ELectronics EXpress

LETTER

IEICE Electronics Express, Vol.10, No.13, 1–6

A low latency semi-systolic multiplier over $GF(2^m)$

Kee-Won Kim[1a)] **and Seung-Hoon Kim**[2b)]

[1] *College of Engineering, Dankook University, Cheonan 330–714, Korea*

[2] *Department of Multimedia Engineering, Dankook University, Cheonan 330–714, Korea*

a) *nirkim@gmail.com*

b) *edina@dankook.ac.kr(corresponding author)*

Abstract: A finite field multiplier is commonly used in implementations of cryptosystems and error correcting codes. In this paper, we present a low latency semi-systolic multiplier over $GF(2^m)$. We propose a finite field multiplication algorithm to reduce latency based on parallel computation. The proposed multiplier saves at least 31% time complexity as compared to the corresponding existing structures.

Keywords: cryptography, finite field arithmetic, modular multiplication, semi-systolic array

Classification: Integrated circuits

References

[1] R. E. Blahut: *Theory and Practice of Error Control Codes* (Addison-Wesley, Reading, 1983).

[2] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone: *Handbook of Applied Cryptography* (CRC Press, Boca Raton, 1996).

[3] S. K. Jain, L. Song and K. K. Parehi: IEEE Trans. Very Large Scale Integr. (VLSI) Syst. **6** [1] (1998) 101.

[4] C. W. Chiou, C. Y. Lee, A. W. Deng and J. M. Lin: IEICE Trans. Fundamentals, **E89-A** [2] (2006) 566.

[5] C. Y. Lee, C. W. Chiou and J. M. Lin: J. Electronic Testing: Theory and Applications **22** (2006) 143.

[6] W. -T. Huang, C. H. Chang, C. W. Chiou and F. H. Chou: IET Information Security **4** [3] (2010) 111.

[7] N. Weste and K. Eshraghian: *Principles of CMOS VLSI Design: A System Perspective* (Addison-Wesley, Reading, 1985).

[8] STMicroelectronics: STMicroelectronics datasheet (2013) http://www.st.com

1 Introduction

Finite field arithmetic operations, especially for the binary field $GF(2^m)$, have been widely used in the areas of data communication and network security applications such as error-correcting codes [1] and cryptosystems [2]. The multiplication among these operations is the most important arithmetic

DOI: 10.1587/elex.10.20130354
Received May 14, 2013
Accepted June 10, 2013
Publicized June 21, 2013
Copyedited July 10, 2013

IEICE Electronics Express, Vol.10, No.13, 1–6

operation. This is because the time-consuming operations such as exponentiation, division, and multiplicative inversion can be decomposed into repeated multiplications. Thus, the fast multiplication architecture with low complexity is needed to design dedicated high-speed circuits.

Many semi-systolic multiplier over $GF(2^m)$ have been developed [3, 4, 5, 6]. Recently, Huang et al. [6] proposed a semi-systolic polynomial basis multiplier over $GF(2^m)$ to reduce both space and time complexities. They also proposed the semi-systolic polynomial basis multipliers with concurrent error detection and correction capability. However, most existing semi-systolic multipliers suffer from several shortcomings, including large time and/or hardware overhead.

In this paper, we propose an improved algorithm and multiplier over $GF(2^m)$ to reduce latency based on parallel computation. This architecture is compared with existing semi-systolic multipliers and the results show that there is a reduction in time complexity.

2 The proposed semi-systolic multiplier over $GF(2^m)$

Let the finite field over $GF(2^m)$ be defined, in general, by an irreducible polynomial of degree m, given by $G = x^m + \sum_{j=0}^{m-1} g_j x^j$, where $g_i \in GF(2)$. The polynomial basis $\{1, \alpha, \cdots, \alpha^{m-2}, \alpha^{m-1}\}$ is used to represent the field elements, so that any two arbitrary elements A and B in $GF(2^m)$ can be represented in the form of polynomials of degree $(m-1)$ as $A = \sum_{j=0}^{m-1} a_j \alpha^j$ and $B = \sum_{j=0}^{m-1} b_j \alpha^j$, where a_j and $b_j \in \{0, 1\}$, for $0 \leq j \leq m-1$. The multiplication of field elements A and B over $GF(2^m)$ is given by $P = AB \bmod G = \sum_{j=0}^{m-1} p_j \alpha^j$.

