CORR 2002-12

Efficient Multiplication Beyond Optimal Normal Bases

A. Reyhani-Masoleh & M.A. Hasan*

Abstract In cryptographic applications, the use of normal bases to represent elements of the finite field $GF(2^m)$ is quite advantageous, especially for hardware implementation. In this article, we consider an important field operation, namely, multiplication which is used in many cryptographic functions. We present a class of algorithms for normal basis multiplication in $GF(2^m)$. Our proposed muliplication algorithm for composite finite fields requires significantly lower number of bit level operations and hence can reduce the space complexity of cryptographic systems.

Keywords Finite fields, multiplication, normal bases, composite fields, optimal bases