Cryptology ePrint Archive: Report 2011/239

Efficient Software Implementations of Modular Exponentiation

Shay Gueron

Abstract: RSA computations have a significant effect on the workloads of SSL/TLS servers, and therefore their software implementations on general purpose processors are an important target for optimization. We concentrate here on 512-bit modular exponentiation, used for 1024-bit RSA. We propose optimizations in two directions. At the primitives' level, we study and improve the performance of an "Almost" Montgomery Multiplication. At the exponentiation level, we propose a method to reduce the cost of protecting the w-ary exponentiation algorithm against cache/timing side channel attacks. Together, these lead to an efficient software implementation of 512-bit modular exponentiation, which outperforms the currently fastest publicly available alternative. When measured on the latest x86-64 architecture, the 2nd Generation Intel® Core™ processor, our implementation is 43% faster than that of the current version of OpenSSL (1.0.0d).

Category / Keywords: modular arithmetic, modular exponentiation, Montgomery multiplication, RSA.

Date: received 13 May 2011, last revised 28 Jun 2011

Contact author: shay at math haifa ac il