Bit-Parallel Systolic Modular Multipliers for a Class of GF(2^m)

Chiou-Yng Lee, Erl-Huei Lu, and Jau-Yien Lee, senior member, IEEE
Dept. of electrical Engineering, Chung Gung University, Taiwan, ROC
Chiou_yng@sina.com.tw

Abstract:

In this paper, an effective algorithm for computing multiplication over a class of $GF(2^m)$ based on irreducible all one polynomials (*AOP*) and equally spaced polynomials (*ESP*) is presented. The structures are the use of two special operations, called the cyclic shifting and the inner product, to construct the low-latency bit-parallel systolic multipliers. The circuits are simple and modular which is important for hardware implementation. The *AOP*-based multiplier is composed of $(m+1)^2$ identical cells, each of which consisting of one 2-bit *AND* gate, one 2-bit *XOR* gate and three 1-bit latches. This multiplier has very low latency and propagation delay, which makes them very fast. Moreover, the *AOP*-based multiplier of small size can also be applied to construct *ESP*-based multiplier of large size, in which the elements are represented with the root of an irreducible equally spaced polynomial of degree nr. It is shown that if, for a certain degree, an irreducible *ESP* of a large degree can be obtained from a corresponding irreducible *AOP* of a very small degree. Then from the complexity point view, the structure of *ESP*-based multiplier is beneficial to construct modular architecture.

1. Introduction

Finite field arithmetic has widely received significant attention in many areas of computer science and communications, such as error control coding [1] and cryptography, [2],[3],[4], etc. The important operations in finite fields are addition, multiplication, exponentiation, division and inversion operations. The addition is very simple and can be implemented with a very simple circuit if field elements are represented in canonical form, while the other operations are much more complex. Since exponentiation, division and inversion can be performed by an iterative multiplications, this study focuses on the hardware implementation of fast and low-complexity multipliers over $GF(2^m)$.

In 1984, Yeh, Reed and Truong [5] developed a parallel-in parallel-out systolic architecture for performing the operation $AB+C$ in a general $GF(2^m)$. Since then, many bit-parallel systolic multipliers have been proposed, (see, e.g., [6], [7], and [8]). However, these multipliers are not efficient for cryptography applications due to the system complexity. Besides, the great computation delay in these systems may cause these multipliers to be unsuitable for some applications. To reduce the system complexity, Itoh and Tsujii [9] designed two low-complexity multipliers for the class of $GF(2^m)$, based on the irreducible all one polynomial (*AOP*) of degree m and the irreducible equally spaced polynomial (*ESP*) of degree nr. Notice that if, for a certain degree, an irreducible *ESP* of a large degree is corresponding to an irreducible *AOP* of a small degree. Later, Hasan, Wang and Bhargava [10] developed an *ESP*-based multiplier using small-scale *AOP*-based multipliers as the processing units. Recently, Koc and Sunor [11],[16] presented a low-complexity bit-parallel canonical basis multiplier based on an *AOP* and trinomials. This multiplier was extended to obtain a bit-parallel normal basis multiplier. Later, A. Halbutogullari and C.K. Koc [17] also proposed the Mastrovito multiplier for general irreducible polynomials. Wu et al. [12] ,[13] also adopted a weakly dual basis in their work. Drolet [14] proposed a representation based on an isomorphism from $GF(2^m)$ into the residue polynomial ring modulo x^n+1. With this representation, he drove a serial multiplier for $GF(2^m)$ and claimed that it comprises the least number of gates of all serial multipliers. Although, the above low-complexity multipliers are suitable for secure cryptosystem applications, none of them is designed with a systolic technique which permits the computation delay for multiplications over $GF(2^m)$ to be very long if the m is large.

In this paper, two special operations, called the cyclic shifting and the inner product, are defined based on the properties of irreducible *AOP* and *ESP*. With the two operations, an effective algorithm for computing multiplications over a class of $GF(2^m)$ is developed. The low-complexity bit-parallel systolic multipliers are presented based on *AOP*'s. The systolic multiplier is composed of $(m+1)^2$ identical cells, each of which consists of one 2-bit *AND* gate, one 2-bit *XOR* gate and three 1-bit latches. Since the latency of each multiplier is only $m+1$ clock cycles and the propagation delay in each cell is very short, they are very fast. This circuit can also be applied to construct the modular systolic architecture over the class of $GF(2^{nr})$, in which the elements are represented with the root of an irreducible *ESP*. This kind of new multiplier is based on an irreducible *AOP* and an irreducible *ESP*, called the *AOP*-based and the *ESP*-based multipliers in this paper.

2. Preliminaries

A polynomial of the form $P(x)=p_0+p_1x+\ldots+p_mx^m$ over $GF(2)$ is called an all one

0-7695-1150-3/01 $10.00 © 2001 IEEE

polynomial (*AOP*) of degree m if $p_i=1$ for $i=0,1,2,\ldots,m$ [9]. It has been shown that an *AOP* is irreducible if and only if $m+1$ is a prime and 2 is a primitive modulo $m+1$ [10]. For $m \le 100$, the possible m for an *AOP* of degree m to be irreducible are *2, 4, 10, 12, 18, 28, 36, 52, 58, 60, 66, 82* and *100*.

