On Low Complexity Bit Parallel Polynomial Basis Multipliers

Arash Reyhani-Masoleh and M. Anwar Hasan

Centre for Applied Cryptographic Research,
University of Waterloo, Waterloo, Ontario, Canada N2L 3G1.
{areyhani, ahasan}@uwaterloo.ca

Abstract. Representing finite field elements with respect to the polynomial (or standard) basis, we consider a bit parallel multiplier architecture for the finite field $GF(2^m)$. Time and space complexities of such a multiplier heavily depend on the field defining irreducible polynomials. Based on a number of important classes of irreducible polynomials, we give exact complexity analyses of the multiplier gate count and time delay. In general, our results match or outperform the previously known best results in similar classes. We also present exact formulations for the coordinates of the multiplier output. Such formulations are expected to be useful to efficiently implement the multiplier using hardware description languages, such as VHDL and Verilog, without having much knowledge of finite field arithmetic.

Keywords: Finite or Galois field, Mastrovito multiplier, pentanomial, polynomial basis, trinomial and equally-spaced polynomial.

1 Introduction

With the rapid expansion of the Internet and wireless communications, more and more digital systems are becoming increasingly equipped with some form of cryptosystems to provide various kinds of data security. Many such cryptosystems rely on computations in very large finite fields and require fast computations in the fields [5,1]. Among the basic arithmetic operations over finite field $GF(2^m)$, addition is easily realized using m two-input XOR gates while multiplication is costly in terms of gate count and time delay.

In the past, many bit parallel multipliers were proposed (see for example [3, 9,2,11,6,10]). In [4,3], Mastrovito proposed an algorithm along with its hardware architecture for polynomial (PB) basis multiplication. In his scheme, first a binary matrix is formed which is then multiplied with a binary vector to obtain the required result. Halbutogullari and Koc have given a method for constructing the Mastrovito multiplier for arbitrary irreducible polynomials [2]. This method considers general as well as special classes of irreducible polynomials such as *trinomials, all-one polynomials* (AOPs) and *equally-spaced polynomials* (ESPs). So far, for these special polynomials, the XOR gate count and time delay of the Halbutogullari-Koc algorithm appear to be the lowest. In [11], Zhang and

C.D. Walter et al. (Eds.): CHES 2003, LNCS 2779, pp. 189–202, 2003.

Parhi give a systematic method to design the Mastrovito multiplier. Moreover, in [11], the method is extended to design the modified Mastrovito multiplication scheme proposed in [8]. They also present new results on the complexities of the Mastrovito multiplier for two classes of irreducible *pentanomials*. Recently, Rodriguez-Henriquez and Koc in [7] have proposed a PB multiplier for special case of pentanomials and have given its time and gate complexities.

In this article, first we review the multiplication scheme and its bit-parallel architecture presented in [6]. Then, using the *reduction* matrix $\mathbf{Q}$, the complexities of the multiplier based on a number of irreducible polynomials are obtained. We also present explicit formulations for the output coordinates of the multiplier in terms of its inputs. Such formulations can be directly coded using VHDL or Verilog languages to implement an efficient multiplier by someone who is not that familiar with finite field arithmetic. It is shown that for general irreducible polynomials, the space and time complexities of the proposed structure are lower than those available in the literature in terms of combined gate count and time delay. Furthermore, this architecture has fewer signals to be routed which is advantageous for VLSI implementation.

2 Polynomial Basis Multiplications over $GF(2^m)$

Let $P(x) = x^m + \sum_{i=0}^{m-1} p_i x^i$ be a monic irreducible polynomial over $GF(2)$ of degree m, where $p_i \in GF(2)$ for $i = 0, 1, \cdots, m-1$. Let $\alpha \in GF(2^m)$ be a root of $P(x)$, *i.e.*, $P(\alpha) = 0$. Then the set $\{1, \alpha, \alpha^2, \cdots, \alpha^{m-1}\}$ is referred to as the polynomial or standard basis and each element of $GF(2^m)$ can be written with respect to (w.r.t.) the polynomial basis (PB). Let A be an element in $GF(2^m)$, then the representation of A w.r.t. the PB is $A = \sum_{i=0}^{m-1} a_i \alpha^i$, $a_i \in \{0, 1\}$, where a_i's are the coordinates. For convenience, these coordinates will be denoted in vector notation[1] as $\mathbf{a} = [\, a_0, a_1, a_2, \cdots, a_{m-1}\,]^T$, where T denotes the transposition. Using this vector notation, the representation of A can be written as $A = \boldsymbol{\alpha}^T \mathbf{a}$, where $\boldsymbol{\alpha} = [1, \alpha, \alpha^2, \cdots, \alpha^{m-1}]^T$. Let S be the binary polynomial of degree not more than $2m-2$ obtained by the direct multiplication of the PB representations of any two elements A and B of $GF(2^m)$, i.e.,

$$S = \left(\sum_{i=0}^{m-1} a_i \alpha^i\right) \cdot \left(\sum_{j=0}^{m-1} b_j \alpha^j\right) = \sum_{k=0}^{m-1} d_k \alpha^k + \sum_{k=0}^{m-2} e_k \alpha^{m+k}, \tag{1}$$

where

$$\mathbf{d} = [d_0, d_1, \cdots, d_{m-1}\,]^T = \mathbf{L}\mathbf{b}, \tag{2}$$

$$\mathbf{e} = [e_0, e_1, \cdots, e_{m-1}\,]^T = \mathbf{U}\mathbf{b}, \tag{3}$$

[1] In this paper, vectors and matrices are shown with small and capital bold faces, respectively.

$$\mathbf{L} \triangleq \begin{bmatrix} a_0 & 0 & 0 & 0 & \cdots & 0 \\ a_1 & a_0 & 0 & 0 & \cdots & 0 \\ a_2 & a_1 & a_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ a_{m-2} & a_{m-3} & \cdots & a_1 & a_0 & 0 \\ a_{m-1} & a_{m-2} & \cdots & a_2 & a_1 & a_0 \end{bmatrix}, \quad \mathbf{U} \triangleq \begin{bmatrix} 0 & a_{m-1} & a_{m-2} & \cdots & a_2 & a_1 \\ 0 & 0 & a_{m-1} & \cdots & a_3 & a_2 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & a_{m-1} & a_{m-2} \\ 0 & 0 & \cdots & 0 & 0 & a_{m-1} \end{bmatrix}. \tag{4}$$

Then, the product $C = A \cdot B$ can be obtained by the following modulo reduction.

$$C \triangleq \sum_{i=0}^{m-1} c_i \alpha^i \equiv S \mod P(\alpha). \tag{5}$$

Definition 1. *[3] The* reduction matrix $\mathbf{Q}$ *is an* $m-1$ *by* m *binary matrix which is obtained from*

$$\boldsymbol{\alpha}^{\uparrow} \equiv \mathbf{Q}\boldsymbol{\alpha} \pmod{P(\alpha)}, \tag{6}$$

where $\boldsymbol{\alpha}^{\uparrow} = [\alpha^m, \alpha^{m+1}, \cdots, \alpha^{2m-2}]^T$.

