Low Complexity Bit Parallel Architectures for Polynomial Basis Multiplication over $GF(2^m)$

21st July 2003

A. Reyhani-Masoleh[1] and M. A. Hasan[2]

Abstract

Representing the field elements with respect to the polynomial (or standard) basis, we consider bit parallel architectures for multiplication over the finite field $GF(2^m)$. In this effect, first we derive a new formulation for polynomial basis multiplication in terms of the *reduction* matrix $\mathbf{Q}$. The main advantage of this new formulation is that it can be used with any field defining irreducible polynomial. Using this formulation, we then develop a generalised architecture for the multiplier and analyze the time and gate complexities of the proposed multiplier as a function of degree m and the *reduction* matrix $\mathbf{Q}$. To the best of our knowledge, this is the first time that these complexities are given in terms of $\mathbf{Q}$. Unlike most other articles on bit parallel finite field multipliers, here we also consider the number of signals to be routed in hardware implementation, and we show that compared to the well known Mastrovito's multiplier, the proposed architecture has fewer number of routed signals. In this report, the proposed generalized architecture is further optimized for three special types of polynomials, namely, equally-spaced polynomials, trinomials and pentanomials. We have obtained expilict formulas and complexities of the multipliers for these three special irreducible polynomials. This makes it very easy for a designer to implement the proposed multipliers using hardware description languages like VHDL and Verilog with minimum knowledge of finite field arithmetic.

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

[1]Centre for Applied Cryptographic Research, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1. E-mail: areyhani@math.uwaterloo.ca.

[2]Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1. E-mail: ahasan@ece.uwaterloo.ca.

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 [14], [2]. Finite field arithmetic operations are also used in error control coding [11], [16], VLSI testing [6], [26] and digital signal processing [5]. Among the basic arithmetic operations over the 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. The other operations of finite fields, such as exponentiation, division, and inversion can be performed by repeated multiplications [20], [25], [1], [7]. In order to satisfy high speed requirements of many such applications, there is a need to develop an efficient architecture for finite field multiplication which is suitable for VLSI implementation. In this report, a new general bit parallel structure for the polynomial basis multiplication which is applicable to all types of irreducible binary polynomials is proposed.

1.1 Summary of Previous Work

The earliest parallel polynomial basis (PB) multiplier over $GF(2^m)$ was suggested by Bartee and Schneider [3]. Depending on the irreducible polynomial, this implementation requires as many as m^3-m two-input adders over $GF(2)$ (i.e., XOR gates) [4]. Because of its high circuit complexity and lack of regularity, it is often advantageous to use other hardware structures to implement the multiplier [16]. In [13, 12], Mastrovito has proposed an algorithm along with its hardware architecture (hereafter referred to as Mastrovito algorithm/multiplier) for PB multiplication. Sunar and Koc [23] have presented a new formulation for the Mastrovito algorithm using trinomials and have shown that m^2-1 XOR and m^2 AND gates are sufficient to implement the multiplier. In [8], Halbutogullari and Koc have generalized the approach of Sunar and Koc and have found a method for constructing the Mastrovito multiplier for arbitrary irreducible polynomials. 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 [27], Zhang and Parhi propose a systematic method to design the Mastrovito multiplier. Moreover, they extend the method to systematicly design the modified Mastrovito multiplication scheme proposed in [22]. They also present new results of the complexities of the Mastrovito multiplier for two classes of irreducible pentanomials.

Unlike Mastrovito's method, a $GF(2^m)$ multiplication can also be performed by a straight forward polynomial multiplication followed by modular reduction. This approach has been used in a number of articles. For example, in [24], Wu has considered irreducible trinomials as reduction polynomials and has shown that a modular multiplication operation in $GF(2^m)$ can be performed with $(\omega - 1)(m - 1)$ bit additions, where ω is the Hamming weight of the irreducible polynomial. In hardware implementation, its multiplication operations can be realized with m^2 AND and $(m-1)^2 + (\omega - 1)(m - 1)$ XOR gates. Recently, Rodriguez-Henriquez and Koc in [19] proposed a PB multiplier for special case of pentanomials and have obtained its time delay and gate count. Although they have referred to it as the Mastrovito multiplier, their architecture is different from the original Mastrovito multiplier and uses the two steps of multiplication separately.

