
`ronald 2 2560`	2560	320	320	784	343	1029
`ronald 2 2688`	2688	336	336	784	359	1045
`ronald 2 2816`	2816	352	352	784	375	1061
`ronald 2 2944`	2944	368	368	784	391	1077
`ronald 2 3072`	3072	384	384	784	407	1093
`ronald 2 3328`	3328	416	416	784	439	1125
`ronald 2 3584`	3584	448	448	784	471	1157
`ronald 2 3840`	3840	480	480	784	503	1189
`ronald 2 4096`	4096	512	512	784	535	1221
`ronald 3 768`	768	96	96	784	96	752
`ronald 3 832`	832	104	104	784	104	752
`ronald 3 896`	896	112	112	784	112	752
`ronald 3 960`	960	120	120	784	120	752
`ronald 3 1024`	1024	128	128	784	128	752
`ronald 3 1088`	1088	136	136	784	136	752
`ronald 3 1152`	1152	144	144	784	144	752
`ronald 3 1216`	1216	152	152	784	152	752
`ronald 3 1280`	1280	160	160	784	160	752
`ronald 3 1344`	1344	168	168	784	168	752
`ronald 3 1408`	1408	176	176	784	176	752
`ronald 3 1472`	1472	184	184	784	184	752
`ronald 3 1536`	1536	192	192	784	192	752
`ronald 3 1664`	1664	208	208	784	208	752
`ronald 3 1792`	1792	224	224	784	224	752
`ronald 3 1920`	1920	240	240	784	240	752
`ronald 3 2048`	2048	256	256	784	256	752
`ronald 3 2176`	2176	272	272	784	272	752
`ronald 3 2304`	2304	288	288	784	288	752
`ronald 3 2432`	2432	304	304	784	304	752
`ronald 3 2560`	2560	320	320	784	320	752
`ronald 3 2688`	2688	336	336	784	336	752
`ronald 3 2816`	2816	352	352	784	352	752
`ronald 3 2944`	2944	368	368	784	368	752
`ronald 3 3072`	3072	384	384	784	384	752
`ronald 3 3328`	3328	416	416	784	416	752
`ronald 3 3584`	3584	448	448	784	448	752
`ronald 3 3840`	3840	480	480	784	480	752
`ronald 3 4096`	4096	512	512	784	512	752

sflashv2 1	2823	19266			60	746
sflashv2 2	2823	19266			60	746
surf127eps 1	32	48	48			

6.12 x86, 900MHz, Athlon (622), thoth

System	key-pair cycles	share cycles	encrypt cycles	decrypt cycles	sign cycles	verify cycles
claus 1	17658909	17564346				
claus++ 1	10309719	10241370				
curve25519-gaudry 1	1511685	1494930				
donald 1 512	1125957				1081050	1352418
donald 1 1024	3171651				2990808	3642624
donald 1 2048	10374462				9727110	11601270
ecdonald 1 nist-b-163	4409337				4543605	8888409
ecdonald 1 nist-b-233	8753139				8922639	17702271
ecdonald 1 nist-b-283	16477086				16659900	33645033
ecdonald 1 nist-b-409	40229982				40502877	80823948
ecdonald 1 nist-b-571	91748565				92441097	185013954
ecdonald 1 nist-k-163	4053139				4203834	8165937
ecdonald 1 nist-k-233	7841655				8077941	16009221
ecdonald 1 nist-k-283	14403660				14767944	29960691
ecdonald 1 nist-k-409	35215461				35526285	70673634
ecdonald 1 nist-k-571	81083880				81403965	162671940
ecdonald 1 nist-p-192	3213966				3341610	3988152
ecdonald 1 nist-p-224	4120488				4340187	5113044
ecdonald 1 nist-p-256	4853284				5061027	6033777
ecdonald 1 nist-p-384	12351900				12442995	15053301
ecdonald 1 nist-p-521	25357293				25625796	31130217
ecdonald 1 secp160r1	3538149				3630759	4372254
ntru-enc 1 ees787ep1	179100898		612651	1124721		
rainbow 1	255411878				1115631	1906029
ronald 1 768	127513545		153936	4564686	4578087	137955
ronald 1 832	138364374		163162	5414484	5419434	151616
ronald 1 896	148798881		170926	6324747	6335412	157623
ronald 1 960	162130122		181542	7242495	7283622	165369
ronald 1 1024	207327429		189732	7676991	7639818	174495
ronald 1 1088	219633543		233285	10076496	10146186	212665
ronald 1 1152	321399702		239624	11375136	11414430	218569
ronald 1 1216	218222064		248174	12747009	12765789	223929
ronald 1 1280	377735802		261348	14055921	14118747	242396
ronald 1 1344	406824696		280142	15905013	16041216	252965
ronald 1 1408	586628478		290585	17597334	17647944	268223
ronald 1 1472	586327842		304760	19453812	19686987	278051
ronald 1 1536	809601675		317718	21590766	21593697	285017
ronald 1 1664	1002717774		347052	27157017	27197226	320487
ronald 1 1792	1176266340		376852	32022196	32178807	350172

ronald 1 1920	1133702505	415722	37665612	37737867	382169
ronald 1 2048	1974406968	436226	40930176	40881117	406500
ronald 1 2176	2019271382	555296	56710854	56623698	514493
ronald 1 2304	1755543384	583440	59974200	60057495	549223
ronald 1 2432	3078536067	636493	69227649	69464151	590433
ronald 1 2560	4116567633	673778	78961950	78911427	630948
ronald 1 2688	4063642794	724329	88811739	89554251	678968
ronald 1 2816	8180348058	772470	99973008	99937728	716885
ronald 1 2944	5934095658	815552	112172790	112552137	766677
ronald 1 3072	7394838804	856104	124554816	124773333	818273
ronald 1 3328	8631421992	983007	155483493	155155158	934449
ronald 1 3584	9752643171	1120047	187511445	187922988	1062518
ronald 1 3840	12683287602	1203797	226791888	226762767	1149393
ronald 1 4096	15518198718	1374039	245499921	245463147	1320768
ronald 2 768	154105182	130572	4578123	4606095	129633
ronald 2 832	131900994	148430	5449452	5457087	138870
ronald 2 896	148576716	154885	6312416	6316897	146897
ronald 2 960	150043713	161331	7242834	7264314	154655
ronald 2 1024	165950208	166289	7642125	7656408	160080
ronald 2 1088	284930505	209112	10166166	10136079	197313
ronald 2 1152	372211218	220041	11484522	11511945	204408
ronald 2 1216	485053308	232029	12852342	12892668	215923
ronald 2 1280	492261309	239311	14174697	14144697	225813
ronald 2 1344	744150627	254401	15924384	16003188	240720
ronald 2 1408	583361838	267371	17584638	17632542	253338
ronald 2 1472	862646490	279537	19824204	19721433	261209
ronald 2 1536	640557378	292276	21675585	22220442	274906
ronald 2 1664	860934078	332082	27251127	27268326	311104
ronald 2 1792	793613943	356071	32174064	32147100	331945
ronald 2 1920	1336987359	394673	37813932	37833255	371097
ronald 2 2048	1148954940	417472	40929618	40896537	389980
ronald 2 2176	2692999152	530472	52964406	53037531	501266
ronald 2 2304	3082652730	563855	59995908	60452757	535875
ronald 2 2432	3074218587	613667	69446043	69351633	577136
ronald 2 2560	4831605189	652882	78799470	78908094	626909
ronald 2 2688	4153370022	701634	88887636	88992342	666794
ronald 2 2816	5649021072	758079	99752319	99894834	705741
ronald 2 2944	5985429885	793822	113182617	113064771	759830
ronald 2 3072	6366382461	840586	124768842	124583634	792698
ronald 2 3328	8142696882	965189	155144448	155591727	915651
ronald 2 3584	12988175589	1135631	188117004	187985640	1038507
ronald 2 3840	15799287105	1264650	226232169	226501524	1150407
ronald 2 4096	11852527266	1352018	245667234	245923890	1293907
ronald 3 768	127866939	127077	4597002	4614057	116382
ronald 3 832	134560146	142367	5384313	5424135	128079
ronald 3 896	101788239	148260	6287076	6302232	134622
ronald 3 960	247998474	157000	7224465	7184484	141822

ronald 3 1024	316537767		163652	7650294	7683375	146067
ronald 3 1088	324016578		205691	10164744	10187820	185291
ronald 3 1152	308381796		218310	11506803	11517009	194451
ronald 3 1216	328625649		227854	12832227	12850263	205921
ronald 3 1280	625419012		237194	14155641	14169471	214210
ronald 3 1344	451963818		255055	15928128	15873399	232554
ronald 3 1408	380261307		267055	17739459	17731062	241422
ronald 3 1472	464447214		288822	20368974	19709991	256857
ronald 3 1536	599854968		286657	22357059	21644211	261980
ronald 3 1664	1010086362		325737	27218754	27176382	292643
ronald 3 1792	1331973441		361076	32125914	32191911	326138
ronald 3 1920	1415075517		391320	37909188	37972476	353827
ronald 3 2048	1045333818		414242	40924647	40848561	374418
ronald 3 2176	2245522122		529548	53198190	53083908	485671
ronald 3 2304	2809471914		558526	60262182	60257577	519045
ronald 3 2432	3290370786		605433	69423444	69504129	556239
ronald 3 2560	4924982718		653627	78828318	78878559	602685
ronald 3 2688	4297002480		707313	89110818	89182278	649074
ronald 3 2816	4586085342		742716	100071141	99641175	691938
ronald 3 2944	5980498641		801780	112695246	112677102	737709
ronald 3 3072	4216497156		840942	124599561	124512948	791181
ronald 3 3328	10637517636		958202	155360700	155146716	892610
ronald 3 3584	10372738086		1108347	187846659	187667658	1037364
ronald 3 3840	12270052422		1261563	226876590	226408110	1120899
ronald 3 4096	20709645948		1352172	245659830	245633346	1216218
sflashv2 1	863543898				2222634	762399
sflashv2 2	863572852				300354	481085
surf127eps 1	1824483	1814211				

System	secret key bytes	public key bytes	shared secret bytes	23-byte encrypt bytes	709-byte encrypt bytes	23-byte signed bytes	709-byte signed bytes
claus 1	256	128	128				
claus++ 1	256	128	128				
curve25519-gaudry 1	32	32	32				
donald 1 512	84	64				63	749
donald 1 1024	148	128				63	749
donald 1 2048	276	256				63	749
ecdonald 1 nist-b-163	63	42				65	751
ecdonald 1 nist-b-233	90	60				83	769
ecdonald 1 nist-b-283	108	72				95	781
ecdonald 1 nist-b-409	156	104				127	813
ecdonald 1 nist-b-571	216	144				167	853
ecdonald 1 nist-k-163	63	42				65	751
ecdonald 1 nist-k-233	90	60				83	769
ecdonald 1 nist-k-283	108	72				95	781
ecdonald 1 nist-k-409	156	104				127	813

`ecdonald 1 nist-k-571`	216	144			167	853
`ecdonald 1 nist-p-192`	72	48			71	757
`ecdonald 1 nist-p-224`	84	56			79	765
`ecdonald 1 nist-p-256`	96	64			87	773
`ecdonald 1 nist-p-384`	144	96			119	805
`ecdonald 1 nist-p-521`	198	132			155	841
`ecdonald 1 secp160r1`	60	40			63	749
`ntru-enc 1 ees787ep1`	1854	1574	1574	2282		
`rainbow 1`	20107	31680			66	752
`ronald 1 768`	768	96	119	805	119	805
`ronald 1 832`	832	104	127	813	127	813
`ronald 1 896`	896	112	135	821	135	821
`ronald 1 960`	960	120	143	829	143	829
`ronald 1 1024`	1024	128	151	837	151	837
`ronald 1 1088`	1088	136	159	845	159	845
`ronald 1 1152`	1152	144	167	853	167	853
`ronald 1 1216`	1216	152	175	861	175	861
`ronald 1 1280`	1280	160	183	869	183	869
`ronald 1 1344`	1344	168	191	877	191	877
`ronald 1 1408`	1408	176	199	885	199	885
`ronald 1 1472`	1472	184	207	893	207	893
`ronald 1 1536`	1536	192	215	901	215	901
`ronald 1 1664`	1664	208	231	917	231	917
`ronald 1 1792`	1792	224	247	933	247	933
`ronald 1 1920`	1920	240	263	949	263	949
`ronald 1 2048`	2048	256	279	965	279	965
`ronald 1 2176`	2176	272	295	981	295	981
`ronald 1 2304`	2304	288	311	997	311	997
`ronald 1 2432`	2432	304	327	1013	327	1013
`ronald 1 2560`	2560	320	343	1029	343	1029
`ronald 1 2688`	2688	336	359	1045	359	1045
`ronald 1 2816`	2816	352	375	1061	375	1061
`ronald 1 2944`	2944	368	391	1077	391	1077
`ronald 1 3072`	3072	384	407	1093	407	1093
`ronald 1 3328`	3328	416	439	1125	439	1125
`ronald 1 3584`	3584	448	471	1157	471	1157
`ronald 1 3840`	3840	480	503	1189	503	1189
`ronald 1 4096`	4096	512	535	1221	535	1221
`ronald 2 768`	768	96	96	784	119	805
`ronald 2 832`	832	104	104	784	127	813
`ronald 2 896`	896	112	112	784	135	821
`ronald 2 960`	960	120	120	784	143	829
`ronald 2 1024`	1024	128	128	784	151	837
`ronald 2 1088`	1088	136	136	784	159	845
`ronald 2 1152`	1152	144	144	784	167	853
`ronald 2 1216`	1216	152	152	784	175	861
`ronald 2 1280`	1280	160	160	784	183	869

ronald 2 1344	1344	168	168	784	191	877
ronald 2 1408	1408	176	176	784	199	885
ronald 2 1472	1472	184	184	784	207	893
ronald 2 1536	1536	192	192	784	215	901
ronald 2 1664	1664	208	208	784	231	917
ronald 2 1792	1792	224	224	784	247	933
ronald 2 1920	1920	240	240	784	263	949
ronald 2 2048	2048	256	256	784	279	965
ronald 2 2176	2176	272	272	784	295	981
ronald 2 2304	2304	288	288	784	311	997
ronald 2 2432	2432	304	304	784	327	1013
ronald 2 2560	2560	320	320	784	343	1029
ronald 2 2688	2688	336	336	784	359	1045
ronald 2 2816	2816	352	352	784	375	1061
ronald 2 2944	2944	368	368	784	391	1077
ronald 2 3072	3072	384	384	784	407	1093
ronald 2 3328	3328	416	416	784	439	1125
ronald 2 3584	3584	448	448	784	471	1157
ronald 2 3840	3840	480	480	784	503	1189
ronald 2 4096	4096	512	512	784	535	1221
ronald 3 768	768	96	96	784	96	752
ronald 3 832	832	104	104	784	104	752
ronald 3 896	896	112	112	784	112	752
ronald 3 960	960	120	120	784	120	752
ronald 3 1024	1024	128	128	784	128	752
ronald 3 1088	1088	136	136	784	136	752
ronald 3 1152	1152	144	144	784	144	752
ronald 3 1216	1216	152	152	784	152	752
ronald 3 1280	1280	160	160	784	160	752
ronald 3 1344	1344	168	168	784	168	752
ronald 3 1408	1408	176	176	784	176	752
ronald 3 1472	1472	184	184	784	184	752
ronald 3 1536	1536	192	192	784	192	752
ronald 3 1664	1664	208	208	784	208	752
ronald 3 1792	1792	224	224	784	224	752
ronald 3 1920	1920	240	240	784	240	752
ronald 3 2048	2048	256	256	784	256	752
ronald 3 2176	2176	272	272	784	272	752
ronald 3 2304	2304	288	288	784	288	752
ronald 3 2432	2432	304	304	784	304	752
ronald 3 2560	2560	320	320	784	320	752
ronald 3 2688	2688	336	336	784	336	752
ronald 3 2816	2816	352	352	784	352	752
ronald 3 2944	2944	368	368	784	368	752
ronald 3 3072	3072	384	384	784	384	752
ronald 3 3328	3328	416	416	784	416	752
ronald 3 3584	3584	448	448	784	448	752

ronald 3 3840	3840	480		480	784	480	752
ronald 3 4096	4096	512		512	784	512	752
sflashv2 1	2823	19266				60	746
sflashv2 2	2823	19266				60	746
surf127eps 1	32	48	48				

6.13 x86, 1000MHz, Pentium III (68a), neumann

System	key-pair cycles	share cycles	encrypt cycles	decrypt cycles	sign cycles	verify cycles
claus 1	21519279	21472765				
claus++ 1	14891482	14864646				
donald 1 512	1340420				1386929	1651997
donald 1 1024	3872852				3729408	4536323
donald 1 2048	12857022				12023567	14715052
ecdonald 1 nist-b-163	5279516				5421656	10723739
ecdonald 1 nist-b-233	10256500				10467772	20654860
ecdonald 1 nist-b-283	19313946				19613428	39027117
ecdonald 1 nist-b-409	46231569				46764044	93211134
ecdonald 1 nist-b-571	109111113				109841010	219482942
ecdonald 1 nist-k-163	4842930				4991552	9843335
ecdonald 1 nist-k-233	9201713				9436419	18701338
ecdonald 1 nist-k-283	17173717				17426340	34572333
ecdonald 1 nist-k-409	40241485				40656251	81214311
ecdonald 1 nist-k-571	94465884				95180280	190164916
ecdonald 1 nist-p-192	4135804				4275010	5165222
ecdonald 1 nist-p-224	5318039				5513189	6650568
ecdonald 1 nist-p-256	6662984				6899259	8318228
ecdonald 1 nist-p-384	16103671				16442744	19676534
ecdonald 1 nist-p-521	32213765				32803017	39584810
ecdonald 1 secp160r1	4348370				4458932	5392373
ntru-enc 1 ees787ep1	150014461		754068	1337603		
rainbow 1	365360190				1717155	3088425
ronald 1 768	143250337		215141	5837050	5827479	196296
ronald 1 832	195767801		230072	6894088	6895337	208238
ronald 1 896	161468547		242468	7966199	8010049	220946
ronald 1 960	175926889		254955	9211890	9208773	231187
ronald 1 1024	289283227		262036	9799646	9819377	241343
ronald 1 1088	274461883		328466	12651243	12692677	306562
ronald 1 1152	400425271		341502	14323129	14267907	315768
ronald 1 1216	351977034		356730	15997351	15956335	330303
ronald 1 1280	440288585		371521	17843248	17844480	343999
ronald 1 1344	537381048		388112	20061512	20019404	359772
ronald 1 1408	756014621		404113	22102877	22152405	375532
ronald 1 1472	744851977		430495	24426745	24453752	390597
ronald 1 1536	760575608		441263	26596528	26482530	408288
ronald 1 1664	1122679127		490754	32254080	32304941	451140

ronald 1 1792	1330054300	529103	38544658	38471192	483924
ronald 1 1920	1908824393	574076	45309970	45275282	528828
ronald 1 2048	2097296068	607141	50930707	51090588	561176
ronald 1 2176	2618363809	771325	61574707	61306728	726121
ronald 1 2304	3485097554	824114	70095623	70219622	772245
ronald 1 2432	2700453090	876777	80126484	79957989	817800
ronald 1 2560	4399433364	924210	90401322	90378077	866465
ronald 1 2688	3682640963	986524	101884464	101775341	924220
ronald 1 2816	3943135529	1043965	114832775	114700343	977140
ronald 1 2944	5765345895	1097276	129004082	128966860	1038133
ronald 1 3072	5320444168	1160162	144696713	144650745	1086624
ronald 1 3328	10749001216	1305054	181511168	181594205	1236575
ronald 1 3584	12516179057	1447828	217514209	217690589	1369283
ronald 1 3840	23230717830	1593507	261342977	261698080	1510219
ronald 1 4096	23974624941	1724622	297235221	297349381	1629515
ronald 2 768	144057939	192819	5857351	5850889	187988
ronald 2 832	150592833	207808	6909981	6881500	200874
ronald 2 896	156788788	218178	8006663	8020167	212415
ronald 2 960	205073703	228341	9192042	9191077	223086
ronald 2 1024	240946983	239602	9802947	9812862	229592
ronald 2 1088	274041562	305010	12692277	12847216	294859
ronald 2 1152	473298606	319616	14338859	14330436	305433
ronald 2 1216	326495512	332605	16009507	16013354	319708
ronald 2 1280	331869265	347533	17906975	17867714	333067
ronald 2 1344	602398898	365810	20016204	20013479	349787
ronald 2 1408	743160385	382292	22115683	22101601	362846
ronald 2 1472	800342838	402868	24495507	24413089	381483
ronald 2 1536	806002831	421261	26600595	26597335	401154
ronald 2 1664	791128434	469556	32177979	32239218	441976
ronald 2 1792	1269234411	502662	38465772	38456769	474926
ronald 2 1920	2244634307	546164	45276960	45265502	516678
ronald 2 2048	1342826174	586625	51070249	50893784	549043
ronald 2 2176	2151006713	753854	61458644	61515403	713830
ronald 2 2304	2341881243	802776	70306745	70209574	758780
ronald 2 2432	3549293976	852847	80050096	80173794	807442
ronald 2 2560	3404374137	901343	90608036	90706787	851738
ronald 2 2688	2327926345	964877	102077631	101836295	913554
ronald 2 2816	4136307248	1020251	114841160	114660165	963099
ronald 2 2944	6350322343	1081071	128799366	129027687	1021486
ronald 2 3072	4663039350	1138153	144379725	144254145	1072544
ronald 2 3328	14650889684	1284172	180432512	180155133	1214517
ronald 2 3584	19959562936	1427825	217928875	217299515	1351941
ronald 2 3840	15853680912	1569289	261779105	260864716	1489619
ronald 2 4096	26679443475	1696158	296978991	296976824	1614509
ronald 3 768	103717157	192285	5833405	5840075	177695
ronald 3 832	182700398	206509	6880725	6871189	192205
ronald 3 896	202736878	218004	7994860	8012193	202976

ronald 3 960	227964540	230716	9181387	9181509	210543
ronald 3 1024	221409183	240127	9784714	9772014	221571
ronald 3 1088	294827517	305448	12649827	12645560	284741
ronald 3 1152	351980488	317741	14312593	14273144	296813
ronald 3 1216	548495563	331986	15965034	15954437	311078
ronald 3 1280	447974140	346716	17762290	17782017	322061
ronald 3 1344	658599765	366857	19957019	19942372	338819
ronald 3 1408	705081203	381940	22099388	22043735	353601
ronald 3 1472	640282673	401032	24346682	24403660	370931
ronald 3 1536	845385960	418468	26564441	26565936	389149
ronald 3 1664	1072980204	468371	32268172	32237251	431599
ronald 3 1792	919950076	501033	38498791	38401241	464918
ronald 3 1920	1610382514	544912	45085060	45111099	507430
ronald 3 2048	2523146194	582013	50826788	50904988	537597
ronald 3 2176	2556680581	748310	61368908	61402484	704320
ronald 3 2304	2806955317	795894	70152479	69988137	749854
ronald 3 2432	3631565580	849520	79964677	79729821	793710
ronald 3 2560	5230134039	902300	90547521	90494414	843367
ronald 3 2688	2428795035	962702	101844457	101796400	902475
ronald 3 2816	4639235445	1014555	114514746	114604272	952635
ronald 3 2944	6777374385	1076144	128398521	128506043	1011091
ronald 3 3072	8427850530	1136939	145049444	144743649	1062757
ronald 3 3328	9482990884	1283620	181668422	181641254	1210724
ronald 3 3584	13692640917	1427091	217554059	217161000	1343664
ronald 3 3840	19094894790	1561266	260804545	260557574	1478962
ronald 3 4096	22329944134	1698389	296526407	296895713	1602028
sflashv2 1	2228988998			2741033	1622550
sflashv2 2	756002354			292951	410592

System	secret key bytes	public key bytes	shared secret bytes	23-byte encrypt bytes	709-byte encrypt bytes	23-byte signed bytes	709-byte signed bytes
claus 1	256	128	128				
claus++ 1	256	128	128				
donald 1 512	84	64				63	749
donald 1 1024	148	128				63	749
donald 1 2048	276	256				63	749
ecdonald 1 nist-b-163	63	42				65	751
ecdonald 1 nist-b-233	90	60				83	769
ecdonald 1 nist-b-283	108	72				95	781
ecdonald 1 nist-b-409	156	104				127	813
ecdonald 1 nist-b-571	216	144				167	853
ecdonald 1 nist-k-163	63	42				65	751
ecdonald 1 nist-k-233	90	60				83	769
ecdonald 1 nist-k-283	108	72				95	781
ecdonald 1 nist-k-409	156	104				127	813
ecdonald 1 nist-k-571	216	144				167	853

ecdonald 1 nist-p-192	72	48			71	757
ecdonald 1 nist-p-224	84	56			79	765
ecdonald 1 nist-p-256	96	64			87	773
ecdonald 1 nist-p-384	144	96			119	805
ecdonald 1 nist-p-521	198	132			155	841
ecdonald 1 secp160r1	60	40			63	749
ntru-enc 1 ees787ep1	1854	1574	1574	2282		
rainbow 1	20107	31680			66	752
ronald 1 768	768	96	119	805	119	805
ronald 1 832	832	104	127	813	127	813
ronald 1 896	896	112	135	821	135	821
ronald 1 960	960	120	143	829	143	829
ronald 1 1024	1024	128	151	837	151	837
ronald 1 1088	1088	136	159	845	159	845
ronald 1 1152	1152	144	167	853	167	853
ronald 1 1216	1216	152	175	861	175	861
ronald 1 1280	1280	160	183	869	183	869
ronald 1 1344	1344	168	191	877	191	877
ronald 1 1408	1408	176	199	885	199	885
ronald 1 1472	1472	184	207	893	207	893
ronald 1 1536	1536	192	215	901	215	901
ronald 1 1664	1664	208	231	917	231	917
ronald 1 1792	1792	224	247	933	247	933
ronald 1 1920	1920	240	263	949	263	949
ronald 1 2048	2048	256	279	965	279	965
ronald 1 2176	2176	272	295	981	295	981
ronald 1 2304	2304	288	311	997	311	997
ronald 1 2432	2432	304	327	1013	327	1013
ronald 1 2560	2560	320	343	1029	343	1029
ronald 1 2688	2688	336	359	1045	359	1045
ronald 1 2816	2816	352	375	1061	375	1061
ronald 1 2944	2944	368	391	1077	391	1077
ronald 1 3072	3072	384	407	1093	407	1093
ronald 1 3328	3328	416	439	1125	439	1125
ronald 1 3584	3584	448	471	1157	471	1157
ronald 1 3840	3840	480	503	1189	503	1189
ronald 1 4096	4096	512	535	1221	535	1221
ronald 2 768	768	96	96	784	119	805
ronald 2 832	832	104	104	784	127	813
ronald 2 896	896	112	112	784	135	821
ronald 2 960	960	120	120	784	143	829
ronald 2 1024	1024	128	128	784	151	837
ronald 2 1088	1088	136	136	784	159	845
ronald 2 1152	1152	144	144	784	167	853
ronald 2 1216	1216	152	152	784	175	861
ronald 2 1280	1280	160	160	784	183	869
ronald 2 1344	1344	168	168	784	191	877

