CORR 2002-27

An Efficient Algorithm for Exponentiation in DH Key Exchange and DSA in Cubic Extension Fields

Guang Gong*, Anwar Hasan*, Huapeng Wu*, and Amr Youssef*

Abstract In this report, an efficient algorithm for exponentiation in cubic extension fields $\mathrm{GF}(q^3)$ for Diffie-Hellman (DH) key exchange and the digital signature algorithm (DSA) is proposed. The complexities of multiplication and squaring in $\mathrm{GF}(q^3)$ are also optimized where q is a prime or a power of prime p. Complexity comparison is made between the proposed exponentiation algorithm and the optimized "square-and-multiply" type methods. It is shown that DH key exchange and DSA utilizing the new algorithm is much more efficient than using the "square-and-multiply" type methods. For example, when $q = p^2$, in the calculation of DSA with the new method takes only 57% of the number of ground field operations required by the standard "square-and-multiply" method.

Keywords Exponentiation, extension field. LFSR sequence, DH key exchange, DSA.