1.2 Scope of Our Work

In this report, we present a new formulation for polynomial basis multiplication and then a generalized bit-parallel hardware architecture. We consider the time delay and gate count of the proposed multiplier as a function of degree m and the *reduction* matrix $\mathbf{Q}$. Using the $\mathbf{Q}$ matrix, the complexities of multipliers based on special reduction polynomials, namely: i) trinomials, ii) ESPs and iii) two classes of pentanomials are obtained. We also present explicit formulas for multiplication for the above three special classes. These formulas maximize the number of intermediate signals that are reused. These formulas can be easily coded using hardware description languages such as, VHDL or Verilog, to implement an optimized multiplier. These coding can be done by a hardware designer without running an algorithm for precomputation or even having any knowledge of finite field arithmetic. In this report, we also show that for general irreducible polynomials both time delay and gate count of the proposed structures are in overall lower than those available in the literature. Furthermore, these architectures have fewer routed signals and are suitable for VLSI implementation.

The organization of this report is as follows. In Section 2, polynomial basis multiplication over $GF(2^m)$ and the Mastrovito multiplier in particular are considered. The new architecture and its complexities are introduced in Section 3. In Sections 4, 5 and 6, optimized multiplication schemes using irreducible equally-spaced polynomials, generic polynomials and trinomials are respectively considered and comparisons between our architectures and other PB multipliers are made. Finally, conclusions are given in Section 8.

2 Polynomial basis multiplication 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[3] 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.,

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

where

$$s_k = \sum_{i+j=k} a_ib_j, \quad 0 \le i, j \le m-1, \quad 0 \le k \le 2m-2. \tag{2}$$

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

$$C \triangleq \sum_{i=0}^{m-1} c_i\alpha^i \equiv S \mod P(\alpha). \tag{3}$$

Using (1) and (3), the product coordinates, i.e., c_i's, are obtained in terms of a_i's, b_i's and the irreducible polynomial $P(x)$. In [12], Mastrovito shows that these coordinates can be calculated using a matrix equation as follows:

$$\mathbf{c} = \mathbf{F}\mathbf{b}, \tag{4}$$

where $\mathbf{b} = [b_0, b_1, \cdots, b_{m-1}]^T$ and $\mathbf{c} = [c_0, c_1, \cdots, c_{m-1}]^T$ are the vectors associated with B and C, respectively. The exact definition of the *product matrix* $\mathbf{F} = [f_{i,j}]_{i,j=0}^{m-1}$, can be found in [13].

Remark 1. *Matrix* $\mathbf{F}$ *is unique and depends on the multiplicand* A *and the irreducible polynomial* $P(x)$.

Using (4), an architecture for the Mastrovito multiplier is shown in Figure 1(a), which basically consists of two blocks, namely f-network and IP-network. The f-network generates the entries of the product matrix $\mathbf{F}$. The IP-network performs the matrix-vector multiplication as shown in (4) and consists of m inner product units, each generating one coordinate of C, i.e., $c_i = [f_{i,0}, f_{i,1}, \cdots, f_{i,m-1}][b_0, b_1, \cdots, b_{m-1}]^T$, $0 \le i \le m-1$.

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

In Figure 1(a), block $IP(m)$ corresponds to an inner product unit which has two input vectors of m elements each. Assuming that only two-input logic gates are used, $IP(k)$ for $k > 0$, requires k AND gates and $k-1$ XOR gates, and has a gate delay of $T_A + \lceil \log_2 k \rceil \, T_X$ where T_A and T_X correspond to the delays due to an AND and an XOR gate respectively (see Figure 1(b) where $k = m$).

In Figure 1(a), there are two buses: the coordinates of B and the interconnection bus IB which contains the coordinates of A. The interconnection bus IB carries the elements $f_{i,j}$ of $\mathbf{F}$ from the f-network to the IP-network. The number of lines on IB depends on the irreducible polynomial $P(x)$ and varies between $2m-1$ (for trinomials) and $\frac{m(m+1)}{2}$ (for AOPs) [13].