Theorem 1. *[6] Let* C *be the product of* A *and* $B \in GF(2^m)$*. Then,*

$$\mathbf{c} = [c_0, c_1, \cdots, c_{m-1}]^T = \mathbf{d} + \mathbf{Q}^T\mathbf{e}, \tag{7}$$

where $\mathbf{d}$*,* $\mathbf{e}$ *and* $\mathbf{Q}$ *are defined in (2), (3), and (6) respectively.*

The corresponding architecture for polynomial basis multiplication over $GF(2^m)$ is shown in Figure1. This structure is divided into two parts: IP-network and $\mathbf{Q}$-network. The IP-network has m blocks (denoted as $I_0, I_1, \cdots, I_{m-1}$) which generates vectors $\mathbf{d}$ and $\mathbf{e}$ in accordance with (2) and (3), using m^2 AND gates and $(m-1)^2$ XOR gates. Using (2) and (3), the delay for d_j, $0 \le j \le m-1$, and e_i, $0 \le i \le m-2$, can be calculated from

$$T(d_j) = T_A + \lceil \log_2(j+1) \rceil T_X, \qquad 0 \le j \le m-1, \tag{8}$$

$$T(e_i) = T_A + \lceil \log_2(m-i-1) \rceil T_X, \qquad 0 \le i \le m-2. \tag{9}$$

In Figure 1, the $\mathbf{Q}$-network takes $\mathbf{d}$ and $\mathbf{e}$ as inputs and generates $\mathbf{c}$. It is noted that the number of lines on the interconnection bus IB is fixed and is equal to the number of e_j's, i.e., $m-1$. In Figure 1, there are three buses, A, B and IB, and the number of lines on the buses is $3m-1$.

In the following sections, we attempt to minimise the number of XOR gates of the $\mathbf{Q}$-network for special irreducible polynomials, namely equally-spaced polynomials, trinomials, and pentanomials. We start with equally-spaced polynomials which are very structured and will help us present the remaining special cases with less difficulties.

3 Multipliers Using Equally-Spaced Polynomials

Definition 2. *A polynomial* $P(x) = x^{ns} + x^{(n-1)s} + \cdots + x^s + 1$*, over* $GF(2)$*, with* $ns = m$ *and* $1 \le s \le \lfloor \frac{m}{2} \rfloor$*, is called an equally-spaced polynomial (denoted as s-ESP) of degree* m*.*

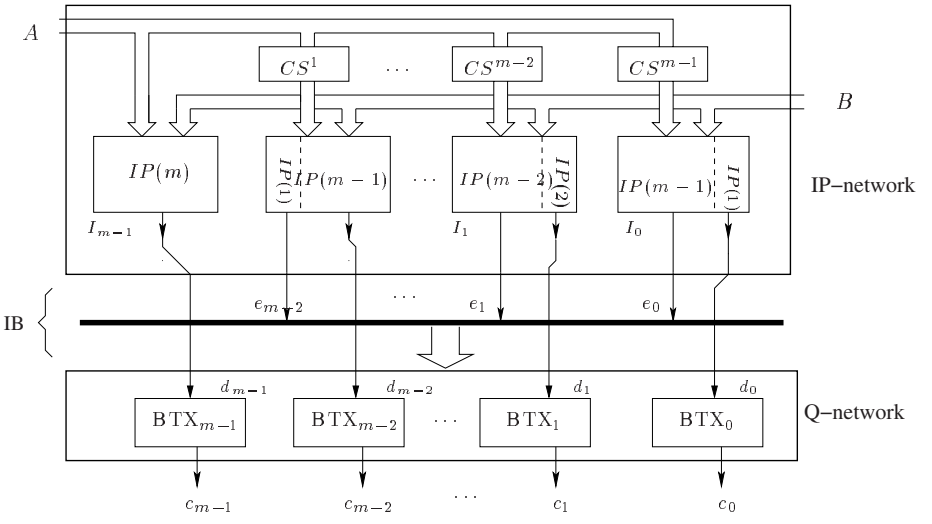

Fig. 1. Architecture of the multiplier over $GF(2^m)$, where CS^i represents an i- fold cyclic shift.

When $s = 1$, we have 1-ESP which is the same as the all-one polynomial (AOP) which has the highest Hamming weight among all polynomials of degree m. On the other hand, $s = \lfloor \frac{m}{2} \rfloor$ results in the least Hamming weight irreducible polynomial (i.e., trinomial) of degree m. It is easy to check that for an equally spaced trinomial m is even and $s = \frac{m}{2}$.

Theorem 2. *For an s-ESP based multiplier over $GF(2^m)$, the number of AND gates (N_A), the number of XOR gates (N_X) and time delay (T_C) are $N_A = m^2$, $N_X = m^2 - s$, and $T_C = T_A + (1 + \lceil \log_2 m \rceil) T_X$, respectively.*

Proof. When α is a root of the s-ESP of degree m as defined above, we have

$$\alpha^{m+i} = \begin{cases} \alpha^i + \alpha^{s+i} + \cdots + \alpha^{(n-1)s+i}, & 0 \le i < s, \\ \alpha^{i-s}, & s \le i \le m-2. \end{cases} \tag{10}$$

Using (10), the reduction matrix $\mathbf{Q}$ is obtained as

$$\mathbf{Q} = \begin{bmatrix} \mathbf{I_s}\ \mathbf{I_s} \cdots \mathbf{I_s} \\ \mathbf{I_{m-s-1}}\ \mathbf{0_{s+1}} \end{bmatrix}, \tag{11}$$

where $\mathbf{I_j}$ is the $j \times j$ unity matrix and $\mathbf{0_{s+1}}$ is a zero matrix which has $m-s-1$ rows and $s+1$ columns. The graphical representations of $\mathbf{Q}$ in (11) for different values of s are shown in Figure 2. In this figure, non-zero entries of $\mathbf{Q}$ are shown with the small squares.

