# A Reconfigurable Most/Least Significant Bit Multiplier for $GF(2^m)$

P. Kitsos and O. Koufopavlou
*VLSI Design Laboratory*
*Electrical and Computer Engineering Department*
*University of Patras, GREECE*
*E-mail: pkitsos@ee.upatras.gr*

## Abstract

*An efficient architecture of a reconfigurable Least/Most Significant Bit multiplier for Galois field $GF(2^m)$ where $1 < m \leq M$, is presented. The proposed multiplier can operate either as a most significant or as a least significant bit first multiplier. The value m, of the irreducible polynomial degree, can be changed and the value of M determines the maximum size that the multiplier can support. This architecture features the high order of flexibility and scalability, which allows an easy configuration for different field size.*

## 1. Introduction

Elliptic Curve Cryptography (ECC) replaces the RSA due to its advantage of using shorter key lengths for the same security level. ECC requires arithmetic in $GF(2^m)$. Multiplication in $GF(2^m)$ is considered as the most critical operation for performing enhancement of practical cryptography applications, like smart cards that use finite field degree from 106 to 170.

Previous published multipliers over $GF(2^m)$ include serial multipliers, Most Significant Bit (MSB)-first [1] and Least Significant Bit (LMSB)-first [2], bit-parallel [3] and hybrid multipliers [4]. Because the infeasible complexity of the bit-parallel multiplier architecture serial and hybrid multipliers are used. In addition, the hybrid multipliers with composite exponent representation are discouraged for ECC [5].

In this paper, a reconfigurable architecture for the Most/Least Significant Bit (MLSB)-first, bit-serial, polynomial basis multiplier over $GF(2^m)$ is introduced, where $1 < m \leq M$. $m$ is the degree of the irreducible polynomial and it can be easily changed according to the application requirements. $M$ is the maximum degree of the irreducible polynomial.

## 2. Proposed architecture

The proposed reconfigurable MLSB-first multiplier can be used for variable field degree, *m*, and is shown in figure 1. The proposed hardware implementation consists first, of a bit-sliced Linear Feedback Shift Register (LFSR) and second *M* multiplexer (MUX), demultiplexers (DEMUX), XOR and OR gates. Each slice, *i*, consists of three subfield multipliers (AND gates), two subfield adder (XOR gate), one 2-input multiplexer, one 2-output demultiplexer, two OR gate, and four one-bit registers (*P*(i), *A*(i), *C*(i) and *D*(i)). The non-zero coefficients, *p*(i), of the irreducible polynomial *P*(x), configure the LFSR, through the OR and AND gates of the feedback path. The maximum value of the field degree is *M*, and it is determined by the application requirements. The multiplexer (MUX) selects the multiplier operation. So the MSB-first is expressed by the continuous line and the LSB-first is expressed by the discontinuous line.

For the MSB-first operation each coefficient, *a*(i), of the multiplicand polynomial *A*(x), is stored in *A*(i) position of the *A*(i) register, while each coefficient *p*(i), of the irreducible polynomial *P*(x), is stored in the *P*(i) position of the *P*(i) register. If an irreducible polynomial of degree *m*, with $m<M$ is required, the remaining *P*(j) and *A*(j) bits of the registers are filled with zeros, where $m<j\leq M$.

For the MSB-first operation each coefficient, *a*(i), of the multiplicand polynomial *A*(x), is stored in *D*(i) position of the LFSR.

Signal *control*(i) selects one of the two demultiplexer outputs. The value of each signal *control*(i), is defined as:

$$control(i) = \begin{cases} 1 & if \ \ i \leq m \\ 0 & if \ \ m < i \leq M \end{cases}$$

In the positions where *control*(i)=1 (out1 is selected) the slice is an active whilst if *control*(i)=0 (out2 is selected) the slice is inactive. Inactive means that this slice is not used during multiplication. o*ut*2 forces the global feedback path with the proper value through the $OR_i$ gate.

When the application requires multiplications with variable field sizes, the value of the *m*, and the set of coefficients of polynomials *A*(x), *B*(x), and *P*(x) are configured again. After *m* clock cycles the right multiplication result is stored in the register *D*(i) for the MSB-first multiplier and the register *C*(i) for the LSB-first multiplier.

The minimum clock cycle period is $3T_{AND}+T_{XOR}+2T_{NOT}+(m+3)T_{OR}$, where $T_{AND}$, $T_{XOR}$, $T_{NOT}$, $T_{OR}$ is the delay of the 2-input AND, 3-input XOR, inverter, and 2-input OR gates, respectively.

Low power consumption can be achieved using clock-gating technique. During computation each one-bit register, *D(*i*)*, can be controlled by the corresponding *control(*i*)* signal. So, all the *D(*j*)* registers, are set inactive by discontinue their clock signal.

Due to the fact that the proposed architecture is the first reconfigurable and reprogrammable (operate either as a least significant or as a most significant bit first) multiplier there are not previous performance metrics.