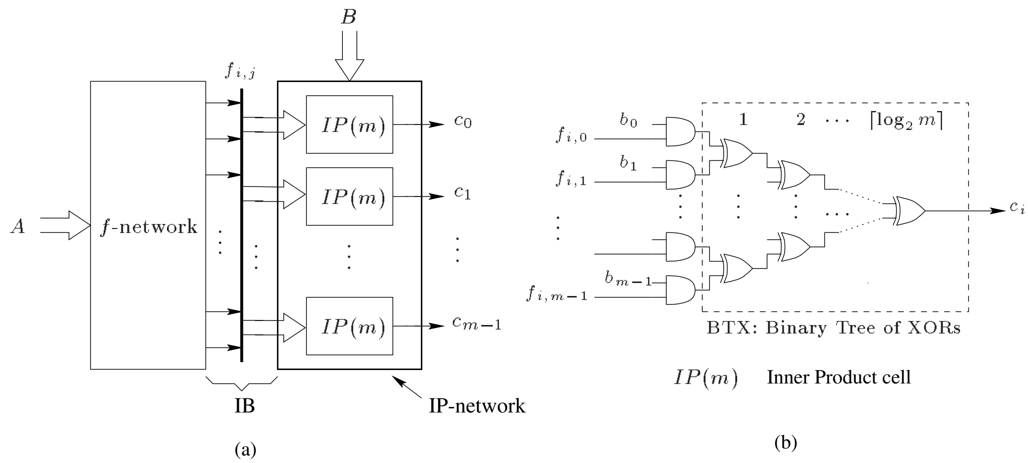


Figure 1: (a) Architecture of the Mastrovito multiplier over $GF(2^m)$. (b) Details of $IP(m)$.

3 An Efficient Multiplication Scheme

In this section, we first give a new formulation for multiplication over $GF(2^m)$. Using this formulation, we then present a bit parallel architecture for the multiplier. At the end, we give upper bounds of the space and time complexities of the architecture.

3.1 New Formulation

Definition 1. *[12] The* reduction matrix $\mathbf{Q}$ *is an $m-1$ by m binary matrix which is obtained from*

$$\boldsymbol{\alpha}^{\uparrow} \equiv \mathbf{Q}\boldsymbol{\alpha} \pmod{P(\alpha)}, \tag{5}$$

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

Remark 2. *For each irreducible $P(x)$, the reduction matrix $\mathbf{Q}$ is unique.*

In order to present our new multiplication scheme, we introduce the following two Toeplitz matrices

$$\mathbf{L} \triangleq \begin{bmatrix} a_0 & 0 & 0 & 0 & \cdots & 0 \\ a_1 & a_0 & 0 & 0 & \cdots & 0 \\ a_2 & a_1 & a_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ a_{m-2} & a_{m-3} & \cdots & a_1 & a_0 & 0 \\ a_{m-1} & a_{m-2} & \cdots & a_2 & a_1 & a_0 \end{bmatrix}, \mathbf{U} \triangleq \begin{bmatrix} 0 & a_{m-1} & a_{m-2} & \cdots & a_2 & a_1 \\ 0 & 0 & a_{m-1} & \cdots & a_3 & a_2 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & a_{m-1} & a_{m-2} \\ 0 & 0 & \cdots & 0 & 0 & a_{m-1} \end{bmatrix}, \quad (6)$$

where a_i's are the coordinates of A. Note that $\mathbf{L}$ is an $m \times m$ lower triangular matrix and $\mathbf{U}$ is an $(m-1) \times m$ upper triangular matrix. Now, define the following two vectors which are functions of A and B.

$$\mathbf{d} = \mathbf{L}\mathbf{b}, \quad (7)$$

$$\mathbf{e} = \mathbf{U}\mathbf{b}. \quad (8)$$

Then, we can state the following theorem which is the key step towards of the development a new architecture for the PB multiplication in $GF(2^m)$.

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

$$\mathbf{c} = \mathbf{d} + \mathbf{Q}^T\mathbf{e}, \quad (9)$$

where $\mathbf{Q}$, $\mathbf{d}$, and $\mathbf{e}$ are defined in (5), (7), and (8) respectively.