Since α is a root of $G(x)$, i.e. $G(\alpha) = 0$, α^m and α^{m+1} are as follows:

$$\alpha^m = \sum_{j=0}^{m-1} g_j \alpha^j \tag{1}$$

and

$$\alpha^{m+1} = \sum_{j=1}^{m-1} (g_{m-1} g_j + g_{j-1}) \alpha^j + g_{m-1} g_0 \equiv \sum_{j=0}^{m-1} g'_j \alpha^j. \tag{2}$$

Assume that $\alpha^{m+1} \bmod G$ is given in advance. Therefore, the $P = AB \bmod G$ can be expressed as follows:

$$P = \sum_{j=0}^{m-1} b_j A \alpha^j = \sum_{j=0}^{\lceil m/2 \rceil - 1} b_{2j} A \alpha^{2j} \bmod G + \alpha \sum_{j=0}^{\lfloor m/2 \rfloor - 1} b_{2j+1} A \alpha^{2j} \bmod G. \tag{3}$$

In the above equation, we can observe that P can be divided into two parts. Let $l = \lceil m/2 \rceil$ and $k = \lfloor m/2 \rfloor$. We define P as follows:

$$P = C + \alpha D \bmod G, \tag{4}$$

where

$$C = \sum_{j=0}^{l-1} b_{2j} A \alpha^{2j} \bmod G \text{ and } D = \sum_{j=0}^{k-1} b_{2j+1} A \alpha^{2j} \bmod G. \tag{5}$$

DOI: 10.1587/elex.10.20130354
Received May 14, 2013
Accepted June 10, 2013
Publicized June 21, 2013
Copyedited July 10, 2013

IEICE Electronics Express, Vol.10, No.13, 1–6

We can observe that the computations of C and D require $A\alpha^{2j}$ in common. Define $A^{(i)} = A\alpha^{2i}$, for $0 \le i \le l-1$. Then, $A^{(i)}$ is $A^{(i)} = \sum_{j=0}^{m-1} a_j^{(i)} \alpha^j \bmod G$.

Then, based on (1) and (2), $A^{(i)}$ can be expressed as

$$\begin{aligned} A^{(i)} &= A^{(i-1)}\alpha^2 \bmod G \\ &= \sum_{j=0}^{m-1} a_j^{(i-1)} \alpha^{j+2} \bmod G \\ &= \sum_{j=0}^{m-3} a_j^{(i-1)} \alpha^{j+2} + (a_{m-2}^{(i-1)}\alpha^m + a_{m-1}^{(i-1)}\alpha^{m+1}) \bmod G \\ &= \sum_{j=0}^{m-3} a_j^{(i-1)} \alpha^{j+2} + \sum_{j=0}^{m-1} a_{m-2}^{(i-1)} g_j \alpha^j + \sum_{j=0}^{m-1} a_{m-1}^{(i-1)} g_j' \alpha^j \\ &= \sum_{j=0}^{m-1} (a_{j-2}^{(i-1)} + a_{m-2}^{(i-1)} g_j + a_{m-1}^{(i-1)} g_j')\alpha^j, \end{aligned} \tag{6}$$

where $A^{(0)} = A$, $a_{-2}^{(i-1)} = a_{-1}^{(i-1)} = 0$, and $1 \le i \le l-1$.

From (6), we can obtain the coefficient of $A^{(i)}$ as follows:

$$a_j^{(i)} = a_{j-2}^{(i-1)} + a_{m-2}^{(i-1)} g_j + a_{m-1}^{(i-1)} g_j', \tag{7}$$

where $a_j^{(0)} = a_j$, $a_{-2}^{(i-1)} = a_{-1}^{(i-1)} = 0$, and $1 \le i \le l-1$.

Using $A^{(i)}$, C and D of (5) are represented as follows:

$$C = \sum_{i=1}^{l} b_{2(i-1)} A^{(i-1)} \text{ and } D = \sum_{i=1}^{k} b_{2i-1} A^{(i-1)}. \tag{8}$$

From (8), the recurrence equations of C and D can be formulated as

$$C^{(i)} = C^{(i-1)} + b_{2(i-1)} A^{(i-1)}, \text{ for } 1 \le i \le l \tag{9}$$

and

$$D^{(i)} = D^{(i-1)} + b_{2i-1} A^{(i-1)}, \text{ for } 1 \le i \le k, \tag{10}$$

where $C^{(0)} = D^{(0)} = 0$, and $C^{(i)} = \sum_{j=0}^{m-1} c_j^{(i)} \alpha^j$ and $D^{(i)} = \sum_{j=0}^{m-1} d_j^{(i)} \alpha^j$ are ith intermediate results.

