New Modular Construction of Low-Complexity bit-parallel Systolic Multipliers for a class of Finite Fields GF(2^m)

Chiou-Yng Lee and Erl-Huei Lu
Chung Gung University, Taiwan, R.O.C.
Lchiou@ms.chttl.com.tw

Abstract

An efficient design for low-complexity and fast computation for the bit-parallel systolic architecture is of practical concern in many digital circuit designs. This paper presents a class of novel bit-parallel systolic multiplier over the finite field GF(2^m), which is generated from the irreducible all one polynomial (AOP) and equally spaced polynomial (ESP). The proposed architectures have properties of highly regularity, simplicity, and shorter latency, which are important in designing the bit-parallel systolic multipliers. Moreover, the AOP-based systolic multipliers of small fields can be used to construct all the corresponding ESP-based systolic multipliers of large fields. The latency of the AOP-based and ESP-based systolic multipliers require m+2 and m+r+1 clock cycles, respectively, which are better than others. The size complexity of the proposed multipliers is smaller than previously developed multipliers of the same class. And as for the parallel systolic multipliers, the bit-parallel structures used in this paper has shorter the computation latency

I. Introduction

Efficient algorithm of real-time system, high-speed and low-complexity of fast computation over finite field GF(2^m) is an extremely important research topic owing to their applications in the areas of computers and communications, e.g., error-control-correcting [10],[14] and cryptography [9],[12],[13]. Significant arithmetic operations for these applications are addition, multiplication, inversion/division. However, multiplication and inversion/division which is proposed by successive multiplication are still complex circuits. Therefore, it is important to introduce an efficient multiplication algorithm for constructing a bit-parallel multiplier of low-complexity for arithmetic circuits. Thus, the bit-parallel systolic architecture is of course the hot topic for us to pursuit.

It is important that the Massey-Omura multiplier (MOM) in [17] is the first modular parallel architectures, which requires the circuit complexity of O(m^3) AND gates and O(m^3) XOR gates. To reduce the time and size complexities, Itoh and Tsujii in 1989 [6], based on special classes of finite fields such as all one polynomial (AOP) and equally spaced polynomial (ESP), proposed the bit-parallel multipliers. If the irreducible polynomial is an AOP, then only $2m^2$-2m XOR and m^2 AND gates are required for the parallel multiplier. Their structure is a modular architecture and has a lower size complexity compared to MOM. Besides, they also extend their multiplication algorithm to the irreducible ESP's. Later, Hasan (1992) [5],[4] used the AOP-based multipliers of small size to construct the ESP-based multipliers of large size. Recently, Koc and Sunor (1998) [3] designed multipliers of the low-complexity bit-parallel with canonical basis and normal basis. And meanwhile, Wu and Hasan (1998) [7],[8] presented another low-complexity parallel multipliers employing the weekly dual basis (WDB). Moreover, from the complexity point of view, Drelot (1998) [16] confirmed that irreducible AOP and ESP have smaller complexity arithmetic circuits. The two polynomials based on an isomorphism can be transformed from GF(2^m) into the residue polynomial ring modulo x^n+1. If the polynomial is irreducible AOP of degree m, then n=m+1. The design mentioned above were at the design of modular architectures, however, and their circuits can not be realized to use the systolic architecture.

To optimize finite-field arithmetic circuit design three criteria have to be considered: 1) short computation delay (latency); 2) less circuit complexity; 3) short clock period (cyclic time). The latency of systolic circuit is defined as the time it takes for an element from the input of a stage to its output. As low-complexity and high-speed computation becomes increasingly attractive, the systolic architectures in the VLSI are a common good choice. Due to the architectures possess concurrent, simple and regular designs that are balanced with I/O. Recently, numerous several of hardwares and algorithms, based on serial and parallel manners, have been proposed for computing arithmetic operations in GF(2^m), which can be implemented in the systolic architectures [1-2],[15],[18]. The systolic multipliers by bit-serial manners have been introduced [18]; furthermore, the parallel-in-parallel-out systolic multipliers have been proposed in [1-2]. In 1984, Yeh [2] produced the parallel systolic multiplier. Its basic cell contains two AND gates, one 3-input XOR gates, and seven latches. Wei(1994) [1] also produced a power-sum systolic multiplier for computing AB^2+C, where A, B, and C are any element in GF(2^m). However, the latency of the exited parallel systolic multipliers still required 3m clock cycles.

For the need of low-complexity circuit with minimized latency, this work presents a new bit-parallel systolic architectures to compute the element multiplication over GF(2^m). The new circuit is an alternative design in canonical basis over the field GF(2^m) generated by irreducible AOP and ESP. The novel AOP-based systolic multiplier applies the proposed multiplication schemes to construct a low-complexity and fast computation with the bit-parallel architectures. The designed multipliers are more efficient for the element multiplication in GF(2^m), as they simplify the architecture and increase computation speed. In addition, applying the AOP-based systolic multiplier of small

fields can construct the ESP-based modular systolic multiplier of large fields. The latency complexity of the developed AOP-based systolic multiplier is more efficient in reducing the clock cycles from 3m to m+2.