In order to obtain exact expressions for N_X and T_C, first we obtain the coordinates of C. To this end, from Theorem 1 and (11), one can write

$$c_j = d'_j + e_{j \bmod s}, \quad 0 \le j \le m-1, \tag{12}$$

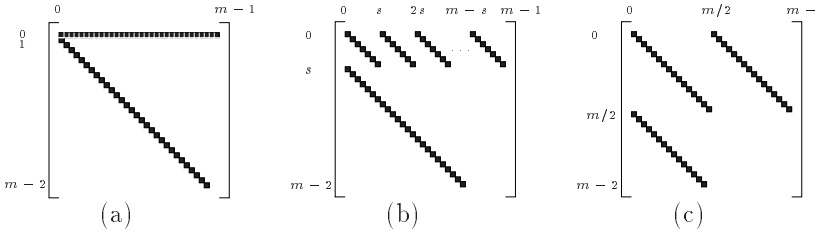

Fig. 2. Graphical representations of the locations of non-zeros entries of $\mathbf{Q}$ for s-ESP $P(x) = x^{ns} + x^{(n-1)s} + \cdots + x^s + 1$, $m = ns$. (a) $s = 1$ (AOP), (b) $1 < s < \frac{m}{2}$, (c) $s = \frac{m}{2}$ (trinomial).

where

$$d'_j = \begin{cases} d_j + e_{j+s} & 0 \le j \le m-s-2, \\ d_j & m-s-1 \le j \le m-1. \end{cases} \tag{13}$$

Thus, using (12) and (13), the exact XOR gate count for an s-ESP based multiplier is $N_X = m^2 - s$. Also, by using (8) and (9), d'_j of (13) can be generated with a maximum gate delay of $T_A + (1 + \lceil \log_2 m \rceil) T_X$.

It is worth mentioning that the resultant number of signal lines on IB reduces from $m-1$ to s, which is considerably lower than the s-ESP based Mastrovito multiplier which has $\frac{m(m-s)}{2s} + m$ signal lines [4]. Thus, the total number of lines on the buses of the multiplier is $2m + s$.

4 Extension to More Generic Polynomials

Here we consider irreducible polynomials of the form $P(x) = x^m + x^{k_t} + \cdots + x^{k_2} + x^{k_1} + 1$, where $1 \le k_1 < k_2 < \cdots < k_t \le \frac{m}{2}$. The Hamming weight of $P(x)$ is $t+2$ and the degree of the second leading term is less than or equal to $\frac{m}{2}$. All five binary fields recommended by NIST for ECDSA can be constructed by such irreducible polynomials.

In order to apply the general formulation stated in Section 2 to these polynomials, first we obtain the corresponding $\mathbf{Q}$ matrix. Note that all the rows of the $\mathbf{Q}$ matrix are the PB representations of α^{m+i}, $0 \le i \le m-2$, where α is a root of $P(x)$. Since $P(\alpha) = 0$, then $\alpha^m = 1 + \alpha^{k_1} + \alpha^{k_2} + \cdots + \alpha^{k_t}$. Thus, the 0-th row, i.e., $i = 0$, has only ones in these $t+1$ columns of $\mathbf{Q}$: 0, k_1, k_2, $\cdots$, k_t. The consecutive rows of this matrix can be obtained by using a linear feedback shift register (LFSR). As a result, the rows with $i = 0$ to $m - k_t - 1$ of $\mathbf{Q}$ have $t+1$ ones.

The $\mathbf{Q}$ matrix for $t = 1$ and $t = 3$ (i.e., trinomials and pentanomials, respectively) are shown in Figure 3. As shown in this figure, row i, $0 \le i \le m - k_t - 1$ of $\mathbf{Q}$ has $t+1$ ones corresponding to the $t+1$ segmented lines. When the last column of $\mathbf{Q}$ contains one which takes place in row $i = m - k_j - 1$, $j = t, \cdots, 2, 1$, the next row originates new $t+1$ lines in columns: 0, k_1, k_2, up to k_t provided

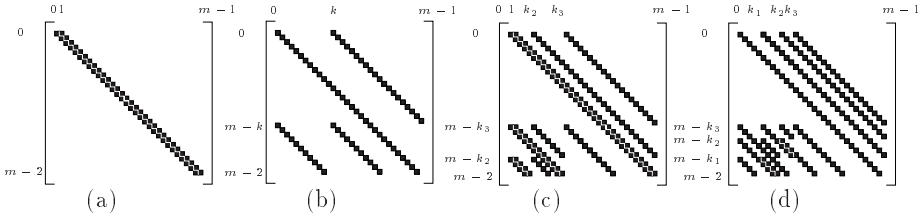

Fig. 3. Graphical representations of the reduction matrix $\mathbf{Q}$ for trinomials: (a) $k = k_1 = 1$ (b) $1 < k < \frac{m}{2}$ (see Figure 2(c) for $k_1 = \frac{m}{2}$); and for pentanomials: (c) $k_1 = 1$ (d) $1 < k_1 \leq \frac{m}{2}$.

that there is no previous lines that pass these columns. If there exists a previous line that passes the column k_j, $1 \leq j \leq t$, then the previous line terminates in column $k_j - 1$ and no new line originates from column k_j due to XORing of two lines. This happens in row $\frac{m}{2}$ and column $\frac{m}{2}$ in Figure 2(c) for trinomials when $k_1 = \frac{m}{2}$. This is also the case for pentanomials where $t = 3$ and it is shown in Figures 3(c) and 3(d) for $k_1 = 1$ and $1 < k_1 \leq \frac{m}{2}$, respectively.

We divide the lines of $\mathbf{Q}$ into $t + 1$ sets (see Figure 4 for $t = 3$) such that $\mathbf{Q} = \mathbf{Q}_0 + \mathbf{Q}_1 + \mathbf{Q}_2 + \cdots + \mathbf{Q}_t$ where non-zero entries of $\mathbf{Q}_i$, $0 \leq i \leq t$ start from the column k_i (assume that $k_0 = 0$). It is noted that the last non-zero entry of sub-matrix $\mathbf{Q}_i$, $1 \leq i \leq t$ is in column $m-1$, whereas the one in $\mathbf{Q}_0$ is in column $m-2$. Moreover, the number of ones in each column of $\mathbf{Q}_i$, $0 \leq i \leq t$ is at most $t + 1$ if $k_1 > 1$, and t if $k_1 = 1$.