Proof. In vector notation, equation (1) can be written as

$$S = \boldsymbol{\alpha}^{\upuparrows T}\mathbf{s}, \quad (10)$$

where $\boldsymbol{\alpha}^{\upuparrows} = [1, \alpha, \cdots, \alpha^{2m-2}]^T = \begin{bmatrix} \boldsymbol{\alpha} \\ \boldsymbol{\alpha}^{\uparrow} \end{bmatrix}$ and $\mathbf{s} = [s_0, s_1, \cdots, s_{2m-2}]^T$. Using (5), we have $\boldsymbol{\alpha}^{\upuparrows} \equiv \begin{bmatrix} \mathbf{I_m} \\ \mathbf{Q} \end{bmatrix} \boldsymbol{\alpha}$, where $\mathbf{I_m}$ is the m by m unity matrix. Note that $d_k = s_k$, $0 \leq k \leq m-1$, and $e_l = s_{l+m}$, $0 \leq l \leq m-2$, then $\mathbf{s} = \begin{bmatrix} \mathbf{d} \\ \mathbf{e} \end{bmatrix} = \begin{bmatrix} \mathbf{L} \\ \mathbf{U} \end{bmatrix} \mathbf{b}$ and using (10), C is obtained as

$$\begin{aligned} C &\equiv S \,(\mathrm{mod} P(\alpha)) \\ &= \left(\begin{bmatrix} \mathbf{I_m} \\ \mathbf{Q} \end{bmatrix} \boldsymbol{\alpha} \right)^T \begin{bmatrix} \mathbf{L} \\ \mathbf{U} \end{bmatrix} \mathbf{b} = \boldsymbol{\alpha}^T \left([\, \mathbf{I_m} \quad \mathbf{Q}^T] \begin{bmatrix} \mathbf{L} \\ \mathbf{U} \end{bmatrix} \right) \mathbf{b} = \boldsymbol{\alpha}^T(\mathbf{L} + \mathbf{Q}^T\mathbf{U})\mathbf{b}. \quad (11) \end{aligned}$$

Since $C = \boldsymbol{\alpha}^T\mathbf{c}$, (11) yields (9) and the proof is complete. □

3.2 Architecture

Using the formulation presented in the previous subsection, an architecture for polynomial basis multiplication over $GF(2^m)$ is shown in Figure 2. This structure is hereafter referred to as low complexity bit parallel (LCBP) multiplier. It is divided into two parts: IP-network and $\mathbf{Q}$-network. The IP-network which has m blocks (denoted as $I_0, I_1, \cdots, I_{m-1}$), generates vectors $\mathbf{d}$ and $\mathbf{e}$ in accordance with (7) and (8). For $0 \le i \le m-2$, block I_i consists of two inner product cells namely $IP(i+1)$ and $IP(m-i-1)$; however the last block I_{m-1} consists of only one such cell namely $IP(m)$.