II. Proposed AOP-based modular systolic multiplier

It is assumed that the reader is familiar with the basic concepts of finite field. The properties of finite fields GF(2^m) are covered in detail in [11].

Definition 1 [6]: A polynomial p(x)= $\sum_{i=0}^{m} p_i x^i$ over GF(2) of degree m is called all one polynomial (AOP) iff $p_i = 1, 0 \le i \le m$.

An AOP has an important property of p(x)| $x^{m+1}+1$. This variety of polynomial is an irreducible iff m+1 is a prime and 2 is a primitive modulo m+1. For example, the possible AOP of degree m to become irreducible are specified by irreducible polynomials, such as m=2, 4, 10, 12, 18, 28, 36, 52, 58, 60, 66, 82, 100, for m ≤ 100. If α is a root of the irreducible AOP p(x), then we obtain

$$\alpha^{m+1+j}=\alpha^j \qquad (0\le j\le m-2) \tag{1}$$

In order to reduce the modulo operations, the field elements are transformed from GF(2^m) into the polynomial ring modulo $x^{m+1}+1$ because of $\alpha^{m+1}=1$, that is, any element $A=\sum_{i=0}^{m-1} \bar{a}_i a^i \in GF(2^m)$ can also be represented as $A=\sum_{i=0}^{m} a_i a^i$, where $\bar{a}_i = a_i + a_m$ $(0 \le i \le m-1)$ [6]. For example, $A=1+a+a^3 \in GF(2^4)$, the element can be represented as $A=1+a+a^3$ by using the canonical representation or $A=a^2+a^4$ by using the extended representation.

Now, let use consider of the case two extended elements $A=\sum_{i=0}^{m} a_i a^i$ and $B=\sum_{i=0}^{m} b_i a^i$ over GF(2^m), it is observably that he multiplication of two elements A and B equals to $AB \pmod{a^{m+1}+1}$. In the following subsection, this type of element representation will be used to develop the multiplication algorithm for designing bit-parallel systolic multipliers.

A. Algorithm

Since m+1 is a prime and 2 is a primitive modulo m+1, we obtain 2^{m-1}= (m+2)/2 mod (m+1). So $j2^{m-1}$ mod (m+1) is a permutation π on {0, 1, 2, …, m}, i.e.,

$$\begin{aligned} p(j) &= j\cdot 2^{m-1} \pmod{m+1} \\ &= j(m+2)/2 \pmod{m+1} \end{aligned} \tag{2}$$

According to (2), we immediately obtain the following properties.

Property 1: $2p(j) = j$

Property 2: $p(i \pm j) = p(i) + p(j)$

Property 3: $p(m+1) = 0$

Applying the Property 1-3, the element A may be re-expressed by shuffling its terms as follows

$$A=\sum_{i=0}^{m} a_{p(i)} a^{p(i)}, \tag{3}$$

Therefore, common multiplication results: in both types of multiplication is the multiply-by-$\alpha^{\pi(1)}$ operation, which can be done by the following rule, i.e., let

$$A^{(1)}=\sum_{i=0}^{m} a_{<p(i)-p(1)>} a^{p(i)} \tag{4}$$

Then,

$$\begin{aligned} A\alpha^{\pi(1)} &= a_{\pi(0)}\alpha^{\pi(0)+\pi(1)} + a_{\pi(1)}\alpha^{\pi(1)+\pi(1)} \\ &\quad + \ldots + a_{\pi(m)}\alpha^{\pi(m)+\pi(1)} \\ &= a_{\pi(m)}\alpha^{\pi(0)} + a_{\pi(0)}\alpha^{\pi(1)} + \ldots + a_{\pi(m-1)}\alpha^{\pi(m)} \\ &= a_{<\pi(0)-\pi(1)>} + a_{<\pi(1)-\pi(1)>}\alpha^{\pi(1)} + \ldots + a_{<\pi(m)-\pi(1)>}\alpha^{\pi(m)} \\ &= A^{(1)} \end{aligned} \tag{5}$$

where <x> is denoted by x modulo m+1. A straightforward multiply-by-$\alpha^{\pi(1)}$ operation is equivalent to shift-right-by-1-bit operation. From (5), we can define cyclic shift-right-by-j-bit operations, i.e.,

$$A^{(j)}=\sum_{i=0}^{m} a_{p(i-j)} a^{p(i)} \tag{6}$$

Similarly, $A^{(-j)}$ is equivalent to cyclically shifting j bit to the left, such as