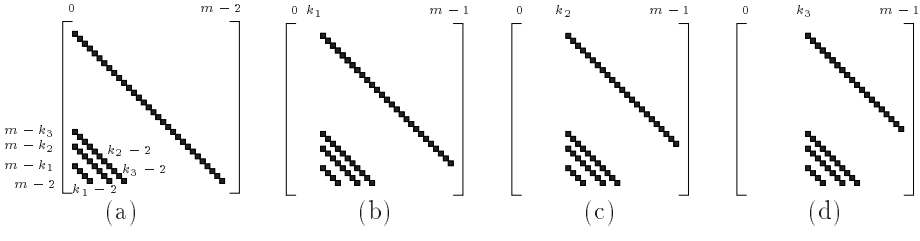

Fig. 4. Graphical representations of submatrices of $\mathbf{Q} = \mathbf{Q}_0 + \mathbf{Q}_1 + \mathbf{Q}_2 + \mathbf{Q}_3$ for pentanomials $P(x) = x^m + x^{k_3} + x^{k_2} + x^{k_1} + 1$, where $1 < k_1 < k_2 < k_3 \leq \frac{m}{2}$, (see Figure 3(d) for $\mathbf{Q}$). (a) $\mathbf{Q}_0$, (b) $\mathbf{Q}_1$, (c) $\mathbf{Q}_2$, (d) $\mathbf{Q}_3$.

Theorem 3. *The number of XOR gates and the time delay of the multiplier based on the irreducible polynomial* $P(x) = x^m + x^{k_t} + \cdots + x^{k_2} + x^{k_1} + 1$, $1 \leq k_1 < k_2 < \cdots < k_t \leq \frac{m}{2}$ *are*

$$N_X = (m + t)(m - 1)$$

and

$$T_C = T_A + \left(\lceil \log_2(t+1) \rceil + \left\lceil \log_2(\left\lceil \frac{t}{2} \right\rceil + 1) \right\rceil + \lceil \log_2(m-1) \rceil \right) T_X.$$

Proof. Let us denote $\mathbf{e}^{(i)} = [e_0^{(i)}, e_1^{(i)}, \cdots, e_{m-1}^{(i)}]^T = \mathbf{Q}_i^T \mathbf{e}$, $0 \le i \le t$, then using Theorem 1, we can obtain the coordinates of the pentanomial based multiplication as

$$\mathbf{c} = \mathbf{d} + \mathbf{e}^{(0)} + \mathbf{e}^{(1)} + \mathbf{e}^{(2)} + \cdots + \mathbf{e}^{(t)}. \tag{14}$$

First, let us assume $k_1 \neq 1$. Using $\mathbf{Q}_0$ (see Figure 4(a) for $t = 3$), the elements of $\mathbf{e}^{(0)}$ are as follows:

$$e_j^{(0)} = \begin{cases} e_j + e_{j+m-k_t} + \cdots + e_{j+m-k_2} + e_{j+m-k_1}, & \text{if } 0 \le j \le k_1 - 2 \\ e_j + e_{j+m-k_t} + \cdots + e_{j+m-k_2} & \text{if } k_1 - 1 \le j \le k_2 - 2 \\ \vdots & \vdots \\ e_j + e_{j+m-k_t} & \text{if } k_{t-1} - 1 \le j \le k_t - 2 \\ e_j & \text{if } k_t - 1 \le j \le m - 2 \\ 0 & \text{if } j = m - 1. \end{cases} \tag{15}$$

The total number of XOR gates to form $e_j^{(0)}$'s, $0 \le j \le k_t - 2$, is $N_1 = t(k_1 - 1) + (t-1)(k_2 - k_1) + \cdots + k_t - k_{t-1} = \sum_{i=1}^{t} k_i - t$. Let $T(e_j^{(0)})$ denote the time delay due to gates to find $e_j^{(0)}$. As seen in (15), the longest path delay is to obtain $e_0^{(0)} = e_0 + e_{m-k_t} + \cdots + e_{m-k_2} + e_{m-k_1}$, i.e., $T(e_j^{(0)}) \le T(e_0^{(0)})$. In order to reduce this delay, we first add any two terms except c_0, e.g., $e_{m-k_j} + e_{m-k_i}$, $1 \le i, j \le t$, $i \neq j$. Then add these $\lceil \frac{t}{2} \rceil$ signals to c_0 using a binary tree of XOR gates. Since $T(e_j) = T_A + \lceil \log_2(m - j - 1) \rceil T_X$, then $T(e_{m-k_j} + e_{m-k_i}) \le T_X + T(e_{m-k_t}) = T_A + (1 + \lceil \log_2(k_t - 1) \rceil) T_X \le T_A + \lceil \log_2(m-1) \rceil T_X$, where the last inequality is due to $k_t \le \frac{m}{2}$. Thus, we have

$$T(e_j^{(0)}) \le \begin{cases} T_A + \left(\left\lceil \log_2(\lceil \frac{t}{2} \rceil + 1) \right\rceil + \lceil \log_2(m-1) \rceil \right) T_X, & \text{if } 0 \le j \le k_t - 2 \\ T_A + \lceil \log_2(m-1) \rceil T_X & \text{if } k_t - 1 \le j \le m - 2. \end{cases} \tag{16}$$

By reusing the signals of $e_j^{(0)}$'s, the coordinates of $\mathbf{e}^{(i)}$, for $1 \le i \le t$, can be obtained as

$$e_j^{(i)} = \begin{cases} 0, & if\ 0 \le j \le k_i - 1 \\ e_{j-k_i}^{(0)} & \text{otherwise.} \end{cases} \tag{17}$$

This results in the coordinates of $C = AB$ as

$$c_j = d_j + \begin{cases} e_j^{(0)} & \text{if } 0 \le j \le k_1 - 1 \\ e_j^{(0)} + e_j^{(1)} & \text{if } k_1 \le j \le k_2 - 1 \\ \vdots & \vdots \\ e_j^{(0)} + e_j^{(1)} + \cdots + e_j^{(t-1)} & \text{if } k_{t-1} \le j \le k_t - 1 \\ e_j^{(0)} + e_j^{(1)} + \cdots + e_j^{(t)} & \text{if } k_t \le j \le m - 2 \\ e_j^{(1)} + e_j^{(2)} + \cdots + e_j^{(t)} & \text{if } j = m - 1 \end{cases} \tag{18}$$

by using (14). To realize (18) in hardware, one requires $N_2 = m + (k_2 - k_1) + 2(k_3 - k_2) + \cdots + (t-1)(k_t - k_{t-1}) + t(m - k_3 - 1) + t - 1 = (t+1)m - \sum_{i=1}^{t} k_i - 1$ XOR gates. Thus, the total XOR gates needed for the multiplier is $(m-1)^2 + N_1 + N_2 = (m+t)(m-1)$.