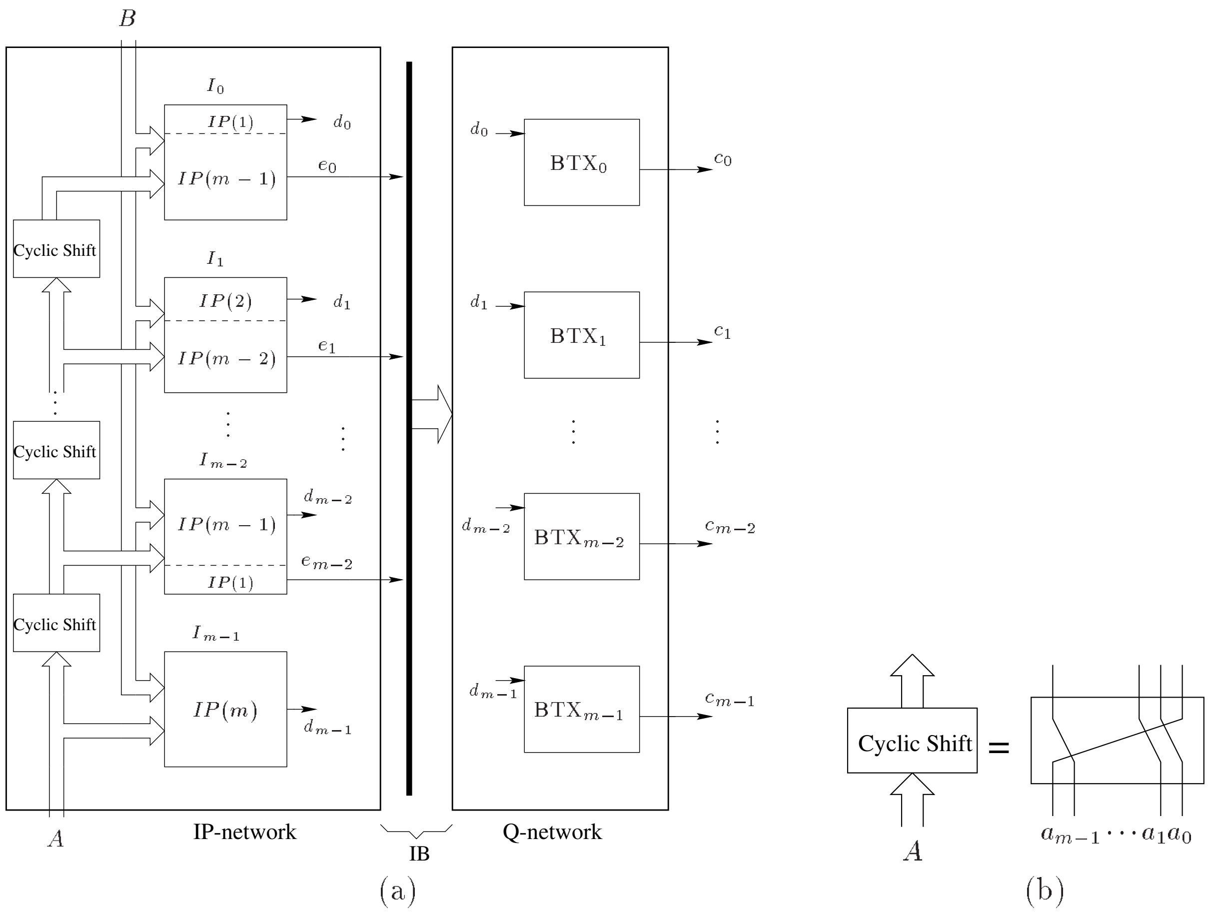


Figure 2: (a) Architecture of the LCBP multiplier over $GF(2^m)$. (b) Detail of cyclic shift block.

In Figure 2, the $\mathbf{Q}$-network takes $\mathbf{d}$ and $\mathbf{e}$ as inputs and generates $\mathbf{c}$. It consists of m binary trees of XOR gates ($\text{BTX}_{0\cdots m-1}$). The number of XOR gates in BTX_i, $0 \le i \le m-1$, is equal to the number of 1's in the i-th column of the $\mathbf{Q}$ matrix. 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 2(a), there are three buses, A, B and IB, and the number of lines on these buses is $3m-1$.

In order to illustrate the new multiplier structure, we consider the finite field of $GF(2^4)$

constructed by irreducible polynomial $P(x) = x^4 + x^3 + 1$. For this field, the circuit diagram based on the new multiplier structure is shown in Figure 3. The total number of XOR gates of this figure can be reduced by reusing signals. This is considered later in this report for special irreducible polynomials.

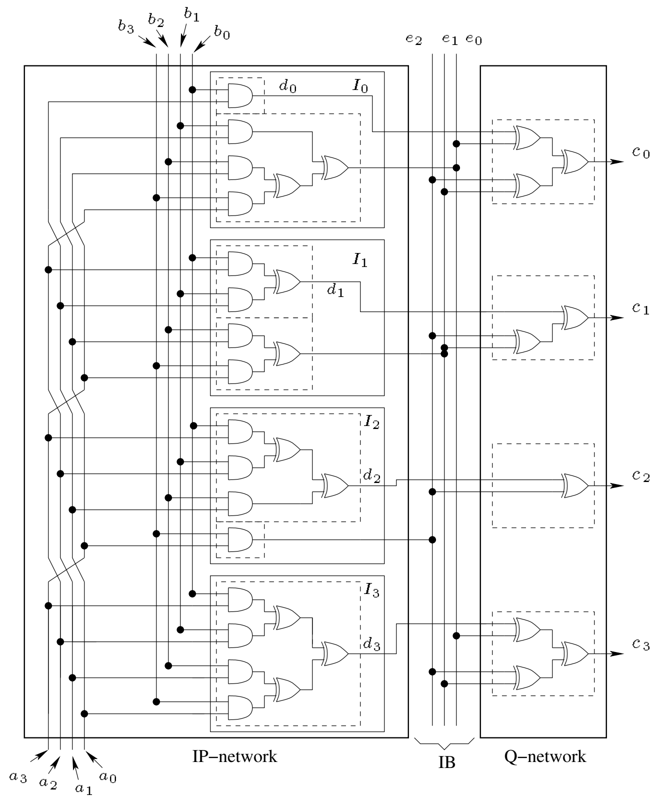


Figure 3: Architecture for the $GF(2^4)$ multiplier with $P(x) = x^4 + x^3 + 1$.