`ronald 2 1408`	1408	176	176	784	199	885
`ronald 2 1472`	1472	184	184	784	207	893
`ronald 2 1536`	1536	192	192	784	215	901
`ronald 2 1664`	1664	208	208	784	231	917
`ronald 2 1792`	1792	224	224	784	247	933
`ronald 2 1920`	1920	240	240	784	263	949
`ronald 2 2048`	2048	256	256	784	279	965
`ronald 2 2176`	2176	272	272	784	295	981
`ronald 2 2304`	2304	288	288	784	311	997
`ronald 2 2432`	2432	304	304	784	327	1013
`ronald 2 2560`	2560	320	320	784	343	1029
`ronald 2 2688`	2688	336	336	784	359	1045
`ronald 2 2816`	2816	352	352	784	375	1061
`ronald 2 2944`	2944	368	368	784	391	1077
`ronald 2 3072`	3072	384	384	784	407	1093
`ronald 2 3328`	3328	416	416	784	439	1125
`ronald 2 3584`	3584	448	448	784	471	1157
`ronald 2 3840`	3840	480	480	784	503	1189
`ronald 2 4096`	4096	512	512	784	535	1221
`ronald 3 768`	768	96	96	784	96	752
`ronald 3 832`	832	104	104	784	104	752
`ronald 3 896`	896	112	112	784	112	752
`ronald 3 960`	960	120	120	784	120	752
`ronald 3 1024`	1024	128	128	784	128	752
`ronald 3 1088`	1088	136	136	784	136	752
`ronald 3 1152`	1152	144	144	784	144	752
`ronald 3 1216`	1216	152	152	784	152	752
`ronald 3 1280`	1280	160	160	784	160	752
`ronald 3 1344`	1344	168	168	784	168	752
`ronald 3 1408`	1408	176	176	784	176	752
`ronald 3 1472`	1472	184	184	784	184	752
`ronald 3 1536`	1536	192	192	784	192	752
`ronald 3 1664`	1664	208	208	784	208	752
`ronald 3 1792`	1792	224	224	784	224	752
`ronald 3 1920`	1920	240	240	784	240	752
`ronald 3 2048`	2048	256	256	784	256	752
`ronald 3 2176`	2176	272	272	784	272	752
`ronald 3 2304`	2304	288	288	784	288	752
`ronald 3 2432`	2432	304	304	784	304	752
`ronald 3 2560`	2560	320	320	784	320	752
`ronald 3 2688`	2688	336	336	784	336	752
`ronald 3 2816`	2816	352	352	784	352	752
`ronald 3 2944`	2944	368	368	784	368	752
`ronald 3 3072`	3072	384	384	784	384	752
`ronald 3 3328`	3328	416	416	784	416	752
`ronald 3 3584`	3584	448	448	784	448	752
`ronald 3 3840`	3840	480	480	784	480	752

ronald 3 4096	4096	512	512	784	512	752
sflashv2 1	2823	19266			60	746
sflashv2 2	2823	19266			60	746

6.14 x86, 1400MHz, Pentium III (6b1), td152

System	key-pair cycles	share cycles	encrypt cycles	decrypt cycles	sign cycles	verify cycles
claus 1	21007340	20979766				
claus++ 1	14912949	14838496				
curve25519-gaudry 1	1851032	1848128				
donald 1 512	1300408				1326761	1577001
donald 1 1024	3829936				3626841	4390348
donald 1 2048	12845568				11942839	14432699
ecdonald 1 nist-b-163	4543466				4681170	9194456
ecdonald 1 nist-b-233	9087054				9192944	18136414
ecdonald 1 nist-b-283	18210556				18418458	34099563
ecdonald 1 nist-b-409	42472529				43302280	86015197
ecdonald 1 nist-b-571	97627789				97881206	195443898
ecdonald 1 nist-k-163	4133098				4267174	8364135
ecdonald 1 nist-k-233	8176954				8286436	16211569
ecdonald 1 nist-k-283	14967863				15101018	30030318
ecdonald 1 nist-k-409	36336946				36482687	72954598
ecdonald 1 nist-k-571	84440361				84810671	168959688
ecdonald 1 nist-p-192	3758489				3887873	4638691
ecdonald 1 nist-p-224	4920957				5076975	6077406
ecdonald 1 nist-p-256	6133193				6302456	7625411
ecdonald 1 nist-p-384	15041113				15318890	18393637
ecdonald 1 nist-p-521	29746001				29919883	36493802
ecdonald 1 secp160r1	3803589				3915498	4751647
ntru-enc 1 ees787ep1	168344971		1096899	1992370		
rainbow 1	247997008				1175765	2167760
ronald 1 768	134570144		214729	5304666	5330443	197919
ronald 1 832	128255027		232672	6264908	6266621	212252
ronald 1 896	200887486		246050	7331999	7338397	222105
ronald 1 960	191878627		256045	8423757	8400446	232083
ronald 1 1024	202732047		264405	9066349	8968665	241670
ronald 1 1088	277238827		323096	11552854	11575344	298722
ronald 1 1152	363161227		344363	13172494	13099080	314748
ronald 1 1216	366150667		354890	14745992	14724390	327429
ronald 1 1280	630830552		372299	16405683	16427744	344788
ronald 1 1344	454009940		385252	18307489	18418974	357070
ronald 1 1408	485246923		405431	20436746	20434818	375234
ronald 1 1472	787539754		421110	22552074	22566335	387022
ronald 1 1536	894586061		446573	24847920	24697067	408853
ronald 1 1664	1009517271		488959	30087578	30053339	450378
ronald 1 1792	1427766880		529666	36008701	36037476	486169

ronald 1 1920	1624204535	572196	42705054	42500607	524456
ronald 1 2048	1960373874	604783	48055800	48004818	557900
ronald 1 2176	2501246370	777021	60646992	60646853	723105
ronald 1 2304	3235308657	821616	69351356	69306868	769035
ronald 1 2432	3267015414	868888	79171461	79494678	813783
ronald 1 2560	5522579441	924424	89523612	89509951	865678
ronald 1 2688	5503079638	983383	100778484	100599117	920322
ronald 1 2816	3725114726	1042152	113936841	113769972	979087
ronald 1 2944	5888754855	1091939	127454082	127608561	1027969
ronald 1 3072	6451838619	1150314	144418265	144692927	1079686
ronald 1 3328	8432057519	1309039	180055192	179978325	1225320
ronald 1 3584	19719210231	1436771	216538314	216401998	1355818
ronald 1 3840	17284136973	1579674	260012251	261099439	1498811
ronald 1 4096	19958215326	1709304	293125481	293252183	1613949
ronald 2 768	110271705	194747	5303774	5315059	188875
ronald 2 832	203964572	210349	6236368	6212287	199239
ronald 2 896	204262013	219492	7298408	7299123	209354
ronald 2 960	151770006	230984	8378919	8408523	219996
ronald 2 1024	227359818	239178	9037206	8973432	232787
ronald 2 1088	175181879	302909	11675265	11697185	290330
ronald 2 1152	218449762	320048	13231350	13178064	303526
ronald 2 1216	427822760	331450	14842865	14882003	318708
ronald 2 1280	436018951	346714	16510807	16606351	331538
ronald 2 1344	421085060	365577	18312072	18464420	344476
ronald 2 1408	544036245	378657	20516691	20464187	359544
ronald 2 1472	684402810	395773	22577955	22754261	376658
ronald 2 1536	673940623	421061	24805331	24840437	395873
ronald 2 1664	815764819	464051	30054428	30145198	438279
ronald 2 1792	1027013001	502042	35904474	36065145	471780
ronald 2 1920	1646364228	548742	42595305	42711423	512258
ronald 2 2048	1734403625	581835	47952812	47956110	544515
ronald 2 2176	2588321996	748868	60714443	60814399	711856
ronald 2 2304	4048078016	798185	69545149	69543872	753306
ronald 2 2432	3241728283	844328	79496879	79508000	801665
ronald 2 2560	4122198473	898978	89656128	89375018	848068
ronald 2 2688	4153007418	955369	100616229	100590245	908452
ronald 2 2816	5681856518	1010536	113369524	113748345	959525
ronald 2 2944	4445059773	1073304	127991776	128041822	1017387
ronald 2 3072	11822492148	1119749	144371771	144411208	1062800
ronald 2 3328	14706143867	1269989	179080533	179268538	1204152
ronald 2 3584	13511428568	1409889	215509105	215621233	1333208
ronald 2 3840	22737498373	1560826	259582671	259571343	1479534
ronald 2 4096	17715211459	1687126	292327900	292349271	1595891
ronald 3 768	134484257	192872	5286920	5289159	177954
ronald 3 832	211850067	207226	6228377	6249885	190677
ronald 3 896	179876117	217155	7258041	7270857	200148
ronald 3 960	214056318	230446	8375497	8386619	208368

ronald 3 1024	268226055		241095	8924950	8960780	220388
ronald 3 1088	247152024		301508	11625310	11671106	280859
ronald 3 1152	305410401		318231	13139288	13133114	294991
ronald 3 1216	461759332		328489	14685936	14665003	304782
ronald 3 1280	325775133		345425	16433367	16445857	321985
ronald 3 1344	826972598		361992	18303194	18330206	335283
ronald 3 1408	545478167		376027	20316325	20326311	347981
ronald 3 1472	616287013		395611	22451382	22477116	362861
ronald 3 1536	808648797		415796	24681660	24651508	383796
ronald 3 1664	1088661682		460675	29904455	29883387	424841
ronald 3 1792	1100204584		499318	35987676	35978298	460751
ronald 3 1920	2040234261		543670	42367545	42341106	502471
ronald 3 2048	2216306537		581539	48126275	47970209	535265
ronald 3 2176	2184515035		749113	60558971	60580192	697460
ronald 3 2304	3625469197		792652	69218790	69335302	742515
ronald 3 2432	3867803626		844586	79164096	79115205	791134
ronald 3 2560	3540755234		890594	89616739	89689451	835513
ronald 3 2688	3886112256		956238	100639683	100711725	895712
ronald 3 2816	6963142889		1007376	113531599	113608409	942170
ronald 3 2944	5500124077		1065819	127602975	127503171	998220
ronald 3 3072	10592313885		1123103	144328963	144355455	1054517
ronald 3 3328	10555437168		1272592	179100881	179088630	1195464
ronald 3 3584	11276872606		1403706	215263056	215280947	1325087
ronald 3 3840	21566008012		1553207	259510523	259496882	1462518
ronald 3 4096	16284563705		1679300	292736647	292453561	1586040
sflashv2 1	436272879				3895846	2256926
sflashv2 2	412413965				378605	619059
surf127eps 1	2061515	2079384				

System	secret key bytes	public key bytes	shared secret bytes	23-byte encrypt bytes	709-byte encrypt bytes	23-byte signed bytes	709-byte signed bytes
claus 1	256	128	128				
claus++ 1	256	128	128				
curve25519-gaudry 1	32	32	32				
donald 1 512	84	64				63	749
donald 1 1024	148	128				63	749
donald 1 2048	276	256				63	749
ecdonald 1 nist-b-163	63	42				65	751
ecdonald 1 nist-b-233	90	60				83	769
ecdonald 1 nist-b-283	108	72				95	781
ecdonald 1 nist-b-409	156	104				127	813
ecdonald 1 nist-b-571	216	144				167	853
ecdonald 1 nist-k-163	63	42				65	751
ecdonald 1 nist-k-233	90	60				83	769
ecdonald 1 nist-k-283	108	72				95	781
ecdonald 1 nist-k-409	156	104				127	813

`ecdonald 1 nist-k-571`	216	144			167	853
`ecdonald 1 nist-p-192`	72	48			71	757
`ecdonald 1 nist-p-224`	84	56			79	765
`ecdonald 1 nist-p-256`	96	64			87	773
`ecdonald 1 nist-p-384`	144	96			119	805
`ecdonald 1 nist-p-521`	198	132			155	841
`ecdonald 1 secp160r1`	60	40			63	749
`ntru-enc 1 ees787ep1`	1854	1574	1574	2282		
`rainbow 1`	20107	31680			66	752
`ronald 1 768`	768	96	119	805	119	805
`ronald 1 832`	832	104	127	813	127	813
`ronald 1 896`	896	112	135	821	135	821
`ronald 1 960`	960	120	143	829	143	829
`ronald 1 1024`	1024	128	151	837	151	837
`ronald 1 1088`	1088	136	159	845	159	845
`ronald 1 1152`	1152	144	167	853	167	853
`ronald 1 1216`	1216	152	175	861	175	861
`ronald 1 1280`	1280	160	183	869	183	869
`ronald 1 1344`	1344	168	191	877	191	877
`ronald 1 1408`	1408	176	199	885	199	885
`ronald 1 1472`	1472	184	207	893	207	893
`ronald 1 1536`	1536	192	215	901	215	901
`ronald 1 1664`	1664	208	231	917	231	917
`ronald 1 1792`	1792	224	247	933	247	933
`ronald 1 1920`	1920	240	263	949	263	949
`ronald 1 2048`	2048	256	279	965	279	965
`ronald 1 2176`	2176	272	295	981	295	981
`ronald 1 2304`	2304	288	311	997	311	997
`ronald 1 2432`	2432	304	327	1013	327	1013
`ronald 1 2560`	2560	320	343	1029	343	1029
`ronald 1 2688`	2688	336	359	1045	359	1045
`ronald 1 2816`	2816	352	375	1061	375	1061
`ronald 1 2944`	2944	368	391	1077	391	1077
`ronald 1 3072`	3072	384	407	1093	407	1093
`ronald 1 3328`	3328	416	439	1125	439	1125
`ronald 1 3584`	3584	448	471	1157	471	1157
`ronald 1 3840`	3840	480	503	1189	503	1189
`ronald 1 4096`	4096	512	535	1221	535	1221
`ronald 2 768`	768	96	96	784	119	805
`ronald 2 832`	832	104	104	784	127	813
`ronald 2 896`	896	112	112	784	135	821
`ronald 2 960`	960	120	120	784	143	829
`ronald 2 1024`	1024	128	128	784	151	837
`ronald 2 1088`	1088	136	136	784	159	845
`ronald 2 1152`	1152	144	144	784	167	853
`ronald 2 1216`	1216	152	152	784	175	861
`ronald 2 1280`	1280	160	160	784	183	869

ronald 2 1344	1344	168	168	784	191	877
ronald 2 1408	1408	176	176	784	199	885
ronald 2 1472	1472	184	184	784	207	893
ronald 2 1536	1536	192	192	784	215	901
ronald 2 1664	1664	208	208	784	231	917
ronald 2 1792	1792	224	224	784	247	933
ronald 2 1920	1920	240	240	784	263	949
ronald 2 2048	2048	256	256	784	279	965
ronald 2 2176	2176	272	272	784	295	981
ronald 2 2304	2304	288	288	784	311	997
ronald 2 2432	2432	304	304	784	327	1013
ronald 2 2560	2560	320	320	784	343	1029
ronald 2 2688	2688	336	336	784	359	1045
ronald 2 2816	2816	352	352	784	375	1061
ronald 2 2944	2944	368	368	784	391	1077
ronald 2 3072	3072	384	384	784	407	1093
ronald 2 3328	3328	416	416	784	439	1125
ronald 2 3584	3584	448	448	784	471	1157
ronald 2 3840	3840	480	480	784	503	1189
ronald 2 4096	4096	512	512	784	535	1221
ronald 3 768	768	96	96	784	96	752
ronald 3 832	832	104	104	784	104	752
ronald 3 896	896	112	112	784	112	752
ronald 3 960	960	120	120	784	120	752
ronald 3 1024	1024	128	128	784	128	752
ronald 3 1088	1088	136	136	784	136	752
ronald 3 1152	1152	144	144	784	144	752
ronald 3 1216	1216	152	152	784	152	752
ronald 3 1280	1280	160	160	784	160	752
ronald 3 1344	1344	168	168	784	168	752
ronald 3 1408	1408	176	176	784	176	752
ronald 3 1472	1472	184	184	784	184	752
ronald 3 1536	1536	192	192	784	192	752
ronald 3 1664	1664	208	208	784	208	752
ronald 3 1792	1792	224	224	784	224	752
ronald 3 1920	1920	240	240	784	240	752
ronald 3 2048	2048	256	256	784	256	752
ronald 3 2176	2176	272	272	784	272	752
ronald 3 2304	2304	288	288	784	288	752
ronald 3 2432	2432	304	304	784	304	752
ronald 3 2560	2560	320	320	784	320	752
ronald 3 2688	2688	336	336	784	336	752
ronald 3 2816	2816	352	352	784	352	752
ronald 3 2944	2944	368	368	784	368	752
ronald 3 3072	3072	384	384	784	384	752
ronald 3 3328	3328	416	416	784	416	752
ronald 3 3584	3584	448	448	784	448	752

ronald 3 3840	3840	480		480	784	480	752
ronald 3 4096	4096	512		512	784	512	752
sflashv2 1	2823	19266				60	746
sflashv2 2	2823	19266				60	746
surf127eps 1	32	48	48				

6.15 x86, 1400MHz, Pentium III (6b1), td158

System	key-pair cycles	share cycles	encrypt cycles	decrypt cycles	sign cycles	verify cycles
claus 1	21098216	21089261				
claus++ 1	14980581	14916854				
curve25519-gaudry 1	1925899	1922410				
donald 1 512	1282434				1308747	1553472
donald 1 1024	3799375				3635010	4329134
donald 1 2048	12666449				11824123	14492703
ecdonald 1 nist-b-163	4910266				5022168	9876021
ecdonald 1 nist-b-233	10015456				10206155	20183806
ecdonald 1 nist-b-283	18638860				18887538	37540452
ecdonald 1 nist-b-409	46633547				47026375	93720100
ecdonald 1 nist-b-571	108780915				109045896	217739901
ecdonald 1 nist-k-163	4495841				4617945	9127080
ecdonald 1 nist-k-233	8999114				9167772	18145747
ecdonald 1 nist-k-283	16473894				16663155	33188887
ecdonald 1 nist-k-409	40401907				40804316	81430404
ecdonald 1 nist-k-571	93633659				94141416	187483542
ecdonald 1 nist-p-192	3996680				4116730	4922680
ecdonald 1 nist-p-224	5203961				5317938	6350653
ecdonald 1 nist-p-256	6365671				6548867	7832242
ecdonald 1 nist-p-384	15593325				15865410	18937958
ecdonald 1 nist-p-521	31018792				31473612	38308680
ecdonald 1 secp160r1	4019904				4177673	5029714
ntru-enc 1 ees787ep1	152366691		693480	1237265		
ronald 1 768	136079054		193216	5422135	5426234	174978
ronald 1 832	133025082		207330	6419546	6451017	188384
ronald 1 896	186982240		221363	7453013	7489814	195284
ronald 1 960	282840313		233350	8625748	8683469	211362
ronald 1 1024	233244892		239397	9189252	9197108	217685
ronald 1 1088	303194292		294416	11966281	12010785	268527
ronald 1 1152	437264123		306856	13571535	13567228	280768
ronald 1 1216	385104703		323174	15091067	15069415	291554
ronald 1 1280	390284317		337532	17045536	16874578	303511
ronald 1 1344	532969752		353366	18984257	18941739	320575
ronald 1 1408	466274931		366751	20916551	20964262	333789
ronald 1 1472	889560224		387499	23224066	23252328	353496
ronald 1 1536	688111289		403174	25289218	25285652	371960
ronald 1 1664	1164680067		453097	30996338	30945073	416147

ronald 1 1792	1132369446	483597	37052817	36922370	443252
ronald 1 1920	1428272362	528962	43567252	43450884	480255
ronald 1 2048	2189940479	560604	48930855	49004361	517735
ronald 1 2176	2730087118	713088	60625407	60631809	664084
ronald 1 2304	3774937561	762194	69261748	69023997	704649
ronald 1 2432	5723504829	808407	79029446	78852653	755437
ronald 1 2560	4347701335	857725	89734708	89614795	799778
ronald 1 2688	4947441541	918503	101032323	100874464	857182
ronald 1 2816	5495857311	967172	113931381	113756508	909676
ronald 1 2944	6972269377	1025925	127489281	128112814	966310
ronald 1 3072	7110633485	1080085	143063923	143180508	1018240
ronald 1 3328	10476716177	1230702	181311714	181132311	1153885
ronald 1 3584	15140446251	1367115	215255845	215034051	1286741
ronald 1 3840	18697098556	1503958	259501994	259109379	1423249
ronald 1 4096	25760529774	1630243	295882584	295420017	1539913
ronald 2 768	130955234	171824	5401439	5424478	167487
ronald 2 832	189478255	185312	6412731	6430898	179447
ronald 2 896	156298139	195806	7516050	7510370	190253
ronald 2 960	214695285	205493	8603029	8612083	199541
ronald 2 1024	191790135	215908	9145549	9178037	207629
ronald 2 1088	336511423	272924	11971174	11973493	260538
ronald 2 1152	363240457	284888	13454944	13495066	272393
ronald 2 1216	376345474	296104	15095809	15127129	283883
ronald 2 1280	455556894	313867	16926579	16902616	299996
ronald 2 1344	435009824	325869	18896741	18960290	312272
ronald 2 1408	617831285	347642	20984426	20940465	327420
ronald 2 1472	599353559	365818	23292212	23234329	344662
ronald 2 1536	919069516	383360	25357312	25292577	359106
ronald 2 1664	981335292	427621	30856753	30792651	403963
ronald 2 1792	1035175795	460833	37027534	37046366	433778
ronald 2 1920	1384404819	503387	43635285	43612427	472220
ronald 2 2048	2265285162	537700	48942400	48897843	503099
ronald 2 2176	3354010748	687816	60462195	60520957	651671
ronald 2 2304	2448047448	733670	69025379	69210271	698402
ronald 2 2432	3694200604	782295	79081054	79039911	744588
ronald 2 2560	4423602888	827726	89647451	89388525	788684
ronald 2 2688	5692364171	890652	100564983	100691419	846820
ronald 2 2816	3278525523	941211	113818486	113719940	893668
ronald 2 2944	4680581598	1002709	127804079	127649865	951038
ronald 2 3072	5852499902	1054459	143839655	143986632	1007110
ronald 2 3328	10973518637	1203778	179999104	180309187	1143839
ronald 2 3584	12309823356	1343158	214861903	214615299	1268632
ronald 2 3840	15244897743	1481611	259048891	258725156	1407403
ronald 2 4096	16059951871	1603384	294755711	295169038	1528693
ronald 3 768	107063574	170359	5407028	5390162	157790
ronald 3 832	123811275	185270	6422581	6442841	172044
ronald 3 896	147471597	195063	7456077	7462139	181899

ronald 3 960	237107837		206863	8603172	8604802	192884
ronald 3 1024	215318942		216298	9186831	9190254	200632
ronald 3 1088	309416838		275614	11965153	11958400	251448
ronald 3 1152	309785080		285816	13532109	13490380	263322
ronald 3 1216	403087263		297061	15130954	15129386	276270
ronald 3 1280	323404043		316445	16943811	16947957	290785
ronald 3 1344	576925703		330479	18964452	18934921	303689
ronald 3 1408	513291660		348243	20956328	20985827	320875
ronald 3 1472	766307032		361379	23157879	23167880	333542
ronald 3 1536	945345313		381125	25210253	25236884	352505
ronald 3 1664	1182591753		429243	30893318	30940495	392803
ronald 3 1792	1210147680		461237	37034728	37068624	424454
ronald 3 1920	1226801207		502674	43443330	43354944	463428
ronald 3 2048	1516966689		540389	49120528	48931258	493933
ronald 3 2176	1616932853		687246	60322442	60307489	646266
ronald 3 2304	2454480179		736286	69419266	69778467	684435
ronald 3 2432	3374277806		783189	79019437	78859916	736220
ronald 3 2560	3582980215		829169	89484632	89489020	780308
ronald 3 2688	4141181179		892083	100760791	100751224	836822
ronald 3 2816	4130319490		943081	113847498	113655899	885652
ronald 3 2944	7491776365		1002330	127721515	127589487	944880
ronald 3 3072	9126480836		1056140	143785189	143561913	990049
ronald 3 3328	9605523039		1203284	179986020	179963989	1133692
ronald 3 3584	16066359372		1339566	214842041	214625333	1257381
ronald 3 3840	11871611514		1481939	258943531	258661567	1398093
ronald 3 4096	17089551486		1601270	295393234	295042197	1515160
sflashv2 1	804528764				2491897	897641
sflashv2 2	746908869				280408	387232
surf127eps 1	1974074	1996332				

System	secret key bytes	public key bytes	shared secret bytes	23-byte encrypt bytes	709-byte encrypt bytes	23-byte signed bytes	709-byte signed bytes
claus 1	256	128	128				
claus++ 1	256	128	128				
curve25519-gaudry 1	32	32	32				
donald 1 512	84	64				63	749
donald 1 1024	148	128				63	749
donald 1 2048	276	256				63	749
ecdonald 1 nist-b-163	63	42				65	751
ecdonald 1 nist-b-233	90	60				83	769
ecdonald 1 nist-b-283	108	72				95	781
ecdonald 1 nist-b-409	156	104				127	813
ecdonald 1 nist-b-571	216	144				167	853
ecdonald 1 nist-k-163	63	42				65	751
ecdonald 1 nist-k-233	90	60				83	769
ecdonald 1 nist-k-283	108	72				95	781

ecdonald 1 nist-k-409	156	104			127	813
ecdonald 1 nist-k-571	216	144			167	853
ecdonald 1 nist-p-192	72	48			71	757
ecdonald 1 nist-p-224	84	56			79	765
ecdonald 1 nist-p-256	96	64			87	773
ecdonald 1 nist-p-384	144	96			119	805
ecdonald 1 nist-p-521	198	132			155	841
ecdonald 1 secp160r1	60	40			63	749
ntru-enc 1 ees787ep1	1854	1574	1574	2282		
ronald 1 768	768	96	119	805	119	805
ronald 1 832	832	104	127	813	127	813
ronald 1 896	896	112	135	821	135	821
ronald 1 960	960	120	143	829	143	829
ronald 1 1024	1024	128	151	837	151	837
ronald 1 1088	1088	136	159	845	159	845
ronald 1 1152	1152	144	167	853	167	853
ronald 1 1216	1216	152	175	861	175	861
ronald 1 1280	1280	160	183	869	183	869
ronald 1 1344	1344	168	191	877	191	877
ronald 1 1408	1408	176	199	885	199	885
ronald 1 1472	1472	184	207	893	207	893
ronald 1 1536	1536	192	215	901	215	901
ronald 1 1664	1664	208	231	917	231	917
ronald 1 1792	1792	224	247	933	247	933
ronald 1 1920	1920	240	263	949	263	949
ronald 1 2048	2048	256	279	965	279	965
ronald 1 2176	2176	272	295	981	295	981
ronald 1 2304	2304	288	311	997	311	997
ronald 1 2432	2432	304	327	1013	327	1013
ronald 1 2560	2560	320	343	1029	343	1029
ronald 1 2688	2688	336	359	1045	359	1045
ronald 1 2816	2816	352	375	1061	375	1061
ronald 1 2944	2944	368	391	1077	391	1077
ronald 1 3072	3072	384	407	1093	407	1093
ronald 1 3328	3328	416	439	1125	439	1125
ronald 1 3584	3584	448	471	1157	471	1157
ronald 1 3840	3840	480	503	1189	503	1189
ronald 1 4096	4096	512	535	1221	535	1221
ronald 2 768	768	96	96	784	119	805
ronald 2 832	832	104	104	784	127	813
ronald 2 896	896	112	112	784	135	821
ronald 2 960	960	120	120	784	143	829
ronald 2 1024	1024	128	128	784	151	837
ronald 2 1088	1088	136	136	784	159	845
ronald 2 1152	1152	144	144	784	167	853
ronald 2 1216	1216	152	152	784	175	861
ronald 2 1280	1280	160	160	784	183	869