Suppose that α is a root of an irreducible *AOP* of degree m. Then any element A in the Galois field $GF(2^m)$ can be represented as $A=a_0+a_1\alpha+ a_2\alpha^2+\ldots+ a_{m-1}\alpha^{m-1}$, where the coordinates $a_i \in GF(2)$ for $0 \le i \le m-1$ and $\{1, \alpha, \alpha^2,\ldots, \alpha^{m-1}\}$ is called a canonical basis of $GF(2^m)$ [10]. The element A can also be represented as $A=A_0+A_1\alpha+ A_2\alpha^2+\ldots+A_m\alpha^m$ with $A_i+A_m=a_i$ for $0 \le i \le m-1$, where A_m and all A_i are in $GF(2)$. And the basis $\{1, \alpha, \alpha^2,\ldots, \alpha^m\}$ is called an extended basis of the canonical basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$. Thus, an element $A \in GF(2^m)$ has two different representations. For example, $A = 1+ \alpha + \alpha^3 \in GF(2^4)$, the element can be represented as $A = 1 + \alpha + \alpha^3$ by using the canonical representation or $A = \alpha^2 + \alpha^4$ by using the extended representation.

To present our multipliers, several notations and theorems are necessary.

Definition 1[15]: Let $A=A_0+A_1\alpha+A_2\alpha^2+\ldots+A_m\alpha^m$ be an element in $GF(2^m)$, which is represented with the extended basis $\{1, \alpha, \alpha^2,\ldots, \alpha^m\}$. Then $A^{(1)}(= A_m+ A_0\alpha+ A_1\alpha^2 +\ldots+ A_{m-1}\alpha^m)$ and $A^{(-1)}(= A_1+ A_2\alpha+ A_3\alpha^2 +\ldots+ A_0\alpha^m)$ denote the elements obtained by shifting A cyclically one position to the right and one position to the left, respectively. Analogously, $A^{(i)}$ and $A^{(-i)}$, where $i=0, 1, \cdots, m$, denote the elements obtained by shifting A cyclically i positions to the right and i positions to the left, respectively.

Let $P(x)=1+x+x^2+\ldots+x^m$ be an irreducible *AOP* of degree m; and let α be a root of $P(x)$, i.e., $P(\alpha)=1 +\alpha+ \alpha^2+\ldots +\alpha^m =0$. Then, we have

$$\alpha^m =1+\alpha+\alpha^2+\ldots+\alpha^{m-1}, \quad (1a)$$

$$\alpha^{m+1}=1, \quad (1b)$$

$$\ldots$$

and $$\alpha^{m+i}=\alpha^{i-1}. \quad (1c)$$

Multiplying $A=A_0+A_1\alpha+A_2\alpha^2+\ldots+A_m\alpha^m$ by α, we have $\alpha A=A_0\alpha+A_1\alpha^2+A_2\alpha^3+\ldots+A_m\alpha^{m+1}$. According to (1b), the equation becomes

$$\alpha A=A_m+A_0\alpha+A_1\alpha^2+\ldots+A_{m-1}\alpha^m. \quad (2)$$

From (2), we have Theorem 1.

Theorem 1: Let A $(=A_0+A_1\alpha+A_2\alpha^2+\ldots+A_m\alpha^m$, where α is a root of the irreducible *AOP* of degree m) be an element in $GF(2^m)$. Then, the operation of multiplying A by α can be performed by shifting A cyclically once to the right. That is

$$\alpha A=A^{(1)}. \quad (3)$$

Since $\alpha^{m+1}=1$, the multiplicative inverse of α (denoted by α^{-1}) is $\alpha^{-1} = \alpha^m$. Multiplying A by α^{-1} can be carried out by $\alpha^{-1}A =\alpha^{-1}(A_0+ A_1\alpha + A_2\alpha^2 +\ldots+ A_m\alpha^m)= A_1 + A_2\alpha + A_3\alpha^2 +\ldots+ A_0\alpha^m$. Thus, we have Theorem 2.

Theorem 2: Let A be the element given in Theorem 1. Shifting A cyclically once to the left can then be perform the operation of multiplying A by α^{-1}, denoted $A^{(-1)}$. That is

$$\alpha^{-1}A=A^{(-1)}. \quad (4)$$

Moreover, Theorem 1 and Theorem 2 can be generalized, respectively, as

$$\alpha A^{(i-1)}=A^{(i)} \quad (5)$$

and

$$\alpha^{-1}A^{(-i+1)}=A^{(-i)} \quad (6)$$

Where $A^{(i)}$ and $A^{(-i)}$ are respectively as the following forms:

$$\begin{aligned} A^{(i)} &= A_{m-i+1} + A_{m-i+2}\alpha+\cdots+A_{m-i}\alpha^m, \\ &= \sum_{j=0}^{m} A_{<j-i>}\alpha^j, \ for\ i=0,1,\ldots,m \end{aligned} \quad (7)$$

and

$$\begin{aligned} A^{(-i)} &= A_i + A_{i+1}\alpha+\cdots+A_{i-1}\alpha^m, \\ &= \sum_{j=0}^{m} A_{<j+i>}\alpha^j, \ for\ i=0,1,\ldots,m. \end{aligned} \quad (8)$$

where $<\theta>$, the subscript of $A_{<\theta>}$, denotes the least nonnegative residues of θ modulo $m+1$. Note that $A^{(0)} = A^{(-0)} = A$. On the other hand, from the equation of (1), $2^{m+1+i}=2^i$, if i is an odd number, then $m+1+i$ equals to an even number. So that any element A might be re-expressed as

$$\begin{aligned} A&=A_0+A_1\alpha+A_2\alpha^2+\ldots+A_m\alpha^m \\ &=\tilde{A}_0+\tilde{A}_1\alpha^2+\tilde{A}_2\alpha^4+\ldots+\tilde{A}_m\alpha^{2m} \end{aligned} \quad (9)$$