$$A^{(-j)}=\sum_{i=0}^{m} a_{p(i+j)} a^{p(i)}. \tag{7}$$

Consider the coefficients of A as they relate to $A^{(j)}$ and $A^{(-j)}$, we therefore obtains

$$A = A^{(-j)}a^{p(j)} = A^{(j)}a^{p(-j)} \tag{8}$$

Definition 2: Given $A=\sum_{i=0}^{m} a_{p(i)} a^{p(i)}$ and $B=\sum_{i=0}^{m} b_{p(i)} a^{p(i)}$, the inner product of A and B, as denotes $A\Theta B$, can be defined as follows

$$A\Theta B=\sum_{i=0}^{m} a_{p(i)} b_{p(i)} a^i \tag{9}$$

Definition 3: Let two elements A and B periodically be shifted by j positions to right and left, $A^{(j)}$ and $B^{(-j)}$, respectively. Then, based on Definition 1, the j^{th} inner product, $A^{(j)}\Theta B^{(-j)}$, is defined as

$$A^{(j)}\Theta B^{(-j)}=\sum_{i=0}^{m} a_{<p(i)-p(j)>} b_{<p(i)+p(j)>} a^i \tag{10}$$

Theorem 1: Given $A=\sum_{i=0}^{m} a_{p(i)} a^{p(i)}$ and

$B=\sum_{i=0}^{m} b_{p(i)}a^{p(i)}$, the product of A and B can be represented by the following recursive formula

$$AB=\sum_{j=0}^{m} A^{(j)}\Theta B^{(-j)}$$

Proof: Let

$A= a_0 +a_1\alpha + a_2\,\alpha^2 +\ldots+a_m\,\alpha^m$
$B=b_0 +b_1\alpha + b_2\,\alpha^2 +\ldots+b_m\,\alpha^m$

Then their circular convolution can be re-expressed by

$$AB = \sum_{i=0}^{m}\sum_{j=0}^{m} a_j b_{<i-j>} a^i$$

From Property 1, we know that $i=2p(i)$, for i = 0, 1, …, m, then

$$AB = \sum_{i=0}^{m}\sum_{j=0}^{m} a_j b_{<2p(i)-j>} a^{2p(i)} \qquad (11)$$

Next, choosing j such that $j=p(i-j)$, for j = 0, 1, …, m. Therefore, AB can be re-expressed by

$$\begin{aligned} AB &= \sum_{i=0}^{m}\sum_{j=0}^{m} a_{p(i-j)} b_{p(i+j)} a^{2p(i)} \\ &= \sum_{i=0}^{m}\sum_{j=0}^{m} a_{p(i-j)} b_{p(i+j)} a^{i} \qquad (12) \\ &= \sum_{j=0}^{m} A^{(j)}\Theta \mathbf{B}^{(-j)} \end{aligned}$$

∎

Example 1: If m=4, then we obtains m+1=5 is a prime. By applying the Property 1-3, we obtains $p(i)$ for $0\le i\le 4$, such as $p(0)=0$, $p(1)=2^3\equiv 3$, $p(2)=2\cdot 2^3\equiv 1$, $p(3)=3\cdot 2^3\equiv 4$, and $p(4)=4\cdot 2^3\equiv 1$. Assume that $\{1,a,a^2,a^3,a^4\}$ is an extended basis of the field GF(2^4), thus, the basis can be transformed into $\{a^{p(0)},a^{p(1)},a^{p(2)},a^{p(3)},a^{p(4)}\}$. Let $A=a_{p(0)}a^{p(0)}+a_{p(1)}a^{p(1)}+a_{p(2)}a^{p(2)}+a_{p(3)}a^{p(3)}+a_{p(4)}a^{p(4)}$ and $B=b_{p(0)}a^{p(0)}+b_{p(1)}a^{p(1)}+b_{p(2)}a^{p(2)}+b_{p(3)}a^{p(3)}+b_{p(4)}a^{p(4)}$ be two elements of the field GF(2^4); and let $C=c_0+c_1a+c_2a^2+c_3a^3+c_4a^4$ be the product of the multiplication A and B. The product C can then be computed by using Theorem 1, as