`ronald 2 1344`	1344	168	168	784	191	877
`ronald 2 1408`	1408	176	176	784	199	885
`ronald 2 1472`	1472	184	184	784	207	893
`ronald 2 1536`	1536	192	192	784	215	901
`ronald 2 1664`	1664	208	208	784	231	917
`ronald 2 1792`	1792	224	224	784	247	933
`ronald 2 1920`	1920	240	240	784	263	949
`ronald 2 2048`	2048	256	256	784	279	965
`ronald 2 2176`	2176	272	272	784	295	981
`ronald 2 2304`	2304	288	288	784	311	997
`ronald 2 2432`	2432	304	304	784	327	1013
`ronald 2 2560`	2560	320	320	784	343	1029
`ronald 2 2688`	2688	336	336	784	359	1045
`ronald 2 2816`	2816	352	352	784	375	1061
`ronald 2 2944`	2944	368	368	784	391	1077
`ronald 2 3072`	3072	384	384	784	407	1093
`ronald 2 3328`	3328	416	416	784	439	1125
`ronald 2 3584`	3584	448	448	784	471	1157
`ronald 2 3840`	3840	480	480	784	503	1189
`ronald 2 4096`	4096	512	512	784	535	1221
`ronald 3 768`	768	96	96	784	96	752
`ronald 3 832`	832	104	104	784	104	752
`ronald 3 896`	896	112	112	784	112	752
`ronald 3 960`	960	120	120	784	120	752
`ronald 3 1024`	1024	128	128	784	128	752
`ronald 3 1088`	1088	136	136	784	136	752
`ronald 3 1152`	1152	144	144	784	144	752
`ronald 3 1216`	1216	152	152	784	152	752
`ronald 3 1280`	1280	160	160	784	160	752
`ronald 3 1344`	1344	168	168	784	168	752
`ronald 3 1408`	1408	176	176	784	176	752
`ronald 3 1472`	1472	184	184	784	184	752
`ronald 3 1536`	1536	192	192	784	192	752
`ronald 3 1664`	1664	208	208	784	208	752
`ronald 3 1792`	1792	224	224	784	224	752
`ronald 3 1920`	1920	240	240	784	240	752
`ronald 3 2048`	2048	256	256	784	256	752
`ronald 3 2176`	2176	272	272	784	272	752
`ronald 3 2304`	2304	288	288	784	288	752
`ronald 3 2432`	2432	304	304	784	304	752
`ronald 3 2560`	2560	320	320	784	320	752
`ronald 3 2688`	2688	336	336	784	336	752
`ronald 3 2816`	2816	352	352	784	352	752
`ronald 3 2944`	2944	368	368	784	368	752
`ronald 3 3072`	3072	384	384	784	384	752
`ronald 3 3328`	3328	416	416	784	416	752
`ronald 3 3584`	3584	448	448	784	448	752

ronald 3 3840	3840	480		480	784	480	752
ronald 3 4096	4096	512		512	784	512	752
sflashv2 1	2823	19266				60	746
sflashv2 2	2823	19266				60	746
surf127eps 1	32	48	48				

6.16 x86, 1900MHz, Pentium 4 (f12), fireball

System	key-pair cycles	share cycles	encrypt cycles	decrypt cycles	sign cycles	verify cycles
bls 1	21250632				2518644	31284144
claus 1	28297756	27791572				
claus++ 1	13847120	13615760				
curve25519-gaudry 1	3009928	2980472				
donald 1 512	1704980				1723360	2033964
donald 1 1024	4952600				4665480	5698008
donald 1 2048	15620648				14527024	17516072
ecdonald 1 nist-b-163	5091492				5211788	10292512
ecdonald 1 nist-b-233	9654532				9760916	19199324
ecdonald 1 nist-b-283	18168684				18377112	36387412
ecdonald 1 nist-b-409	41792580				42489320	83737752
ecdonald 1 nist-b-571	102161896				103128176	205927812
ecdonald 1 nist-k-163	4724124				4886360	9600584
ecdonald 1 nist-k-233	8662276				8833920	17384188
ecdonald 1 nist-k-283	16216536				16409252	32643644
ecdonald 1 nist-k-409	36481900				37314900	73381952
ecdonald 1 nist-k-571	85919464				86536312	177257912
ecdonald 1 nist-p-192	4549492				4619136	5577260
ecdonald 1 nist-p-224	5992048				6159636	7506480
ecdonald 1 nist-p-256	8709876				8912608	10781636
ecdonald 1 nist-p-384	19008900				19612240	23234092
ecdonald 1 nist-p-521	49828728				50376444	62036392
ecdonald 1 secp160r1	4831576				5011828	6006680
ntru-enc 1 ees787ep1	168553584		783632	1320508		
rainbow 1	307584408				1082924	1828628
ronald 1 768	179580536		209964	6960664	6984956	191808
ronald 1 832	279204952		237736	8284596	8322636	216520
ronald 1 896	212284220		250276	9612520	9647196	229956
ronald 1 960	278832504		265564	11326200	11132104	246080
ronald 1 1024	354906576		273172	12103260	12188284	252300
ronald 1 1088	357982608		339804	15522036	15541636	321036
ronald 1 1152	475799084		360856	17642004	17662752	338960
ronald 1 1216	695611704		387492	19825668	19866056	358468
ronald 1 1280	783240900		375816	23855392	22153980	356348
ronald 1 1344	966623436		393896	24867504	24945332	367416
ronald 1 1408	478116564		417128	28144720	28000472	394156
ronald 1 1472	965625484		448680	29673872	29684508	417476

ronald 1 1536	726425112	447652	28527292	28509972	413792
ronald 1 1664	1202353804	508112	37746468	38162708	471608
ronald 1 1792	1220984992	537836	45543532	45601180	499064
ronald 1 1920	1694247612	599860	54441676	53981792	560796
ronald 1 2048	2410201840	630608	63232304	63334460	591396
ronald 1 2176	3136103492	851768	73715716	74868128	802672
ronald 1 2304	2455458044	869148	84195460	84949344	819436
ronald 1 2432	3982063248	949876	108821188	96506748	901092
ronald 1 2560	5898520684	970168	97474204	97045204	917780
ronald 1 2688	4885632020	1065220	112428832	112794092	1016196
ronald 1 2816	4956724012	1091540	132192444	131264212	1029580
ronald 1 2944	6258558904	1182216	149126156	147644648	1120780
ronald 1 3072	9227961628	1222356	148132996	148025680	1162260
ronald 1 3328	11540203964	1371784	194595820	194956648	1300440
ronald 1 3584	11948728476	1501220	214341376	215679680	1442140
ronald 1 3840	12263267184	1649232	272315632	273036324	1573412
ronald 1 4096	24358642228	1841120	365002728	367158516	1751400
ronald 2 768	162126180	188836	7033012	6985548	185508
ronald 2 832	158368388	209880	9598500	9836776	210168
ronald 2 896	227424280	228104	9681488	9732788	223256
ronald 2 960	339842516	242484	11076544	11082628	238612
ronald 2 1024	463904684	243520	12140368	12115804	240372
ronald 2 1088	476158956	320340	15501304	15589560	312272
ronald 2 1152	449741300	340856	17560568	17581328	331712
ronald 2 1216	384494108	362504	19784536	19733996	344552
ronald 2 1280	640271288	350872	22098068	22006912	334704
ronald 2 1344	775853196	380180	24862532	24811180	372720
ronald 2 1408	1064591796	404044	29355216	28134572	390240
ronald 2 1472	982426004	435896	29587620	29547748	411620
ronald 2 1536	2017167200	424736	28611980	28527404	404568
ronald 2 1664	1404965624	496380	37128872	37129204	473868
ronald 2 1792	1032766088	519392	44438736	44815144	492984
ronald 2 1920	1454584704	589388	53929588	53157952	554504
ronald 2 2048	2539082728	615800	65049504	63499468	587196
ronald 2 2176	2640945492	835296	73168560	73852028	798500
ronald 2 2304	4181942068	856444	86691728	84806332	827320
ronald 2 2432	3368189092	931524	96905844	96847404	887272
ronald 2 2560	5093197096	949920	97401000	96939180	904568
ronald 2 2688	6620302640	1054356	113749576	114918876	1006624
ronald 2 2816	5485418220	1073508	128004620	128266032	1025844
ronald 2 2944	6821580184	1163180	148910956	147565536	1111896
ronald 2 3072	8959009516	1179148	148940696	148562624	1130592
ronald 2 3328	8924059996	1356392	192880584	193663812	1295596
ronald 2 3584	15070894012	1487428	214045696	213864972	1418332
ronald 2 3840	15856706120	1649184	271804624	273913008	1595968
ronald 2 4096	25448776644	1822736	362546468	362868744	1742208
ronald 3 768	182062032	190096	6981332	6931784	178464

ronald 3 832	163992068		213540	8422544	8392200	200844
ronald 3 896	233531748		228236	9659864	9603632	214328
ronald 3 960	284976088		245372	11110800	11100080	230084
ronald 3 1024	290951132		246384	12096796	11960032	228448
ronald 3 1088	330971100		325496	15632356	15718860	301580
ronald 3 1152	480949152		342040	17544564	17547220	319180
ronald 3 1216	646566444		361312	19742712	19676092	341280
ronald 3 1280	769967476		351556	22019624	22006528	327896
ronald 3 1344	774372008		378508	24548324	24724060	354728
ronald 3 1408	381326940		402664	27746380	27708844	378840
ronald 3 1472	962027812		436624	29819576	29882040	401588
ronald 3 1536	1043232140		431156	28701112	28695344	397428
ronald 3 1664	1180574308		489748	37323796	37340612	461688
ronald 3 1792	2096154516		530224	44821128	44778760	484708
ronald 3 1920	2035117476		586432	57440116	56777236	541740
ronald 3 2048	1575184820		618344	63663896	63682600	578836
ronald 3 2176	2427056996		839968	72869756	73354128	794824
ronald 3 2304	3293427208		856076	83573004	83724168	811956
ronald 3 2432	2913760792		930912	96088560	95832276	877180
ronald 3 2560	5678676004		964368	97586560	97392792	917148
ronald 3 2688	5544519976		1045940	111319948	111071036	997912
ronald 3 2816	5296295976		1078440	126465272	126244788	1021148
ronald 3 2944	7110366180		1159160	144339864	143890196	1104248
ronald 3 3072	9574509044		1230880	150086340	148443668	1132348
ronald 3 3328	11383435884		1351272	192428000	191190744	1287608
ronald 3 3584	13350344352		1491956	215697316	214803244	1422416
ronald 3 3840	18147298848		1639788	270587224	270314400	1558676
ronald 3 4096	24578526856		1834288	364287340	363993004	1742360
sflashv2 1	468589824				1909484	655584
sflashv2 2	463778560				353624	388996
surf127eps 1	3204468	3219688				

System	secret key bytes	public key bytes	shared secret bytes	23-byte encrypt bytes	709-byte encrypt bytes	23-byte signed bytes	709-byte signed bytes
bls 1	20	120				43	729
claus 1	256	128	128				
claus++ 1	256	128	128				
curve25519-gaudry 1	32	32	32				
donald 1 512	84	64				63	749
donald 1 1024	148	128				63	749
donald 1 2048	276	256				63	749
ecdonald 1 nist-b-163	63	42				65	751
ecdonald 1 nist-b-233	90	60				83	769
ecdonald 1 nist-b-283	108	72				95	781
ecdonald 1 nist-b-409	156	104				127	813
ecdonald 1 nist-b-571	216	144				167	853

`ecdonald 1 nist-k-163`	63	42			65	751
`ecdonald 1 nist-k-233`	90	60			83	769
`ecdonald 1 nist-k-283`	108	72			95	781
`ecdonald 1 nist-k-409`	156	104			127	813
`ecdonald 1 nist-k-571`	216	144			167	853
`ecdonald 1 nist-p-192`	72	48			71	757
`ecdonald 1 nist-p-224`	84	56			79	765
`ecdonald 1 nist-p-256`	96	64			87	773
`ecdonald 1 nist-p-384`	144	96			119	805
`ecdonald 1 nist-p-521`	198	132			155	841
`ecdonald 1 secp160r1`	60	40			63	749
`ntru-enc 1 ees787ep1`	1854	1574	1574	2282		
`rainbow 1`	20107	31680			66	752
`ronald 1 768`	768	96	119	805	119	805
`ronald 1 832`	832	104	127	813	127	813
`ronald 1 896`	896	112	135	821	135	821
`ronald 1 960`	960	120	143	829	143	829
`ronald 1 1024`	1024	128	151	837	151	837
`ronald 1 1088`	1088	136	159	845	159	845
`ronald 1 1152`	1152	144	167	853	167	853
`ronald 1 1216`	1216	152	175	861	175	861
`ronald 1 1280`	1280	160	183	869	183	869
`ronald 1 1344`	1344	168	191	877	191	877
`ronald 1 1408`	1408	176	199	885	199	885
`ronald 1 1472`	1472	184	207	893	207	893
`ronald 1 1536`	1536	192	215	901	215	901
`ronald 1 1664`	1664	208	231	917	231	917
`ronald 1 1792`	1792	224	247	933	247	933
`ronald 1 1920`	1920	240	263	949	263	949
`ronald 1 2048`	2048	256	279	965	279	965
`ronald 1 2176`	2176	272	295	981	295	981
`ronald 1 2304`	2304	288	311	997	311	997
`ronald 1 2432`	2432	304	327	1013	327	1013
`ronald 1 2560`	2560	320	343	1029	343	1029
`ronald 1 2688`	2688	336	359	1045	359	1045
`ronald 1 2816`	2816	352	375	1061	375	1061
`ronald 1 2944`	2944	368	391	1077	391	1077
`ronald 1 3072`	3072	384	407	1093	407	1093
`ronald 1 3328`	3328	416	439	1125	439	1125
`ronald 1 3584`	3584	448	471	1157	471	1157
`ronald 1 3840`	3840	480	503	1189	503	1189
`ronald 1 4096`	4096	512	535	1221	535	1221
`ronald 2 768`	768	96	96	784	119	805
`ronald 2 832`	832	104	104	784	127	813
`ronald 2 896`	896	112	112	784	135	821
`ronald 2 960`	960	120	120	784	143	829
`ronald 2 1024`	1024	128	128	784	151	837

ronald 2 1088	1088	136	136	784	159	845
ronald 2 1152	1152	144	144	784	167	853
ronald 2 1216	1216	152	152	784	175	861
ronald 2 1280	1280	160	160	784	183	869
ronald 2 1344	1344	168	168	784	191	877
ronald 2 1408	1408	176	176	784	199	885
ronald 2 1472	1472	184	184	784	207	893
ronald 2 1536	1536	192	192	784	215	901
ronald 2 1664	1664	208	208	784	231	917
ronald 2 1792	1792	224	224	784	247	933
ronald 2 1920	1920	240	240	784	263	949
ronald 2 2048	2048	256	256	784	279	965
ronald 2 2176	2176	272	272	784	295	981
ronald 2 2304	2304	288	288	784	311	997
ronald 2 2432	2432	304	304	784	327	1013
ronald 2 2560	2560	320	320	784	343	1029
ronald 2 2688	2688	336	336	784	359	1045
ronald 2 2816	2816	352	352	784	375	1061
ronald 2 2944	2944	368	368	784	391	1077
ronald 2 3072	3072	384	384	784	407	1093
ronald 2 3328	3328	416	416	784	439	1125
ronald 2 3584	3584	448	448	784	471	1157
ronald 2 3840	3840	480	480	784	503	1189
ronald 2 4096	4096	512	512	784	535	1221
ronald 3 768	768	96	96	784	96	752
ronald 3 832	832	104	104	784	104	752
ronald 3 896	896	112	112	784	112	752
ronald 3 960	960	120	120	784	120	752
ronald 3 1024	1024	128	128	784	128	752
ronald 3 1088	1088	136	136	784	136	752
ronald 3 1152	1152	144	144	784	144	752
ronald 3 1216	1216	152	152	784	152	752
ronald 3 1280	1280	160	160	784	160	752
ronald 3 1344	1344	168	168	784	168	752
ronald 3 1408	1408	176	176	784	176	752
ronald 3 1472	1472	184	184	784	184	752
ronald 3 1536	1536	192	192	784	192	752
ronald 3 1664	1664	208	208	784	208	752
ronald 3 1792	1792	224	224	784	224	752
ronald 3 1920	1920	240	240	784	240	752
ronald 3 2048	2048	256	256	784	256	752
ronald 3 2176	2176	272	272	784	272	752
ronald 3 2304	2304	288	288	784	288	752
ronald 3 2432	2432	304	304	784	304	752
ronald 3 2560	2560	320	320	784	320	752
ronald 3 2688	2688	336	336	784	336	752
ronald 3 2816	2816	352	352	784	352	752

ronald 3 2944	2944	368		368	784	368	752
ronald 3 3072	3072	384		384	784	384	752
ronald 3 3328	3328	416		416	784	416	752
ronald 3 3584	3584	448		448	784	448	752
ronald 3 3840	3840	480		480	784	480	752
ronald 3 4096	4096	512		512	784	512	752
sflashv2 1	2823	19266				60	746
sflashv2 2	2823	19266				60	746
surf127eps 1	32	48	48				

6.17 x86, 2800MHz, Pentium 4 (f29), poema

System	key-pair cycles	share cycles	encrypt cycles	decrypt cycles	sign cycles	verify cycles
bls 1	20060932				2498280	30479432
claus 1	24422484	24430688				
claus++ 1	13644364	13598112				
curve25519-gaudry 1	3119684	3102580				
donald 1 512	1554448				1562072	1880388
donald 1 1024	4380304				4212528	5108824
donald 1 2048	14435940				12417592	15037960
ecdonald 1 nist-b-163	4698672				4906424	9453380
ecdonald 1 nist-b-233	9166912				9478188	18846084
ecdonald 1 nist-b-283	17845824				18310480	35276548
ecdonald 1 nist-b-409	41041040				41316336	81651948
ecdonald 1 nist-b-571	97265232				96859900	191853072
ecdonald 1 nist-k-163	4291112				5111836	9791124
ecdonald 1 nist-k-233	8352444				8326872	16534568
ecdonald 1 nist-k-283	16305324				16729408	31940436
ecdonald 1 nist-k-409	35709948				36225884	71318788
ecdonald 1 nist-k-571	84780740				85026956	169665056
ecdonald 1 nist-p-192	4410428				4527152	5621296
ecdonald 1 nist-p-224	5849084				6056560	7555792
ecdonald 1 nist-p-256	7819568				8021896	9692816
ecdonald 1 nist-p-384	18257608				18494928	22190992
ecdonald 1 nist-p-521	48460540				48688812	59473480
ecdonald 1 secp160r1	4840000				4944572	5888680
ntru-enc 1 ees787ep1	171874188		783652	1307984		
rainbow 1	275282008				1254616	2939944
ronald 1 768	177439408		206476	6511940	6562492	191004
ronald 1 832	267721676		225324	7882468	7942836	210584
ronald 1 896	227655300		238592	9331968	9504416	230712
ronald 1 960	348302668		257760	10599880	10736880	239688
ronald 1 1024	294341448		247400	11076232	11119080	228192
ronald 1 1088	484140632		330324	14296352	14384228	310912
ronald 1 1152	449799272		347032	16313028	16423652	321928
ronald 1 1216	547091992		362548	18648952	18592444	362236

ronald 1 1280	751543876	362024	20813112	20871308	330584
ronald 1 1344	917946120	382164	23634680	23772300	349372
ronald 1 1408	691516700	408748	26005656	26021308	380388
ronald 1 1472	928290620	436388	27956376	27823072	399000
ronald 1 1536	1290352516	414468	27443448	27845488	383788
ronald 1 1664	971220108	510792	35066952	35122112	473304
ronald 1 1792	1366809664	519648	42858976	42361492	485204
ronald 1 1920	2070857660	573352	49954996	49429692	531628
ronald 1 2048	2190859692	589008	57209812	57876960	544332
ronald 1 2176	2489589190	794592	68427660	68179028	754008
ronald 1 2304	3724252032	791848	78159096	77034292	749000
ronald 1 2432	5663058740	887868	90917112	91339480	831720
ronald 1 2560	5908517620	924728	91390552	91503096	856924
ronald 1 2688	6739693824	1008544	106721892	107785760	941704
ronald 1 2816	6023726560	1022572	123468772	122000212	951832
ronald 1 2944	5971554948	1116864	141283644	141420156	1051800
ronald 1 3072	7563331188	1124364	140903532	139196956	1063308
ronald 1 3328	11834896404	1291160	187375548	186483404	1206888
ronald 1 3584	9034396312	1411956	212100636	211701200	1343668
ronald 1 3840	14268989928	1559492	260583644	263515928	1476188
ronald 1 4096	19765395044	1724056	322966028	317377944	1638528
ronald 2 768	152332120	184292	6568524	6643412	180068
ronald 2 832	247298328	205800	7893640	7935220	201308
ronald 2 896	207509404	220688	9313440	9353328	218368
ronald 2 960	226752656	240720	10717684	11155104	243424
ronald 2 1024	304763120	233620	11065136	11035512	224808
ronald 2 1088	511385628	304544	14369404	14422628	294280
ronald 2 1152	449003132	322432	16062076	16129824	311428
ronald 2 1216	817323240	340216	18574372	18488556	329116
ronald 2 1280	548316484	336808	20925376	20908580	315028
ronald 2 1344	583492632	357744	23742340	23643772	338908
ronald 2 1408	1097237400	386260	25854904	25873944	366364
ronald 2 1472	781954384	407148	28087584	27995496	389808
ronald 2 1536	1151263632	417000	28159412	27974364	378000
ronald 2 1664	1035750852	474500	35756032	35335056	448320
ronald 2 1792	1796273180	492316	42411240	42568984	470692
ronald 2 1920	2565687920	553116	50612392	50883856	524276
ronald 2 2048	3233961916	553280	57330932	57807860	529608
ronald 2 2176	2736196008	776272	68402656	68299276	741640
ronald 2 2304	2604024860	779728	77908712	77221768	738116
ronald 2 2432	2967205352	867740	94878460	95464228	825744
ronald 2 2560	3803331632	892984	91468856	90864156	838048
ronald 2 2688	6843714564	975576	106070916	105875208	929620
ronald 2 2816	4428394500	995824	122137824	121721700	940240
ronald 2 2944	3355456164	1094976	139522516	138980544	1035680
ronald 2 3072	7152922624	1113120	140800628	137476064	1057524
ronald 2 3328	10777239908	1268796	187049592	186759780	1204456

ronald 2 3584	14259665652		1382272	209013152	207306416	1311112
ronald 2 3840	23525325480		1559256	263244116	260990480	1456716
ronald 2 4096	16746025264		1703096	318664484	315049468	1617276
ronald 3 768	167657764		191332	6552484	6550028	179764
ronald 3 832	223553340		208248	7892524	7925940	191956
ronald 3 896	205778076		221844	9169348	9208784	207352
ronald 3 960	235037332		239696	10743844	10699064	221088
ronald 3 1024	226258044		235912	11130380	11041108	216488
ronald 3 1088	373720956		308948	14461100	14556740	284816
ronald 3 1152	408398388		329184	16407212	16381592	306048
ronald 3 1216	584616616		349944	19160692	19033228	324880
ronald 3 1280	533908216		336212	22567128	23005404	309968
ronald 3 1344	1172360028		365628	24017048	24121492	337428
ronald 3 1408	564152056		388924	26248124	26084328	360088
ronald 3 1472	831207720		425568	28625164	28153092	383208
ronald 3 1536	1097841844		404808	27697636	27763844	371896
ronald 3 1664	1845319416		494920	35777308	35322716	446792
ronald 3 1792	1071664280		494460	42448092	42039016	455416
ronald 3 1920	2364554348		555156	49675424	50045988	516544
ronald 3 2048	2273511680		561180	57884288	57801612	535888
ronald 3 2176	2294723844		791860	69001496	69328944	748388
ronald 3 2304	2449272564		809244	78525220	78800264	752832
ronald 3 2432	4547492604		883972	92517412	90733052	821664
ronald 3 2560	3459776520		904844	92623312	90770696	834396
ronald 3 2688	10223906344		985936	106069500	105794788	936420
ronald 3 2816	14000951264		1002436	120902672	121381544	949720
ronald 3 2944	14527791916		1109056	143108224	143019444	1051708
ronald 3 3072	24718189672		1118628	140027072	418105276	1061076
ronald 3 3328	8929706228		1293880	187843524	185371900	1214692
ronald 3 3584	15394544720		1405184	209862692	210739576	1329680
ronald 3 3840	11216737560		1551780	260347456	260288188	1469372
ronald 3 4096	23087093020		1730808	325538160	318750812	1643700
sflashv2 1	470374896				3861394	2410004
sflashv2 2	447858256				327292	421428
surf127eps 1	3105704	3134004				

System	secret key bytes	public key bytes	shared secret bytes	23-byte encrypt bytes	709-byte encrypt bytes	23-byte signed bytes	709-byte signed bytes
bls 1	20	120				43	729
claus 1	256	128	128				
claus++ 1	256	128	128				
curve25519-gaudry 1	32	32	32				
donald 1 512	84	64				63	749
donald 1 1024	148	128				63	749
donald 1 2048	276	256				63	749
ecdonald 1 nist-b-163	63	42				65	751

ecdonald 1 nist-b-233	90	60			83	769
ecdonald 1 nist-b-283	108	72			95	781
ecdonald 1 nist-b-409	156	104			127	813
ecdonald 1 nist-b-571	216	144			167	853
ecdonald 1 nist-k-163	63	42			65	751
ecdonald 1 nist-k-233	90	60			83	769
ecdonald 1 nist-k-283	108	72			95	781
ecdonald 1 nist-k-409	156	104			127	813
ecdonald 1 nist-k-571	216	144			167	853
ecdonald 1 nist-p-192	72	48			71	757
ecdonald 1 nist-p-224	84	56			79	765
ecdonald 1 nist-p-256	96	64			87	773
ecdonald 1 nist-p-384	144	96			119	805
ecdonald 1 nist-p-521	198	132			155	841
ecdonald 1 secp160r1	60	40			63	749
ntru-enc 1 ees787ep1	1854	1574	1574	2282		
rainbow 1	20107	31680			66	752
ronald 1 768	768	96	119	805	119	805
ronald 1 832	832	104	127	813	127	813
ronald 1 896	896	112	135	821	135	821
ronald 1 960	960	120	143	829	143	829
ronald 1 1024	1024	128	151	837	151	837
ronald 1 1088	1088	136	159	845	159	845
ronald 1 1152	1152	144	167	853	167	853
ronald 1 1216	1216	152	175	861	175	861
ronald 1 1280	1280	160	183	869	183	869
ronald 1 1344	1344	168	191	877	191	877
ronald 1 1408	1408	176	199	885	199	885
ronald 1 1472	1472	184	207	893	207	893
ronald 1 1536	1536	192	215	901	215	901
ronald 1 1664	1664	208	231	917	231	917
ronald 1 1792	1792	224	247	933	247	933
ronald 1 1920	1920	240	263	949	263	949
ronald 1 2048	2048	256	279	965	279	965
ronald 1 2176	2176	272	295	981	295	981
ronald 1 2304	2304	288	311	997	311	997
ronald 1 2432	2432	304	327	1013	327	1013
ronald 1 2560	2560	320	343	1029	343	1029
ronald 1 2688	2688	336	359	1045	359	1045
ronald 1 2816	2816	352	375	1061	375	1061
ronald 1 2944	2944	368	391	1077	391	1077
ronald 1 3072	3072	384	407	1093	407	1093
ronald 1 3328	3328	416	439	1125	439	1125
ronald 1 3584	3584	448	471	1157	471	1157
ronald 1 3840	3840	480	503	1189	503	1189
ronald 1 4096	4096	512	535	1221	535	1221
ronald 2 768	768	96	96	784	119	805