, where $<x>$ denotes x modulo $m+1$ and $\tilde{A}_i=A_{<2i>}$. By applying two types of element representation, an important operation, called inner product, is defined as

Definition 2: Let $A=A_0+A_1\alpha+A_2\alpha^2+\ldots+A_m\alpha^m$ and $B=B_0+B_1\alpha+B_2\alpha^2+\ldots+B_m\alpha^m= \overline{B}_0+\overline{B}_1\alpha^2+\cdots+\overline{B}_m\alpha^{2m}$ be two elements of $GF(2^m)$, where α is a root of the irreducible *AOP* of degree m and $\overline{B}_i = B_{<2i>}$. Then the inner product of A and B is defined as

$$\begin{aligned} A \bullet B &= (A_m\alpha^m)(\overline{B}_0)+(A_{m-1}\alpha^{m-1})(\overline{B}_1\alpha^2)+ \\ &\quad \cdots+(A_0)(\overline{B}_m\alpha^{2m}) \\ &= \alpha^m(A_m\overline{B}_0+A_{m-1}\overline{B}_1\alpha+\cdots+A_0\overline{B}_m\alpha^m) \\ &= \alpha^m\sum_{i=0}^{m} A_{m-i}\overline{B}_i\alpha^i \end{aligned} \quad (10)$$

By Definition 2, the inner product of $A^{(j)}$ and B is

then as

$$A^{(j)} \bullet B = \alpha^m \sum_{i=0}^{m} A_{<m-i-j>} \overline{B}_i \alpha^i \qquad (11)$$

For $j = 0$, the inner product $A^{(0)}$ and B is the same as the inner product of A and B, that is, $A^{(0)} \bullet B = A \bullet B$.

With the above preliminaries, the principle of the algorithm for computing multiplication over $GF(2^m)$, based on an irreducible AOP, is introduced in Section 3.

3. Algorithm

Let α be a root of the irreducible AOP of degree m over $GF(2)$. Suppose that $A = A_0 + A_1\alpha + A_2\alpha^2 + \ldots + A_m\alpha^m$ and $B = \overline{B}_0 + \overline{B}_1\alpha^2 + \cdots + \overline{B}_m\alpha^{2m}$ are two elements in the field $GF(2^m)$, where both A and B are represented with the extended basis $\{1, \alpha, \alpha^2, \ldots, \alpha^m\}$ and $\{1, \alpha^2, \alpha^4, \ldots, \alpha^{2m}\}$, respectively.

Theorem 3: Assume that $A = A_0 + A_1\alpha + A_2\alpha^2 + \ldots + A_m\alpha^m$ and $B = \overline{B}_0 + \overline{B}_1\alpha^2 + \cdots + \overline{B}_m\alpha^{2m}$ are two elements in $GF(2^m)$, where α is a root of the irreducible AOP of degree m. Then the operation of computing the multiplication of A and B over $GF(2^m)$ can be carried out using

$$\begin{aligned} AB &= (A^{(m)} \bullet B)^{(-m)} + (A^{(m-1)} \bullet B)^{(-m+1)} + \\ &\quad \ldots + (A^{(0)} \bullet B)^{(-0)} \\ &= (\ldots((A^{(m)} \bullet B)^{(-1)} + (A^{(m-1)} \bullet B)^{(-1)} + \\ &\quad \ldots)^{(-1)} + (A^{(0)} \bullet B) \end{aligned} \qquad (12)$$

Proof: Assume that $A = A_0 + A_1\alpha + A_2\alpha^2 + \ldots + A_m\alpha^m$ and $B = B_0 + B_1\alpha + B_2\alpha^2 + \ldots + B_m\alpha^m$ are two elements. Thus, let us consider the case of $B = \sum_{i=0}^{m-1} \overline{B}_i \alpha^{2i}$ where $\overline{B}_i = B_{<2i>}$ $(0 \le i \le m)$. Generally, AB can be obtained by

$$AB = \sum_{i=0}^{m} \sum_{j=0}^{m} A_i \overline{B}_j \alpha^{i+2j} \qquad (13)$$

Since the arithmetic reduction operation, $\alpha^{i+2j} \bmod(\alpha^{m+1}+1), 0 \le i,j \le m$, it is easily to show that $1 \le \alpha^{i+2j} \bmod(\alpha^{m+1}+1) \le \alpha^m$. Thus, let us define $j' = j$ and $i' = \langle i+2j \rangle$, where $0 \le i', j' \le m$, ones obtain $i = \langle i'-2j' \rangle$. Substituting i,j into (13), we obtains

$$AB = \sum_{i'=0}^{m} \sum_{j'=0}^{m} A_{<i'-2j'>} \overline{B}_{j'} \alpha^{i'} \qquad (14)$$

