The article has been accepted for inclusion in a future issue of ETRI journal, but has not been fully edited. Content may change prior to final publication
https://doi.org/10.4218/etrij.17.0116.0770

# Low-Power and Low-Hardware Bit-Parallel Polynomial Basis Systolic Multiplier over GF($2^m$) for Irreducible Polynomials

Sudha Ellison Mathe and Lakshmi Boppana

**Multiplication in finite fields is used in many applications, especially in cryptography. It is a basic and the most computationally intensive operation from among all such operations. Several systolic multipliers are proposed in the literature that offer low hardware complexity or high speed. In this paper, a bit-parallel polynomial basis systolic multiplier for generic irreducible polynomials is proposed based on a modified interleaved multiplication method. The hardware complexity and delay of the proposed multiplier are estimated, and a comparison with the corresponding multipliers available in the literature is presented. Of the corresponding multipliers, the proposed multiplier achieves a reduction in the hardware complexity of up to 20% when compared to the best multiplier for $m$ = 163. The synthesis results of application-specific integrated circuit and field-programmable gate array implementations of the proposed multiplier are also presented. From the synthesis results, it is inferred that the proposed multiplier achieves low power consumption and low area complexity when compared to the best of the corresponding multipliers.**

**Keywords: Finite field, Cryptography, Systolic, Polynomial basis, Application-specific integrated circuit, Field programmable gate arrays.**

Manuscript received Oct. 28, 2016; revised Mar. 11, 2017; accepted Mar. 28, 2017.

Sudha Ellison Mathe (corresponding author, ellison@nitw.ac.in) and Lakshmi Boppana (lakshmi@nitw.ac.in) are with the Department of Electronics and Communication Engineering, National Institute of Technology-Warangal, India.



## I. Introduction

Cryptography is the art of efficiently hiding data and transmitting it over any insecure channel to prevent unauthorized access. Modern cryptography mainly depends on the foundation principles of mathematical theory and computer science. It mainly deals with the development of cryptographic algorithms that are designed around assumptions regarding computational hardness. Cryptography can be broadly categorized as symmetric-key cryptography and asymmetric-key cryptography [1]. Symmetric-key cryptography performs the encryption and decryption processes using the same secret key. The techniques developed using this principle are the data encryption standard [2] and the advanced encryption standard (AES) [3]. Asymmetric-key cryptography performs the encryption and decryption processes using different keys. Elliptic curve cryptography (ECC) [4], [5] and Rivest and others [6] are some techniques that have been developed using this principle.

Many cryptographic algorithms utilize the multiplication operation in finite fields. Basic operations in a finite field, such as addition and subtraction, are realized using the logical exclusive-OR (XOR), whereas complex operations such as division, exponentiation, and inversion are realized using recursive multiplications [7]. Therefore, the basic unit for all of these arithmetic operations is the multiplication operation. Multiplication in a finite field can be performed over three basis representations, namely Normal Basis (NB), Polynomial Basis (PB), and Dual Basis (DB) [8], each of which has its distinct advantages. Hardware implementations of NB multipliers typically consume less power compared to other bases, and they are mainly used to realize squaring and exponentiation operations. Multiplications in PB are less complex, but the hardware implementations consume more power compared to NB multipliers. DB multipliers require a low area compared to the other two bases. However, PB