`ronald 2 832`	832	104	104	784	127	813
`ronald 2 896`	896	112	112	784	135	821
`ronald 2 960`	960	120	120	784	143	829
`ronald 2 1024`	1024	128	128	784	151	837
`ronald 2 1088`	1088	136	136	784	159	845
`ronald 2 1152`	1152	144	144	784	167	853
`ronald 2 1216`	1216	152	152	784	175	861
`ronald 2 1280`	1280	160	160	784	183	869
`ronald 2 1344`	1344	168	168	784	191	877
`ronald 2 1408`	1408	176	176	784	199	885
`ronald 2 1472`	1472	184	184	784	207	893
`ronald 2 1536`	1536	192	192	784	215	901
`ronald 2 1664`	1664	208	208	784	231	917
`ronald 2 1792`	1792	224	224	784	247	933
`ronald 2 1920`	1920	240	240	784	263	949
`ronald 2 2048`	2048	256	256	784	279	965
`ronald 2 2176`	2176	272	272	784	295	981
`ronald 2 2304`	2304	288	288	784	311	997
`ronald 2 2432`	2432	304	304	784	327	1013
`ronald 2 2560`	2560	320	320	784	343	1029
`ronald 2 2688`	2688	336	336	784	359	1045
`ronald 2 2816`	2816	352	352	784	375	1061
`ronald 2 2944`	2944	368	368	784	391	1077
`ronald 2 3072`	3072	384	384	784	407	1093
`ronald 2 3328`	3328	416	416	784	439	1125
`ronald 2 3584`	3584	448	448	784	471	1157
`ronald 2 3840`	3840	480	480	784	503	1189
`ronald 2 4096`	4096	512	512	784	535	1221
`ronald 3 768`	768	96	96	784	96	752
`ronald 3 832`	832	104	104	784	104	752
`ronald 3 896`	896	112	112	784	112	752
`ronald 3 960`	960	120	120	784	120	752
`ronald 3 1024`	1024	128	128	784	128	752
`ronald 3 1088`	1088	136	136	784	136	752
`ronald 3 1152`	1152	144	144	784	144	752
`ronald 3 1216`	1216	152	152	784	152	752
`ronald 3 1280`	1280	160	160	784	160	752
`ronald 3 1344`	1344	168	168	784	168	752
`ronald 3 1408`	1408	176	176	784	176	752
`ronald 3 1472`	1472	184	184	784	184	752
`ronald 3 1536`	1536	192	192	784	192	752
`ronald 3 1664`	1664	208	208	784	208	752
`ronald 3 1792`	1792	224	224	784	224	752
`ronald 3 1920`	1920	240	240	784	240	752
`ronald 3 2048`	2048	256	256	784	256	752
`ronald 3 2176`	2176	272	272	784	272	752
`ronald 3 2304`	2304	288	288	784	288	752

ronald 3 2432	2432	304		304	784	304	752
ronald 3 2560	2560	320		320	784	320	752
ronald 3 2688	2688	336		336	784	336	752
ronald 3 2816	2816	352		352	784	352	752
ronald 3 2944	2944	368		368	784	368	752
ronald 3 3072	3072	384		384	784	384	752
ronald 3 3328	3328	416		416	784	416	752
ronald 3 3584	3584	448		448	784	448	752
ronald 3 3840	3840	480		480	784	480	752
ronald 3 4096	4096	512		512	784	512	752
sflashv2 1	2823	19266				60	746
sflashv2 2	2823	19266				60	746
surf127eps 1	32	48	48				

6.18 x86, 2991MHz, Pentium 4 (f26), td185

System	key-pair cycles	share cycles	encrypt cycles	decrypt cycles	sign cycles	verify cycles
bls 1	20501032				2469704	31213548
claus 1	24390376	24552912				
claus++ 1	13593592	13524804				
curve25519-gaudry 1	3087428	3084212				
donald 1 512	1569704				1561600	1833024
donald 1 1024	4375164				4185764	5114692
donald 1 2048	14074016				13145028	15678580
ecdonald 1 nist-b-163	4785672				4844776	9449548
ecdonald 1 nist-b-233	9293968				9507184	18805492
ecdonald 1 nist-b-283	18024816				18544556	36775628
ecdonald 1 nist-b-409	40956080				41396088	82482148
ecdonald 1 nist-b-571	96300172				96776412	193826744
ecdonald 1 nist-k-163	4312076				4425040	8659820
ecdonald 1 nist-k-233	8387860				8454620	16928292
ecdonald 1 nist-k-283	16464576				16633436	32017452
ecdonald 1 nist-k-409	35665800				36099212	71741528
ecdonald 1 nist-k-571	82604780				82825000	166229880
ecdonald 1 nist-p-192	4365964				4501108	5287520
ecdonald 1 nist-p-224	5763048				5876672	6995796
ecdonald 1 nist-p-256	7972012				8201676	9927404
ecdonald 1 nist-p-384	17743232				18282360	21831348
ecdonald 1 nist-p-521	43873800				44276088	54173892
ecdonald 1 secp160r1	4885072				4963012	5972192
ntru-enc 1 ees787ep1	173344124		786676	1338008		
rainbow 1	277642332				1168504	2471096
ronald 1 768	187400120		208132	6479376	6517556	193180
ronald 1 832	265914972		227204	7896928	7812624	210864
ronald 1 896	319273296		241876	9361284	9347444	225136
ronald 1 960	370296660		261064	10877236	10928592	240568

ronald 1 1024	243518744	255596	11141532	11144620	234624
ronald 1 1088	476009572	326228	14526660	14466260	302704
ronald 1 1152	460035900	341860	16189920	16112488	319488
ronald 1 1216	697171496	354816	18647664	18672388	326556
ronald 1 1280	730287576	361608	20756604	21001916	331560
ronald 1 1344	720178936	379344	23711444	23766976	348656
ronald 1 1408	600117052	409116	26073692	26218232	374492
ronald 1 1472	735095072	427572	28929028	28681732	396360
ronald 1 1536	901815432	429952	27915180	27742976	391668
ronald 1 1664	1349034820	499948	35022328	35323568	464704
ronald 1 1792	1759687484	520324	42508812	42693380	480396
ronald 1 1920	3464332732	582484	50860456	51236012	537228
ronald 1 2048	2579238972	598220	57572876	58289264	558044
ronald 1 2176	3470897776	803472	67116380	68496904	748864
ronald 1 2304	3771289320	817076	78336256	77222712	771228
ronald 1 2432	5090963880	895992	88251076	88230076	846372
ronald 1 2560	4570810276	911916	92371308	91737608	855800
ronald 1 2688	8182321116	999404	105864628	107053080	945612
ronald 1 2816	5652666768	1024924	122488620	122654380	967008
ronald 1 2944	6628955840	1115132	139143420	139467984	1056124
ronald 1 3072	9348977372	1134768	141190032	140331824	1068468
ronald 1 3328	11884663784	1288880	186991196	187463096	1220844
ronald 1 3584	12262157892	1423236	211399888	211408748	1347264
ronald 1 3840	14134553804	1567016	260546828	260041036	1482664
ronald 1 4096	33377626272	1741780	329281120	327917804	1635532
ronald 2 768	220598052	189368	6595984	6599760	185324
ronald 2 832	236006736	205368	7865624	7910908	202536
ronald 2 896	237453948	222604	9412204	9460340	216212
ronald 2 960	315981768	238712	10884920	10896344	231276
ronald 2 1024	470683740	236228	11172988	11140452	224872
ronald 2 1088	334068724	305228	14469280	14534316	294396
ronald 2 1152	522776336	322044	16212928	16229908	309604
ronald 2 1216	574161500	330584	18702820	18736504	317160
ronald 2 1280	461936128	339044	21127740	20923608	319416
ronald 2 1344	810463708	357644	23718108	23666460	338080
ronald 2 1408	646631420	389016	26114208	26119436	368088
ronald 2 1472	1035475940	410640	28877308	28790080	389300
ronald 2 1536	806831848	398228	27853748	27818616	378980
ronald 2 1664	1333810740	478540	35062328	34994740	450944
ronald 2 1792	1511292804	499108	42723672	43008032	465592
ronald 2 1920	1750774416	554048	50816932	50813436	520476
ronald 2 2048	2150436028	579008	57526212	57504904	546712
ronald 2 2176	1824123644	774200	68735320	68455888	739996
ronald 2 2304	2743005564	803816	77669276	77674688	753068
ronald 2 2432	4389012984	864580	87830116	87479636	819716
ronald 2 2560	3656840752	889548	92310952	92144232	849216
ronald 2 2688	2887395160	982160	105805456	106181612	931992

ronald 2 2816	6787193948		1007392	123674184	123231456	962536
ronald 2 2944	7223365136		1090308	139651372	139871272	1046980
ronald 2 3072	7985690904		1114956	141550188	141205692	1059612
ronald 2 3328	10304408112		1268080	188844204	188195460	1207316
ronald 2 3584	11464294680		1388828	210398632	210599704	1322908
ronald 2 3840	12480253856		1528452	262134856	262136540	1463748
ronald 2 4096	19803051488		1711968	327920248	329972644	1630476
ronald 3 768	176743588		186068	6602356	6608276	171828
ronald 3 832	132489604		207928	7858936	7881548	193600
ronald 3 896	284624252		222500	9419660	9300152	206764
ronald 3 960	261636072		237832	10955044	10934996	220372
ronald 3 1024	526635056		234460	11175568	11153812	218468
ronald 3 1088	409190848		312676	14451916	14482992	289168
ronald 3 1152	415622248		327780	16233064	16302088	307388
ronald 3 1216	870392984		331388	18776368	18685784	311532
ronald 3 1280	827816400		340124	21011312	20994392	317632
ronald 3 1344	635417132		358496	23671436	23646420	335192
ronald 3 1408	756037204		391312	26204764	26045416	361716
ronald 3 1472	781355368		412236	28839284	28714120	382252
ronald 3 1536	847103960		400760	27615732	27681604	371984
ronald 3 1664	1146930448		480940	34860020	34780236	446056
ronald 3 1792	1398748224		501808	42012068	42330628	460156
ronald 3 1920	2206210876		555084	50145068	50519352	517872
ronald 3 2048	2740922776		579788	57424548	57406888	538580
ronald 3 2176	3189531240		776560	67955868	67875916	732836
ronald 3 2304	3042685372		793888	76942716	77049612	750816
ronald 3 2432	4893301312		867432	87523924	87158708	814880
ronald 3 2560	5379185616		886112	91655848	92065076	833072
ronald 3 2688	3530923360		981256	106609688	106115932	919036
ronald 3 2816	6119092168		1007740	122049616	121594052	941972
ronald 3 2944	8204747148		1086428	139835032	140042528	1034032
ronald 3 3072	7565524280		1114040	141699840	140469008	1049988
ronald 3 3328	15386175472		1278684	188388364	187313564	1193672
ronald 3 3584	13890709596		1389400	211127404	210402848	1326468
ronald 3 3840	15069935168		1544472	261261864	260799984	1456248
ronald 3 4096	16363248660		1702140	327669560	330556480	1617736
sflashv2 1	463149872				3455922	1867740
sflashv2 2	442110020				334692	421336
surf127eps 1	3063508	3073116				

System	secret key bytes	public key bytes	shared secret bytes	23-byte encrypt bytes	709-byte encrypt bytes	23-byte signed bytes	709-byte signed bytes
bls 1	20	120				43	729
claus 1	256	128	128				
claus++ 1	256	128	128				
curve25519-gaudry 1	32	32	32				

`donald 1 512`	84	64			63	749
`donald 1 1024`	148	128			63	749
`donald 1 2048`	276	256			63	749
`ecdonald 1 nist-b-163`	63	42			65	751
`ecdonald 1 nist-b-233`	90	60			83	769
`ecdonald 1 nist-b-283`	108	72			95	781
`ecdonald 1 nist-b-409`	156	104			127	813
`ecdonald 1 nist-b-571`	216	144			167	853
`ecdonald 1 nist-k-163`	63	42			65	751
`ecdonald 1 nist-k-233`	90	60			83	769
`ecdonald 1 nist-k-283`	108	72			95	781
`ecdonald 1 nist-k-409`	156	104			127	813
`ecdonald 1 nist-k-571`	216	144			167	853
`ecdonald 1 nist-p-192`	72	48			71	757
`ecdonald 1 nist-p-224`	84	56			79	765
`ecdonald 1 nist-p-256`	96	64			87	773
`ecdonald 1 nist-p-384`	144	96			119	805
`ecdonald 1 nist-p-521`	198	132			155	841
`ecdonald 1 secp160r1`	60	40			63	749
`ntru-enc 1 ees787ep1`	1854	1574	1574	2282		
`rainbow 1`	20107	31680			66	752
`ronald 1 768`	768	96	119	805	119	805
`ronald 1 832`	832	104	127	813	127	813
`ronald 1 896`	896	112	135	821	135	821
`ronald 1 960`	960	120	143	829	143	829
`ronald 1 1024`	1024	128	151	837	151	837
`ronald 1 1088`	1088	136	159	845	159	845
`ronald 1 1152`	1152	144	167	853	167	853
`ronald 1 1216`	1216	152	175	861	175	861
`ronald 1 1280`	1280	160	183	869	183	869
`ronald 1 1344`	1344	168	191	877	191	877
`ronald 1 1408`	1408	176	199	885	199	885
`ronald 1 1472`	1472	184	207	893	207	893
`ronald 1 1536`	1536	192	215	901	215	901
`ronald 1 1664`	1664	208	231	917	231	917
`ronald 1 1792`	1792	224	247	933	247	933
`ronald 1 1920`	1920	240	263	949	263	949
`ronald 1 2048`	2048	256	279	965	279	965
`ronald 1 2176`	2176	272	295	981	295	981
`ronald 1 2304`	2304	288	311	997	311	997
`ronald 1 2432`	2432	304	327	1013	327	1013
`ronald 1 2560`	2560	320	343	1029	343	1029
`ronald 1 2688`	2688	336	359	1045	359	1045
`ronald 1 2816`	2816	352	375	1061	375	1061
`ronald 1 2944`	2944	368	391	1077	391	1077
`ronald 1 3072`	3072	384	407	1093	407	1093
`ronald 1 3328`	3328	416	439	1125	439	1125

ronald 1 3584	3584	448	471	1157	471	1157
ronald 1 3840	3840	480	503	1189	503	1189
ronald 1 4096	4096	512	535	1221	535	1221
ronald 2 768	768	96	96	784	119	805
ronald 2 832	832	104	104	784	127	813
ronald 2 896	896	112	112	784	135	821
ronald 2 960	960	120	120	784	143	829
ronald 2 1024	1024	128	128	784	151	837
ronald 2 1088	1088	136	136	784	159	845
ronald 2 1152	1152	144	144	784	167	853
ronald 2 1216	1216	152	152	784	175	861
ronald 2 1280	1280	160	160	784	183	869
ronald 2 1344	1344	168	168	784	191	877
ronald 2 1408	1408	176	176	784	199	885
ronald 2 1472	1472	184	184	784	207	893
ronald 2 1536	1536	192	192	784	215	901
ronald 2 1664	1664	208	208	784	231	917
ronald 2 1792	1792	224	224	784	247	933
ronald 2 1920	1920	240	240	784	263	949
ronald 2 2048	2048	256	256	784	279	965
ronald 2 2176	2176	272	272	784	295	981
ronald 2 2304	2304	288	288	784	311	997
ronald 2 2432	2432	304	304	784	327	1013
ronald 2 2560	2560	320	320	784	343	1029
ronald 2 2688	2688	336	336	784	359	1045
ronald 2 2816	2816	352	352	784	375	1061
ronald 2 2944	2944	368	368	784	391	1077
ronald 2 3072	3072	384	384	784	407	1093
ronald 2 3328	3328	416	416	784	439	1125
ronald 2 3584	3584	448	448	784	471	1157
ronald 2 3840	3840	480	480	784	503	1189
ronald 2 4096	4096	512	512	784	535	1221
ronald 3 768	768	96	96	784	96	752
ronald 3 832	832	104	104	784	104	752
ronald 3 896	896	112	112	784	112	752
ronald 3 960	960	120	120	784	120	752
ronald 3 1024	1024	128	128	784	128	752
ronald 3 1088	1088	136	136	784	136	752
ronald 3 1152	1152	144	144	784	144	752
ronald 3 1216	1216	152	152	784	152	752
ronald 3 1280	1280	160	160	784	160	752
ronald 3 1344	1344	168	168	784	168	752
ronald 3 1408	1408	176	176	784	176	752
ronald 3 1472	1472	184	184	784	184	752
ronald 3 1536	1536	192	192	784	192	752
ronald 3 1664	1664	208	208	784	208	752
ronald 3 1792	1792	224	224	784	224	752

ronald 3 1920	1920	240		240	784	240	752
ronald 3 2048	2048	256		256	784	256	752
ronald 3 2176	2176	272		272	784	272	752
ronald 3 2304	2304	288		288	784	288	752
ronald 3 2432	2432	304		304	784	304	752
ronald 3 2560	2560	320		320	784	320	752
ronald 3 2688	2688	336		336	784	336	752
ronald 3 2816	2816	352		352	784	352	752
ronald 3 2944	2944	368		368	784	368	752
ronald 3 3072	3072	384		384	784	384	752
ronald 3 3328	3328	416		416	784	416	752
ronald 3 3584	3584	448		448	784	448	752
ronald 3 3840	3840	480		480	784	480	752
ronald 3 4096	4096	512		512	784	512	752
sflashv2 1	2823	19266				60	746
sflashv2 2	2823	19266				60	746
surf127eps 1	32	48	48				

6.19 x86, 3000MHz, Pentium 4 (f41), pclin118

System	key-pair cycles	share cycles	encrypt cycles	decrypt cycles	sign cycles	verify cycles
bls 1	24767190				2931922	34416563
claus 1	24882690	24841793				
claus++ 1	13912387	13858238				
curve25519-gaudry 1	3281505	3203602				
donald 1 512	1564358				1604497	1883115
donald 1 1024	4429267				4252822	5226810
donald 1 2048	13879680				12953340	15582517
ecdonald 1 nist-b-163	5387272				5590440	10968060
ecdonald 1 nist-b-233	10560570				10932900	21496155
ecdonald 1 nist-b-283	19715220				19977615	39450120
ecdonald 1 nist-b-409	48159622				47947395	95951535
ecdonald 1 nist-b-571	106086278				106847640	212917710
ecdonald 1 nist-k-163	5026110				5178293	10061108
ecdonald 1 nist-k-233	9636127				9900300	19568820
ecdonald 1 nist-k-283	17467800				17809650	35552528
ecdonald 1 nist-k-409	41404253				41318617	83612145
ecdonald 1 nist-k-571	92288355				93035497	186545205
ecdonald 1 nist-p-192	5050238				5277690	6292440
ecdonald 1 nist-p-224	6895890				7186530	8614845
ecdonald 1 nist-p-256	9006187				9305085	11182065
ecdonald 1 nist-p-384	21033248				21397492	25563608
ecdonald 1 nist-p-521	48217125				49074345	59789887
ecdonald 1 secp160r1	5201745				5392650	6465570
ntru-enc 1 ees787ep1	207816518		953648	1682273		
rainbow 1	352393575				1602495	2773328

ronald 1 768	156407948	223890	7255402	7242757	202920
ronald 1 832	198279248	243480	8623313	8634585	226425
ronald 1 896	240727740	257115	10094175	10104908	240180
ronald 1 960	258613170	274237	11541750	11600588	253793
ronald 1 1024	296476140	275175	12068760	12034432	252833
ronald 1 1088	488801482	350685	15345517	15376718	325680
ronald 1 1152	465349560	365077	17143125	17245695	338423
ronald 1 1216	456053505	382230	19319497	19331407	355777
ronald 1 1280	614028443	388590	21480893	21455205	357945
ronald 1 1344	749261580	405517	24209002	24159660	374895
ronald 1 1408	824731260	425295	26768520	26684273	390518
ronald 1 1472	900819832	445365	29651693	29793862	413378
ronald 1 1536	849448267	454455	28817550	28840807	417472
ronald 1 1664	1063252687	510600	35933715	35804235	473557
ronald 1 1792	1000758757	529777	43208550	42993563	491078
ronald 1 1920	1621808055	586237	51196223	51011220	541928
ronald 1 2048	2069300992	618285	61656158	60670972	577297
ronald 1 2176	2997402098	825547	66331058	65845012	773033
ronald 1 2304	2830435702	848250	76041653	76435275	796118
ronald 1 2432	4133556825	910897	87664095	87277890	859313
ronald 1 2560	4409285707	942068	89695575	89347140	884460
ronald 1 2688	4163014755	1040175	102707760	102546555	971775
ronald 1 2816	8194821660	1052325	116228055	116484922	999795
ronald 1 2944	7950791872	1144770	131670563	131520983	1077173
ronald 1 3072	8143912065	1282515	133684373	133956038	1217063
ronald 1 3328	11759174340	1485833	173299222	173917403	1424610
ronald 1 3584	15488835578	1629945	194613457	194381460	1533607
ronald 1 3840	13509507735	1795298	241153935	241496205	1713540
ronald 1 4096	21072384720	2009903	328525958	328223183	1918965
ronald 2 768	169090710	197542	7087343	7093552	193777
ronald 2 832	176672963	219540	8534955	8551327	211403
ronald 2 896	246996255	232973	10003095	10011322	227220
ronald 2 960	205410345	247410	11480827	11539508	239903
ronald 2 1024	233444925	248010	11914440	11864700	239985
ronald 2 1088	336081757	327322	15150855	15150945	310605
ronald 2 1152	553352715	340455	17087123	17132655	326092
ronald 2 1216	548562075	360675	19232498	19215098	340567
ronald 2 1280	799174687	358073	21341610	21321270	340447
ronald 2 1344	890457052	379388	23983237	24045652	358448
ronald 2 1408	606489442	397718	26473613	26538300	375795
ronald 2 1472	517464405	428108	30292268	29446417	400868
ronald 2 1536	1154027085	422040	28726928	28719563	395858
ronald 2 1664	1233683123	487193	35745833	35726512	458677
ronald 2 1792	1842899820	505552	43050105	42940733	474570
ronald 2 1920	1304451637	561615	51341145	51052935	524528
ronald 2 2048	2551950517	590130	60075143	60212445	558562
ronald 2 2176	2814149385	794370	66433815	66222803	759825

ronald 2 2304	3199341060	825525	76166393	76106235	782377	
ronald 2 2432	3344331045	887753	87605820	87481095	842797	
ronald 2 2560	2765973427	912923	89825340	89628262	870968	
ronald 2 2688	4488481898	1021410	102926115	102768608	974340	
ronald 2 2816	4757979525	1026885	116703165	116521680	1027493	
ronald 2 2944	5958175545	1197098	132226485	131851020	1062683	
ronald 2 3072	6551103720	1264252	134713342	134913727	1208595	
ronald 2 3328	10468273215	1375005	173759370	173774153	1382003	
ronald 2 3584	10744213635	1594260	195204165	195571568	1527127	
ronald 2 3840	12914374305	1767030	241614157	241358175	1701593	
ronald 2 4096	20577362978	1979873	328262205	328098960	1902383	
ronald 3 768	188014417	194205	7111800	7128360	185107	
ronald 3 832	187242960	217110	8492138	8496510	202305	
ronald 3 896	260397870	230220	9909900	9951517	215745	
ronald 3 960	323756153	247515	11482822	11486610	230407	
ronald 3 1024	256946340	247792	11838203	11872162	228240	
ronald 3 1088	280724010	321930	15126900	15143558	296587	
ronald 3 1152	441348555	335197	17131057	17194462	315128	
ronald 3 1216	464053223	355575	19210043	19140908	333352	
ronald 3 1280	428585453	354802	21454215	21469087	328785	
ronald 3 1344	685981875	379073	23902920	23989778	350437	
ronald 3 1408	733984980	397148	26485995	26536972	367425	
ronald 3 1472	948202463	418410	29426738	29410905	390945	
ronald 3 1536	1031617222	413722	28533488	28495687	386265	
ronald 3 1664	1083558195	478305	35518762	35582070	447667	
ronald 3 1792	865503855	505462	42673358	42807758	465772	
ronald 3 1920	2291759978	559530	50841015	50581905	519893	
ronald 3 2048	1798454033	595028	60353505	60802095	549720	
ronald 3 2176	2370543893	796185	66648157	67064280	752805	
ronald 3 2304	2696083762	823613	75954000	76033980	771015	
ronald 3 2432	3958271205	888840	88005142	87827932	834180	
ronald 3 2560	3624900915	916118	89324085	89328802	862672	
ronald 3 2688	5461552425	997965	102907425	102402225	966225	
ronald 3 2816	8663701320	1030418	117554490	116481015	1020758	
ronald 3 2944	8446478025	1189043	132399855	132414165	1052047	
ronald 3 3072	7965225022	1264568	134078888	134209755	1075260	
ronald 3 3328	16112353980	1378305	472146577	472365660	1376438	
ronald 3 3584	10363615755	1604918	196281772	494156655	1503735	
ronald 3 3840	42197740553	1764848	540898290	540583830	1697160	
ronald 3 4096	47654510535	1980720	628212540	627968025	1892925	
sflashv2 1	575777895			4011068	2181428	
sflashv2 2	562249560			387983	474255	
surf127eps 1	3117330	3145080				