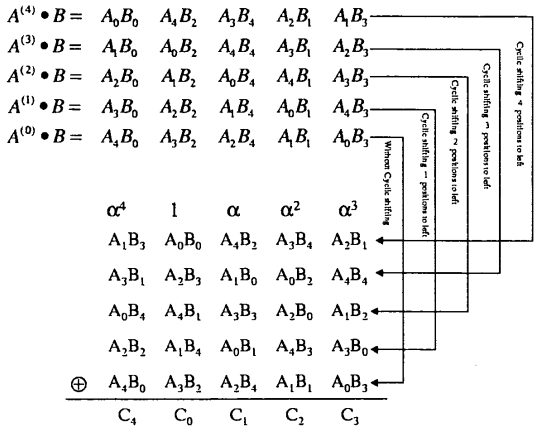
By taking $p = \langle i'-j' \rangle$ and $j' = j$ into (14), then

$$\begin{aligned} AB &= \sum_{p=0}^{m} \sum_{j=0}^{m} A_{<p-j>} \overline{B}_j \alpha^{p+j} \\ &= \sum_{p=0}^{m} \alpha^p \sum_{j=0}^{m} A_{<p-j>} \overline{B}_j \alpha^j \\ &= \sum_{j=0}^{m} A_{<-j>} \overline{B}_j \alpha^j + \alpha \sum_{j=0}^{m} A_{<1-j>} \overline{B}_j \alpha^j \\ &\quad + \cdots + \alpha^m \sum_{j=0}^{m} A_{<m-1-j>} \overline{B}_j \alpha^j \end{aligned}$$

According to (11), we obtains

$$\begin{aligned} AB &= \alpha^{-m}(A^{(m)} \bullet B) + \alpha^{-m+1}(A^{(m-1)} \bullet B) + \ldots + (A^{(0)} \bullet B) \\ &= (A^{(m)} \bullet B)^{(-m)} + (A^{(m-1)} \bullet B)^{(-m+1)} + \ldots + (A^{(0)} \bullet B)^{(-0)} \\ &= (\ldots((A^{(m)} \bullet B)^{(-1)} + (A^{(m-1)} \bullet B)^{(-1)} + \ldots)^{(-1)} + (A^{(0)} \bullet B) \quad \blacksquare \end{aligned}$$

Example 1: By employing the properties of $\alpha^{m+1+i} = \alpha^i \bmod(\alpha^{m+1}+1)$ for $m=4$, we obtains $\alpha^5(=1), \alpha^6(=\alpha), \alpha^7(=\alpha^2), \alpha^8(=\alpha^3)$. Assume that the two integer numbers, A and B, is given by $A = A_0 + A_1\alpha + A_2\alpha^2 + A_3\alpha^3 + A_4\alpha^4$ and $B = B_0 + B_1\alpha + B_2\alpha^2 + B_3\alpha^3 + B_4\alpha^4 = B_0 + B_2\alpha^2 + B_4\alpha^4 + B_1\alpha^6 + B_3\alpha^8$. According to (12), the following is shown that the product of AB.



where $\oplus$ denotes the operations of a multiplication and an addition over $GF(2)$. In Example 1, the proposed AOP-based multiplication, AB, is clearly to see that the structure requires the inner product operations of $m+1$ times. Before two elements A and B enter the first inner product operation scheme, in which two elements, B and A, are permuted by the form of (9) and $A^{(m)}$, respectively. After each of the inner product operation, the coefficients of A must be cyclically shifted to the right to propagate the next inner product operation. Moreover, the accumulated sum is cyclically shifted to the left to propagate next inner product. As above inner product proceeding, the result of multiplication for the $m+1^{th}$ inner product operation is shown in the form of Example 1. From the equation (12) can be

recursively computed as follows:

$$C_{-1}=0 \tag{15a}$$
$$C_i = C_{j-1}^{(-1)} + A^{(m-i)} \bullet B \tag{15b}$$
$$AB=C_m \tag{15c}$$

4. AOP-Based Multipliers

In this section, the parallel-in parallel-out systolic architecture for computing multiplication over the field $GF(2^m)$ in which the elements is presented with the root of an irreducible *AOP* are presented, as shown in Fig. 1. The multiplier is divided into two modular units: the inner product multiplication (*IPM*) unit and the reduced final modulo (*RFM*) unit. The *IPM* is based on Theorem 3 to approach the new bit-parallel systolic architecture. The *RFM* is to perform the reduced final modulo $P(x)$ operations as shown in Fig. 1, i.e., let $C=C_0+ C_1\alpha+ C_2\alpha^2+ \ldots+C_m\alpha^m$ and $C=c_0+c_1\alpha+c_2\alpha^2+\ldots+c_{m-1}\alpha^{m-1}$ be the final result of he multiplication A and B and the final output of the *IPM* unit, respectively. Then their relationships are $c_i=C_i+C_m$, for $0\le i\le m-1$.