3.3 Complexities

For the LCBP multiplier structure shown in Figure 2, we now give its complexities, in terms of gate counts and time delay due to gates. For this purpose, let $\mathbf{q}_j$, $0 \leq j \leq m-1$, be the j-th column of the reduction matrix, i.e.,

$$\mathbf{Q} = [\mathbf{q}_0,\ \mathbf{q}_1,\ \cdots,\ \mathbf{q}_{\mathbf{m}-1}]$$

and $H(\mathbf{q}_j)$ be the Hamming weight (i.e., the number of 1's) of $\mathbf{q}_j$. We denote θ as the maximum Hamming weight of a column of $\mathbf{Q}$, i.e.,

$$\theta = \max\{H(\mathbf{q}_j) : \ \ 0 \leq j \leq m-1\} \tag{12}$$

and $H(\mathbf{Q})$ as the Hamming weight of $\mathbf{Q}$, i.e.,

$$H(\mathbf{Q}) = \sum_{j=0}^{m-1} H(\mathbf{q}_j). \tag{13}$$

Now, consider the IP-network of the multiplier in Figure 2. Since each I_i for $0 \leq i \leq m-2$, has m AND and $(m-2)$ XOR gates, and I_{m-1} has m AND and $(m-1)$ XOR gates, the IP-network has a total of m^2 AND gates and $(m-1)(m-2)+m-1 = (m-1)^2$ XOR gates. For the $\mathbf{Q}$-network, using (13) one can determine the maximum number of XOR gates needed as $H(\mathbf{Q})$.

To determine the time complexity of this architecture, we need to consider the time delays due to gates of the IP as well as $\mathbf{Q}$-networks. Using (7) and (8), the delays for d_j, $0 \leq j \leq m-1$, and e_i, $0 \leq i \leq m-2$, are given as

$$\begin{aligned} T(d_j) &= T_A + \lceil \log_2(j+1) \rceil \, T_X, \qquad 0 \leq j \leq m-1, &(14)\\ T(e_i) &= T_A + \lceil \log_2(m-i-1) \rceil \, T_X, \quad 0 \leq i \leq m-2, &(15)\end{aligned}$$

respectively. In the IP-network, the maximum gate delay is due to the I_{m-1} cell and is equal to $T_A + \lceil \log_2 m \rceil \, T_X$. Using (12), it is not difficult to see that the maximum gate delay in the $\mathbf{Q}$-network is $\lceil \log_2(\theta+1) \rceil \, T_X$. In the worst case, a signal will have maximum delays of both the IP and $\mathbf{Q}$-networks. Thus, an upper bound for the time delay of the entire multiplier structure is $T_C \leq T_A + (\lceil \log_2 m \rceil + \lceil \log_2(\theta+1) \rceil) \, T_X$. The following theorem summarizes the above results on the complexities of the proposed multiplier structure.

Theorem 2. *For the LCBP multiplier, the number of two-input AND gates is*

$$N_A = m^2 \tag{16}$$

and the number of XOR gates and time delay due to gates are upper bounded by

$$N_X \leq (m-1)^2 + H(\mathbf{Q}), \tag{17}$$

$$T_C \leq T_A + (\lceil \log_2 m \rceil + \lceil \log_2(\theta+1) \rceil) \, T_X. \tag{18}$$

The above theorem gives upper bounds for the number of XOR gates and time delay. However, the exact values can be obtained by designing a multiplier which is either highly space efficient or very fast. In order to minimize the number of XOR gates, the intermediate signals can be reused. This is illustrated in the following example.

3.4 An Example

We consider the field $GF(2^7)$ defined by the irreducible polynomial $P(x) = x^7 + x^5 + x^3 + x + 1$ for which gate and time complexities have been reported in [8]. For this irreducible polynomial, one has

$$\mathbf{Q} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}. \tag{19}$$

Since $H(\mathbf{Q}) = 20$ and $\theta = 4$, then using (17) and (18) the upper bounds of XOR gate count and time delay are $N_X \leq (7-1)^2+20 = 56$ and $T_C \leq T_A + (\lceil \log_2 7 \rceil + \lceil \log_2 5 \rceil) T_X = T_A + 6T_X$, respectively.