X	$a_{p(0)}$ $b_{p(0)}$	$a_{p(1)}$ $b_{p(1)}$	$a_{p(2)}$ $b_{p(2)}$	$a_{p(3)}$ $b_{p(3)}$	$a_{p(4)}$ $b_{p(4)}$
$A\Theta B=$	$a_{p(0)}b_{p(0)}$	$a_{p(1)}b_{p(1)}$	$a_{p(2)}b_{p(2)}$	$a_{p(3)}b_{p(3)}$	$a_{p(4)}b_{p(4)}$
$A^{(1)}\Theta B^{(-1)}=$	$a_{p(4)}b_{p(1)}$	$a_{p(0)}b_{p(2)}$	$a_{p(1)}b_{p(3)}$	$a_{p(2)}b_{p(4)}$	$a_{p(3)}b_{p(0)}$
$A^{(1)}\Theta B^{(-2)}=$	$a_{p(3)}b_{p(2)}$	$a_{p(4)}b_{p(3)}$	$a_{p(0)}b_{p(4)}$	$a_{p(1)}b_{p(0)}$	$a_{p(2)}b_{p(1)}$
$A^{(2)}\Theta B^{(-3)}=$	$a_{p(2)}b_{p(3)}$	$a_{p(3)}b_{p(4)}$	$a_{p(4)}b_{p(0)}$	$a_{p(0)}b_{p(1)}$	$a_{p(1)}b_{p(2)}$
$+\ A^{(4)}\Theta B^{(-4)}=$	$a_{p(1)}b_{p(4)}$	$a_{p(2)}b_{p(0)}$	$a_{p(3)}b_{p(1)}$	$a_{p(4)}b_{p(2)}$	$a_{p(0)}b_{p(3)}$
$C=$	c_0	c_1	c_2	c_3	c_4

As stated above, the multiplication scheme is focused in the extended element to obtain AB=$\sum_{j=0}^{m} c_j a^j$, where $c_j=\sum_{i=0}^{m} a_{<p(j)-p(i)>}b_{<p(j)+p(i)>}$ (mod 2). In order to obtain completely multiplication scheme, the proposed multiplication in (12) must be to perform the reduced modulo $p(a)$ operation to obtain the desired multiplication of two elements. Therefore, let $AB=\sum_{j=0}^{m-1}\bar{c}_j a^j$ be the results of AB, the coefficients $\bar{c}_j$ can be obtained using the following relationships

$$\bar{c}_j = c_j + c_m \qquad \text{(mod 2)} \qquad (13)$$

B. Structure and comparison

We call the circuits which realize (12) and (13) as two operation units: the inner product multiplication (IPM) unit and the final reduced modulo p(α) (FRM) unit, respectively. According to Theorem 1, it is obvious that the IPM unit of Fig. 3 requires m+1 inner-product step procedures (IPSPs). The structure of each IPSP is shown in Fig. 1(a) includes m+1 basic cells. The basic cell is the realization of $c_i+a_{<\pi(i)-\pi(j)>}b_{<\pi(i)+\pi(j)>}$ mod 2, which includes one 2-input AND gate, one 2-input XOR gate and three 1-bit latches, as shown in Fig. 1(b). Fig. 2 depicts that the structure of FRM unit is operation unit of (13), which includes m 2-input XOR gate and m 1-bit latches. Fig. 3 illustrates that based on Fig. 1-2, the proposed AOP-based systolic multiplier over GF(2^4) is comprised of two parts: the IPM unit and the FRM unit.

In the IPM unit of Fig. 3, the i^{th} column cells denote the order of α^i. The j^{th} row cells is identical to the j^{th} IPSP for $A^{(j)}\Theta B^{(-j)}$ operations. Hereafter, the i^{th} cell of the j^{th} IPSP of IPM unit is denoted by the (i,j) cell. With coefficients c_i, $a_{p(i-j)}$, $b_{p(i+j)}$ enter the cell (i,j), the cell operates $c_i=c_i+a_{p(i-j)}b_{p(i+j)}$ (mod 2) computations. The basic cells consist of one 2-input AND gate, one 2-input XOR gate and three 1-bit latches. When the input data of three elements A, B, C enter the array, all coefficients are distributed over the first row cell. Fig. 3 presents that all coefficients in the j^{th} IPSP ($0\le j\le 4$) are also distributed over the j^{th} row cells. As the operations of the j^{th} IPSP, the coefficients $a_{p(i-j)}$ and $a_{p(i+j)}$ in the cell (i,j), for $0\le i\le m$, respectively propagate to the cells (i+1, j+1) and (i+1, j-1). As previously stated, neighborhood communications among cells is performed by transportation of all neighbor coefficients in the array. This instructs us to take advantage of the bit-parallel systolic architectures for the circuit design with which each IPSP only requires one clock cycle.

In the successive computations, the input data can continuously enters the array, and each IPSP only demands one clock cycle to complete the inner-product operations. From Fig. 3, the proposed AOP-based systolic multiplier comprises two parts: the IPM unit and

the FRM unit. The IPM unit consists of m+1 IPSPs, that is, the latency of the IPM unit requires m+1 clock cycles. According to Fig. 2, the FRM unit only demands one clock cycle. Therefore, the latency complexity of the proposed multiplier requires only m+2 clock cycles to compute AB for the first input data that enters the planned systolic multiplier. A possible clock period of latency requires a minimum of one 2-input AND gate and one 2-input XOR gate delays, as shown in Fig. 2(b). The total gate complexity in this circuit comprises $(m+1)^2$ 2-input AND, $(m+1)^2+m$ 2-input XOR gates and $3(m+1)^2+m$ 1-bit latches. Since the operation works every clock cycle and no cycle is wasted, the proposed architecture yields the maximum possible throughput. Therefore, this architecture is highly regular and simple in structure, and has a shorter latency to perform the element multiplication.