Two types of extended basis $\{1, \alpha, \alpha^2, \ldots, \alpha^m\}$and $\{1, \alpha^2, \alpha^4,\ldots, \alpha^{2m}\}$ are corresponding to the two elements A and B to enter the array, respectively. According to the iterative procedure of (15), the coefficients of A, B, and C at first cycle enter the *IPM* systolic array as shown in Fig. 2. Each cell (denoted by U-cell) employs one 2-input *AND* gate and one 2-input *XOR* gate to realize the equation $C_i^{(j)} = C_{i+1}^{(j-1)} + A_{i-1}^{(j-1)} B_i'^{(j-1)}$, as shown in Fig.3. The three 1-bit latches in each cell are used to delay each output of the cell one clock cycle. From (10), it is clear to see that each inner product operation is only accomplished by one cycle, because of all coefficients are located in different order degree. For each of inner product operation, all coefficients are also located in different order degree. So that the latency of the *IPM*, based on (12), only requires $m+1$ clock cycles to complete the product of A and B. Therefore, the structure of the *IPM* for performing the above computing procedure is shown in Fig.1. The multiplier is composed of $(m+1)^2$ U-cells and m 2-input *XOR* gates.

There are several points to be addressed. The latency of the systolic architecture for multiplication over $GF(2^m)$ is only $m+1$ clock cycles while most other bit-parallel systolic multipliers, such as these in [5] and [6], require $3m$. 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.

5. ESP-Based Multipliers

The new multiplication algorithm based on an irreducible *AOP* is discussed in the section 3-4. Due to irreducible *ESP* of large degree nr can be readily obtained from a corresponding irreducible *AOP* of a small degree n. For irreducible *ESP's*, many of algorithms and hardware implementations have founded in the literatures. Moreover, Hasan et al. in 1992 is proposed that the *AOP*-based multipliers of a small degree can be to construct the *ESP*-based multipliers of high degree with the modular architectures. Therefore, it is important that irreducible *ESP*'s are of practical implementations. In this section, we present the *ESP*-based systolic multiplier that is the use of *AOP*-based systolic multiplier to construct the modular systolic architecture as well as low circuit complexity.

A polynomial of the form $g(x)=1+x^r+x^{2r}+\ldots+x^{nr}$ is called a r-equally spaced polynomial (*r-ESP*) of degree nr. Let $g(x) = p(x^r)$. Then $p(x)$ is an *AOP* of degree n. It has been shown that if $p(x)$ is an irreducible *AOP*, the *r-ESP* $g(x)$ needs to be irreducible if and only if $r =(n+1)^j \neq 1 \bmod (n+1)^2$, for $j\ge 1$ [9]. For $nr\le 100$, the possible pairs (nr, r) for an *r-ESP* of degree nr to be irreducible are *(6,3), (18,9), (20,5), (54,27)* and *(100,25)*. Now suppose that α is a root of the irreducible *r-ESP* of degree nr. Then an element A in the Galois field $GF(2^{nr})$ can be represented as $A= \hat{a}_0+ \hat{a}_1\alpha+ \hat{a}_2\alpha^2+\ldots+ \hat{a}_{nr-1}\alpha^{nr-1}$ by using the canonical basis $\{1,\alpha,\alpha^2,\ldots, \alpha^{nr-1}\}$, where $\hat{a}_i\in GF(2)$ for $0\le i\le nr-1$. The element A can also be represented by using the extended basis of $\{1, \alpha,\alpha^2,\ldots, \alpha^{(n+1)r-1}\}$, as

$$A = a_0 + a_1\alpha + \cdots + a_{nr-1}\alpha^{nr-1} = \sum_{i=0}^{(n+1)r-1} a_i\alpha^i \tag{16}$$

where $a_{ir+j}+a_{nr+j}=\hat{a}_{ir+j}$, for $0\le j\le r-1$ and $0\le i\le n-1$ [9] ◦

Example 2: Assume that α is a root of the *r-ESP* $g(x)=1+ x^3+ x^6$ (i.e., $g(x)$ is an irreducible *ESP* of $nr=6$ and $r=3$). Then $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$ is a canonical basis of the Galois field $GF(2^6)$ and $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8\}$ can be used as an extended basis of the canonical basis. Thus, an element in $GF(2^6)$ can be represented as $A = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4 + a_5\alpha^5 + a_6\alpha^6 + a_7\alpha^7 + a_8\alpha^8$ by using the extended basis.

Since α is a root of the irreducible *r-ESP* $g(x)=1+x^r+x^{2r}+\ldots+x^{nr}$, we have $1+\alpha^r+\alpha^{2r}+\ldots+\alpha^{nr}=0$. Thus,

$$\alpha^{nr}=1+\alpha^r+\ldots+\alpha^{(n-1)r} \tag{17a}$$
$$\alpha^{(n+1)r}=1 \tag{17b}$$
$$\alpha^{(n+1)r+i}=\alpha^i, \text{ for } i=1,2,\ldots,(n+1)r-2 \tag{17c}$$

Since $n+1$ is a prime and 2 is a primitive modulo 2, $\alpha^{(n+1)r}=1$, let any element $A \in GF(2^{nr})$ might be defined as

$$A=\sum_{k=0}^{r-1} A_k \alpha^k \tag{18a}$$

where

$$A_k=\sum_{i=0}^{n} a_{ir+k}\alpha^{ir} \tag{18b}$$

If we split the right side of the equation (18b) into two terms with i = *even* and i = *odd*, respectively; we have

$$A_k=\sum_{\substack{i=0\\ even}}^{n} a_{ir+k}\alpha^{ir}+\sum_{\substack{i=1\\ odd}}^{n} a_{ir+k}\alpha^{ir} \tag{19}$$