To obtain the time delay of the proposed multiplier, we use a binary tree for each coordinate in (18). For $j \notin [k_t, m-2]$, it is seen in (18) that $T_C \leq \lceil \log_2(t+1) \rceil T_X + T(e_0^{(0)})$ and the proof is complete by using (16). Now, we need only to obtain the time delay of $c_j's$ for $k_t \leq j \leq m-2$. For $j \in [k_t, m-2]$, if we form $c_j = (d_j + e_j^{(0)}) + e_j^{(1)} + e_j^{(2)} + \cdots + e_j^{(t)}$ such that $d_j + e_j^{(0)}$ is calculated first, then

$$\begin{aligned} T(d_j + e_j^{(0)}) &\leq T_A + (1 + \lceil \log_2(m-1) \rceil) T_X \\ &\leq T_A + \left(\left\lceil \log_2 \left(\left\lceil \frac{t}{2} \right\rceil + 1 \right) \right\rceil + \lceil \log_2(m-1) \rceil \right) T_X. \end{aligned}$$

Also, using (17) and (16), one can see

$$T(e_j^{(t)}) \leq T_A + \left(\left\lceil \log_2 \left(\left\lceil \frac{t}{2} \right\rceil + 1 \right) \right\rceil + \lceil \log_2(m-1) \rceil \right) T_X$$

which implies that

$$T_C \leq T_A + \left(\lceil \log_2(t+1) \rceil + \left\lceil \log_2 \left(\left\lceil \frac{t}{2} \right\rceil + 1 \right) \right\rceil + \lceil \log_2(m-1) \rceil \right) T_X$$

and the proof is complete.

In addition to the three buses shown in Figure 1 now, there will be another bus in the middle of the **Q**-network for signals $e_j^{(0)}$ for $0 \leq j \leq k_t - 2$. Thus, the total number of lines on the buses is $3m + k_t - 2$.

Corollary 1. *For $k_1 = 1$ and $t > 1$, the time delay would reduce to*

$$T_A + \left(\lceil \log_2(t+1) \rceil + \left\lceil \log_2 \left\lceil \frac{t}{2} \right\rceil \right\rceil + \lceil \log_2(m-1) \rceil \right) T_X.$$

Based on the above results, one can obtain the time delay and the number of XOR gates for the trinomial based multiplier by substituting $t = 1$ in Theorem 3, for $k_1 \neq \frac{m}{2}$ and $s = \frac{m}{2}$ in Theorem 2 for $k_1 = \frac{m}{2}$. Note that the results for $k_1 = \frac{m}{2}$ are obtained using the implementation of the $\frac{m}{2}$-ESP based multiplier.

5 Special Classes of Pentanomials

A polynomial with five non-zero coefficients, i.e., $P(x) = x^m + x^{k_3} + x^{k_2} + x^{k_1} + 1$, where $1 \leq k_1 < k_2 < k_3 \leq m-1$, is called a *pentanomial* of degree m. The non-zero constant term is due to the irreducibility properly needed to define the field. In terms of the values of k_is, the pentanomials can be divided into a number of different classes. Below we consider two special classes of irreducible pentanomials as proposed in [11].

5.1 Class 1: $k_3 \leq \frac{m}{2}$

For this class of irreducible pentanomial where $k_3 \leq \frac{m}{2}$, one can apply $t = 3$ to the complexity results we have presented in Section 4. This yields the following.

Corollary 2. *The gate counts and time delay of the multiplier for the the pentanomial* $P(x) = x^m + x^{k_3} + x^{k_2} + x^{k_1} + 1$, *where* $1 \leq k_1 < k_2 < k_3 \leq \frac{m}{2}$, *are*

$$\begin{aligned} N_A &= m^2, \\ N_X &= m^2 + 2m - 3, \\ T_C &= \begin{cases} T_A + (3 + \lceil \log_2(m-1) \rceil)\, T_X, \text{ if } k_1 = 1 \\ T_A + (4 + \lceil \log_2(m-1) \rceil)\, T_X, \text{ otherwise,} \end{cases} \end{aligned}$$

and the number of lines on the buses is $3m + k_3 - 2$.

The number of XOR gates can be reduced if we choose a pentanomial such that $k_1 = k_3 - k_2$. Towards this, let us introduce the following set of new signals

$$e'_j = e_{j+m-k_3} + e_{j+m-k_2},\ 0 \leq j \leq k_2 - 2. \tag{19}$$

Equation (19) can be used to generate $e_j^{(0)}$, $0 \leq j \leq k_2 - 2$, by substituting $t = 3$ in (15) as follows

$$e_j^{(0)} = \begin{cases} e_j + e'_j + e_{j+m-k_1}, & \text{if } 0 \leq j \leq k_1 - 2 \\ e_j + e'_j & \text{if } k_1 - 1 \leq j \leq k_2 - 2 \\ e_j + e_{j+m-k_3} & \text{if } k_2 - 1 \leq j \leq k_3 - 2 \\ e_j & \text{if } k_3 - 1 \leq j \leq m - 2 \\ 0 & \text{if } j = m - 1. \end{cases} \tag{20}$$