System	secret key	public key	shared secret	23-byte encrypt	709-byte encrypt	23-byte signed	709-byte signed

	bytes	bytes	bytes	bytes	bytes	bytes	bytes
bls 1	20	120				43	729
claus 1	256	128	128				
claus++ 1	256	128	128				
curve25519-gaudry 1	32	32	32				
donald 1 512	84	64				63	749
donald 1 1024	148	128				63	749
donald 1 2048	276	256				63	749
ecdonald 1 nist-b-163	63	42				65	751
ecdonald 1 nist-b-233	90	60				83	769
ecdonald 1 nist-b-283	108	72				95	781
ecdonald 1 nist-b-409	156	104				127	813
ecdonald 1 nist-b-571	216	144				167	853
ecdonald 1 nist-k-163	63	42				65	751
ecdonald 1 nist-k-233	90	60				83	769
ecdonald 1 nist-k-283	108	72				95	781
ecdonald 1 nist-k-409	156	104				127	813
ecdonald 1 nist-k-571	216	144				167	853
ecdonald 1 nist-p-192	72	48				71	757
ecdonald 1 nist-p-224	84	56				79	765
ecdonald 1 nist-p-256	96	64				87	773
ecdonald 1 nist-p-384	144	96				119	805
ecdonald 1 nist-p-521	198	132				155	841
ecdonald 1 secp160r1	60	40				63	749
ntru-enc 1 ees787ep1	1854	1574		1574	2282		
rainbow 1	20107	31680				66	752
ronald 1 768	768	96		119	805	119	805
ronald 1 832	832	104		127	813	127	813
ronald 1 896	896	112		135	821	135	821
ronald 1 960	960	120		143	829	143	829
ronald 1 1024	1024	128		151	837	151	837
ronald 1 1088	1088	136		159	845	159	845
ronald 1 1152	1152	144		167	853	167	853
ronald 1 1216	1216	152		175	861	175	861
ronald 1 1280	1280	160		183	869	183	869
ronald 1 1344	1344	168		191	877	191	877
ronald 1 1408	1408	176		199	885	199	885
ronald 1 1472	1472	184		207	893	207	893
ronald 1 1536	1536	192		215	901	215	901
ronald 1 1664	1664	208		231	917	231	917
ronald 1 1792	1792	224		247	933	247	933
ronald 1 1920	1920	240		263	949	263	949
ronald 1 2048	2048	256		279	965	279	965
ronald 1 2176	2176	272		295	981	295	981
ronald 1 2304	2304	288		311	997	311	997
ronald 1 2432	2432	304		327	1013	327	1013

`ronald 1 2560`	2560	320	343	1029	343	1029
`ronald 1 2688`	2688	336	359	1045	359	1045
`ronald 1 2816`	2816	352	375	1061	375	1061
`ronald 1 2944`	2944	368	391	1077	391	1077
`ronald 1 3072`	3072	384	407	1093	407	1093
`ronald 1 3328`	3328	416	439	1125	439	1125
`ronald 1 3584`	3584	448	471	1157	471	1157
`ronald 1 3840`	3840	480	503	1189	503	1189
`ronald 1 4096`	4096	512	535	1221	535	1221
`ronald 2 768`	768	96	96	784	119	805
`ronald 2 832`	832	104	104	784	127	813
`ronald 2 896`	896	112	112	784	135	821
`ronald 2 960`	960	120	120	784	143	829
`ronald 2 1024`	1024	128	128	784	151	837
`ronald 2 1088`	1088	136	136	784	159	845
`ronald 2 1152`	1152	144	144	784	167	853
`ronald 2 1216`	1216	152	152	784	175	861
`ronald 2 1280`	1280	160	160	784	183	869
`ronald 2 1344`	1344	168	168	784	191	877
`ronald 2 1408`	1408	176	176	784	199	885
`ronald 2 1472`	1472	184	184	784	207	893
`ronald 2 1536`	1536	192	192	784	215	901
`ronald 2 1664`	1664	208	208	784	231	917
`ronald 2 1792`	1792	224	224	784	247	933
`ronald 2 1920`	1920	240	240	784	263	949
`ronald 2 2048`	2048	256	256	784	279	965
`ronald 2 2176`	2176	272	272	784	295	981
`ronald 2 2304`	2304	288	288	784	311	997
`ronald 2 2432`	2432	304	304	784	327	1013
`ronald 2 2560`	2560	320	320	784	343	1029
`ronald 2 2688`	2688	336	336	784	359	1045
`ronald 2 2816`	2816	352	352	784	375	1061
`ronald 2 2944`	2944	368	368	784	391	1077
`ronald 2 3072`	3072	384	384	784	407	1093
`ronald 2 3328`	3328	416	416	784	439	1125
`ronald 2 3584`	3584	448	448	784	471	1157
`ronald 2 3840`	3840	480	480	784	503	1189
`ronald 2 4096`	4096	512	512	784	535	1221
`ronald 3 768`	768	96	96	784	96	752
`ronald 3 832`	832	104	104	784	104	752
`ronald 3 896`	896	112	112	784	112	752
`ronald 3 960`	960	120	120	784	120	752
`ronald 3 1024`	1024	128	128	784	128	752
`ronald 3 1088`	1088	136	136	784	136	752
`ronald 3 1152`	1152	144	144	784	144	752
`ronald 3 1216`	1216	152	152	784	152	752
`ronald 3 1280`	1280	160	160	784	160	752

ronald 3 1344	1344	168		168	784	168	752
ronald 3 1408	1408	176		176	784	176	752
ronald 3 1472	1472	184		184	784	184	752
ronald 3 1536	1536	192		192	784	192	752
ronald 3 1664	1664	208		208	784	208	752
ronald 3 1792	1792	224		224	784	224	752
ronald 3 1920	1920	240		240	784	240	752
ronald 3 2048	2048	256		256	784	256	752
ronald 3 2176	2176	272		272	784	272	752
ronald 3 2304	2304	288		288	784	288	752
ronald 3 2432	2432	304		304	784	304	752
ronald 3 2560	2560	320		320	784	320	752
ronald 3 2688	2688	336		336	784	336	752
ronald 3 2816	2816	352		352	784	352	752
ronald 3 2944	2944	368		368	784	368	752
ronald 3 3072	3072	384		384	784	384	752
ronald 3 3328	3328	416		416	784	416	752
ronald 3 3584	3584	448		448	784	448	752
ronald 3 3840	3840	480		480	784	480	752
ronald 3 4096	4096	512		512	784	512	752
sflashv2 1	2823	19266				60	746
sflashv2 2	2823	19266				60	746
surf127eps 1	32	48	48				

6.20 x86, 3066MHz, Xeon (f25), td162

System	key-pair cycles	share cycles	encrypt cycles	decrypt cycles	sign cycles	verify cycles
bls 1	19164992				2535888	27243672
claus 1	25438436	25214408				
claus++ 1	13985056	13644332				
curve25519-gaudry 1	5517220	3202072				
donald 1 512	2427180				1540064	1833740
donald 1 1024	4437296				4411412	5208460
donald 1 2048	14593212				13279464	16047064
ecdonald 1 nist-b-163	10775288				5462284	10719484
ecdonald 1 nist-b-233	11115916				10211296	20181616
ecdonald 1 nist-b-283	18933712				19172052	38064364
ecdonald 1 nist-b-409	43603848				43932220	87260112
ecdonald 1 nist-b-571	98343240				98678700	197305044
ecdonald 1 nist-k-163	4959256				5104284	10034852
ecdonald 1 nist-k-233	9116116				9244552	18120232
ecdonald 1 nist-k-283	16987396				17213468	34739324
ecdonald 1 nist-k-409	38092552				38329680	76450100
ecdonald 1 nist-k-571	86972116				87577760	175411492
ecdonald 1 nist-p-192	7680332				4517456	5538364
ecdonald 1 nist-p-224	10352688				5726008	7077376

ecdonald 1 nist-p-256	13263004			7741932	9371084
ecdonald 1 nist-p-384	16846440			16994640	20779408
ecdonald 1 nist-p-521	43538048			43900468	53745752
ecdonald 1 secp160r1	8112080			4828112	5797168
ntru-enc 1 ees787ep1	166482280	766008	1297288		
ronald 1 768	152321860	200588	6960656	6867152	183344
ronald 1 832	165154568	222276	8007052	8173724	206644
ronald 1 896	208933948	240272	9501772	9532604	219488
ronald 1 960	299902124	255816	11263856	11342240	234892
ronald 1 1024	319776340	253972	11091516	11171448	235344
ronald 1 1088	395720760	316748	15128212	14626224	298404
ronald 1 1152	309479796	344544	16178128	16173384	318720
ronald 1 1216	612024652	358452	18749692	18664428	340388
ronald 1 1280	554206528	356156	20392680	20372580	328844
ronald 1 1344	523884104	381520	23237452	23438896	356004
ronald 1 1408	942464108	394836	25950916	25917168	374364
ronald 1 1472	570497612	423280	28275788	28485584	398096
ronald 1 1536	846369736	434640	28374296	28347332	410480
ronald 1 1664	955375584	493644	35019344	34404360	455184
ronald 1 1792	1238233104	521084	42885788	43354124	488172
ronald 1 1920	1687476964	578152	50482068	50251040	543960
ronald 1 2048	2260306908	604552	58072348	58475736	566996
ronald 1 2176	3733974080	802604	69104108	69603448	757444
ronald 1 2304	3374482808	825964	78801204	79255672	778820
ronald 1 2432	2445977128	891244	91220524	91140560	845264
ronald 1 2560	4244300668	905896	93681236	93834784	856372
ronald 1 2688	4816654436	989680	108220380	108390668	934360
ronald 1 2816	5504915092	1031116	122613200	123973088	975792
ronald 1 2944	6991563852	1106324	138166848	140795776	1053764
ronald 1 3072	8080495404	1149224	146489164	145667492	1096656
ronald 1 3328	12869825396	1311408	190009796	190435012	1244160
ronald 1 3584	20695459524	1404720	214519184	214665616	1336928
ronald 1 3840	17507674752	1542764	266193924	264759500	1490616
ronald 1 4096	19922068812	1742900	331012476	329356168	1657220
ronald 2 768	199320688	185812	6936144	6959480	184288
ronald 2 832	189776916	201072	8087184	8033212	202208
ronald 2 896	210301420	222496	9808768	9755468	219016
ronald 2 960	269812248	241416	11302384	11378340	230744
ronald 2 1024	442422364	242448	10983392	10926736	229380
ronald 2 1088	474350072	302692	14636956	14603432	294724
ronald 2 1152	371616920	324248	15991756	15992448	310996
ronald 2 1216	705366824	367320	18674848	18640624	337676
ronald 2 1280	476353616	331868	20710360	20712256	323436
ronald 2 1344	608970344	359384	23382220	23373192	342188
ronald 2 1408	695293724	382968	30429376	26460996	354916
ronald 2 1472	1187182452	402928	28358116	28369264	381764
ronald 2 1536	1339083364	395636	27464096	27847344	378016

ronald 2 1664	926725140	476932	35008948	44183008	504228
ronald 2 1792	2077625388	769356	65739316	77763420	847772
ronald 2 1920	1653257580	562120	51847112	51385124	519368
ronald 2 2048	1839072616	586952	58557496	58832040	560384
ronald 2 2176	2663608220	778012	69521552	70168940	739516
ronald 2 2304	2697364248	786652	78710012	79136728	756124
ronald 2 2432	3419290864	858320	92124544	92203680	823968
ronald 2 2560	6879846848	900160	93595516	93324596	864168
ronald 2 2688	6148581948	988520	108191020	108203972	945144
ronald 2 2816	5872852484	1013240	123575376	123200244	969324
ronald 2 2944	8744244524	1078524	138779608	138653280	1034732
ronald 2 3072	9518247632	1132288	145701952	145411484	1085752
ronald 2 3328	11721728124	1282772	190082104	190504964	1233340
ronald 2 3584	12946561264	1419284	212123456	212108696	1359292
ronald 2 3840	20843621696	1563052	269447764	268809480	1480688
ronald 2 4096	24049748192	1714744	333110380	334959924	1640220
ronald 3 768	128497368	189492	6856932	6891524	175608
ronald 3 832	170650536	208504	8430848	8392152	194084
ronald 3 896	221652592	217212	9799724	9813648	207120
ronald 3 960	276926148	234468	11077108	11133136	221016
ronald 3 1024	440476160	240796	11573144	11593932	225880
ronald 3 1088	285693976	311800	14696612	14644728	286272
ronald 3 1152	522635616	323300	16688896	16829288	300396
ronald 3 1216	488818300	343096	18675000	18493600	321356
ronald 3 1280	643341712	338936	20819320	20859728	312748
ronald 3 1344	680456136	366988	23433868	23461128	338264
ronald 3 1408	907007324	382356	25998312	26034744	353200
ronald 3 1472	924128932	407344	28348772	28412848	382680
ronald 3 1536	810922708	404544	27450808	27366344	376464
ronald 3 1664	1484574656	479416	35934804	36325452	434764
ronald 3 1792	1178151748	481096	41207836	42495700	458228
ronald 3 1920	1485726848	554840	51089620	51220068	514272
ronald 3 2048	2055933780	577672	58058000	58688020	539804
ronald 3 2176	2937098320	769304	68897372	68830024	736168
ronald 3 2304	4290550084	806444	80527216	80079656	764540
ronald 3 2432	3333974908	895664	91049392	90630232	829760
ronald 3 2560	3037188064	897008	94369668	93925968	851580
ronald 3 2688	4088607280	988296	107857980	107265652	938596
ronald 3 2816	5474062728	1009696	123648924	123245432	957912
ronald 3 2944	6071768712	1094868	138281484	138193276	1040864
ronald 3 3072	8740358364	1113448	144729236	144227980	1045628
ronald 3 3328	12124210568	1283464	190397616	190842536	1208236
ronald 3 3584	19400219560	1417600	218906220	218403064	1338184
ronald 3 3840	16419986320	1549128	269691976	271004536	1489836
ronald 3 4096	27694017652	1701184	331164784	333165788	1658624
sflashv2 1	821709082			3733820	1762760
sflashv2 2	847617032			368996	365800

`surf127eps 1`	5432716	3077504

System	secret key bytes	public key bytes	shared secret bytes	23-byte encrypt bytes	709-byte encrypt bytes	23-byte signed bytes	709-byte signed bytes
`bls 1`	20	120				43	729
`claus 1`	256	128	128				
`claus++ 1`	256	128	128				
`curve25519-gaudry 1`	32	32	32				
`donald 1 512`	84	64				63	749
`donald 1 1024`	148	128				63	749
`donald 1 2048`	276	256				63	749
`ecdonald 1 nist-b-163`	63	42				65	751
`ecdonald 1 nist-b-233`	90	60				83	769
`ecdonald 1 nist-b-283`	108	72				95	781
`ecdonald 1 nist-b-409`	156	104				127	813
`ecdonald 1 nist-b-571`	216	144				167	853
`ecdonald 1 nist-k-163`	63	42				65	751
`ecdonald 1 nist-k-233`	90	60				83	769
`ecdonald 1 nist-k-283`	108	72				95	781
`ecdonald 1 nist-k-409`	156	104				127	813
`ecdonald 1 nist-k-571`	216	144				167	853
`ecdonald 1 nist-p-192`	72	48				71	757
`ecdonald 1 nist-p-224`	84	56				79	765
`ecdonald 1 nist-p-256`	96	64				87	773
`ecdonald 1 nist-p-384`	144	96				119	805
`ecdonald 1 nist-p-521`	198	132				155	841
`ecdonald 1 secp160r1`	60	40				63	749
`ntru-enc 1 ees787ep1`	1854	1574		1574	2282		
`ronald 1 768`	768	96		119	805	119	805
`ronald 1 832`	832	104		127	813	127	813
`ronald 1 896`	896	112		135	821	135	821
`ronald 1 960`	960	120		143	829	143	829
`ronald 1 1024`	1024	128		151	837	151	837
`ronald 1 1088`	1088	136		159	845	159	845
`ronald 1 1152`	1152	144		167	853	167	853
`ronald 1 1216`	1216	152		175	861	175	861
`ronald 1 1280`	1280	160		183	869	183	869
`ronald 1 1344`	1344	168		191	877	191	877
`ronald 1 1408`	1408	176		199	885	199	885
`ronald 1 1472`	1472	184		207	893	207	893
`ronald 1 1536`	1536	192		215	901	215	901
`ronald 1 1664`	1664	208		231	917	231	917
`ronald 1 1792`	1792	224		247	933	247	933
`ronald 1 1920`	1920	240		263	949	263	949
`ronald 1 2048`	2048	256		279	965	279	965
`ronald 1 2176`	2176	272		295	981	295	981

ronald 1 2304	2304	288	311	997	311	997
ronald 1 2432	2432	304	327	1013	327	1013
ronald 1 2560	2560	320	343	1029	343	1029
ronald 1 2688	2688	336	359	1045	359	1045
ronald 1 2816	2816	352	375	1061	375	1061
ronald 1 2944	2944	368	391	1077	391	1077
ronald 1 3072	3072	384	407	1093	407	1093
ronald 1 3328	3328	416	439	1125	439	1125
ronald 1 3584	3584	448	471	1157	471	1157
ronald 1 3840	3840	480	503	1189	503	1189
ronald 1 4096	4096	512	535	1221	535	1221
ronald 2 768	768	96	96	784	119	805
ronald 2 832	832	104	104	784	127	813
ronald 2 896	896	112	112	784	135	821
ronald 2 960	960	120	120	784	143	829
ronald 2 1024	1024	128	128	784	151	837
ronald 2 1088	1088	136	136	784	159	845
ronald 2 1152	1152	144	144	784	167	853
ronald 2 1216	1216	152	152	784	175	861
ronald 2 1280	1280	160	160	784	183	869
ronald 2 1344	1344	168	168	784	191	877
ronald 2 1408	1408	176	176	784	199	885
ronald 2 1472	1472	184	184	784	207	893
ronald 2 1536	1536	192	192	784	215	901
ronald 2 1664	1664	208	208	784	231	917
ronald 2 1792	1792	224	224	784	247	933
ronald 2 1920	1920	240	240	784	263	949
ronald 2 2048	2048	256	256	784	279	965
ronald 2 2176	2176	272	272	784	295	981
ronald 2 2304	2304	288	288	784	311	997
ronald 2 2432	2432	304	304	784	327	1013
ronald 2 2560	2560	320	320	784	343	1029
ronald 2 2688	2688	336	336	784	359	1045
ronald 2 2816	2816	352	352	784	375	1061
ronald 2 2944	2944	368	368	784	391	1077
ronald 2 3072	3072	384	384	784	407	1093
ronald 2 3328	3328	416	416	784	439	1125
ronald 2 3584	3584	448	448	784	471	1157
ronald 2 3840	3840	480	480	784	503	1189
ronald 2 4096	4096	512	512	784	535	1221
ronald 3 768	768	96	96	784	96	752
ronald 3 832	832	104	104	784	104	752
ronald 3 896	896	112	112	784	112	752
ronald 3 960	960	120	120	784	120	752
ronald 3 1024	1024	128	128	784	128	752
ronald 3 1088	1088	136	136	784	136	752
ronald 3 1152	1152	144	144	784	144	752

ronald 3 1216	1216	152		152	784	152	752
ronald 3 1280	1280	160		160	784	160	752
ronald 3 1344	1344	168		168	784	168	752
ronald 3 1408	1408	176		176	784	176	752
ronald 3 1472	1472	184		184	784	184	752
ronald 3 1536	1536	192		192	784	192	752
ronald 3 1664	1664	208		208	784	208	752
ronald 3 1792	1792	224		224	784	224	752
ronald 3 1920	1920	240		240	784	240	752
ronald 3 2048	2048	256		256	784	256	752
ronald 3 2176	2176	272		272	784	272	752
ronald 3 2304	2304	288		288	784	288	752
ronald 3 2432	2432	304		304	784	304	752
ronald 3 2560	2560	320		320	784	320	752
ronald 3 2688	2688	336		336	784	336	752
ronald 3 2816	2816	352		352	784	352	752
ronald 3 2944	2944	368		368	784	368	752
ronald 3 3072	3072	384		384	784	384	752
ronald 3 3328	3328	416		416	784	416	752
ronald 3 3584	3584	448		448	784	448	752
ronald 3 3840	3840	480		480	784	480	752
ronald 3 4096	4096	512		512	784	512	752
sflashv2 1	2823	19266				60	746
sflashv2 2	2823	19266				60	746
surf127eps 1	32	48	48				

6.21 x86, 3200MHz, Xeon (f25), td186

System	key-pair cycles	share cycles	encrypt cycles	decrypt cycles	sign cycles	verify cycles
bls 1	26910340				2530200	28937656
claus 1	30774424	25769432				
claus++ 1	19381280	13708076				
curve25519-gaudry 1	5243400	4948936				
donald 1 512	2151660				1542400	1816656
donald 1 1024	6174012				4152620	5059788
donald 1 2048	19508868				13125084	16011252
ecdonald 1 nist-b-163	8931756				5514972	10770980
ecdonald 1 nist-b-233	17724112				10186964	19974228
ecdonald 1 nist-b-283	25140764				19270476	38429144
ecdonald 1 nist-b-409	43842724				43826084	87518116
ecdonald 1 nist-b-571	98542824				99164948	197840224
ecdonald 1 nist-k-163	8255300				5135076	9994932
ecdonald 1 nist-k-233	16369744				9396468	18237000
ecdonald 1 nist-k-283	29526412				17261036	34216932
ecdonald 1 nist-k-409	38367876				38517556	76489836
ecdonald 1 nist-k-571	87177520				87826844	174525480

ecdonald 1 nist-p-192	7310232			4416432	5307432
ecdonald 1 nist-p-224	9660504			10264932	7235168
ecdonald 1 nist-p-256	12935896			7565300	9170652
ecdonald 1 nist-p-384	27119272			17282648	20611016
ecdonald 1 nist-p-521	43830280			44379988	54112780
ecdonald 1 secp160r1	7451176			5008008	6017824
ntru-enc 1 ees787ep1	172763240	729644	1254100		
ronald 1 768	188191760	206860	6901300	6969812	184944
ronald 1 832	226196616	225408	8275712	8252788	202604
ronald 1 896	221475528	245212	9791728	9730068	216492
ronald 1 960	270598796	255580	11312504	11321024	230324
ronald 1 1024	320626440	253380	11013660	11000264	228684
ronald 1 1088	377129420	321772	14624712	14654384	294672
ronald 1 1152	428473756	339552	16216200	16096992	311488
ronald 1 1216	487820876	363392	18705492	18775492	330084
ronald 1 1280	599260580	366544	20862156	20767116	326536
ronald 1 1344	718289012	379268	23366856	23536872	350632
ronald 1 1408	727771612	398596	30394980	25826908	360308
ronald 1 1472	1184411388	424168	28491096	28348140	388160
ronald 1 1536	777531204	431176	28486656	28409972	387224
ronald 1 1664	1389161800	496452	35096536	35702768	451588
ronald 1 1792	1544188720	517892	43398968	43127760	477288
ronald 1 1920	2205423520	580560	49852092	50234264	534692
ronald 1 2048	2547032408	616616	57867220	57841520	556000
ronald 1 2176	3148794120	804828	68386184	68406232	745608
ronald 1 2304	4423893256	830616	79482640	79057408	770404
ronald 1 2432	3959744688	884548	91559880	91357952	829388
ronald 1 2560	6573383488	923092	93730564	93851272	866100
ronald 1 2688	4847545032	995092	108557836	108354084	937264
ronald 1 2816	4684159756	1046052	124205732	123294668	979720
ronald 1 2944	9226987692	1105148	139404480	140154368	1037352
ronald 1 3072	6379728984	1142996	144384048	143275564	1076040
ronald 1 3328	8901095588	1277832	189234108	188745580	1214228
ronald 1 3584	11556557784	1444572	216146340	215629252	1340104
ronald 1 3840	13624077332	1552500	265353724	267099100	1474664
ronald 1 4096	12863759832	1723128	329345976	330924120	1625048
ronald 2 768	188925032	190484	6534584	6510820	188292
ronald 2 832	245799484	359456	14266040	10805656	260088
ronald 2 896	355315948	226396	13029616	9811968	217616
ronald 2 960	398662024	416000	19906876	11295960	231244
ronald 2 1024	368898512	238312	11049040	11024428	230564
ronald 2 1088	15956899192	302676	14563536	14629044	296412
ronald 2 1152	422662080	334536	16774180	16426748	317684
ronald 2 1216	533824932	343412	18608732	18506020	323100
ronald 2 1280	640862636	339044	20714576	20718864	313204
ronald 2 1344	1138211984	422064	69712560	69604796	399360
ronald 2 1408	5762564928	390240	25919544	25760208	364968

ronald 2 1472	897088152	402092	28302536	28464696	381820
ronald 2 1536	747115980	403364	27501852	27547144	382448
ronald 2 1664	1203621464	499816	35941584	36201100	464580
ronald 2 1792	1269760272	499080	42515200	42616256	465124
ronald 2 1920	1909159332	700756	51437360	50743972	640668
ronald 2 2048	1939212888	593224	58378816	58678444	552232
ronald 2 2176	2239705956	766052	69042428	69097928	726496
ronald 2 2304	3592555092	797424	79783332	79305436	747820
ronald 2 2432	2171383220	862868	91175596	92931660	828516
ronald 2 2560	4495124632	900700	93032056	93343004	853424
ronald 2 2688	5675273900	969344	109621288	109183168	916580
ronald 2 2816	18651520728	1175480	345849420	343117396	1099368
ronald 2 2944	6087225408	1076288	140080796	140535860	1020128
ronald 2 3072	8263999092	1810572	173213736	172276524	1754712
ronald 2 3328	9973183100	1286348	190294164	189890760	1218368
ronald 2 3584	12356495136	1430180	216216860	214189944	1341152
ronald 2 3840	22749245520	1544572	269412464	267918728	1473180
ronald 2 4096	44517895824	3363460	627259448	626521600	3287972
ronald 3 768	195528848	189796	6914356	6934636	174944
ronald 3 832	259380832	236176	8456992	8350344	197244
ronald 3 896	254852064	226944	9186612	9442988	203136
ronald 3 960	313171346	234152	11007232	10983036	214808
ronald 3 1024	336216600	240504	11078884	11059308	215328
ronald 3 1088	378973356	303632	14532988	14553128	278848
ronald 3 1152	364160028	321336	16718332	16423420	295876
ronald 3 1216	578477772	339492	18884988	18826828	316700
ronald 3 1280	801372200	334800	20655704	20618804	308884
ronald 3 1344	1309110980	4880212	65618168	64560172	4494888
ronald 3 1408	763036212	378212	26218144	26088184	348024
ronald 3 1472	636755488	404268	28809196	28451380	376172
ronald 3 1536	907488292	398704	27750232	27850776	372408
ronald 3 1664	1032484460	470412	35899740	35860408	436404
ronald 3 1792	1189957132	494820	42774264	42898848	449256
ronald 3 1920	1510861912	558052	49614640	50478812	517012
ronald 3 2048	1826410156	583388	59206724	58715936	543860
ronald 3 2176	3468789264	793448	68647380	68572364	726520
ronald 3 2304	2984208624	13357532	144388200	144826408	13091332
ronald 3 2432	3930061592	861044	91472632	91090192	819304
ronald 3 2560	3573821660	894800	93631828	93943184	832672
ronald 3 2688	3764662584	983276	107310032	107616792	922720
ronald 3 2816	5911869148	992480	123869028	123488760	940316
ronald 3 2944	6486411884	1107840	139621404	138541376	1027344
ronald 3 3072	7460961936	1119944	145636312	145000292	1044420
ronald 3 3328	6439339548	1347312	191783992	190169368	1200768
ronald 3 3584	10185309072	1379480	215037960	214153896	1329352
ronald 3 3840	14447634696	1552432	267837884	269060728	1462096
ronald 3 4096	23847890832	1696364	332153920	334468196	1653552

sflashv2 1	5516995872			21152132	5143532
sflashv2 2	793121996			368776	425020
surf127eps 1	4925164	4871236			