Note that the possible n must be even for an irreducible *ESP* of degree nr. Substituting $\alpha^i=\alpha^{n+1+i}$ into the second term on the right side of (19), the equation becomes

$$\begin{aligned} A_k &= \sum_{i=0}^{\frac{n}{2}} a_{\|2ir+k\|}\alpha^{2ir}+\sum_{i=\frac{n}{2}+1}^{n} a_{\|2ir+k\|}\alpha^{2ir} \\ &= \sum_{i=0}^{n} \bar{a}_{ir+k}\alpha^{2ir} \end{aligned} \tag{20}$$

where $\|x\|$ denotes x modulo $(n+1)r$ and $\bar{a}_{ir+k}=a_{\|2ir+k\|}$. Moreover, according to Theorem 1 and Theorem 2 can be generalized, respectively, as

$$\alpha^{jr}A_k^{(j-1)}=A_k^{(j)} \tag{21}$$

and

$$\alpha^{-jr}A_k^{(-j+1)}=A_k^{(-j)} \tag{22}$$

where $A_k^{(j)}$ and $A_k^{(-j)}$ are respectively as the following forms:

$$\begin{aligned} A_k^{(j)} &= a_{(n-j+1)r+k}+a_{(n-j+2)r+k}\alpha^r+ \\ &\quad \cdots+a_{(n-j)r+k}\alpha^{nr} \\ &= \sum_{i=0}^{n} a_{\|(i-j)r+k\|}\alpha^{ir} \end{aligned} \tag{23}$$

and

$$\begin{aligned} A_k^{(-j)} &= a_{jr+k}+A_{(j+1)r+k}\alpha^r+ \\ &\quad \cdots+a_{(j-1)r+k}\alpha^{nr}, \\ &= \sum_{i=0}^{m} a_{\|(j+i)r+k\|}\alpha^{i} \end{aligned} \tag{24}$$

According to (18b) and (20), two sub-elements are given by $A_k=\sum_{i=0}^{n} a_{ir+k}\alpha^{ir}$ and $B_h=\sum_{i=0}^{n} \bar{b}_{ir+h}\alpha^{2ir}$ $(0\le k,h \le r-1)$, respectively. Thus, the inner product of $A_k^{(j)}$ and B_h, denoted as $A_k^{(j)} \bullet \mathbf{B}_h$, is based on Definition 2 to obtain the following results

$$A_k^{(j)} \bullet B_h = \alpha^{nr}\sum_{i=0}^{n} a_{\|(n-i-j)r+k\|}\bar{b}_{ir+h}\alpha^{ir}$$

Similarly, the product of A_k and B_h, according to Theorem 3, can be obtained the following results

$$\begin{aligned} A_kB_h &= (A_k^{(n)} \bullet B_h)^{(-n)}+(A_k^{(n)} \bullet B_h)^{(-n+1)} \\ &\quad +\cdots+(A_k^{(0)} \bullet B_h)^{(0)} \\ &= (\cdots((A_k^{(n)} \bullet B_h)^{(-1)}+A_k^{(n-1)} \bullet B_h)^{(-1)} \\ &\quad +\cdots)^{(-1)}+A_k^{(0)} \bullet B_h \end{aligned} \tag{25}$$

Theorem 4: Given two sub-element A_k and B_h $(0\le k,h \le r-1)$, then A_kB_h multiplied by α^r is equivalent to $\{A_kB_h\}^{(1)}$.

Proof: Since Theorem 2, the results of A_kB_h obtain

$$A_kB_h=\alpha^{nr}\sum_{i=0}^{n} c_i\alpha^{ir}$$

where

$$c_i=\sum_{j=0}^{n} a_{\|(i-j)r+k\|}b_{\|(i+j)r+h\|}$$

Therefore, A_kB_h multiplied by α^r obtains

$$\begin{aligned} \alpha^r A_kB_h &= \alpha^{nr}(c_0\alpha^r+c_1\alpha^{2r}+\ldots+c_n\alpha^{nr+r}) \\ &= \alpha^{nr}(c_n+c_0\alpha^r+c_1\alpha^{2r}+\ldots+c_{n-1}\alpha^{nr}) \\ &= \{A_kB_h\}^{(1)} \end{aligned} \tag{26}$$ ■

As stated above, the multiplication algorithm for two sub-elements is verified. Now, we will be combined with the multiplication algorithm of two sub-elements to construct modular systolic architecture. Assume that two elements $A = A_0 + A_1\alpha + A_2\alpha^2 + \ldots + A_{r-1}\alpha^{r-1}$ and $B = B_0 + B_1\alpha + B_2\alpha^2 + \ldots + B_{r-1}\alpha^{r-1} \in GF(2^{mr})$, then the multiplication of A and B, based on (26), can be re-expressed as

$$\begin{aligned} AB &= \sum_{i=0}^{r-1}\sum_{j=0}^{r-1}\{A_{\langle i-j\rangle}B_j\}^{(w_j)}\alpha^i \\ &= C_0+\alpha C_1+\cdots+\alpha^{r-1}C_{r-1} \end{aligned} \tag{27}$$

where

$$\begin{aligned} C_i &= \sum_{j=0}^{r-1}(\{A_{\langle\langle i-j\rangle\rangle}B_j\}^{(w_j)} \\ &= c_i+c_{i+r}\alpha^r+\cdots+c_{i+nr}\alpha^{nr} \end{aligned} \tag{28}$$