There are several points to be addressed. The latency of the systolic architecture for multiplications over GF(2^m) is only m+1 clock cycles while most other bit-parallel systolic multipliers, such as these in [1] and [2], require 3m. Table 1 reveals that our AOP-based multipliers require more logic circuit than the two low-complexity design but they are much simple than Wei's and Yeh's multipliers. The propagation delay of each cell is short being the total delay of one 2-input AND gate, one 2-input XOR gate and one 1-bit latch, and the multiplier generates a product in each clock cycle. The throughput is therefore very high. Finally, this architecture is highly regular, simple and with very few global connections.

III. Proposed ESP-based bit-parallel modular systolic multiplier

Definition 4[6]: A polynomial $g(x)=x^{mr}+x^{r(m-1)}+\cdots+x^r+1=p(x^r)$ over GF(2), where p(x) is an AOP of degree m, is termed r-equally spaced polynomial (r-ESP) of degree mr.

It is well known that if p(x) is an irreducible AOP of degree m over GF(2), then $g(x)=p(x^r)$ is irreducible over GF(2) iff $r=(m+1)^j \neq 1 \mod (m+1)^2$ for $j \geq 1$. An r-ESP also has an important property of $a^{r(m+1)}=1$, where α is a root of g(x). Now, let us consider the property of $a^{r(m+1)}=1$, for any element $A=\sum_{i=0}^{mr-1}\bar{a}_i a^i \in \mathrm{GF}(2^{mr})$ can be represented by

$$A=\sum_{i=0}^{(m+1)r-1} a_i a^i \tag{14}$$

where $\bar{a}_{ir+j}=a_{ir+j}+a_{mr+j}, 0\leq j\leq r-1, 0\leq i\leq m-1$ [6].

Therefore, any element $A\in GF(2^{mr})$ can might be defined as

$$A=\sum_{i=0}^{r-1} A_i a^i \tag{15}$$

where

$$A_k=\sum_{i=0}^{m} a_{ir+k} a^{ir},\ 0\leq k\leq r-1$$

Since m+1 is a prime and 2 is a primitive modulo m+1, we obtain $2^{m-1}=(m+2)/2 \mod (m+1)$. So $jr2^{m-1} \mod (m+1)r$ is a permutation σ on {0, r, 2r, …, mr}, i.e.,

$$\begin{aligned} s(j) &= jr2^{m-1} \mod (m+1)r \\ &= jr(m+2)/2 \mod (m+1) \end{aligned} \tag{16}$$

Therefore, the element A_k ($0\leq k\leq r-1$) can be re-expressed by shuffling its terms as follows

$$A_k=\sum_{i=0}^{m} a_{s(i)+k} a^{w(i)}, \tag{17}$$

With Property 1-3, hence, we concludes that $2\sigma(j)=jr$, $\sigma(i\pm j)=\sigma(i)\pm\sigma(j)$, and $\sigma(m+1)=0$. For two sub-elements $A_k=\sum_{i=0}^{m} a_{s(i)+k} a^{s(i)}$ and $B_h=\sum_{i=0}^{m} b_{s(i)+h} a^{s(i)}$ $(0\leq k,h\leq r-1)$, straightforwardly, the product of A_kB_h is based on Theorem 1 to obtain the following results

$$A_k B_h=\sum_{j=0}^{m} A_k^{(j)} \Theta B_h^{(-j)} \tag{18}$$

Theorem 2: Given two sub-element A_k and B_h($0\leq k,h\leq r-1$), then A_kB_h multiplied by α^r is equivalent to $\{A_k B_h\}^{(1)}$.

Proof: Since Theorem 2, the results of A_kB_h obtain

$$A_k B_h=\sum_{i=0}^{m} c_i a^{ir}$$

where

$$c_i=\sum_{j=0}^{m} a_{<p(i)-p(j)+k>} b_{<p(i)+p(j)+h>}$$

Therefore, A_kB_h multiplied by α^{r+q} obtains

$$\begin{aligned} \alpha^r A_k B_h &= c_0\alpha^r + c_1\alpha^{2r} + \ldots + c_m\alpha^{mr+r} \\ &= c_m + c_0\alpha^r + c_1\alpha^{2r} + \ldots + c_{m-1}\alpha^{mr} \\ &= \{A_k B_h\}^{(1)} \end{aligned} \tag{19}$$