System	secret key bytes	public key bytes	shared secret bytes	23-byte encrypt bytes	709-byte encrypt bytes	23-byte signed bytes	709-byte signed bytes
bls 1	20	120				43	729
claus 1	256	128	128				
claus++ 1	256	128	128				
curve25519-gaudry 1	32	32	32				
donald 1 512	84	64				63	749
donald 1 1024	148	128				63	749
donald 1 2048	276	256				63	749
ecdonald 1 nist-b-163	63	42				65	751
ecdonald 1 nist-b-233	90	60				83	769
ecdonald 1 nist-b-283	108	72				95	781
ecdonald 1 nist-b-409	156	104				127	813
ecdonald 1 nist-b-571	216	144				167	853
ecdonald 1 nist-k-163	63	42				65	751
ecdonald 1 nist-k-233	90	60				83	769
ecdonald 1 nist-k-283	108	72				95	781
ecdonald 1 nist-k-409	156	104				127	813
ecdonald 1 nist-k-571	216	144				167	853
ecdonald 1 nist-p-192	72	48				71	757
ecdonald 1 nist-p-224	84	56				79	765
ecdonald 1 nist-p-256	96	64				87	773
ecdonald 1 nist-p-384	144	96				119	805
ecdonald 1 nist-p-521	198	132				155	841
ecdonald 1 secp160r1	60	40				63	749
ntru-enc 1 ees787ep1	1854	1574		1574	2282		
ronald 1 768	768	96		119	805	119	805
ronald 1 832	832	104		127	813	127	813
ronald 1 896	896	112		135	821	135	821
ronald 1 960	960	120		143	829	143	829
ronald 1 1024	1024	128		151	837	151	837
ronald 1 1088	1088	136		159	845	159	845
ronald 1 1152	1152	144		167	853	167	853
ronald 1 1216	1216	152		175	861	175	861
ronald 1 1280	1280	160		183	869	183	869
ronald 1 1344	1344	168		191	877	191	877
ronald 1 1408	1408	176		199	885	199	885
ronald 1 1472	1472	184		207	893	207	893
ronald 1 1536	1536	192		215	901	215	901
ronald 1 1664	1664	208		231	917	231	917
ronald 1 1792	1792	224		247	933	247	933
ronald 1 1920	1920	240		263	949	263	949

`ronald 1 2048`	2048	256	279	965	279	965
`ronald 1 2176`	2176	272	295	981	295	981
`ronald 1 2304`	2304	288	311	997	311	997
`ronald 1 2432`	2432	304	327	1013	327	1013
`ronald 1 2560`	2560	320	343	1029	343	1029
`ronald 1 2688`	2688	336	359	1045	359	1045
`ronald 1 2816`	2816	352	375	1061	375	1061
`ronald 1 2944`	2944	368	391	1077	391	1077
`ronald 1 3072`	3072	384	407	1093	407	1093
`ronald 1 3328`	3328	416	439	1125	439	1125
`ronald 1 3584`	3584	448	471	1157	471	1157
`ronald 1 3840`	3840	480	503	1189	503	1189
`ronald 1 4096`	4096	512	535	1221	535	1221
`ronald 2 768`	768	96	96	784	119	805
`ronald 2 832`	832	104	104	784	127	813
`ronald 2 896`	896	112	112	784	135	821
`ronald 2 960`	960	120	120	784	143	829
`ronald 2 1024`	1024	128	128	784	151	837
`ronald 2 1088`	1088	136	136	784	159	845
`ronald 2 1152`	1152	144	144	784	167	853
`ronald 2 1216`	1216	152	152	784	175	861
`ronald 2 1280`	1280	160	160	784	183	869
`ronald 2 1344`	1344	168	168	784	191	877
`ronald 2 1408`	1408	176	176	784	199	885
`ronald 2 1472`	1472	184	184	784	207	893
`ronald 2 1536`	1536	192	192	784	215	901
`ronald 2 1664`	1664	208	208	784	231	917
`ronald 2 1792`	1792	224	224	784	247	933
`ronald 2 1920`	1920	240	240	784	263	949
`ronald 2 2048`	2048	256	256	784	279	965
`ronald 2 2176`	2176	272	272	784	295	981
`ronald 2 2304`	2304	288	288	784	311	997
`ronald 2 2432`	2432	304	304	784	327	1013
`ronald 2 2560`	2560	320	320	784	343	1029
`ronald 2 2688`	2688	336	336	784	359	1045
`ronald 2 2816`	2816	352	352	784	375	1061
`ronald 2 2944`	2944	368	368	784	391	1077
`ronald 2 3072`	3072	384	384	784	407	1093
`ronald 2 3328`	3328	416	416	784	439	1125
`ronald 2 3584`	3584	448	448	784	471	1157
`ronald 2 3840`	3840	480	480	784	503	1189
`ronald 2 4096`	4096	512	512	784	535	1221
`ronald 3 768`	768	96	96	784	96	752
`ronald 3 832`	832	104	104	784	104	752
`ronald 3 896`	896	112	112	784	112	752
`ronald 3 960`	960	120	120	784	120	752
`ronald 3 1024`	1024	128	128	784	128	752

ronald 3 1088	1088	136		136	784	136	752
ronald 3 1152	1152	144		144	784	144	752
ronald 3 1216	1216	152		152	784	152	752
ronald 3 1280	1280	160		160	784	160	752
ronald 3 1344	1344	168		168	784	168	752
ronald 3 1408	1408	176		176	784	176	752
ronald 3 1472	1472	184		184	784	184	752
ronald 3 1536	1536	192		192	784	192	752
ronald 3 1664	1664	208		208	784	208	752
ronald 3 1792	1792	224		224	784	224	752
ronald 3 1920	1920	240		240	784	240	752
ronald 3 2048	2048	256		256	784	256	752
ronald 3 2176	2176	272		272	784	272	752
ronald 3 2304	2304	288		288	784	288	752
ronald 3 2432	2432	304		304	784	304	752
ronald 3 2560	2560	320		320	784	320	752
ronald 3 2688	2688	336		336	784	336	752
ronald 3 2816	2816	352		352	784	352	752
ronald 3 2944	2944	368		368	784	368	752
ronald 3 3072	3072	384		384	784	384	752
ronald 3 3328	3328	416		416	784	416	752
ronald 3 3584	3584	448		448	784	448	752
ronald 3 3840	3840	480		480	784	480	752
ronald 3 4096	4096	512		512	784	512	752
sflashv2 1	2823	19266				60	746
sflashv2 2	2823	19266				60	746
surf127eps 1	32	48	48				

6.22 x86, 3400MHz, Pentium 4 (f29), shell

System	key-pair cycles	share cycles	encrypt cycles	decrypt cycles	sign cycles	verify cycles
bls 1	22491252				2523516	35962568
claus 1	24632432	24581864				
claus++ 1	13409956	13438772				
curve25519-gaudry 1	3286776	3313996				
donald 1 512	1577324				1592312	1899520
donald 1 1024	4460696				4228256	5137792
donald 1 2048	14158664				13031100	16394008
ecdonald 1 nist-b-163	5337952				5510212	10739288
ecdonald 1 nist-b-233	9621984				9781220	19423732
ecdonald 1 nist-b-283	20036984				20269364	40689604
ecdonald 1 nist-b-409	42355404				42979948	86029984
ecdonald 1 nist-b-571	105197192				105615128	211169612
ecdonald 1 nist-k-163	4930432				5061336	9894292
ecdonald 1 nist-k-233	8685124				8815440	17479476
ecdonald 1 nist-k-283	17882148				18266548	36090308

`ecdonald 1 nist-k-409`	37093020			37672292	74906856
`ecdonald 1 nist-k-571`	91639800			92038092	184591044
`ecdonald 1 nist-p-192`	4468104			4623512	5498736
`ecdonald 1 nist-p-224`	5899144			6157548	7301432
`ecdonald 1 nist-p-256`	8098032			8275456	10066832
`ecdonald 1 nist-p-384`	18078744			18237456	21847076
`ecdonald 1 nist-p-521`	43950152			44262416	54704712
`ecdonald 1 secp160r1`	5129320			5182184	6408256
`ntru-enc 1 ees787ep1`	165941620	792148	1326160		
`rainbow 1`	318955016			1222944	2307964
`ronald 1 768`	142666032	219324	6724748	6685804	201424
`ronald 1 832`	243589892	236368	8417776	8766816	219568
`ronald 1 896`	223236428	261764	9730488	10079300	237276
`ronald 1 960`	340373960	275384	11453076	11517200	248596
`ronald 1 1024`	211592328	275196	11257996	11179404	250584
`ronald 1 1088`	324205528	346004	14694460	14657708	317356
`ronald 1 1152`	417407476	361228	17197664	17384544	332408
`ronald 1 1216`	708868664	373936	18915768	18758048	340704
`ronald 1 1280`	655387784	375240	20932232	20970072	346500
`ronald 1 1344`	908104152	403356	23962376	24047016	368500
`ronald 1 1408`	887373200	425692	26634032	26821824	392036
`ronald 1 1472`	638734208	451956	28655920	28628652	411408
`ronald 1 1536`	1033622176	441964	27980420	27871188	399552
`ronald 1 1664`	1258593848	517668	36738276	36998432	473904
`ronald 1 1792`	1760159896	524832	44547972	43971992	481396
`ronald 1 1920`	1988942376	593888	52464928	52038636	547128
`ronald 1 2048`	1544563932	626224	58111612	58437356	570344
`ronald 1 2176`	2477554760	816232	71248528	70287188	761276
`ronald 1 2304`	5106932352	839344	81815704	82585400	788636
`ronald 1 2432`	3087367584	906616	94082468	94386540	849348
`ronald 1 2560`	4113963640	938184	95430680	95972444	870732
`ronald 1 2688`	5665365700	1029832	110548104	110012452	957440
`ronald 1 2816`	6738326020	1045564	125123216	125328472	970516
`ronald 1 2944`	7357390152	1130336	143575832	143210188	1054920
`ronald 1 3072`	8355102252	1168020	148157012	148740420	1071688
`ronald 1 3328`	8710300620	1318692	191259584	190380972	1229684
`ronald 1 3584`	11426870024	1444016	213408552	213656396	1346676
`ronald 1 3840`	13161754028	1574264	267224516	261546452	1480676
`ronald 1 4096`	25725149476	1747988	330840004	330163192	1678916
`ronald 2 768`	169176864	198484	7091000	7077772	197868
`ronald 2 832`	182460212	215188	8482920	8500396	208796
`ronald 2 896`	292242812	234904	10063280	10021464	224320
`ronald 2 960`	296321772	252364	11508844	11510044	239332
`ronald 2 1024`	259388660	248204	11308292	11294028	237256
`ronald 2 1088`	420404156	318696	14536392	14540316	307924
`ronald 2 1152`	482201460	334860	16833588	16959676	323676
`ronald 2 1216`	617410748	348212	18927444	19186712	333532

ronald 2 1280	881480780	350360	21340596	21380488	330628
ronald 2 1344	636695264	377608	24126600	24081160	360096
ronald 2 1408	668297188	428028	31317720	26715120	376432
ronald 2 1472	1046666904	428172	28772812	28699044	400704
ronald 2 1536	1465888932	413164	28619508	28920164	393288
ronald 2 1664	879322612	500164	37216320	37611024	464672
ronald 2 1792	1212281260	505672	44591300	44797856	464440
ronald 2 1920	2944754912	567312	52378200	52256664	537764
ronald 2 2048	2195823632	597392	58086576	58013700	564504
ronald 2 2176	2511995140	794844	69892904	69996732	751900
ronald 2 2304	4401440592	814580	82269052	82572664	765168
ronald 2 2432	3050061040	887304	93030244	91568260	831768
ronald 2 2560	5797685612	911216	96963612	97057236	854676
ronald 2 2688	4005205688	998172	110535756	111274792	944848
ronald 2 2816	10801564788	1018124	129356680	129061300	959252
ronald 2 2944	6832934048	1105476	146489908	147086508	1046660
ronald 2 3072	4624623664	1124544	147678740	147570704	1055680
ronald 2 3328	14606536952	1291484	192332952	191918976	1221968
ronald 2 3584	9670986772	1412000	211607960	211191788	1336752
ronald 2 3840	13490205060	1566640	265097440	264935480	1497732
ronald 2 4096	33641523940	1725320	329810624	329704456	1636140
ronald 3 768	179788308	198628	7031884	7038480	182932
ronald 3 832	189261140	217496	8462812	8473924	200784
ronald 3 896	181013428	233836	10005252	10052964	215928
ronald 3 960	195336612	249288	11278488	11091612	232236
ronald 3 1024	299255916	252084	11304552	11374092	229548
ronald 3 1088	350785804	322000	14494032	14635200	300084
ronald 3 1152	731651436	336120	17165644	17180252	307756
ronald 3 1216	852266264	348996	18853880	18729684	322948
ronald 3 1280	408032148	346780	21301688	21199856	323828
ronald 3 1344	958984180	376296	24127584	24250824	349336
ronald 3 1408	956070316	400404	26818932	26801820	369532
ronald 3 1472	1048068724	426548	28709108	28852444	396984
ronald 3 1536	738519848	415808	27920184	27910500	389512
ronald 3 1664	1066820308	492680	34304152	36091404	457004
ronald 3 1792	1618760816	499224	45906344	46017632	459912
ronald 3 1920	2554915824	573860	52231028	51963992	527504
ronald 3 2048	2135799928	596600	58427716	58699152	549348
ronald 3 2176	2964029372	791756	70761024	71061212	743664
ronald 3 2304	2869323192	811116	81855116	82322680	762284
ronald 3 2432	4944993680	880484	92176044	92550148	824696
ronald 3 2560	3808910960	903684	96272508	96209640	848360
ronald 3 2688	3709605960	998676	112541064	113152312	937752
ronald 3 2816	6951428020	1013092	128188684	128268532	954760
ronald 3 2944	6251345680	1105116	144384668	144969960	1043092
ronald 3 3072	7790380424	1120408	148859544	147761004	1054908
ronald 3 3328	11127268416	1286804	192348916	191829880	1210524

ronald 3 3584	15556887272		1466844	205073872	205089748	1376600
ronald 3 3840	14145517652		1562924	265191680	265192004	1474388
ronald 3 4096	23837793092		1727556	331671224	331263564	1648932
sflashv2 1	912734400				1809480	554500
sflashv2 2	893056932				349728	379248
surf127eps 1	3719132	3766596				

System	secret key bytes	public key bytes	shared secret bytes	23-byte encrypt bytes	709-byte encrypt bytes	23-byte signed bytes	709-byte signed bytes
bls 1	20	120				43	729
claus 1	256	128	128				
claus++ 1	256	128	128				
curve25519-gaudry 1	32	32	32				
donald 1 512	84	64				63	749
donald 1 1024	148	128				63	749
donald 1 2048	276	256				63	749
ecdonald 1 nist-b-163	63	42				65	751
ecdonald 1 nist-b-233	90	60				83	769
ecdonald 1 nist-b-283	108	72				95	781
ecdonald 1 nist-b-409	156	104				127	813
ecdonald 1 nist-b-571	216	144				167	853
ecdonald 1 nist-k-163	63	42				65	751
ecdonald 1 nist-k-233	90	60				83	769
ecdonald 1 nist-k-283	108	72				95	781
ecdonald 1 nist-k-409	156	104				127	813
ecdonald 1 nist-k-571	216	144				167	853
ecdonald 1 nist-p-192	72	48				71	757
ecdonald 1 nist-p-224	84	56				79	765
ecdonald 1 nist-p-256	96	64				87	773
ecdonald 1 nist-p-384	144	96				119	805
ecdonald 1 nist-p-521	198	132				155	841
ecdonald 1 secp160r1	60	40				63	749
ntru-enc 1 ees787ep1	1854	1574		1574	2282		
rainbow 1	20107	31680				66	752
ronald 1 768	768	96		119	805	119	805
ronald 1 832	832	104		127	813	127	813
ronald 1 896	896	112		135	821	135	821
ronald 1 960	960	120		143	829	143	829
ronald 1 1024	1024	128		151	837	151	837
ronald 1 1088	1088	136		159	845	159	845
ronald 1 1152	1152	144		167	853	167	853
ronald 1 1216	1216	152		175	861	175	861
ronald 1 1280	1280	160		183	869	183	869
ronald 1 1344	1344	168		191	877	191	877
ronald 1 1408	1408	176		199	885	199	885
ronald 1 1472	1472	184		207	893	207	893

ronald 1 1536	1536	192	215	901	215	901
ronald 1 1664	1664	208	231	917	231	917
ronald 1 1792	1792	224	247	933	247	933
ronald 1 1920	1920	240	263	949	263	949
ronald 1 2048	2048	256	279	965	279	965
ronald 1 2176	2176	272	295	981	295	981
ronald 1 2304	2304	288	311	997	311	997
ronald 1 2432	2432	304	327	1013	327	1013
ronald 1 2560	2560	320	343	1029	343	1029
ronald 1 2688	2688	336	359	1045	359	1045
ronald 1 2816	2816	352	375	1061	375	1061
ronald 1 2944	2944	368	391	1077	391	1077
ronald 1 3072	3072	384	407	1093	407	1093
ronald 1 3328	3328	416	439	1125	439	1125
ronald 1 3584	3584	448	471	1157	471	1157
ronald 1 3840	3840	480	503	1189	503	1189
ronald 1 4096	4096	512	535	1221	535	1221
ronald 2 768	768	96	96	784	119	805
ronald 2 832	832	104	104	784	127	813
ronald 2 896	896	112	112	784	135	821
ronald 2 960	960	120	120	784	143	829
ronald 2 1024	1024	128	128	784	151	837
ronald 2 1088	1088	136	136	784	159	845
ronald 2 1152	1152	144	144	784	167	853
ronald 2 1216	1216	152	152	784	175	861
ronald 2 1280	1280	160	160	784	183	869
ronald 2 1344	1344	168	168	784	191	877
ronald 2 1408	1408	176	176	784	199	885
ronald 2 1472	1472	184	184	784	207	893
ronald 2 1536	1536	192	192	784	215	901
ronald 2 1664	1664	208	208	784	231	917
ronald 2 1792	1792	224	224	784	247	933
ronald 2 1920	1920	240	240	784	263	949
ronald 2 2048	2048	256	256	784	279	965
ronald 2 2176	2176	272	272	784	295	981
ronald 2 2304	2304	288	288	784	311	997
ronald 2 2432	2432	304	304	784	327	1013
ronald 2 2560	2560	320	320	784	343	1029
ronald 2 2688	2688	336	336	784	359	1045
ronald 2 2816	2816	352	352	784	375	1061
ronald 2 2944	2944	368	368	784	391	1077
ronald 2 3072	3072	384	384	784	407	1093
ronald 2 3328	3328	416	416	784	439	1125
ronald 2 3584	3584	448	448	784	471	1157
ronald 2 3840	3840	480	480	784	503	1189
ronald 2 4096	4096	512	512	784	535	1221
ronald 3 768	768	96	96	784	96	752

`ronald 3 832`	832	104		104	784	104	752
`ronald 3 896`	896	112		112	784	112	752
`ronald 3 960`	960	120		120	784	120	752
`ronald 3 1024`	1024	128		128	784	128	752
`ronald 3 1088`	1088	136		136	784	136	752
`ronald 3 1152`	1152	144		144	784	144	752
`ronald 3 1216`	1216	152		152	784	152	752
`ronald 3 1280`	1280	160		160	784	160	752
`ronald 3 1344`	1344	168		168	784	168	752
`ronald 3 1408`	1408	176		176	784	176	752
`ronald 3 1472`	1472	184		184	784	184	752
`ronald 3 1536`	1536	192		192	784	192	752
`ronald 3 1664`	1664	208		208	784	208	752
`ronald 3 1792`	1792	224		224	784	224	752
`ronald 3 1920`	1920	240		240	784	240	752
`ronald 3 2048`	2048	256		256	784	256	752
`ronald 3 2176`	2176	272		272	784	272	752
`ronald 3 2304`	2304	288		288	784	288	752
`ronald 3 2432`	2432	304		304	784	304	752
`ronald 3 2560`	2560	320		320	784	320	752
`ronald 3 2688`	2688	336		336	784	336	752
`ronald 3 2816`	2816	352		352	784	352	752
`ronald 3 2944`	2944	368		368	784	368	752
`ronald 3 3072`	3072	384		384	784	384	752
`ronald 3 3328`	3328	416		416	784	416	752
`ronald 3 3584`	3584	448		448	784	448	752
`ronald 3 3840`	3840	480		480	784	480	752
`ronald 3 4096`	4096	512		512	784	512	752
`sflashv2 1`	2823	19266				60	746
`sflashv2 2`	2823	19266				60	746
`surf127eps 1`	32	48	48				

Chapter 7

The eBATS database of measurements

7.1 Introduction

BATMAN, the eBATS benchmarking toolkit, produces an extensive database of performance measurements in a format designed for easy computer processing. The tables and graphs in previous chapters of this report were generated from the database. The database is available to the public at `http://www.ecrypt.eu.org/ebats/results.html`.

The current database has 3227696 lines, each line having the format described in Section 7.3. The database occupies nearly 70 megabytes in compressed form. The database has more information than the tables and graphs in this report; in particular, as discussed in Section 7.2, the database contains a series of measurements of each operation, whereas the tables and graphs report only the median of the series.

7.2 Notes on time variability

BATMAN performs each operation 16 times, checking the CPU's cycle counter before each operation and then reporting the 15 successive differences as 15 measurements of the time taken by the operation. There are several important reasons for variability in these 15 measurements:

- Code-access delays: e.g., instruction-cache misses. These delays are most noticeable in the first measurement.
- Data-access delays: e.g., code-cache misses. These delays are most noticeable in the first measurement.
- Higher-level cryptographic variability. For example, RSA key generation takes a variable amount of time.
- Interruptions. For example, the operating system might stop BATMAN for 20000 cycles to handle a network packet, or for much longer to give another program a chance to run. An interruption can have quite drastic effects on BATMAN's cycle counts—even producing negative measurements!—if the operating system decides to move BATMAN

from one core to another core without a synchronized cycle counter. These delays can occur at any moment.

The tables and graphs in this report replace these 15 measurements by their median. This replacement filters out typical interruptions, filters out typical cache misses, and saves space. (Measurements in the literature often use the average rather than the median, but the median is much more stable than the average in the presence of interruptions.) On the other hand, the 15 measurements carry more information than the median does; for example, cache misses are important for many applications. All 15 measurements are included in the database.

In the case of encryption, decryption, signing, and verification, BATMAN reports 15 measurements with one key, then 15 measurements with a second key, then 15 measurements with a third key. This repetition sometimes reveals key-dependent variability in timings.

7.3 Database format

Each database entry is a line consisting of the following space-separated words:

1. BATMAN version; e.g., `20070214`.
2. Computer name; e.g., `katana`.
3. Measurement start date; e.g., `20070215`. If a computer changes—for example, having its compilers upgraded—then this start date will allow measurements before the change to be distinguished from measurements after the change.
4. BAT name; e.g., `ronald`.
5. BAT version; e.g., `3`.
6. BAT parameter list; e.g., `4096`.
7. Operation or object measured; e.g., `signedmessage`.
8. Number of bytes in the original (unencrypted, unsigned) message (or a hyphen for operations not involving a message); e.g., `1109`.
9. Type of measurement; e.g., `cycles`.
10. Measurement, or median of all measurements if there were multiple measurements: e.g., `79319912`. The `ronald 3` BAT with parameter `4096` (4096-bit RSA key) used 79319912 cycles on `katana` to sign an 1109-byte message.
11. All measurements if there were multiple measurements: e.g., `79426336 79064112 79089856 79521104 79111288 79307056 80360128 79402624 79512728 79319912 79312904 79251560 79416288 79289520 80807048`.

The lines are collected into `bzip2`-compressed files indexed by BATMAN version and computer name.

There are five types of measurements in the database. First, there are operations whose speed is measured by BATMAN, measurement type `cycles`:

- `ciphertext`, for encrypting BATs: encrypting a message.

- `keypair`, for all BATs: generating a secret key and public key.
- `messagesigned`, for signing BATs: verifying a signed message and a public key, returning the original message that was signed.
- `plaintext`, for encrypting BATs: decrypting an encrypted message.
- `sharedsecret`, for secret-sharing BATs: computing a shared secret.
- `signedmessage`, for signing BATs: signing a message.

Second, there are objects whose size is measured by BATMAN, measurement type `bytes`:

- `ciphertext`, for encrypting BATs: an encrypted message.
- `messagesigned`, for signing BATs: a message extracted from a signed message. Should always be the same as the original message.
- `plaintext`, for encrypting BATs: a message produced by decrypting an encrypted message. Should always be the same as the original message.
- `publickey`, for all BATs: a public key.
- `secretkey`, for all BATs: a secret key.
- `sharedsecret`, for secret-sharing BATs: a shared secret.
- `signedmessage`, for signing BATs: a signed message.

Third, there are security statements reported by the BAT:

- `ccattacks`, measurement type `attack`, for encrypting BATs: `100` if adaptive chosen-ciphertext attacks (IND-CCA2) are more effective than chosen-plaintext attacks; or `0` if adaptive chosen-ciphertext attacks are no more effective than chosen-plaintext attacks. `-1` means unreported.
- `cdhchance`, measurement type `chance`, for secret-sharing BATs: the log base 2 of the number of euros spent by the attacker; then the log base 2 of the number of keys simultaneously attacked; then 256 times the log base 0.5 of the probability that an attacker spending 1 second will succeed at deducing at least one shared secret; then the same for an attacker spending 2 seconds; then the same for an attacker spending 4 seconds; and so on through 2^{40} seconds. `-1` means unreported.
- `distinguishingchance`, measurement type `chance`, for encrypting BATs: the log base 2 of the number of euros spent by the attacker; then the log base 2 of the number of keys simultaneously attacked; then 256 times the log base 0.5 of the ciphertext-distinguishing (IND-CPA) probability for an attacker spending 1 second; then the same for an attacker spending 2 seconds; then the same for an attacker spending 4 seconds; and so on through 2^{40} seconds. `-1` means unreported.
- `fakekeyattacks`, measurement type `attack`, for secret-sharing BATs: `100` if an active attacker can save time by providing fake keys (in applications that do not go to any extra effort to validate keys); or `0` if an active attacker obtains no benefit from fake keys (for example, if the `sharedsecret` function includes all necessary key validation). `-1` means unreported.

- `forgerychance`, measurement type `chance`, for signing BATs: the log base 2 of the number of euros spent by the attacker; then the log base 2 of the number of keys simultaneously attacked; then 256 times the log base 0.5 of the probability that an attacker spending 1 second will succeed at forging at least one signed message; then the same for an attacker spending 2 seconds; then the same for an attacker spending 4 seconds; and so on through 2^{40} seconds. `-1` means unreported.