Note that $\langle\langle x\rangle\rangle$ denotes x modulo r; $w_j=1$ if $\langle\langle i-j\rangle\rangle+j\ge r$, else $w_j=0$. From $r=(n+1)^j \ne 1 \bmod (n+1)^2$, for $j\ge 1$, it turns out that r exists on an odd number. For $2^{r-2}\equiv(r+1)/2 \pmod r$ [15], if $\pi(i)=i2^{r-2}$

$=i(r+1)/2 \pmod r$, then we obtain

$$2\pi(i)=i \quad (29a)$$
$$\pi(i)\pm\pi(i)=\pi(i\pm j) \quad (29b)$$
$$\pi(r)=0 \quad (29c)$$

Therefore, by taking $i = 2\pi(i)$ and $j = \pi(i)+\pi(j)$, the equation (27) can be to become as follows

$$AB=\sum_{i=0}^{r-1}\sum_{j=0}^{r-1}\{A_{\langle\langle i-j\rangle\rangle}B_j\}^{(w_i)}\alpha^i$$
$$=\sum_{i=0}^{r-1}\sum_{j=0}^{r-1}\{A_{\pi(i-j)}B_{\pi(i+j)}\}^{(w_i)}\alpha^i$$

In order to deal with the final reduced operations, let $AB=\sum_{i=0}^{r-1}\overline{C}_i\alpha^i$ be the final result of the multiplication, AB, where $\overline{C}_i=\sum_{j=0}^{n-1}\overline{c}_{i+qj}\alpha^{jr}$, then the coefficients between C_i and $\overline{C}_i$ have the following relations

$$\overline{c}_{i+jr}=c_{i+jr}+c_{i+nr} \quad (0\le j\le n-1,\ 0\le i\le r-1) \quad (30)$$

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 (25); the *FRM* unit is for (30). 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. 2 and 1 demonstrate the details of *IPM* and *FRM* circuits. In Fig. 4, the $IPM_{\pi(k),\pi(h)}$ denotes the proposed that two elements $A_{\pi(k)}$ and $B_{\pi(h)}$ enter the *IPM* unit. According to (26) the input elements are shuffled before enter the *IPM* unit. The computed result $C_{\pi(k+h)}$ of $IPM_{\pi(k),\pi(h)}$ is to propagate to the $IPM_{\pi(k-1),\pi(h+1)}$ unit. The coefficients of $C_{\pi(k+h)}$ which is the output of $IPM_{\pi(k),\pi(h)}$ unit must performs a periodic shift-rght-by-1-bit operation if $\pi(k)+\pi(h)\ge r$, subjected to the relations of Theorem 4.

Generally, the proposed ESP-based multiplier over $GF(2^{nr})$ which has modular systolic architecture requires $(nr+r)^2$ *AND* gates, $(nr+r)^2+nr$ *XOR* gates, $nr+r$ clock cycles. The proposed *ESP*-based systolic multiplier of a large fields can be constructed by the corresponding is based on AOP-based systolic multiplier of a small fields.

6. Comparisons and Discussions

The parallel systolic *AOP*-based and *ESP*-based multipliers for $GF(2^m)$ have been presented in this paper. The proposed *ESP*-based systolic multiplier of a large degree can be constructed by the corresponding is based on *AOP*-based systolic multiplier of a small degree. This kind of multiplier has high throughput due to the low propagation delay in each cell. Moreover, the latency of *AOP*-based multiplier in the former kind is only $m+1$ clock cycles for computing a multiplication in $GF(2^m)$. The latency in the *ESP*-based multiplier requires $(n+1)r$ clock cycles for computing a multiplication in $GF(2^{nr})$.

We therefore compare our multipliers with the parallel systolic multipliers of a general $GF(2^m)$ from [5],[6]. Table 1 reveals that our *AOP*-based multiplier requires less logic circuit than the two bit-parallel systolic multipliers but they are much simple than Wei's and Yeh's multipliers. The latency of each of ours multipliers is less than any parallel-in parallel-out systolic multiplier of $GF(2^m)$. For consecutive computation, the proposed multipliers has shorter latency than the other designs. In this contribution, it is efficiently desgins that the ESP-based systolic multiplier is beneficial to construct modular systolic architecture by using the AOP-based systolic multiplier.

References

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

[2] D. E. R. Denning, Cryptography and Data Security. Reading, MA: Addison-Wesley, 1983.

[3] 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.

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

[5] 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.

[6] 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.

[7] C. L. Wang, "Bit-level Systolic Array for Fast Exponentiation in GF(2^m)," IEEE Trans. on Computers vol. 43, no. 7, pp. 838-841, Jul. 1994.

[8] J. J. Wonziak, "Systolic Dual Basis Serial Multiplier, " IEE Proc.-Comput. Digit. Tech. Vol. 145, No. 3, pp. 237-241, May 1998.

[9] 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.

[10] M. A. Hasan, M. Z. Wang, and V. K. Bhargava, "Modular Construction of Low 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.

[11] 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.

[12]H. Wu, and M. 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.

