The CLAUS++ BAT

Daniel J. Bernstein [*]

djb@cr.yp.to

CLAUS++ is a variant of CLAUS. It's written in C++ rather than C. It doesn't use OpenSSL; instead it uses either NTL, http://www.shoup.net/ntl/, or the C++ interface to the GMP library, http://www.swox.com/gmp/, depending on how it's tuned.