Cryptology ePrint Archive: Report 2011/444

Generalised Mersenne Numbers Revisited

Robert Granger and Andrew Moss

Abstract: Generalised Mersenne Numbers (GMNs) were defined by Solinas in 1999 and feature in the NIST Digital Signature Standard (FIPS 186-2) for use in elliptic curve cryptography. Their form is such that modular reduction is extremely efficient, thus making them an attractive choice for modular multiplication implementation. However, the issue of residue multiplication efficiency seems to have been overlooked. Asymptotically, using a cyclic rather than a linear convolution, residue multiplication modulo a Mersenne number is twice as fast as integer multiplication; this property does not hold for prime GMNs, unless they are of Mersenne's form. In this work we exploit an alternative generalisation of Mersenne numbers for which an analogue of the above property --- and hence the same efficiency ratio --- holds, even at bitlengths for which schoolbook multiplication is optimal, while also maintaining very efficient reduction. Moreover, our proposed primes are abundant at any bitlength, whereas GMNs are extremely rare. Our multiplication and reduction algorithms can also be easily parallelised, making our arithmetic particularly suitable for hardware implementation. Furthermore, the field representation we propose also naturally protects against side-channel attacks, including timing attacks, simple power analysis and differential power analysis, which is essential in many cryptographic scenarios, in constrast to GMNs.

Category / Keywords: implementation / elliptic curve cryptography, high-speed arithmetic, generalised Mersenne numbers, cyclotomic primes, generalised repunit primes

Publication Info: Submitted

Date: received 15 Aug 2011

Contact author: rgranger at computing dcu ie