The total number of XOR gates needed to generate $e_j^{(0)}$'s (see (20)) is $N_1 = k_1 + k_2 + k_3 - 3$ where $k_2 - 1$ of which is due to (19). Also, the maximum delay due to gates in (20) is

$$T(e_j^{(0)}) \leq \begin{cases} T_A + (2 + \lceil \log_2(m-1) \rceil)\, T_X & \text{if } 0 \leq j \leq k_1 - 2 \\ T_A + (1 + \lceil \log_2(m-1) \rceil)\, T_X & \text{if } k_1 - 1 \leq j \leq k_3 - 2 \\ T_A + \lceil \log_2(m-1) \rceil\, T_X & \text{if } k_3 - 1 \leq j \leq m - 1. \end{cases} \tag{21}$$

Lemma 1. *With symbols defined as above, one has*

$$\begin{aligned} e_j^{(0)} + e_j^{(1)} &= e'_{j+k_2-m}, \text{ for } m - k_2 \leq j \leq m - 2, \\ e_j^{(2)} + e_j^{(3)} &= e_{j-k_2}^{(0)} + e_{j-k_2}^{(1)}, \text{ for } k_3 \leq j \leq m - 1. \end{aligned}$$

Let us represent $e_j^{(01)}$, $0 \leq j \leq m - 1$, as the elements of $(\mathbf{Q}_0 + \mathbf{Q}_1)^T \mathbf{e}$, where $\mathbf{Q}_0$ and $\mathbf{Q}_1$ are shown in Figure 4(a) and Figure 4(b), respectively. Then, substituting $t = 3$ in the general case given in (18) and using the above lemma, we can obtain the coordinates of $C = AB$ as follows:

$$c_j = d_j + e_j^{(01)} + e_{j-k_2}^{(01)},\ 0 \leq j \leq m - 1, \tag{22}$$

where $e_{j-k_2}^{(01)} = 0$ for $j < k_2$, and

$$e_j^{(01)} = \begin{cases} e_j^{(0)} & \text{if } 0 \le j \le k_1 - 1 \\ e_j^{(0)} + e_j^{(1)} & \text{if } k_1 \le j \le m - k_2 - 1 \\ e'_{j+k_2-m} & \text{if } m - k_2 \le j \le m - 2 \\ e_j^{(1)} & \text{if } j = m - 1. \end{cases} \tag{23}$$

As seen in (23), one has to realize $e_j^{(0)} + e_j^{(1)}$ for all $k_1 \le j \le m - k_2 - 1$ which requires $m - k_2 - k_1$ XOR gates. Once $e_j^{(01)}$'s are obtained, then equation (22) requires $2m-k_2$ XOR gates. Thus, the total number of XOR gates needed for the multiplier is $(m-1)^2+N_1+m-k_2-k_1+2m-k_2 = m^2+m+k_1-2$. Due to the reuse of terms e'_j, $0 \le j \le k_2 - 1$, and $e_j^{(0)} + e_j^{(1)}$, $k_1 \le j \le m - k_2 - 1$, additional lines needed on the bus in the **Q**-network are $(k_2 - 1)$ and $(m - k_1 - k_2)$, respectively. Thus, the total number of lines on the buses is increased to $4m + k_2 - 3$.

To obtain the time delay of the proposed multiplier, we use Table 1 which shows the maximum delay of the used signals in (22) for the given ranges of j in each row. In this figure i, $0 \le i \le 4$, represents the time delay of $T_A + (i + \lceil \log_2(m-1) \rceil) T_X$, and the numbers inside brackets are for $k_1 = 1$. Also, x determines either $e_j^{(01)}$ or $e_{j-k_2}^{(01)}$ to be added with d_j first to obtain c_j. In each row of this table, the delays are obtained for the first digit of the given range. This is because as j increases, the time delays of the used signals in each row of this table decreases. As seen in this table, the maximum delay of the multiplier is $T_A + (4 + \lceil \log_2(m-1) \rceil) T_X$. For $k_1 = 1$, only one signal, i.e., c_{k_3}, has the delay of $T_A + (4 + \lceil \log_2(m-1) \rceil) T_X$. One can reduce this delay to $T_A + (3 + \lceil \log_2(m-1) \rceil) T_X$ if only c_{k_3} is realized as $c_{k_3} = ((d_{k_3} + e_j^{(0)}) + e_j^{(1)}) + e_{k_3-k_2}^{(01)}$ by using one extra XOR gate.

Table 1. Maximum time delays of the signals, where i, $0 \le i \le 4$, represents the time delay of $T_A + (i + \lceil \log_2(m-1) \rceil) T_X$, numbers inside brackets are for $k_1 = 1$, and x determines either $e_j^{(01)}$ or $e_{j-k_2}^{(01)}$ to be added first with d_j.

j	$e_j^{(0)}$	$e_j^{(1)}$	$e_j^{(01)}$	$e_{j-k_2}^{(01)}$	$d_j + x$	c_j
$0 \le j \le k_1 - 1$	2(1)	-	$2(1), x$	-	3	3
$k_1 \le j \le k_2 - 1$	1	2(1)	$3(2), x$	-	4(3)	4(3)
$k_2 \le j \le k_3 - 1$	1	2(1)	3(2)	$2(1), x$	3(2)	4(3)
$k_3 \le j \le k_3 + k_1 - 1$	0	1	$2, x$	3(2)	3	4
$k_3 + k_1 \le j \le m - k_2 - 1$	0	0	$1, x$	3(2)	2	4(3)
$m - k_2 \le j \le m - 1$	0	0	$1, x$	3(2)	2	4(3)
$j = m - 1$	-	0	$1, x$	1	2	3

Based on the above results, we can state the following.

Theorem 4. *The gate counts and time delay of the multiplier based on the pentanomial* $P(x) = x^m + x^{k_3} + x^{k_2} + x^{k_1} + 1$, *where* $1 \le k_1 < k_2 < k_3 \le \frac{m}{2}$, *and* $k_3 - k_2 = k_1$ *are*

$$N_A = m^2,$$

$$N_X = \begin{cases} m^2 + m & \text{if } k_1 = 1 \\ m^2 + m + k_1 - 2 & \text{otherwise,} \end{cases}$$

$$T_C = \begin{cases} T_A + (3 + \lceil \log_2(m-1) \rceil)\, T_X, & \text{if } k_1 = 1 \\ T_A + (4 + \lceil \log_2(m-1) \rceil)\, T_X, & \text{otherwise,} \end{cases}$$

and the number of lines on the buses is $4m + k_2 - 3$.