Finally, assume that two elements $A = A_0 + A_1\alpha + A_2\alpha^2 + \ldots + A_{r-1}\alpha^{r-1}$ and $B = B_0 + B_1\alpha + B_2\alpha^2 + \ldots + B_{r-1}\alpha^{r-1} \in \mathrm{GF}(2^{mr})$, then the multiplication of A and B based on Theorem 2 and 3, can be re-expressed as

$$\begin{aligned} AB &= \sum_{i=0}^{r-1}\sum_{j=0}^{r-1} \{A_{\|(i-j)\frac{r+1}{2}\|} B_{\|(i+j)\frac{r+1}{2}\|}\}^{(w_i)} a^i \\ &= C_0 + aC_1 + \cdots + a^{r-1}C_{r-1} \end{aligned} \tag{20}$$

where

$$C_i = \sum_{j=0}^{r-1} (\{A_{\left\|(i-j)\frac{r+1}{2}\right\|} B_{\left\|(i+j)\frac{r+1}{2}\right\|}\}^{(w_i)} = c_i + c_{i+r}a^r + \cdots + c_{i+mr}a^{mr} \quad (21)$$

Note that $\|x\|$ denotes x modulo r; w_i=1 if $\left\|(i-j)\frac{r+1}{2}\right\| + \left\|(i+j)\frac{r+1}{2}\right\| \geq r$, else w_j=0. Let $AB = \sum_{i=0}^{r-1} \overline{C}_i a^i$, where $\overline{C}_i = \sum_{j=0}^{m-1} \overline{c}_{i+rj} a^{jr}$, then the coefficients between C_i and $\overline{C}_i$ have the following relations

$$\overline{c}_{i+jr} = c_{i+jr} + c_{i+mr} \quad (0 \leq j \leq m\text{-}1,\ 0 \leq i \leq r\text{-}1) \quad (22)$$

As previously stated, the proposed ESP-based systolic multiplier comprises r^2 IPM and r FRM units, in which the IPM array is for computing (19); the FRM unit is for (22). As a simple illustration, the bit-parallel systolic multiplier based on 3-ESP $x^6 + x^3 + 1$ corresponding to the irreducible AOP $x^2 + x + 1$ is shown in Fig. 4. Fig. 3 demonstrates the details of IPM and FRM circuits. In Fig. 4, the $IPM_{k,h}$ denotes the proposed that two elements A_k and B_h enter the IPM unit. According to (17) the input elements are shuffled before enter the IPM unit The computed result $C_{k+h(\mathrm{mod}r)}$ of $IPM_{k,h}$ is to propagate to the $IPM_{k-\frac{r+1}{2},h+\frac{r+1}{2}}$ unit. The coefficients of $C_{k+h(\mathrm{mod}r)}$ which is the output of $IPM_{k,h}$ unit must performs a periodic shift-rght-by-1-bit operation if h+k≥r, subjected to the relations of Theorem 2.

Generally, the proposed ESP-based multiplier over GF(2^m) which has modular systolic architecture requires $(m+r)^2$ AND gates, $(m+r)^2+m$ XOR gates, $m+r+1$ clock cycles. The proposed ESP-based systolic multiplier of larger fields can be constructed by the corresponding is based on AOP-based systolic multiplier of smaller fields. We therefore ascertain both irreducible AOP and ESP, for example of m and r, 6(3), 18(9), 20(5), 54(27), and 100(25). Table 2 presents a comparison among ESP-based bit-parallel multipliers. It is evident that our proposed ESP-based multiplier is able to design the bit-parallel systolic multiplier with modular architectures.

IV. Conclusions

This paper examined a novel systolic multiplier over finite field GF(2^m), which are generated by an irreducible AOP and ESP. An element representation is based on a field isomorphism from GF(2^m) into the residue polynomial ring modulo $x^{m+1}+1$ and $x^{mr+r}+1$, respectively. All of which are highly regular and able to realize with bit-parallel systolic architectures. The proposed AOP-based bit-parallel systolic multipliers efficiently improve the latency complexity from 3m to m+2 clock cycles. Moreover, the AOP-based systolic multipliers of smaller fields can be applied to construct all the corresponding ESP-based systolic multipliers of larger fields. From the hardware implementation pointing of view, the primary contribution of our architectures is only able to construct the bit-parallel systolic architectures.

References

[1] S. W. Wei, "A systolic power-sum circuit for GF(2^m)," IEEE trans. on computers vol. 43, no. 2, pp. 226-229, Feb. 1994.

[2] C. S. Yeh, S. Reed, and T.K. Truong, "Systolic multipliers for finite fields GF(2^m)," IEEE trans. on computers vol. C-33, pp. 357-360, Apr. 1984.

[3] C. K. Koc and B. Sunar, "Low complexity bit-parallel canonical and normal basis multipliers for a class of finite fields," IEEE trans. on computers vol. 47, no. 3, pp. 353-356, Mar. 1998.

