Cryptology ePrint Archive: Report 2011/556

GF(2^n) redundant representation using matrix embedding

Yongjia Wang and Haining Fan

Abstract: By embedding a Toeplitz matrix-vector product (MVP) of dimension n into a circulant MVP of dimension $N=2n+\delta -1$, where $\delta $ can be any nonnegative integer, we present a $GF(2^n)$ multiplication algorithm. This algorithm leads to a new redundant representation, and it has two merits: 1. The flexible choices of δ make it possible to select a proper N such that the multiplication operation in ring $GF(2)[x]/(x^N+1$) can be performed using some asymptotically faster algorithms, e.g. the Fast Fourier Transformation (FFT)-based multiplication algorithm; 2. The redundant degrees, which are defined as N/n, are smaller than those of most previous $GF(2^n)$ redundant representations, and in fact they are approximately equal to 2 for all applicable cases.

Category / Keywords: implementation

Publication Info: not published

Date: received 9 Oct 2011, last revised 10 Oct 2011

Contact author: fhn at tsinghua edu cn