[13]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.

[14] 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.

[15]C. Y. Lee, E. H. Lu, and L. F. Sun, "The Design of a Low-Complexity Systolic Architecture for Fast Bit-Parallel Exponentiation in a Class of GF(2^m)," Proc. 16th IFIP Word Computer Congress Int. Conf. on Signal Processing, WCC-ICSP2000, Beijing, China.

[16]B. Sinar and C.K. Koc, "Mastrovito multiplier for all trinomials," IEEE Trans. on Computers, vol. 48, no. 5, pp. 522-527, May. 1999.

[17]A. Halbutogullari and C.K. Koc, "Mastrovito multiplier for general irreducible polynomials," IEEE Trans. on Computers, vol. 49, no. 5, pp. 503-518, May. 2000.

Table 1: Comparison of the related parallel multipliers over GF(2^m)

Multiplier / iterms	Yeh [5]	Wei[6]	Proposed AOP-based multiplier	Proposed ESP-based multiplier
# of total gates				
2-input AND	$2m^2$	$3m^2$	$(m+1)^2$	$(m+r)^2$
2-input XOR	$2m^2$	$2m^2$	m^2+3m+1	$(m+r)^2+3(m+r)$
3-input XOR	0	m^2	0	0
1-bit latches	$7m^2$	$10m^2$	$4(m+1)^2$	$4(m+1)^2$
Maxmum possible clock period	$T_A+T_X+2T_L$	$T_A+T_{X3}+2T_L$	$T_A+T_X+T_L$	$T_A+T_X+T_L$
Minimum latency	5m	3m	m+1	m+r

Note: T_A= the propagation delay of one 2-input AND gate
T_X= the propagation delay of one 2-input XOR gate
T_{3X}= the propagation delay of one 3-input XOR gate
T_L= the propagation delay of one latch

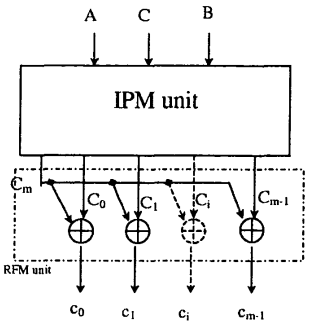


Fig. 1. The bit-parallel systolic architecture for multiplication over GF(2^m) based on AOP

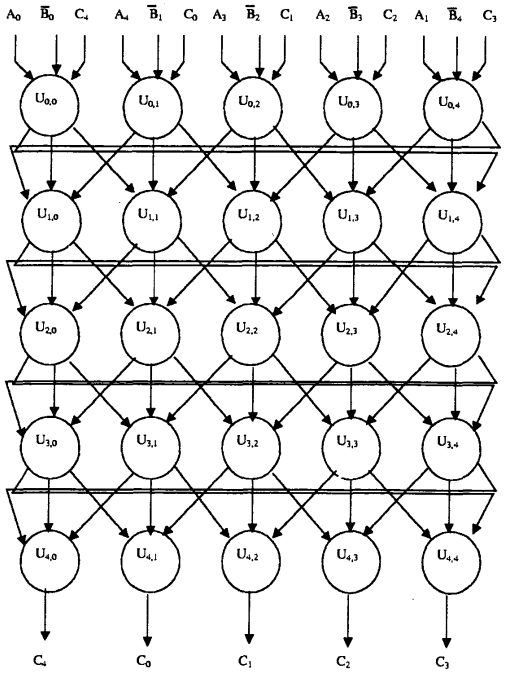
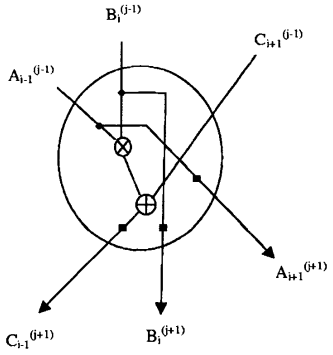


Fig. 2. The bit-parallel systolic architecture for the IPM unit over GF(2^4)



⊕ denotes the operations of an addition over GF(2)

⊗ denotes the operations of a multiplication over

Fig. 3. The detailed circuit of $U_{(i,j)}$-cell

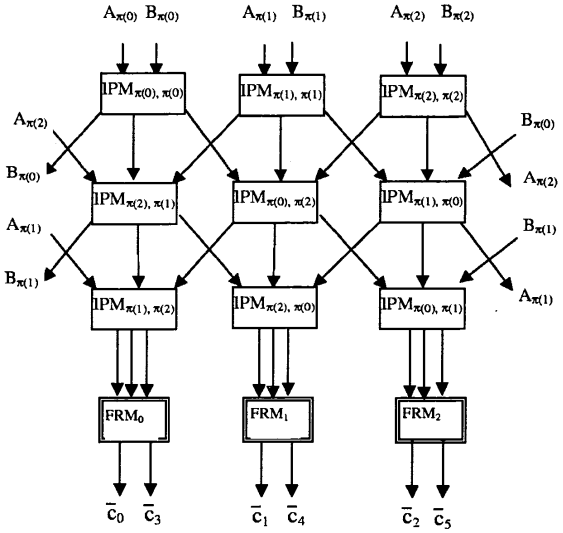


Fig. 4. The configuration of ESP-based systolic multiplier over GF(2^6)