Therefore, the coefficients of $C^{(i)}$ and $D^{(i)}$ can be computed as follows:

$$c_j^{(i)} = c_j^{(i-1)} + b_{2(i-1)} a_j^{(i-1)}, \text{ for } 1 \le i \le l \tag{11}$$

and

$$d_j^{(i)} = d_j^{(i-1)} + b_{2i-1} a_j^{(i-1)}, \text{ for } 1 \le i \le k, \tag{12}$$

where $c_j^{(0)} = d_j^{(0)} = 0$ and $0 \le j \le m-1$.

The equations (11) and (12) can be simultaneously executed because therie is no data dependency between computations of C and D.

Therefore, the result of multiplication is represented as follows:

$$P = C^{(l)} + \alpha D^{(k)}$$

DOI: 10.1587/elex.10.20130354
Received May 14, 2013
Accepted June 10, 2013
Publicized June 21, 2013
Copyedited July 10, 2013

$$\begin{aligned} &= \sum_{j=0}^{m-1} c_j^{(l)}\alpha^j + \alpha\sum_{j=0}^{m-1} d_j^{(k)}\alpha^j \bmod G \\ &= \sum_{j=0}^{m-1} c_j^{(l)}\alpha^j + \sum_{j=0}^{m-2} d_j^{(k)}\alpha^{j+1} + d_{m-1}^{(k)}\alpha^m \bmod G \\ &= \sum_{j=0}^{m-1} (c_j^{(l)} + d_{m-1}^{(k)} g_j + d_{j-1}^{(k)})\alpha^j, \end{aligned} \tag{13}$$

where $d_{-1}^{(k)} = 0$.

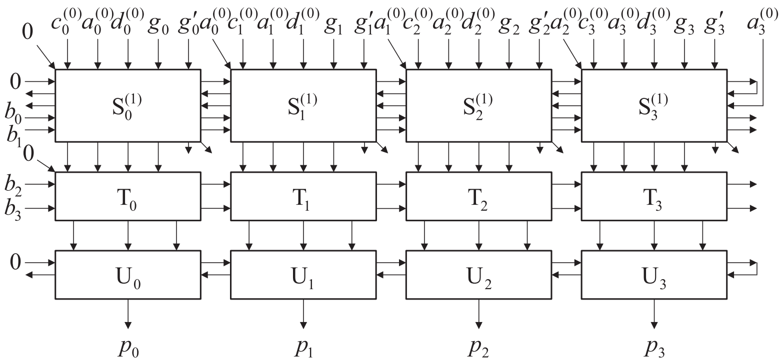

Fig. 1. The proposed multiplier over $GF(2^4)$

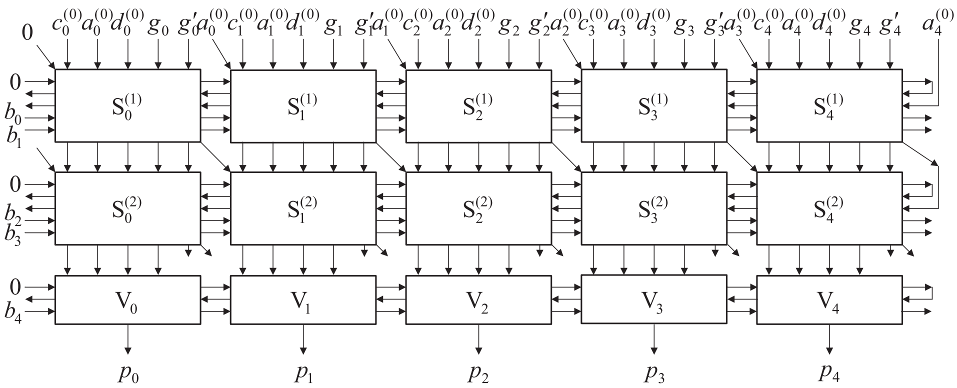

Fig. 2. The proposed multiplier over $GF(2^5)$

Based on the proposed algorithm, the hardware architectures of the proposed semi-systolic multiplier are shown in Fig. 1 and 2. When m is even, the computations of both C and D take equally k clock cycles. Otherwise, the computations of C and D take l and k clock cycles, respectively. Therefore, our proposed architecture is different depending on m. The detailed circuits of the cells in Fig. 1 and 2 are depicted in Fig. 3, and $\oplus$, $\otimes$, and the boxed "D" denote XOR gate, AND gate, and one-bit latch(flip-flop), respectively.

