Cryptology ePrint Archive: Report 2011/606

$GF(2^{n})$ Subquadratic Polynomial Basis Multipliers for Some Irreducible Trinomials

Xi Xiong and Haining Fan

Abstract: The $GF(2^{n})$ multiplication operation in polynomial basis can be represented as a matrix-vector product form, and the matrix is called the Mastrovito matrix. The Toeplitz matrix-vector product approach has been used to design subquadratic shifted polynomial basis multip In order to apply this approach to subquadratic polynomial basis multipliers, this Mastrovito matrix should be transformed into a Toeplitz matrix. this paper, two transformation methods are proposed for irreducible trinomial $x^{n}+x^{k}+1$, where $2k+1\leq n$.

Category / Keywords: foundations /

Date: received 9 Nov 2011, withdrawn 8 Dec 2011

Contact author: yqnyhdjn at gmail com

Available formats: (-- withdrawn --)

Version: 20111208:160557 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]