Remark 1. To verify that class 1 irreducible pentanomials exist, we have used a Maple$^{\text{TM}}$ program for $m \in [160, 600]$ and have found that at least one irreducible pentanomial exists for each m in the range of 160 to 600. This is of interest to elliptic curve cryptosystem designers. In order to minimise the number of XOR gates of the multiplier, we have obtained irreducible pentanomials such that k_1 is minimum. We have also observed that, k_1 is less than or equal six for all m in the above mentioned range.

It is noted that the pentanomial presented in [7] is a special case when $k_1 = 1$.

5.2 Class 2: $m - k_3 = k_3 - k_2 = k_2 - k_1 = s$, $\frac{m-1}{8} \le s \le \frac{m-1}{3}$

We refer to polynomials $P(x) = x^m + x^{k_3} + x^{k_2} + x^{k_1} + 1$, where $1 \le k_1 < k_2 < k_3 \le m - 1$, and $m - k_3 = k_3 - k_2 = k_2 - k_1 = s$ as class 2 type. Similar to the other special irreducible polynomials, here we first obtain the corresponding reduction matrix. Then the coordinates and complexities of the multiplier can be obtained. Based on the values of s (or $k_1 = m - 3s$), we can divide the reduction matrix into different forms. Because of lack of space, only three of them are presented here. These $\mathbf{Q}$ matrices for $\frac{m-1}{8} \le s \le \frac{m-1}{3}$ (or $1 \le k_1 \le 5s + 1$) are shown in Figure 5. Based on this figure, we can state the following theorem.

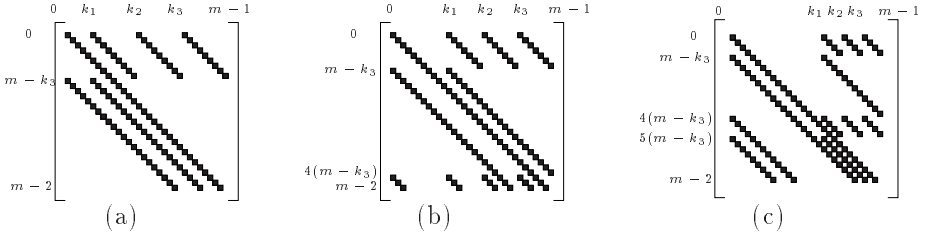

Fig. 5. Graphical representations of the reduction matrix $\mathbf{Q}$ for class 2 pentanomials $P(x) = x^m + x^{k_3} + x^{k_2} + x^{k_1} + 1$, where $m - k_3 = k_3 - k_2 = k_2 - k_1 = s$. (a) $\frac{m-1}{4} \le s \le \frac{m-1}{3}$ or $1 \le k_1 \le s + 1$ (see Figure 2(a) for $k_1 = s$), (b) $\frac{m-1}{5} \le s < \frac{m-1}{4}$ or $s + 1 < k_1 \le 2s + 1$, (c) $\frac{m-1}{8} \le s < \frac{m-1}{5}$ or $2s + 1 < k_1 \le 5s + 1$.

Theorem 5. *The gate counts and the time delay of the multiplier for the pentanomial* $P(x) = x^m + x^{m-s} + x^{m-2s} + x^{m-3s} + 1$, *for* $\frac{m-1}{8} \leq s \leq \frac{m-1}{3}$ *are* $N_A = m^2$,

$$N_X = \begin{cases} m^2 + m - s - 1, & \text{if } \frac{m-1}{4} \leq s \leq \frac{m-1}{3} \\ m^2 + 2m - 5s - 2 & \text{if } \frac{m-1}{5} \leq s < \frac{m-1}{4} \\ m^2 + m - 2 & \text{if } \frac{m-1}{8} \leq s < \frac{m-1}{5} \end{cases}$$

$$T_C = \begin{cases} T_A + (3 + \lceil \log_2(m-1) \rceil)\, T_X, \text{ if } \frac{m-1}{5} \leq s \leq \frac{m-1}{3} \\ T_A + (4 + \lceil \log_2(m-1) \rceil)\, T_X, \text{ otherwise.} \end{cases}$$

Remark 2. Using Maple$^{\text{TM}}$, we have found that there exists 147 values of m, where $m \in [160, 600]$ such that polynomial $P(x) = x^m + x^{m-s} + x^{m-2s} + x^{m-3s} + 1$, $1 \leq s \leq \frac{m-1}{3}$ is irreducible. Among them only 23 have $1 \leq s < \frac{m-1}{8}$.

Table 2. Comparison of related polynomial basis multipliers.

Reference	Special Case	#XOR	Time delay
$P(x) = x^{ns} + x^{(n-1)s} + \cdots + x^s + 1$, $m = ns$			
This paper,[2,11]	-	$m^2 - s$	$T_A + (1 + \lceil \log_2 m \rceil)\, T_X$
$P(x) = x^m + x^k + 1$			
[9,2,11]	$k = 1$	$m^2 - 1$	$T_A + (1 + \lceil \log_2 m \rceil)\, T_X$
[9,2,11]	$1 < k \leq \frac{m}{2}$	$m^2 - 1$	$T_A + (2 + \lceil \log_2 m \rceil)\, T_X$
This paper,[10]	$1 \leq k \leq \frac{m}{2}$	$m^2 - 1$	$T_A + (2 + \lceil \log_2(m-1) \rceil)\, T_X$
$P(x) = x^m + x^{k_t} + \cdots + x^{k_2} + x^{k_1} + 1$, $1 \leq k_1 < k_2 < \cdots < k_t \leq \frac{m}{2}$			
[11]	$t > 1$	$(m+t)(m-1)$	$T_A + (2t + \lceil \log_2 m \rceil)\, T_X$
This paper	$t > 1$	$(m+t)(m-1)$	$T_A + (\lceil \log_2(\lceil \frac{t}{2} \rceil + 1) \rceil + \lceil \log_2(t+1) \rceil + \lceil \log_2(m-1) \rceil) T_X$
$P(x) = x^m + x^{k_3} + x^{k_2} + x^{k_1} + 1$, $1 < k_1 < k_2 < k_3 \leq \frac{m}{2}$			
[11]	$k_1 \geq 1$	$m^2 + 2m - 3$	$T_A + (6 + \lceil \log_2 m \rceil)\, T_X$
This paper	$k_1 > 1$	$m^2 + 2m - 3$	$T_A + (4 + \lceil \log_2(m-1) \rceil)\, T_X$
This paper	$k_1 = 1$	$m^2 + 2m - 3$	$T_A + (3 + \lceil \log_2(m-1) \rceil)\, T_X$
This paper	$k_3 - k_2 = k_1$	$m^2 + m + k_1 - 2$	$T_A + (4 + \lceil \log_2(m-1) \rceil)\, T_X$
[7]	$k_3 - k_2 = k_1 = 1$	$m^2 + m + 2k_2$	$T_A + (3 + \lceil \log_2(m-1) \rceil)\, T_X$
This paper	$k_3 - k_2 = k_1 = 1$	$m^2 + m$	$T_A + (3 + \lceil \log_2(m-1) \rceil)\, T_X$
This paper,[7]	$k_i = i$	$m^2 + m$	$T_A + (3 + \lceil \log_2(m-1) \rceil)\, T_X$
$P(x) = x^m + x^{m-s} + x^{m-2s} + x^{m-3s} + 1$			
[11]	$1 \leq s \leq \frac{m-1}{3}$	$m^2 + 4m - 5s - 5$	$T_A + (\lfloor \frac{d}{4} \rfloor + 4 + \lceil \log_2(m-1) \rceil)\, T_X$
[11]	$s \leq \frac{m-1}{3}$	$\geq m^2 + 2.33m - 7$	$\geq T_A + (4 + \lceil \log_2(m-1) \rceil)\, T_X$
This paper	$\frac{m-1}{8} \leq s \leq \frac{m-1}{3}$	$\leq m^2 + m$	$\leq T_A + (4 + \lceil \log_2(m-1) \rceil)\, T_X$