When m is even, our architecture is composed of $0.5m^2 - m$ $\mathrm{S}_\mathrm{j}^{(\mathrm{i})}$ cells, m $\mathrm{T_j}$ cells, and m $\mathrm{U_j}$ cells. Otherwise, it includes $0.5m^2 - 0.5m$ $\mathrm{S}_\mathrm{j}^{(\mathrm{i})}$ cells and m $\mathrm{V_j}$ cells. As shown in Fig. 3, each $\mathrm{S}_\mathrm{j}^{(\mathrm{i})}$ cell employs four 2-input AND gates, two 2-input XOR gates, one 3-input XOR gate, and five 1-bit

© IEICE 2013
DOI: 10.1587/elex.10.20130354
Received May 14, 2013
Accepted June 10, 2013
Publicized June 21, 2013
Copyedited July 10, 2013

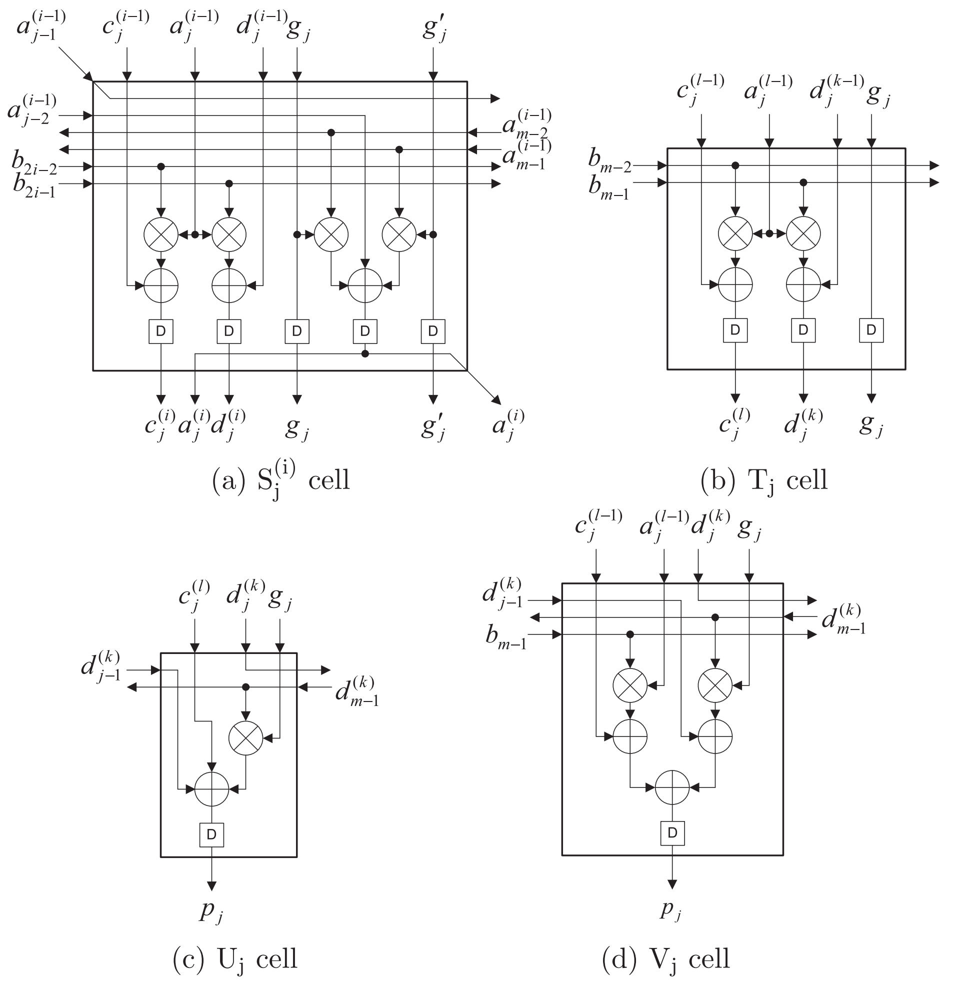

Fig. 3. The detailed circuits.