- `timingattacks`, measurement type `attack`, for all BATs: `0` if the software does not leak any secret information through timing (variable time for branching, variable time for memory access, etc.); or `100` if the software leaks secret information through timing. `-1` means unreported.

Fourth, there are intellectual-property statements reported by the BAT:

- `copyrightclaims`, measurement type `restriction`, for all BATs: `0` if there are no known present or future claims by a copyright holder that the distribution of this software infringes the copyright; `10` if the author is aware of third parties making such claims, but the author disputes those claims; `20` if the author is aware of third parties making such claims, and the author agrees with the claims, but the author has no financial connections to the copyright; `30` if the author has financial connections to a copyright restricting distribution of the software. `-1` means unreported.

- `patentclaims`, measurement type `restriction`, for all BATs: `0` if there are no known present or future claims by a patent holder that the use of this software infringes the patent; `10` if the author is aware of third parties making such claims, but the author disputes those claims; `20` if the author is aware of third parties making such claims, and the author agrees with the claims, but the author has no financial connections to the patent; `30` if the author has financial connections to a patent restricting use of the software. `-1` means unreported.

Fifth, there are some extra CPU notes and tuning notes included in the database, in unspecified formats subject to change:

- `bat_tuning`: the BAT tuning, or a hyphen for untuned BATs.

- `compiler`: the compiler used; e.g., `gcc_-m64_-march=k8_-O2_-fomit-frame-pointer`.

- `compiler_version`: e.g., `4.0.3_(Ubuntu_4.0.3-1ubuntu5)`.

- `cpucycles_implementation`: e.g., `amd64cpuinfo`.

- `cpucycles_persecond`: the number of cycles carried out by the CPU in one second.

- `cpuid`: details of the CPU being used; e.g., `GenuineIntel-000006f6-bfebfbff_`.

Chapter 8

Writing a BAT

8.1 Introduction

This chapter describes the process of creating a new BAT that fits within the eBATS framework:

- Section 8.2 describes the BAT development environment.
- Section 8.3 describes the files contained in a BAT.
- Section 8.4 explains how to parametrize a BAT, supporting more than one public-key system inside a single BAT.
- Section 8.5 explains how to tune a BAT.
- Section 8.6 describes an easy way for BATs to obtain cryptographically strong random numbers.
- Section 8.7 describes an easy way for BATs to hash data.
- Section 8.8 describes an easy way for BATs to use a secret-key stream cipher.
- Section 8.9 explains the `keypair()` function that all BATs must implement.
- Sections 8.10 through 8.14 explain the encryption and decryption functions that encrypting BATs must implement.
- Sections 8.15 through 8.21 explain the signature and verification functions that signing BATs must implement.
- Section 8.22 explains the secret-sharing function that secret-sharing BATs must implement.
- Sections 8.23 through 8.32 explain optional functions that BATs can implement to make security statements.
- Sections 8.33 and 8.34 explain optional functions that BATs can implement to make intellectual-property statements.

This process was designed to make the BAT implementor's job as easy as possible.

8.2 BAT development environment

Implementors can use the following procedure to inspect existing BATs, build a new BAT, and test the new BAT using BATMAN.

First, download and unpack the BATMAN program:

```
wget http://hyperelliptic.org/ebats/batman-20070214.tar.gz
gunzip < batman-20070214.tar.gz | tar -xf -
cd batman-20070214
```

Second, download the available BATs as examples, and move them to the `sleepingbats` directory:

```
wget http://hyperelliptic.org/ebats/bats-20070214.tar.gz
gunzip < bats-20070214.tar.gz | tar -xf -
mv bats/* sleepingbats
```

Third, download m4 1.4.8, GMP 4.2.1, NTL 5.4, and OpenSSL 0.9.8d:

```
cd libraries
wget --passive-ftp ftp://ftp.gnu.org/gnu/m4/m4-1.4.8.tar.bz2
wget --passive-ftp ftp://ftp.gnu.org/gnu/gmp/gmp-4.2.1.tar.bz2
wget http://www.shoup.net/ntl/ntl-5.4.tar.gz
wget http://www.openssl.org/source/openssl-0.9.8d.tar.gz
cd ..
```

BATs are free to call functions from GMP, NTL, and OpenSSL, after an appropriate `#include <gmp.h>` etc. Other libraries may be integrated into BATMAN upon request. Fourth, choose a name for the new BAT; let's say it's Furry, version 1. Fifth, create a new directory for the new BAT:

```
mkdir bats/furry-1
cd bats/furry-1
```

Sixth, inside the new directory, create the files required by the eBATS API, such as `sizes.h`. Seventh, once the BAT is written, test it using BATMAN:

```
cd ../..
./do
```

BATMAN creates a new file `20070214-xyz` for the resulting measurements, and a new file `20070214-xyz-notes` for logs, if the machine is named `xyz`. Beware that the `./do` script compiles GMP, NTL, and OpenSSL before it begins measurements; this takes 15 minutes on a 2000MHz Athlon 64, and can take much longer on slower machines.

To submit the finished BAT to eBATS, package it into a `tar.gz` file:

```
cd bats
tar -cf furry-1.tar furry-1
gzip -9 furry-1.tar
```

Put the `tar.gz` file on the web, and send the URL to `batsubmission2@ebats.cr.yp.to`.

See the web page `http://www.ecrypt.eu.org/ebats/batman.html` for the latest updates of this procedure.

8.3 Files in a BAT

A BAT is a `tar.gz` file containing one directory. The directory contains a file `sizes.h`, any number of additional `*.S`, `*.c`, and `*.cpp` files implementing the eBATS API, and a file `documentation.pdf` with references and other comments for cryptographers.

The directory name is the BAT name followed by a dash and a version number: e.g., `ronald-1` for a BAT named `ronald`, version 1. eBATS will rename BATs if there is a conflict in names.

The file `sizes.h` defines various macros discussed below:

- `SECRETKEY_BYTES`, required for all BATs.
- `PUBLICKEY_BYTES`, required for all BATs.
- `ENCRYPTION_BYTES`, required for encrypting BATs.
- `SHORTPLAINTEXT_BYTES`, required for short-message-encrypting BATs.
- `SIGNATURE_BYTES`, required for signing BATs.
- `SHORTMESSAGE_BYTES`, required for short-message-recovery signing BATs.
- `SHORTHASH_BYTES`, required for hash-verification signing BATs.
- `SHAREDSECRET_BYTES`, required for secret-sharing BATs.

BATMAN will automatically decide whether the BAT is a C BAT, providing the eBATS API functions in C, or a C++ BAT, providing the eBATS API functions in C++. Either way, the BAT can call C functions in its `*.c` files and assembly-language functions in its `*.S` files. BATs written in other languages have to be compiled to C++, C, or assembly language.

8.4 Parametrized BATs

Some BATs allow parameters. For example, a typical RSA implementation allows a wide range of key sizes. On the other hand, some RSA implementations gain speed by focusing on particular key sizes.

The eBATS API can support BATs of either type. A parametrized BAT includes, in the same directory as `sizes.h`, a `parameters` file with several lines; each line specifies compilation options that select a particular parameter choice. A parameter choice is specified by BAT-specific macros, which are used by `sizes.h` etc., and by a `PARAMETERS` macro, which is used to identify parameters in the eBATS results.

For example, version 1 of the RONALD BAT has a 29-line `parameters` file starting

```
-DMODULUS_BITS=768 -DPARAMETERS="768"
-DMODULUS_BITS=832 -DPARAMETERS="832"
-DMODULUS_BITS=896 -DPARAMETERS="896"
-DMODULUS_BITS=960 -DPARAMETERS="960"
-DMODULUS_BITS=1024 -DPARAMETERS="1024"
```

and continuing (in roughly geometric progression) until

```
-DMODULUS_BITS=4096 -DPARAMETERS="4096"
```

The `MODULUS_BITS` macro controls `PUBLICKEY_BYTES` etc. through the lines

```
#define MODULUS_BYTES (MODULUS_BITS / 8)
#define PUBLICKEY_BYTES (MODULUS_BYTES)
```

in the `sizes.h` file. The `PARAMETERS` macro is printed in the eBATS measurements.

The `parameters` file can omit `-DPARAMETERS=...` if `sizes.h` defines `PARAMETERS`. For example, version 2 of the RONALD BAT has a 29-line `parameters` file starting

```
-DMODULUS_BITS=768
-DMODULUS_BITS=832
-DMODULUS_BITS=896
-DMODULUS_BITS=960
-DMODULUS_BITS=1024
```

and the following lines in `sizes.h`:

```
#define XSTRINGIFY(N) #N
#define STRINGIFY(N) XSTRINGIFY(N)
#define PARAMETERS (STRINGIFY(MODULUS_BITS))
```

8.5 Tuned BATs

A BAT can contain several implementations of the same functions: e.g., a P4-tuned implementation, a G5-tuned implementation, etc. A tuned BAT includes, in the same directory as `sizes.h`, a `tunings` file with several lines; each line specifies compilation options that select a particular tuning. A tuning is specified by BAT-specific macros, which are used by `sizes.h` etc., and by a `TUNING` macro, which is used to identify tuning in the eBATS results.

BATMAN will automatically try each tuning and select the tuning where `sharedsecret`, `signedmessage`, or `ciphertext` runs most quickly. A BAT can define a `TUNETARGET` macro in `sizes.h`; in that case BATMAN will select the tuning where `TUNETARGET()` runs most quickly.

Any particular tuning is allowed to be unportable, failing to compile on most platforms. BATMAN will skip tunings that fail to compile or that flunk some simple tests.

8.6 Generating random numbers

BATMAN sets up file descriptor 0 reading from a neverending source of hard-to-predict secret random bytes. BATs are free to assume this: the `keypair` function, for example, can obtain secret bytes using `getchar()`.

Functions are permitted, but not encouraged, to generate randomness in other ways, such as by opening `/dev/urandom`. These functions will not be benchmarkable on systems that do not have `/dev/urandom`, and they will not be suitable for black-box regression testing.

8.7 Using hash functions

BATMAN provides a cryptographic hash function `hash256` callable from a BAT as follows:

```
const unsigned char m[...]; unsigned long long mlen;
unsigned char h[32];
hash256(h,m,mlen);
```

`hash256` hashes bytes `m[0]`, `m[1]`, ..., `m[mlen-1]` and puts the output into `h[0]`, `h[1]`, ..., `h[31]`. Currently `hash256` is implemented as SHA-256.

To simplify comparisons of public-key systems, eBATS recommends that all BATs use this `hash256` function for all necessary hashing. This is *not* a recommendation of SHA-256 for any purpose other than public-key benchmarking. Public-key systems may be able to gain speed and security by choosing different hash functions.

To the extent that eBATS considers security of public-key systems, it focuses on *generic* attacks, i.e., attacks that work with any hash function. Any security problems in SHA-256 are outside the scope of eBATS, although obviously they should be discussed elsewhere.

8.8 Using stream ciphers

BATMAN provides an additive stream cipher `stream256` callable from a BAT as follows:

```
const unsigned char m[...]; unsigned long long mlen;
unsigned char c[...];
const unsigned char k[32];
const unsigned char n[8];
stream256(c,m,mlen,k,n);
```

`stream256` encrypts (or decrypts) bytes `m[0]`, `m[1]`, ..., `m[mlen-1]` and puts the output into `c[0]`, `c[1]`, ..., `c[mlen-1]`. It uses a 32-byte key `k[0]`, `k[1]`, ..., `k[31]` and an 8-byte nonce `n[0]`, `n[1]`, ..., `n[7]`. Currently `stream256` is implemented as Salsa20.

To simplify comparisons of public-key systems, eBATS recommends that all BATs use this `stream256` function for all necessary stream generation. This is *not* a recommendation of Salsa20 for any purpose other than public-key benchmarking. Public-key systems may be able to gain speed and security by choosing different ciphers.

To the extent that eBATS considers security of public-key systems, it focuses on *generic* attacks, i.e., attacks that work with any stream cipher. Any security problems in Salsa20 are outside the scope of eBATS, although obviously they should be discussed elsewhere.

8.9 `keypair`: generate a new secret key and public key

Every BAT must provide a `keypair` function callable as follows:

```
#include "sizes.h"

unsigned char sk[SECRETKEY_BYTES]; unsigned long long sklen;
unsigned char pk[PUBLICKEY_BYTES]; unsigned long long pklen;

keypair(sk,&sklen,pk,&pklen);
```

The `keypair` function generates a new secret key and a new public key. It puts the number of bytes of the secret key into `sklen`; puts the number of bytes of the public key into `pklen`; puts the secret key into `sk[0]`, `sk[1]`, ..., `sk[sklen-1]`; and puts the public key into `pk[0]`, `pk[1]`, ..., `pk[pklen-1]`. It then returns 0.

`keypair` guarantees that `sklen` is at most `SECRETKEY_BYTES`, and that `pklen` is at most `PUBLICKEY_BYTES`, so that the caller can allocate enough space.

If key generation is impossible for some reason (e.g., not enough memory), `keypair` returns a negative number, possibly after modifying `sk[0]`, `sk[1]`, etc. Current implementations should return `-1`; other return values with special meanings may be defined in the future.

8.10 Different types of encrypting BATs

Public-key encryption functions are often described—and implemented—as functions to encrypt *short* messages. For example, RSA encryption functions are often limited to messages shorter than the RSA public key. However, users often need to encrypt much longer messages; BATMAN measures encryption speeds and ciphertext lengths for a wide variety of message lengths.

To minimize the amount of effort required to create a BAT, without constraining the optimizations that can be reflected in the eBATS measurements, BATMAN supports two different types of encrypting BATs:

- A short-message-encrypting BATs provides a `shortciphertext` function that encrypts a short message, and a corresponding `shortplaintext` function that decrypts the message.
- A long-message-encrypting BAT provides a `ciphertext` function that encrypts a message of any length, and a corresponding `plaintext` function that decrypts the message.

BATMAN automatically converts the first type of BAT into the second type using a stream cipher; see below for the details. Implementors who want to handle long messages in a different way—perhaps saving time or space—can directly implement the second type of BAT.

8.11 `ciphertext`: encrypt a message using a public key

A long-message-encrypting BAT must provide a `ciphertext` function callable as follows:

```
#include "sizes.h"

const unsigned char pk[PUBLICKEY_BYTES]; unsigned long long pklen;
const unsigned char m[...]; unsigned long long mlen;
unsigned char c[...]; unsigned long long clen;

ciphertext(c,&clen,m,mlen,pk,pklen);
```

The `ciphertext` function uses a public key `pk[0]`, `pk[1]`, ..., `pk[pklen-1]` to encrypt a message `m[0]`, `m[1]`, ..., `m[mlen-1]`. It puts the length of the encrypted message into `clen` and puts the encrypted message into `c[0]`, `c[1]`, ..., `c[clen-1]`. It then returns 0.

The `ciphertext` function guarantees that `clen` is at most `mlen+ENCRYPTION_BYTES`. The `ENCRYPTION_BYTES` macro is defined in `sizes.h`.

The `ciphertext` function is free to assume that `pk[0]`, `pk[1]`, ..., `pk[pklen-1]` was generated by a successful call to the `keypair` function.

If encryption is impossible for some reason, `ciphertext` returns a negative number, possibly after modifying `c[0]`, `c[1]`, etc. Current implementations should return `-1`; other return values with special meanings may be defined in the future.

Implementors of the `ciphertext` function are warned that they should not go to extra effort to compress the message `m`. Higher-level applications should be presumed to compress messages before calling the `ciphertext` function; in particular, BATMAN uses random messages to make compression ineffective. On the other hand, the *encrypted* message `c` is longer than the original message `m` and might be compressible; any reduction of the encryption overhead will be visible in the eBATS measurements.

8.12 `plaintext`: decrypt a message using a secret key

A long-message-encrypting BAT must provide a `plaintext` function callable as follows:

```
#include "sizes.h"

const unsigned char sk[SECRETKEY_BYTES]; unsigned long long sklen;
const unsigned char c[...]; unsigned long long clen;
unsigned char m[...]; unsigned long long mlen;

plaintext(m,&mlen,c,clen,sk,sklen);
```

The `plaintext` function uses a secret key `sk[0]`, `sk[1]`, ..., `sk[sklen-1]` to decrypt a ciphertext `c[0]`, `c[1]`, ..., `c[clen-1]`. The `plaintext` function puts the length of the decrypted message into `mlen`, puts the decrypted message into `m[0]`, `m[1]`, ..., `m[mlen-1]`, and returns 0.

The `plaintext` function guarantees that `mlen` is at most `clen`.

The `plaintext` function is free to assume that `sk[0]`, `sk[1]`, ..., `sk[sklen-1]` was generated by a successful call to the `secretkey` function.

If decryption is impossible for some reason, `plaintext` returns a negative number, possibly after modifying `m[0]`, `m[1]`, etc. Current implementations should return `-100` for invalid ciphertexts, and `-1` for all other problems; other return values with special meanings may be defined in the future.

8.13 `shortciphertext`: encrypt a message using a public key

A short-message-encrypting BAT must provide a `shortciphertext` function callable as follows:

```
#include "sizes.h"

const unsigned char pk[PUBLICKEY_BYTES]; unsigned long long pklen;
const unsigned char m[SHORTPLAINTEXT_BYTES]; unsigned long long mlen;
```

```
unsigned char c[ENCRYPTION_BYTES]; unsigned long long clen;

shortciphertext(c,&clen,m,mlen,pk,pklen);
```

The `shortciphertext` function uses a public key `pk[0]`, `pk[1]`, ..., `pk[pklen-1]` to encrypt a message `m[0]`, `m[1]`, ..., `m[mlen-1]`. It puts the length of the encrypted message into `clen` and puts the encrypted message into `c[0]`, `c[1]`, ..., `c[clen-1]`. It then returns 0.

The `shortciphertext` function is free to assume that `mlen` is smaller than or equal to `SHORTPLAINTEXT_BYTES`. The `shortciphertext` function guarantees that `clen` is *exactly* `ENCRYPTION_BYTES`. The `SHORTPLAINTEXT_BYTES` and `ENCRYPTION_BYTES` macros are defined in `sizes.h`.

The `shortciphertext` function is free to assume that the public key `pk[0]`, `pk[1]`, ..., `pk[pklen-1]` was generated by a successful call to the `keypair` function.

If encryption is impossible for some reason, `shortciphertext` returns a negative number, possibly after modifying `c[0]`, `c[1]`, etc. Current implementations should return `-1`; other return values with special meanings may be defined in the future.

Implementors of the `shortciphertext` function are warned that they should not go to extra effort to compress the message `m`. Higher-level applications should be presumed to compress messages before calling the `shortciphertext` function; in particular, BATMAN uses random messages to make compression ineffective. On the other hand, the *encrypted* message `c` is longer than the original message `m` and might be compressible; any reduction of the encryption overhead will be visible in the eBATS measurements.

BATMAN automatically builds `ciphertext` on top of `shortciphertext` as follows. A message with fewer than `SHORTPLAINTEXT_BYTES` bytes is encrypted with `shortciphertext`. A message with `SHORTPLAINTEXT_BYTES` or more bytes is handled as follows:

- The message is encrypted with Salsa20 using a random 32-byte key, producing an initial encryption `e`.
- The 32-byte key for Salsa20, the 32-byte SHA-256 hash of the encryption `e`, and the first `SHORTPLAINTEXT_BYTES-64` bytes of `e` are encrypted with `shortciphertext`.
- The rest of `e` is appended.

`SHORTPLAINTEXT_BYTES` must be at least 64. Criticisms of the speed and security of Salsa20 and SHA-256 are outside the scope of eBATS; eBATS focuses on public-key cryptography, not on stream ciphers and hash functions.

8.14 `shortplaintext`: decrypt a message using a secret key

A short-message-encrypting BAT must provide a `shortplaintext` function callable as follows:

```
#include "sizes.h"

const unsigned char sk[SECRETKEY_BYTES]; unsigned long long sklen;
const unsigned char c[ENCRYPTION_BYTES]; unsigned long long clen;
unsigned char m[SHORTPLAINTEXT_BYTES]; unsigned long long mlen;

shortplaintext(m,&mlen,c,clen,sk,sklen);
```

The `shortplaintext` function uses a secret key `sk[0]`, `sk[1]`, ..., `sk[sklen-1]` to decrypt a ciphertext `c[0]`, `c[1]`, ..., `c[clen-1]`. The `shortplaintext` function puts the length of the decrypted message into `mlen`, puts the decrypted message into `m[0]`, `m[1]`, ..., `m[mlen-1]`, and returns 0.

The `shortplaintext` function is free to assume that `clen` is exactly `ENCRYPTION_BYTES`. The `shortplaintext` function guarantees that `mlen` is at most `SHORTPLAINTEXT_BYTES`.

The `shortplaintext` function is free to assume that the secret key `sk[0]`, `sk[1]`, ..., `sk[sklen-1]` was generated by a successful call to the `secretkey` function.

If decryption is impossible for some reason, `plaintext` returns a negative number, possibly after modifying `m[0]`, `m[1]`, etc. Current implementations should return `-100` for invalid ciphertexts, and `-1` for all other problems; other return values with special meanings may be defined in the future.

BATMAN automatically builds `plaintext` on top of `shortplaintext` by reversing the construction of `ciphertext` from `shortciphertext`.

8.15 Different types of signing BATs

Public-key signature functions, like public-key encryption functions discussed in Section 8.10, have a gap between what is simplest to implement and what users actually need. To minimize the amount of effort required to create a BAT, without constraining the optimizations that can be reflected in the eBATS measurements, BATMAN supports three different types of signing BATs:

- Hash-verification BATs provide a `signatureofshorthash` function that computes a signature of a short message and a `verification` function that verifies a signature.
- Short-message-recovery BATs provide a `signedshortmessage` function that converts a short message into a signed message and a `shortmessagesigned` function that verifies a signed message, returning the original short message.
- Long-message-recovery BATs provide a `signedmessage` function that converts a message of any length into a signed message and a `messagesigned` function that verifies a signed message, returning the original message.

BATMAN automatically converts the first two types into the third type, using a hash function, and then measures the third type.

8.16 `signedmessage`: sign a message using a secret key

A long-message-recovery BAT must provide a `signedmessage` function callable as follows:

```
#include "sizes.h"

const unsigned char sk[SECRETKEY_BYTES]; unsigned long long sklen;
const unsigned char m[...]; unsigned long long mlen;
unsigned char sm[...]; unsigned long long smlen;

signedmessage(sm,&smlen,m,mlen,sk,sklen);
```

The `signedmessage` function uses a secret key `sk[0]`, `sk[1]`, ..., `sk[sklen-1]` to sign a message `m[0]`, `m[1]`, ..., `m[mlen-1]`. It puts the length of the signed message into `smlen` and puts the signed message into `sm[0]`, `sm[1]`, ..., `sm[smlen-1]`. It then returns 0.

The `signedmessage` function guarantees that `smlen` is at most `mlen+SIGNATURE_BYTES`. The `SIGNATURE_BYTES` macro is defined in `sizes.h`.

The `signedmessage` function is free to assume that the secret key `sk[0]`, `sk[1]`, ..., `sk[sklen-1]` was generated by a successful call to the `keypair` function.

If signing is impossible for some reason, `signedmessage` returns a negative number, possibly after modifying `sm[0]`, `sm[1]`, etc. Current implementations should return `-1`; other return values with special meanings may be defined in the future.

Implementors of the `signedmessage` function are warned that they should not go to extra effort to compress the message `m`. Higher-level applications should be presumed to compress messages before calling the `signedmessage` function; in particular, BATMAN uses random messages to make compression ineffective. On the other hand, the *signed* message `sm` is longer than the original message `m` and might be compressible; any reduction of the signature overhead will be visible in the eBATS measurements.

8.17 `messagesigned`: verify a message using a public key

A long-message-recovery BAT must provide a `messagesigned` function callable as follows:

```
#include "sizes.h"

const unsigned char pk[PUBLICKEY_BYTES]; unsigned long long pklen;
const unsigned char sm[...]; unsigned long long smlen;
unsigned char m[...]; unsigned long long mlen;

messagesigned(m,&mlen,sm,smlen,pk,pklen);
```

The `messagesigned` function uses a public key `pk[0]`, `pk[1]`, ..., `pk[pklen-1]` to verify an allegedly signed message `sm[0]`, `sm[1]`, ..., `sm[smlen-1]`. If the message has a valid signature, the `messagesigned` function puts the length of the original message (without the signature) into `mlen`, puts the original message into `m[0]`, `m[1]`, ..., `m[mlen-1]`, and returns 0.

The `messagesigned` function guarantees that `mlen` is at most `smlen`.

The `messagesigned` function is free to assume that `pk[0]`, `pk[1]`, ..., `pk[pklen-1]` was generated by a successful call to the `publickey` function. The `messagesigned` function is not permitted to assume that `sm[0]`, `sm[1]`, ..., `sm[smlen-1]` was generated by a call to the `signedmessage` function; the `messagesigned` function is responsible for detecting and eliminating forgeries.

If signature verification is impossible for some reason, `messagesigned` returns a negative number, possibly after modifying `m[0]`, `m[1]`, etc. Current implementations should return `-100` for invalid signatures, and `-1` for all other problems; other return values with special meanings may be defined in the future.

8.18 `signedshortmessage`: sign a message using a secret key

A short-message-recovery BAT must provide a `signedshortmessage` function callable as follows:

```
#include "sizes.h"

const unsigned char sk[SECRETKEY_BYTES]; unsigned long long sklen;
const unsigned char m[SHORTMESSAGE_BYTES]; unsigned long long mlen;
unsigned char sm[SIGNATURE_BYTES]; unsigned long long smlen;

signedshortmessage(sm,&smlen,m,mlen,sk,sklen);
```

The `signedshortmessage` function uses a secret key `sk[0]`, `sk[1]`, ..., `sk[sklen-1]` to sign a message `m[0]`, `m[1]`, ..., `m[mlen-1]`. It puts the length of the signed message into `smlen` and puts the signed message into `sm[0]`, `sm[1]`, ..., `sm[smlen-1]`. It then returns 0.

The `signedshortmessage` function is free to assume that `mlen` is smaller than or equal to `SHORTMESSAGE_BYTES`. The `signedshortmessage` function guarantees that `smlen` is *exactly* `SIGNATURE_BYTES`. The `SHORTMESSAGE_BYTES` and `SIGNATURE_BYTES` macros are defined in `sizes.h`.

The `signedshortmessage` function is free to assume that the secret key `sk[0]`, `sk[1]`, ..., `sk[sklen-1]` was generated by a successful call to the `keypair` function.

If signing is impossible for some reason, `signedshortmessage` returns a negative number, possibly after modifying `sm[0]`, `sm[1]`, etc. Current implementations should return `-1`; other return values with special meanings may be defined in the future.

Implementors of the `signedshortmessage` function are warned that they should not go to extra effort to compress the message `m`. Higher-level applications should be presumed to compress messages before calling the `signedshortmessage` function; in particular, BATMAN uses random messages to make compression ineffective. On the other hand, the *signed* message `sm` is longer than the original message `m` and might be compressible; any reduction of the signature overhead will be visible in the eBATS measurements.