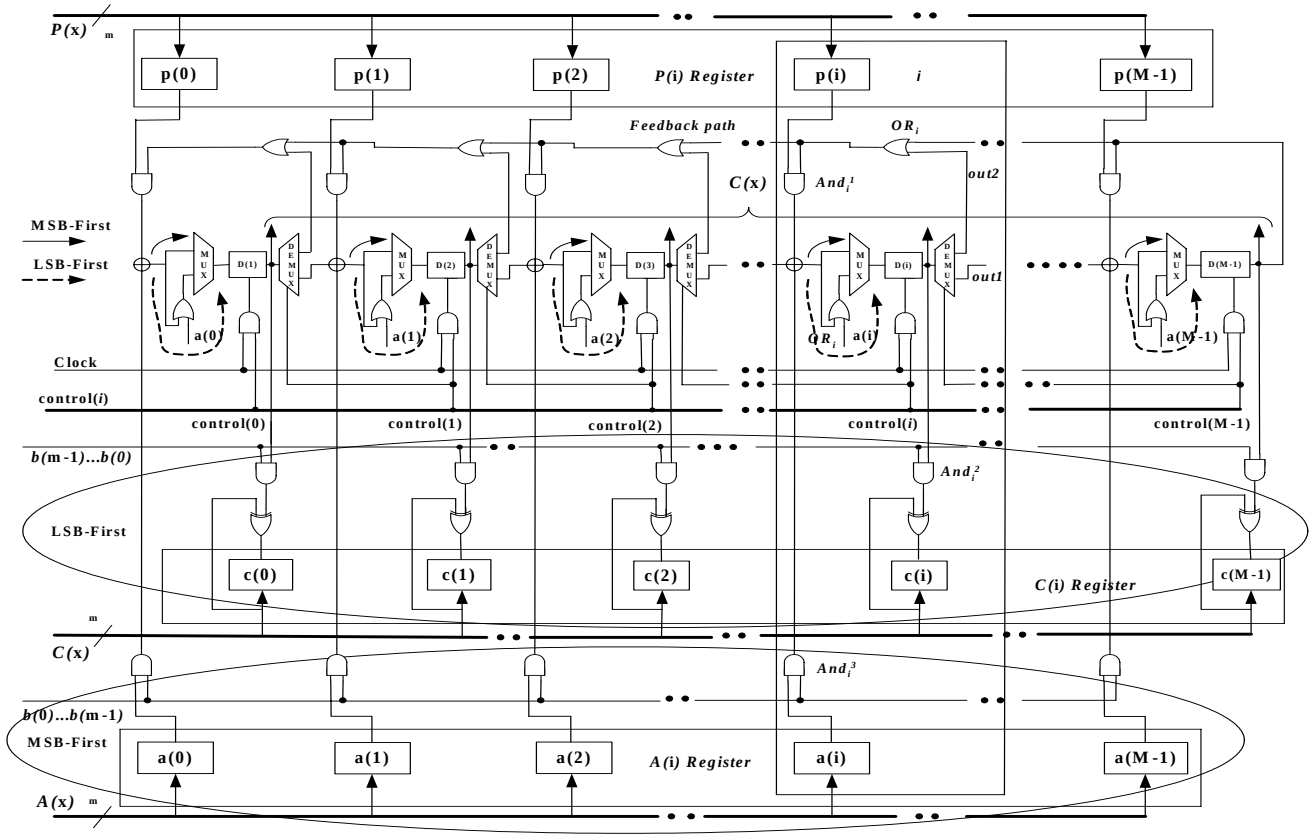


**Figure 1.** Proposed Reconfigurable Most/ Least Significant Bit (MLSB)-first Multiplier

## 3. Conclusions

In this paper a reconfigurable Most/Least Significant Bit (MLSB)-first, bit-serial GF multiplier architecture is proposed. The multiplier is reprogrammable and reconfigurable because it can perform with any arbitrary irreducible polynomial degree *m*, either in MSB-first or LSB-first fashion. The multiplication result is computed after m clock cycles. The advantages of the proposed architecture are the high order of flexibility and scalability that allow an easy configuration for variable field size m. The performance measurements in FPGA with field size from 106 to 170 prove that the proposed multiplier can operates from 32 MHz to 18 MHz clock frequency respectively.

## 4. References


[1] P. A. Scott, S. E. Travares, and L. E. Peppard, "A Fast VLSI Multiplier for GF(2m)", IEEE Journal on Selected Areas in Communications, Vol. sac-4, pp: 62-65, January 1986.

[2] C. S. Yeh, I.S. Reed, and T.K. Truong, "Systolic multipliers for finite fields GF($2^m$). IEEE Transactions on Computers, 33(4), pp: 357-360, April 1984.

[3] Ç. K. Koç, B. Sunar, "Low-Complexity Bit-Parallel Canonical and Normal Basis Multipliers for a Class of Finite Fields", IEEE Transactions on Computers, 47(3), pp. 353-356, March 1998.

[4] C. Paar, P. Fleischmann, and P. Soria-Rodriguez, "Fast Arithmetic for Public-Key Algorithms in Galois Field with Composite Exponents", IEEE Transaction of Computers, 48 (10), pp. 1025-1034, October 1999.

[5] Nigel P. Smart, "How Secure Are Elliptic Curves over Composite Extension Fields?", Advances in Cryptology - EUROCRYPT 2001, Innsbruck, Austria, May 6-10, 2001.