CORR 2001-03

Efficient Computation of Multiplicative Inverses for Cryptographic Applications

M.A. Hasan*

Abstract Among the basic arithmetic operations over finite fields, the computation of a multiplicative inverse is the most time consuming operation. In this report, a number of methods are presented to efficiently compute the inverse using the extended Euclidean algorithm. The proposed methods can significantly reduce the computation time over large fields where the field elements are represented using a multi-precision format. A hardware structure for the inverter is also presented. The structure is area efficient and is suitable for resource constrained systems.

Index Terms Computer arithmetic, Galois (or finite) fields, multiplicative inversion, elliptic curve cryptography, Euclidean algorithm.