BATMAN automatically builds `signedmessage` on top of the `signedshortmessage` function as follows. Messages with fewer than `SHORTMESSAGE_BYTES` bytes are simply signed with `signedshortmessage`. Messages with `SHORTMESSAGE_BYTES` or more bytes are first hashed with SHA-256; the 32-byte hash and the first `SHORTMESSAGE_BYTES-32` bytes of the message are signed with `signedshortmessage`; the rest of the message is appended. `SHORTMESSAGE_BYTES` must be at least 32.

8.19 `shortmessagesigned`: verify a message using a public key

A short-message-recovery BAT must provide a `shortmessagesigned` function callable as follows:

```
#include "sizes.h"

const unsigned char pk[PUBLICKEY_BYTES]; unsigned long long pklen;
const unsigned char sm[SIGNATURE_BYTES]; unsigned long long smlen;
unsigned char m[SHORTMESSAGE_BYTES]; unsigned long long mlen;
```

```
shortmessagesigned(m,&mlen,sm,smlen,pk,pklen);
```

The `shortmessagesigned` function uses a public key `pk[0]`, `pk[1]`, ..., `pk[pklen-1]` to verify an allegedly signed message `sm[0]`, `sm[1]`, ..., `sm[smlen-1]`. If the message has a valid signature, the `shortmessagesigned` function puts the length of the original message (without the signature) into `mlen`, puts the original message into `m[0]`, `m[1]`, ..., `m[mlen-1]`, and returns 0.

The `shortmessagesigned` function is free to assume that `smlen` equals `SIGNATURE_BYTES`. The `shortmessagesigned` function guarantees that `mlen` is at most `SHORTMESSAGE_BYTES`.

The `shortmessagesigned` function is free to assume that `pk[0]`, `pk[1]`, ..., `pk[pklen-1]` was generated by a successful call to the `publickey` function. The `shortmessagesigned` function is not permitted to assume that `sm[0]`, `sm[1]`, ..., `sm[smlen-1]` was generated by a call to the `signedshortmessage` function; the `shortmessagesigned` function is responsible for detecting and eliminating forgeries.

If signature verification is impossible for some reason, `shortmessagesigned` returns a negative number, possibly after modifying `m[0]`, `m[1]`, etc. Current implementations should return `-100` for invalid signatures, and `-1` for all other problems; other return values with special meanings may be defined in the future.

BATMAN automatically builds `messagesigned` on top of `shortmessagesigned` by feeding the first `SIGNATURE_BYTES` bytes of the signed message to `shortmessagesigned`.

8.20 `signatureofshorthash`: sign a message using a secret key

A hash-verification BAT must provide a `signatureofshorthash` function callable as follows:

```
#include "sizes.h"

const unsigned char sk[SECRETKEY_BYTES]; unsigned long long sklen;
const unsigned char m[SHORTHASH_BYTES]; unsigned long long mlen;
unsigned char sm[SIGNATURE_BYTES]; unsigned long long smlen;

signatureofshorthash(sm,&smlen,m,mlen,sk,sklen);
```

The `signatureofshorthash` function uses a secret key `sk[0]`, `sk[1]`, ..., `sk[sklen-1]` to sign a message `m[0]`, `m[1]`, ..., `m[mlen-1]`. It puts the length of the signature into `smlen` and puts the signature into `sm[0]`, `sm[1]`, ..., `sm[smlen-1]`. It then returns 0.

The `signatureofshorthash` function is free to assume that `mlen` is smaller than or equal to `SHORTHASH_BYTES`. The `signatureofshorthash` function guarantees that `smlen` is *exactly* `SIGNATURE_BYTES`. The `SHORTHASH_BYTES` and `SIGNATURE_BYTES` macros are defined in `sizes.h`.

The `signatureofshorthash` function is free to assume that the secret key `sk[0]`, `sk[1]`, ..., `sk[sklen-1]` was generated by a successful call to the `keypair` function.

If signing is impossible for some reason, `signatureofshorthash` returns a negative number, possibly after modifying `sm[0]`, `sm[1]`, etc. Current implementations should return `-1`; other return values with special meanings may be defined in the future.

BATMAN automatically builds `signedmessage` on top of `signatureofshorthash` by applying `signatureofshorthash` to a 32-byte SHA-256 hash of the message being signed. This

means that `signatureofshorthash` is always given a 32-byte input, no matter what the original message length was; `SHORTHASH_BYTES` must be at least 32. Criticisms of the speed and security of SHA-256 are outside the scope of eBATS; eBATS focuses on public-key cryptography, not on hash functions.

8.21 `verification`: verify a message using a public key

A hash-verification BAT must provide a `verification` function callable as follows:

```
#include "sizes.h"

const unsigned char pk[PUBLICKEY_BYTES]; unsigned long long pklen;
const unsigned char sm[SIGNATURE_BYTES]; unsigned long long smlen;
const unsigned char m[SHORTHASH_BYTES]; unsigned long long mlen;

verification(m,mlen,sm,smlen,pk,pklen);
```

The `verification` function uses a public key `pk[0]`, `pk[1]`, ..., `pk[pklen-1]` to verify an alleged signature `sm[0]`, `sm[1]`, ..., `sm[smlen-1]` on a message `m[0]`, `m[1]`, ..., `m[mlen-1]`. If the message has a valid signature, the `verification` function returns 0.

The `verification` function is free to assume that `smlen` is exactly `SIGNATURE_BYTES` and that `mlen` is at most `SHORTHASH_BYTES`.

The `verification` function is free to assume that the public key `pk[0]`, `pk[1]`, ..., `pk[pklen-1]` was generated by a successful call to the `publickey` function. However, the `verification` function is not permitted to assume that `sm[0]`, `sm[1]`, ..., `sm[smlen-1]` was generated by a call to the `signatureofshorthash` function; the `verification` function is responsible for detecting and eliminating forgeries.

If signature verification is impossible for some reason, `verification` returns a negative number, possibly after modifying `m[0]`, `m[1]`, etc. Current implementations should return `-100` for invalid signatures, and `-1` for all other problems; other return values with special meanings may be defined in the future.

BATMAN automatically builds `messagesigned` on top of `verification` by extracting the first `SIGNATURE_BYTES` bytes of the signed message as a signature, extracting the remaining bytes as the original message, and applying `verification` to a 32-byte SHA-256 hash of the original message.

8.22 `sharedsecret`: generate a shared secret using a secret key and another user's public key

A secret-sharing BAT must provide a `sharedsecret` function callable as follows:

```
#include "sizes.h"

const unsigned char sk[PUBLICKEY_BYTES]; unsigned long long sklen;
const unsigned char pk[PUBLICKEY_BYTES]; unsigned long long pklen;
unsigned char s[SHAREDSECRET_BYTES]; unsigned long long slen;

sharedsecret(s,&slen,sk,sklen,pk,pklen);
```

The `sharedsecret` function uses a secret key `sk[0]`, `sk[1]`, ..., `sk[sklen-1]` and another user's public key `pk[0]`, `pk[1]`, ..., `pk[pklen-1]` to compute a shared secret. It puts the length of the shared secret into `slen` and puts the shared secret into `s[0]`, `s[1]`, ..., `s[slen-1]`. It then returns 0.

The `sharedsecret` function guarantees that `slen` is at most `SHAREDSECRET_BYTES`. The `SHAREDSECRET_BYTES` macro is defined in `sizes.h`.

The `sharedsecret` function is free to assume that the secret key `sk[0]`, `sk[1]`, ..., `sk[sklen-1]` was generated by a successful call to the `keypair` function.

If shared-secret generation is impossible for some reason, `sharedsecret` returns a negative number, possibly after modifying `s[0]`, `s[1]`, etc. Current implementations should return `-1`; other return values with special meanings may be defined in the future.

8.23 Notes on security evaluations

Subsequent sections in this chapter explain how BATs can make statements regarding the complexity of the best attacks known. These statements do not have the same level of verifiability as the eBATS measurements of key size, signing time, etc., but they will nevertheless be recorded and reported in the eBATS database for public discussion.

BATs can be submitted without security documentation. It is better to have benchmarks first, and figure out the security level later, than to have no benchmarks at all. But security documentation is important: BAT implementors who at first omit security documentation are encouraged to include the security documentation as soon as they can.

BATs can be submitted with rough estimates of security levels. It is better to have rough estimates first, and to have more accurate estimates later, than to have no estimates at all. Sometimes rough estimates are enough to show that one system is considerably more secure than another system with similar efficiency. On the other hand, sometimes systems are close. BAT implementors are encouraged to point out (in `documentation.pdf`) any troublesome points in their estimates, and to improve their estimates as soon as possible.

BAT security evaluations should not worry about future improvements in attack methods. Security evaluations should assume that attackers are limited to today's best attack algorithms. The reader is expected to already be aware that security levels are merely conjectures, and that improved attacks may reduce a system from an acceptable security level to an unacceptable security level.

BAT security evaluations should not worry about future improvements in costs for electronics. Security evaluations should assume that attackers will incur today's costs for computation. The reader is expected to already be aware that improvements in computer technology are continuing to make computations less expensive.

Final BAT security estimates must account for massively parallel computation. This means not just many computers working simultaneously, but also many chips working simultaneously inside one computer, and many computations working simultaneously inside one chip.

With 1000 euros, for example, an attacker can build a computer with several 110-euro FPGAs, each of which can handle 12 parallel high-speed ECM computations using a recently published ECM circuit. This computer is much more cost-effective than a typical Athlon 64 X2 workstation carrying out just two parallel high-speed ECM computations for the same price. Well-funded attackers can do even better with ASICs instead of FPGAs. Of course,

computations benefit much less from parallelism if they rely on frequent random access to large amounts of storage.

BAT implementors are free to ask for help in evaluating attack costs. VAMPIRE's SHARCS (Special-purpose Hardware for Attacking Cryptographic Systems) workshops in 2005 and 2006 have featured talks from many people analyzing the cost of cryptanalytic computations. Another SHARCS workshop will take place in 2007.

BAT security estimates against timing attacks must account for high-capacity timing channels. Delaying results until a constant time does not stop all timing attacks; for example, hyperthreading attacks see the time for each memory access. A return value of 0 from the `timingattacks` function is a strong statement. On the other hand, the `distinguishingchance`, `forgerychance`, and `cdhchance` functions are free to assume that timing is not visible to attackers; many cryptographic applications are offline applications that do not reveal timing to attackers.

8.24 `distinguishingchance`: report effectiveness of best attack known

An encrypting BAT can provide a `distinguishingchance` function callable as follows:

```
#include "sizes.h"

double e;
double s;
double p = distinguishingchance(e,s);
```

The `distinguishingchance` function returns a number between 0 and 1, the ciphertext-distinguishing (IND-CPA) probability for an attacker spending `e` euros and `s` seconds against one public key. Here `e` and `s` are powers of 2 between 2^0 and 2^{40}.

The attacker is given a ciphertext obtained either by encrypting m_0 or by encrypting m_1, where m_0 and m_1 are messages of the same length. The attacker's goal is to guess, with probability at least 50%+`p`, whether the decryption is m_0 or m_1. The attacker is not required to carry out a passive attack; the attacker is presumed to be able to specify m_0 and m_1. The attacker is not required to use meaningful messages m_0 and m_1; any distinguished messages, no matter how random they look, are presumed to be a disaster. These presumptions are standard: without them, every application would need a separate analysis of the message space.

8.25 `multiplekeydistinguishingchance`: report effectiveness of best attack known

An encrypting BAT can provide a `multiplekeydistinguishingchance` function callable as follows:

```
#include "sizes.h"

double e;
double s;
```

```
double k;
double p = multiplekeydistinguishingchance(e,s,k);
```

The `multiplekeydistinguishingchance` function returns a number between 0 and 1, namely the ciphertext-distinguishing (IND-CPA) probability for an attacker spending `e` euros and `s` seconds against `k` public keys. Here `e`, `s`, and `k` are powers of 2 between 2^0 and 2^{40}.

The result of `multiplekeydistinguishingchance` can be larger—as much as `k` times larger—than the result of `distinguishingchance`.

8.26 `ccattacks`: report extra effectiveness of chosen-ciphertext attacks

An encrypting BAT can provide a `ccattacks` function callable as follows:

```
#include "sizes.h"

int x = ccattacks();
```

The `ccattacks` function returns 100 if adaptive chosen-ciphertext attacks (IND-CCA2) are more effective than chosen-plaintext attacks. It returns 0 if adaptive chosen-ciphertext attacks are no more effective than chosen-plaintext attacks.

8.27 `forgerychance`: report effectiveness of best attack known

A signing BAT can provide a `forgerychance` function callable as follows:

```
#include "sizes.h"

double e;
double s;
double p = forgerychance(e,s);
```

The `forgerychance` function returns a number between 0 and 1, namely the probability that an attacker spending `e` euros will succeed at forging at least one signed message within `s` seconds, given a public key. Here `e` and `s` are powers of 2 between 2^0 and 2^{40}.

The attacker is not required to carry out a selective forgery, i.e., a forgery on a message chosen in advance by the attacker. Any forged message, no matter how random it looks, is presumed to be a disaster if it was not signed by the legitimate key owner. This is a standard presumption: without it, every application would need a separate analysis of potential forgeries within the application's message space.

The attacker is not required to carry out a blind attack. The attacker is presumed to be able to see many legitimate signatures. This is a standard presumption: most signature applications do not keep signatures secret.

The attacker is not required to carry out a passive attack. The attacker is presumed to be able to influence the legitimately signed messages. This is a standard presumption: without it, every application would need a separate analysis of the attacker's influence.

8.28 `multiplekeyforgerychance`: report effectiveness of best attack known

A signing BAT can provide a `multiplekeyforgerychance` function callable as follows:

```
#include "sizes.h"

double e;
double s;
double k;
double p = multiplekeyforgerychance(e,s,k);
```

The `multiplekeyforgerychance` function returns a number between 0 and 1, namely the probability that an attacker spending `e` euros will succeed at forging at least one signed message within `s` seconds, given `k` public keys. Here `e`, `s`, and `k` are powers of 2 between 2^0 and 2^{40}.

The result of `multiplekeyforgerychance` can be larger than the result of `forgerychance` by a factor as large as `k`.

8.29 `cdhchance`: report effectiveness of best attack known

A secret-sharing BAT can provide a `cdhchance` function callable as follows:

```
#include "sizes.h"

double e;
double s;
double p = cdhchance(e,s);
```

The `cdhchance` function returns a number between 0 and 1, namely the probability that an attacker spending `e` euros and `s` seconds can deduce a shared secret given two public keys. Here `e` and `s` are powers of 2 between 2^0 and 2^{40}.

The `cdhchance` function is free to ignore attacks that merely distinguish the shared secret from uniform ("generalized DDH" attacks) without computing the shared secret ("generalized CDH" attacks); shared secrets are presumed to be hashed before they are used.

8.30 `multiplekeycdhchance`: report effectiveness of best attack known

A secret-sharing BAT can provide a `multiplekeycdhchance` function callable as follows:

```
#include "sizes.h"

double e;
double s;
double k;
double p = multiplekeycdhchance(e,s,k);
```

The `multiplekeycdhchance` function returns a number between 0 and 1, namely the probability that an attacker spending `e` euros and `s` seconds can deduce at least one shared secret given `k` public keys. (More precisely, there are public keys `key_1`, `key_2`, ..., `key_k`; the attack is successful if it prints a vector `i`, `j`, `z` where $1 \leq \texttt{i} \leq \texttt{j} \leq \texttt{k}$ and `z` is the secret shared between `key_i` and `key_j`.) Here `e`, `s`, and `k` are powers of 2 between 2^0 and 2^{40}.

The result of `multiplekeycdhchance` can be larger than the result of `cdhchance` by a factor as large as `k(k-1)/2`.

8.31 `fakekeyattacks`: report extra effectiveness of fake-key attacks

A secret-sharing BAT can provide an `fakekeyattacks` function callable as follows:

```
#include "sizes.h"

int x = fakekeyattacks();
```

The `fakekeyattacks` function returns 100 if an active attacker can save time by providing fake keys (in applications that do not go to any extra effort to validate keys). It returns 0 if an active attacker obtains no benefit from fake keys (for example, if the `sharedsecret` function includes all necessary key validation).

8.32 `timingattacks`: report extra effectiveness of timing attacks

A BAT can provide a `timingattacks` function callable as follows:

```
#include "sizes.h"

int x = timingattacks();
```

The `timingattacks` function returns 0 if the software does not leak any secret information through timing (variable time for branching, variable time for memory access, etc.): i.e., if the best attack known that sees timings is as difficult as the best attack known that does not see timings. It returns 100 if the software leaks secret information through timing.

8.33 `copyrightclaims`: report copyright claims

A BAT can provide a `copyrightclaims` function callable as follows:

```
#include "sizes.h"

int x = copyrightclaims();
```

The `copyrightclaims` function returns one of the following numbers:

- 0: There are no known present or future claims by a copyright holder that the distribution of this software infringes the copyright. In particular, the author of the software is not making such claims and does not intend to make such claims.

- 10: The author is aware of third parties making such claims, but the author disputes those claims.
- 20: The author is aware of third parties making such claims, and the author agrees with the claims, but the author has no financial connections to the copyright.
- 30: The author has financial connections to a copyright restricting distribution of this software.

More numbers may be defined in the future.

No matter what the BAT's copyright status is, eBATS will publicly distribute copies of the BAT for benchmarking. The submitter must ensure before submission that publication is legal.

8.34 `patentclaims`: report patent claims

A BAT can provide a `patentclaims` function callable as follows:

```
#include "sizes.h"

int x = patentclaims();
```

The `patentclaims` function returns one of the following numbers:

- 0: There are no known present or future claims by a patent holder that the use of this software infringes the patent. In particular, the author of the software is not making such claims and does not intend to make such claims.
- 10: The author is aware of third parties making such claims, but the author disputes those claims.
- 20: The author is aware of third parties making such claims, and the author agrees with the claims, but the author has no financial connections to the patent.
- 30: The author has financial connections to a patent restricting use of this software.

More numbers may be defined in the future.

No matter what the BAT's patent status is, eBATS will publicly distribute copies of the BAT for benchmarking.

Chapter 9

Collecting measurements

9.1 Using BATMAN

On a computer running a UNIX-compatible operating system such as Linux, FreeBSD, or Solaris, measuring all the available BATs is a simple matter of downloading, unpacking, and running the BATMAN program:

```
wget http://hyperelliptic.org/ebats/batman-20070214.tar.gz
gunzip < batman-20070214.tar.gz | tar -xf -
cd batman-20070214
wget http://hyperelliptic.org/ebats/bats-20070214.tar.gz
gunzip < bats-20070214.tar.gz | tar -xf -
cd libraries
wget --passive-ftp ftp://ftp.gnu.org/gnu/m4/m4-1.4.8.tar.bz2
wget --passive-ftp ftp://ftp.gnu.org/gnu/gmp/gmp-4.2.1.tar.bz2
wget http://www.shoup.net/ntl/ntl-5.4.tar.gz
wget http://www.openssl.org/source/openssl-0.9.8d.tar.gz
cd ..
./do
```

This process creates a file `20070214-xyz` of new database entries and an accompanying log `20070214-xyz-notes`, where `xyz` is the machine name.

The complete suite of measurements took 24818 seconds on `td178`, 26297 seconds on `td159`, 26308 seconds on `td189`, 27010 seconds on `mace`, 27819 seconds on `katana`, 39416 seconds on `pclin153`, 42245 seconds on `td156`, 59004 seconds on `shell`, 83353 seconds on `td185`, 85490 seconds on `td162`, 90039 seconds on `pclin118`, 92700 seconds on `poema`, 109283 seconds on `td186`, 134461 seconds on `fireball`, 164582 seconds on `td158`, 177673 seconds on `td152`, 178911 seconds on `neumann`, 202831 seconds on `atlas`, 229156 seconds on `thoth`, 262574 seconds on `hald`, and 548297 seconds on `gggg`, totalling more than $3 \cdot 10^{15}$ CPU cycles.

The eBATS project is open to contributions of third-party measurements on computers that have enough time to benchmark all the available BATs (preferably with no other tasks consuming CPU power) and that will have enough time in the future for updated benchmarks. Computers do not have to be of different types from computers in the existing list; independent verification on similar computers is useful. Contributors should consult `http://www.ecrypt.eu.org/ebats/batman.html` for the latest BATMAN instructions, and should send URLs of results to `batmanresults2@ebats.cr.yp.to`.

9.2 A peek inside BATMAN

The current version of BATMAN contains 4966 lines of code, not counting the M4, GMP, NTL, and OpenSSL libraries, and not counting the BATs.

BATMAN puts considerable effort into working around differences between computers, hiding those differences from the BATMAN user and the BAT developers. For example, BAT developers are free to assume that the latest version of GMP is installed; but, in reality, some computers do not have GMP installed, and some computers have an obsolete version of GMP installed. Users installing cryptographic software that relies on GMP will, presumably, also install the latest version of GMP, but requiring this installation before benchmarking would limit the pool of computers available for benchmarking. BATMAN shields BATs from these complications by compiling the latest version of GMP and using that version for measurements. Similar comments apply to NTL and OpenSSL. Unfortunately, some of the compilation scripts in these libraries are quite fragile. A large part of the BATMAN development effort consists of improving the portability of these libraries. This is a continuing project; for example, BATMAN has not yet succeeded in compiling OpenSSL for the ppc64 architecture.

9.3 Creating tables and graphs

The tables in this report were created from the eBATS database by a straightforward 114-line `data2tables` script. Similar comments apply to the graphs in this report.

VAMPIRE has also developed CAVE (Comparison and Visualization Environment), a program allowing users to dynamically explore various graphs of BATMAN output, sliding between selected slices and projections of the database. This program can be found at `http://www.ecrypt.eu.org/ebats/cave.html`.

Chapter 10

eBATS continues

10.1 Introduction

eBATS is a continuing project. This chapter describes various plans, goals, and ideas for eBATS.

10.2 The SPEED workshop

The VAMPIRE lab is organizing a SPEED (Software Performance Enhancement for Encryption and Decryption) workshop this year. SPEED addresses the speed of secret-key and public-key cryptography. One of SPEED's purposes is to provide a forum for the BAT submitters and encourage work investigating the security of the BATs. Important dates:

- April 6, 2007: Submission of papers.
- May 11, 2007: Notification of acceptance or rejection.
- May 25, 2007: Revised versions of papers.
- June 11–12, 2007: SPEED workshop in Amsterdam.

The program committee includes Daniel J. Bernstein (University of Illinois at Chicago), Tanja Lange (Technische Universiteit Eindhoven), Christof Paar (Ruhr-Universität Bochum), Daniel Page (University of Bristol), Nigel Smart (University of Bristol), and Andre Weimerskirch (escrypt). The invited speakers include Daniel J. Bernstein (University of Illinois at Chicago), Torbjörn Granlund (SWOX), Dag Arne Osvik (EPFL), Daniel Page (University of Bristol), and Matt Robshaw (France Telecom).

10.3 Security evaluations

Do users want the smallest, fastest cryptosystems? Not exactly. Users want the smallest, fastest cryptosystems *that provide an acceptable security level*. There is a tradeoff between security and efficiency: one can reduce time and space by reducing security level.

eBATS measures the time and space consumed by various BATs. Users comparing these measurements also want to compare security levels, so BATs are encouraged to make statements regarding security levels. These statements are already supported by the eBATS API, and VAMPIRE plans to highlight comparisons of this type in the next eBATS report.

See Section 8.23 for further comments on security evaluations.

10.4 More BATs; faster BATs

The existing BATs—see Chapter 2—include many different public-key systems, often using state-of-the-art implementation techniques. However, there is clearly room for more public-key systems, and for faster implementations of those systems.

VAMPIRE is developing additional BATs and is continuing to solicit BATs from cryptographic implementors worldwide. VAMPIRE's fair benchmarking of all submitted systems has the effect of advertising the systems that offer high speed, small keys, etc., and thereby motivating the implementors of those systems to join the eBATS competition. Implementors have to go to a small amount of work to support the eBATS API, but the API was designed to minimize this work.

Most of the existing BATs have no protection against side-channel attacks, such as timing attacks. VAMPIRE is particularly interested in investigating the minimum cost of public-key systems protected against side-channel attacks. This work is shared between VAM1 and VAM3, taking input from AZTEC 3.

Some potential efficiency improvements are not reflected in the existing benchmarking framework:

- Signers with state. Merkle's hash-based signatures, for example, are efficient only if the signer can record information after each signature. Benchmarking these signatures would require additional API functions.
- Batch speedups. For example, some signature systems allow a batch of signatures to be verified in less time than any known method to verify each signature separately. Benchmarking batch operations would require additional API functions.
- Compression of key-message-signature vectors. Daniel Bleichenbacher has discovered a method of reducing the bandwidth to transmit (k, m, s) below the bandwidth needed to transmit k and (m, s) separately; here k is an RSA public key, m is a message, and s is a signature of m under k. Benchmarking this compression method would require additional API functions.

Authors interested in demonstrating efficiency improvements that go beyond the existing benchmarking framework are encouraged to contact `batsubmission2@ebats.cr.yp.to` to discuss API details. Every real-world improvement in the efficiency of public-key cryptography should, ideally, be visible in the results of eBATS.

10.5 More CPUs

The eBATS measurements demonstrate that the performance of public-key software is heavily influenced by—among other things!—the choice of CPU. Often one system is faster than another on some CPUs but slower on other CPUs. The results on other types of CPUs are difficult to predict in advance and need to be measured. VAMPIRE expects its Pentium 1 benchmarks to finish this month, has recently acquired CPU time on a Pentium 4 model not reflected in this report, and is exploring benchmarks for the ppc64 architecture.

10.6 Automatic benchmarking of new and updated software

After a new BAT is written and successfully tested with BATMAN, it can be measured on a wide variety of machines without much additional human effort. However, there is no obvious reason that there should be *any* additional human effort. In an ideal world, benchmark machines would automatically run new software, subject to security constraints—each BAT must be confined to its own sandbox, preventing any damage to the rest of the computer—and resource limits; furthermore, results would be automatically collated and made available to the public. This is not a short-term goal.

10.7 Additional public-key primitives

There are many public-key primitives beyond public-key encryption, public-key signatures, and public-key secret sharing. For example, there is extensive research activity in identity-based cryptography, where public keys are arbitrary strings and a trusted server generates secret keys from public keys. Implementors interested in seeing new primitives benchmarked are encouraged to contact `batsubmission2@ebats.cr.yp.to` to discuss API details.

10.8 Synergy with other benchmarking projects

Large portions of the BATMAN structure and software were successfully transported from the eBATS project to the context of eSTREAM, a stream-cipher project run by the STVL lab. Reports from `ciphercycles`, a new benchmarking toolkit for secret-key authenticated-encryption systems, were presented at STVL's SASC 2007 workshop and are available online at `http://cr.yp.to/streamciphers/timings.html`. VAMPIRE is currently evaluating the feasibility of a grand unified benchmarking project that covers all primitives of interest to the cryptographic community, including public-key systems, secret-key systems, and hash functions, in cooperation with other parts of ECRYPT.