[4] M.A. Hasan, M. Z. Wang, and V.K. Bhargava, "A modified Massey-Omura multiplier for a class of finite fields," IEEE trans. on computers vol. C-42 , No.10, pp.1278-1280, Oct. 1992.

[5] M. A. Hasan, M. Z. Wang, and V. K. Bhargava, "Modular construction of bw complexity parallel multipliers for a class of finite fields GF(2^m)," IEEE trans. on computers vol. 41, no. 8, pp. 962-971, Aug. 1992.

[6] T. Itoh and S. Tsujii, "Structure of parallel multipliers for a class of fields GF(2^m)," Info. Comp. Vol. 83, pp. 21-40, 1989.

[7] H. Wu, M. A. Hasan, and L. F. Blake, "New low-complexity bit-parallel finite field multipliers using weakly dual bases," IEEE trans. on computers vol. 47, no. 11, pp. 1223-1234, Nov. 1998.

[8] H. Wu, M. and A. Hasan, "Low-complexity bit-parallel multipliers for a class of finite fields," IEEE trans. on computers vol. 47, no. 8, pp. 883-887, Nov. 1998.

[9] W. Diffe and M. Hellman, "New directions in cryptography," IEEE trans. Inform. theory, vol. IT-22, pp. 644-654, 1976.

[10] Y. R. Shayan, Tho Le-Ngoc, and V.K. Bhargava, "Binary-decision approach to fast chien search for software decoding of BCH codes," IEE proc. Vol. I34, Pt.F, No.6, pp. 629-632, Oct. 1987.

[11] E. R. Berlekamp, Algebraic Coding Theory, revised Laguna Hills, CA: Aegean Park, 1984.

[12] D. E. R. Denning, Cryptography and data security. Reading, MA: Addison-Wesley, 1983.

[13] A. M. Odlyzko, "discrete logarithms in finite fields and their cryptographic significance, " in Adv. Cryptol. , proc. Eurocrypt '84, Paris, France, pp. 224-314, Apr. 1984.

[14] M. A. Hasan and V. K. Bhargava, "Architecture for a low complexity rate-adaptive Reed-Solomon encoder, " IEEE trans. on computers, vol. 44, no. 7, pp. 938-942, Jul. 1995.

[15] J. J. Wonziak, "Systolic dual basis serial multiplier, " IEE Proc.-Comput. Digit. Tech. Vol. 145, No. 3, pp. 237-241, May 1998.

[16] G. Drolet, "A new representation of elements of finite fields GF(2^m) yielding small complexity arithmetic," IEEE trans. on computers, vol. 47, no. 9, pp. 938-946, Sep. 1998.

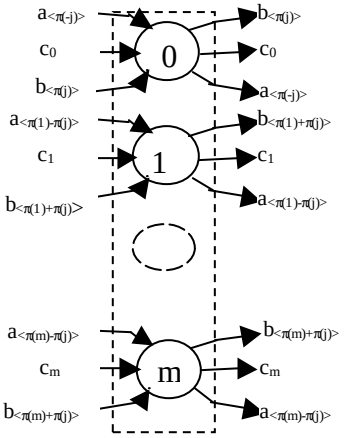
[17] J. Omura and J. Massey, "Computational method

and apparatus for finite field arithmetic," U.S. Patent Number 4587627, May 1986.

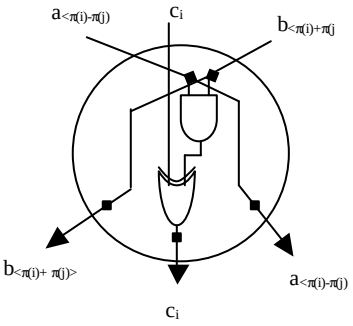
[18] M. Diab and A. Poli, "New bit-serial systolic multiplier for GF(2^m) using irreducible trinomials," Electron. Letters, vol.27, No. 13, pp. 1884-1885, Jul. 1991.

Table 1: Comparison of the related parallel systolic multipliers

Multiplier / Item	Wei [1]	Yeh [2]	Proposed AOPM (Fig. 3)
Architecture	systolic	Systolic	Bit-parallel systolic
Function	AB^2+C	AB	AB+C
The total of gates Complexity			
# 2-input AND	$3m^2$	$2\,m^2$	$(m+1)^2$
# 2-input XOR	m^2	$2\,m^2$	$(m+1)^2+m$
# 3-input XOR	m^2	0	0
# 1-bit latches	$10\,m^2$	$7\,m^2$	$3\,(m+1)^2+m$
Computation time per cell	$T_{AND}+T_{3XOR}$	$T_{AND}+T_{XOR}$	$T_{AND}+T_{XOR}$
latency	3m	3m	m +2