latches in order to simultaneously compute $a_j^{(i)}$, $c_j^{(i)}$, and $d_j^{(i)}$ in (7), (11), and (12), respectively. Each T_j cell consists of two 2-input AND gates, two 2-input XOR gates, and three 1-bit latches in order to simultaneously compute $c_j^{(l)}$ and $d_j^{(k)}$ in (11) and (12), and each U_j cell includes one 2-input AND gate, one 3-input XOR gate, and one 1-bit latch for the sake of computing $p_j = c_j^{(l)} + d_{m-1}^{(k)} g_j + d_{j-1}^{(k)}$ in (13). Each V_j cell is composed of two 2-input AND gates, three 2-input XOR gates, and one 1-bit latch for computing $c_j^{(l)}$ in (11) and $p_j = c_j^{(l)} + d_{m-1}^{(k)} g_j + d_{j-1}^{(k)}$ in (13).

3 Analysis of performance

In CMOS VLSI technology, each gate is composed of several transistors [7]. We adopt $A_{AND_2} = 6$, $A_{XOR_2} = 6$, and $A_{LATCH} = 8$, where A_{GATE_n} denotes transistor count of an n-input gate, respectively. Also, for a further comparison of time complexity, we adopt the practical integrated circuits in [8] and the following assumptions, as discussed in detail in [6], are made: $T_{AND_2} = 7$, $T_{XOR_2} = 12$, and $T_{LATCH} = 13$, where T_{GATE_n} denotes the propagation delay of an i-input gate, respectively.

A circuit comparison between the proposed multiplier and the related multipliers is given in Table I. By reducing the latency by half, the proposed

DOI: 10.1587/elex.10.20130354
Received May 14, 2013
Accepted June 10, 2013
Publicized June 21, 2013
Copyedited July 10, 2013

architecture has not only a better space complexity but also a reduced time complexity as compared to the existing architectures. In detail, the results show that the proposed semi-systolic multiplier saves about 50, 50, 57 and 31% time complexities as compared to the existing multipliers by Jain et al. [3], Chiou et al. [4], Lee et al. [5], and Huang [6], respectively.

Table I. Comparison of semi-systolic multipliers

	Jain et al. [3]	Chiou et al. [4]	Lee et al. [5]	Huang et al. [6]	The proposed multiplier	
					even m	odd m
AND_2	$2m^2$	$2m^2+2m$	$2m^2$	$2m^2$	$2m^2-m$	$2m^2$
XOR_2	$2m^2$	0	$2m^2$	$2m^2$	m^2	m^2+2m
XOR_3	0	m^2+m	0	0	$0.5m^2$	$0.5m^2-0.5m$
Latch	$3m^2$	$3.5m^2+3.5m$	$2m^2$	$3m^2$	$2.5m^2-m$	$2.5m^2-1.5m$
Transistors	$48m^2$	$52m^2+52m$	$40m^2$	$48m^2$	$44m^2-14m$	$44m^2-6m$
Cell delay	44	44	51	32	44	44
Latency	m	$m+1$	m	m	$0.5m+1$	$0.5m+0.5$
Total delay	$44m$	$44m+44$	$51m$	$32m$	$22m+44$	$22m+22$

4 Conclusion

In this paper, we have proposed a new finite field multiplication algorithm of which the latency is reduced by half as compared to the existing algorithms. Based on the proposed algorithm, a low latency semi-systolic multiplier is proposed. We have achieved a significant improvement. By reducing the latency by half, the proposed architecture has not only a better space complexity but also a reduced time complexity as compared to the existing architectures. We expect that our architecture can be efficiently used for various applications, which demand high-speed computation.

Acknowledgments

The present research was conducted by the research fund of Dankook University in 2012.

DOI: 10.1587/elex.10.20130354
Received May 14, 2013
Accepted June 10, 2013
Publicized June 21, 2013
Copyedited July 10, 2013