6 Complexity Results and Concluding Remarks

In this article, time and space complexities of bit parallel multipliers for $GF(2^m)$ have been considered. A comparison of our newly derived gate counts and delays

Table 3. Comparison of the structure of Figure 1 with the Mastrovito multiplier in terms of number of number of lines on the buses.

Multipliers	# Lines on the buses			
	trinomial	s-ESP	pentanomial	generic
Mastrovito [4]	$3m-1$	$\frac{m(m-s)}{2s}+2m$	$5m-3$	$(t+2)(m-1)+2$
This paper	$3m-1$	$2m+s$	$\leq 4m+k_2$	$3m+k_t-2$

with those of existing ones is shown in Table 2. As seen in this table, for trinomial x^m+x+1, the multiplier of Figure 1 has one additional XOR gate delay compared to the best one available in the literature, i.e., [2,11]. However, our results for the ESPs and trinomials ($k \neq 1$) match the corresponding best results available ([2, 11] and [9]). Also, the resultant gate and time complexities for trinomials match those presented in [10].

For a more generic irreducible polynomial as discussed in Section 4, the multiplier in Figure 1 has the same gate count but a shorter time delay compared to [11]. For class 1 pentanomials, this multiplier is faster than [11] and has fewer XOR gates if the special case of $k_3 - k_2 = k_1$ is used. This proposed special case of class 1 covers the case of pentanomials reported in [7], where $k_1 = 1$. Compared to the multiplier proposed in [7], the multiplier discussed in this paper for the special case of $k_1 = k_3 - k_2 = 1$ has $2k_2$ fewer XOR gates and match the ones proposed in [7] for $k_1 = 1$ and $k_2 = 2$. Also, for class 2 pentanomials, our multiplier is either faster or has the same gate delay and has at least $1.33m - 7$ fewer XOR gates than the multiplier reported in [11].

In VLSI implementation, in addition to the gate counts, the number of lines on the buses is also an important parameter which determines the space complexity and consequently its actual time delay. Table 3 compares this metric of the proposed architecture with that of Mastrovito multiplier [4]. As shown in this table, the architectures discussed here have a fewer number of lines on the buses compared to the well known Mastrovito multiplier.

Acknowledgements. This work has been supported in part by an NSERC postdoctoral fellowship awarded to A. Reyhani-Masoleh and in part by an NSERC grant awarded to M. A. Hasan.

References

1. G. B. Agnew, R. C. Mullin, and S. A. Vanstone. "An Implementation of Elliptic Curve Cryptosystems Over $F_{2^{155}}$". *IEEE J. Selected Areas in Communications*, 11(5):804–813, June 1993.
2. A. Halbutogullari and C. K. Koc. "Mastrovito Multiplier for General Irreducible Polynomials". *IEEE Transactions on Computers*, 49(5):503–518, May 2000.
3. E. D. Mastrovito. "VLSI Designs for Multiplication over Finite Fields $GF(2^m)$". In *LNCS-357, Proc. AAECC-6*, pages 297–309, Rome, July 1988. Springer-Verlag.
4. E. D. Mastrovito. *VLSI Architectures for Computation in Galois Fields.* PhD thesis, Linkoping Univ., Linkoping Sweden, 1991.

5. A.J. Menezes, I.F. Blake, X. Gao, R.C. Mullin, S.A. Vanstone, and T. Yaghoobian. *Applications of Finite Fields*. Kluwer Academic Publishers, 1993.
6. A. Reyhani-Masoleh and M. A. Hasan. "A New Efficient Architecture of Mastrovito Multiplier over $GF(2^m)$". In 20^{th} *Biennial Symposium on Communications*, pages 59–63, Kingston, Ontario, Canada, May 2000.
7. F. Rodriguez-Henriquez and C. K. Koc. "Parallel Multipliers Based on Special Irreducible Pentanomials". *IEEE Transactions on Computers*, to appear, 2003, available at http://islab.oregonstate.edu/koc/Publications.html.
8. L. Song and K. K. Parhi. "Low Complexity Modified Mastrovito Multipliers over Finite Fields $GF(2^M)$". In *ISCAS-99, Proc. IEEE International Symposium on Circuits and Systems*, pages 508–512, 1999.
9. B. Sunar and C. K. Koc. "Mastrovito Multiplier for All Trinomials". *IEEE Transactions on Computers*, 48(5):522–527, May 1999.
10. H. Wu. "Bit-Parallel Finite Field Multiplier and Squarer Using Polynomial Basis". *IEEE Transactions on Computers*, 51(7):750–758, July 2002.
11. T. Zhang and K. K. Parhi. "Systematic Design of Original and Modified Mastrovito Multipliers for General Irreducible Polynomials". *IEEE Transactions on Computers*, 50(7):734–748, July 2001.