(a) The i^{th} IPSP



(b) The cell

Fig. 1. The circuit of the j^{th} inner product step procedures (IPSP)

Table 2: Comparison of parallel multipliers of GF(2^m) generated by an irreducible r-ESP of degree m

multipliers	architecture	basis	function	#AND	#XOR	Cycle time
ITM[6]	modular	polynomial	AB	$(m+r)^2$	$(m+r)^2-r$	$T_A+(\lceil \log_2 m \rceil+\lceil \log_2(m-r+1) \rceil)T_X$
HWBM[5]	modular	polynomial	AB	m^2	m^2+m-2r	$T_A+(m/r+\lceil \log_2 m \rceil)T_X$
WDBM[7]	modular	weakly dual	AB	m^2	m^2-r	$T_A+\{\left\lceil \log_2 \frac{m}{r} \right\rceil+\left\lceil \log_2(r+\left\lceil \frac{m-r}{2\left\lceil \log_2 \frac{m}{r} \right\rceil} \right\rceil) \right\rceil\}T_x$
Presented ESPM (Fig. 4)	Modular systolic	polynomial	AB+C	$(m+r)^2$	$(m+r)^2+m$	T_A+T_X

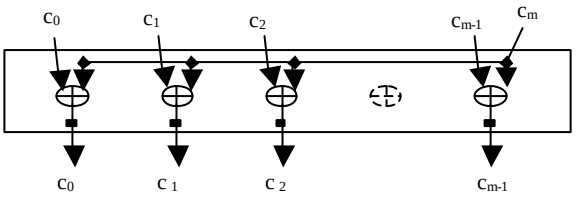


Fig. 2. The final reduced modulo p(α) (FRM) unit

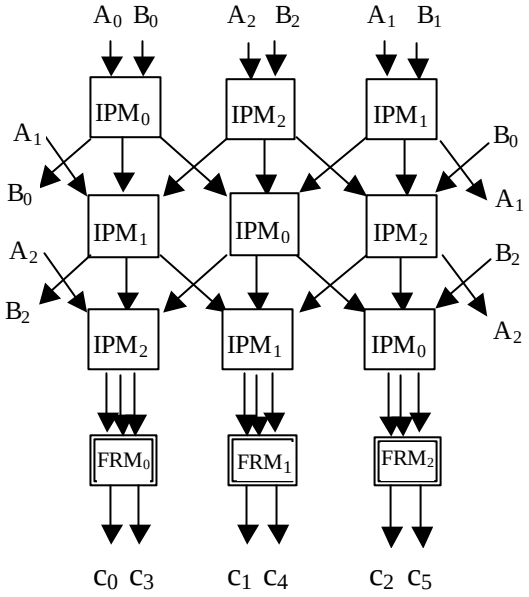
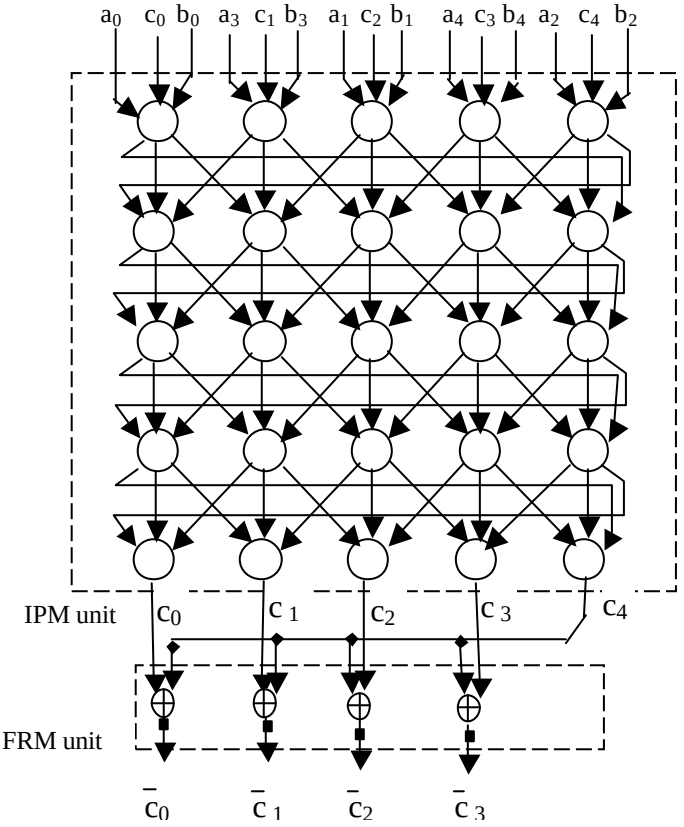


Fig. 4. The configuration of ESP-based systolic multiplier over GF(2^6)



Fig, 3. The bit-parallel systolic multiplier over GF(2^4) based on an irreducible AOP