Substituting (19) into Theorem 1, the coordinates of the product $C = AB$ over $GF(2^7)$ can be obtained as

$$\begin{aligned}
c_0 &= d_0 + e_0 + e_2 \\
c_1 &= (d_1 + e_0) + (e_1 + (e_2 + e_3)) \\
c_2 &= (d_2 + e_4) + (e_1 + (e_2 + e_3)) \\
c_3 &= (d_3 + e_0) + (e_3 + (e_4 + e_5)) \\
c_4 &= d_4 + (e_1 + (e_4 + e_5)) \\
c_5 &= d_5 + e_0 + e_5 \\
c_6 &= d_6 + e_1,
\end{aligned} \tag{20}$$

where d_j, $0 \leq j \leq 6$ and e_i, $0 \leq i \leq 5$ are from (7) and (8), respectively. Note that the brackets in (20) show the order of modulo two addition which defines the position of XOR gates in the $\mathbf{Q}$-network. Since we reuse partial sums $(e_1 + (e_2 + e_3))$ and $(e_4 + e_5)$ in (20), for the realization of (20), 17 XOR gates are needed in the $\mathbf{Q}$-network and the total number XOR gates of the entire multiplier is $(7-1)^2 + 17 = 53$. Also, since the time delay of d_j, $0 \leq j \leq 6$ and e_i, $0 \leq i \leq 5$ are $T_A + \lceil \log_2(j+1) \rceil T_X$ and $T_A + \lceil \log_2(6-i) \rceil T_X$, respectively, the time delay of the entire multiplier is $T_C = T_A + 5T_X$.

In the following sections, we attempt to minimize the number of XOR gates for special irreducible polynomials namely, equally-spaced polynomials, trinomials, and pentanomials. The LCBP multipliers for the above mentioned irreducible polynomials are achieved by properly defining some intermediate signals and then reusing them as much as possible. We start with equally-spaced polynomials which are very structured and will help us present the remaining special cases with less difficulties.

4 Multipliers Using Equally-Spaced Polynomials

Definition 2. *A polynomial*

$$P(x) = x^{ns} + x^{(n-1)s} + \cdots + x^s + 1, \tag{21}$$

over $GF(2)$, with $ns = m$, is called an equally-spaced polynomial (denoted as s-ESP) of degree m.

An s-ESP is a self reciprocal polynomial. In (21) both n and s are integers and $1 \leq s \leq \frac{m}{2}$. When $s = 1$, we have 1-ESP and it is the same as the all-one polynomial (AOP). The latter has the highest Hamming weight among all polynomials of degree m. On the other hand, $s = \frac{m}{2}$ results in the least Hamming weight irreducible polynomial (i.e., trinomial) of degree m.

Theorem 3. *For an s-ESP based LCBP multiplier over $GF(2^m)$, the gate counts, time delay and number of lines on the buses are $N_A = m^2$, $N_X = m^2 - s$, $T_C = T_A + (1 + \lceil \log_2 m \rceil)\, T_X$, and $N_L = 2m + s$, respectively.*

Proof. When α is a root of the s-ESP in (21), we have

$$\alpha^{m+i} = \begin{cases} \alpha^i + \alpha^{s+i} + \cdots + \alpha^{(n-1)s+i}, & 0 \leq i < s, \\ \alpha^{i-s}, & s \leq i \leq m-2. \end{cases} \tag{22}$$

Using (22), the reduction matrix $\mathbf{Q}$ is obtained as

$$\mathbf{Q} = \begin{bmatrix} \mathbf{I_s} & \mathbf{I_s} & \cdots & \mathbf{I_s} \\ \mathbf{I_{m-s-1}} & & \mathbf{0}_{s+1} & \end{bmatrix}, \tag{23}$$

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 (23) for different values of s are shown in Figure 4. 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 attempt to obtain the coordinates of C. Using (23) into Theorem 1, one can write

$$c_j = d'_j + e_{j \bmod s}, \quad 0 \leq j \leq m-1, \tag{24}$$

where

$$d'_j = \begin{cases} d_j + e_{j+s} & 0 \leq j \leq m-s-2, \\ d_j & m-s-1 \leq j \leq m-1. \end{cases} \tag{25}$$

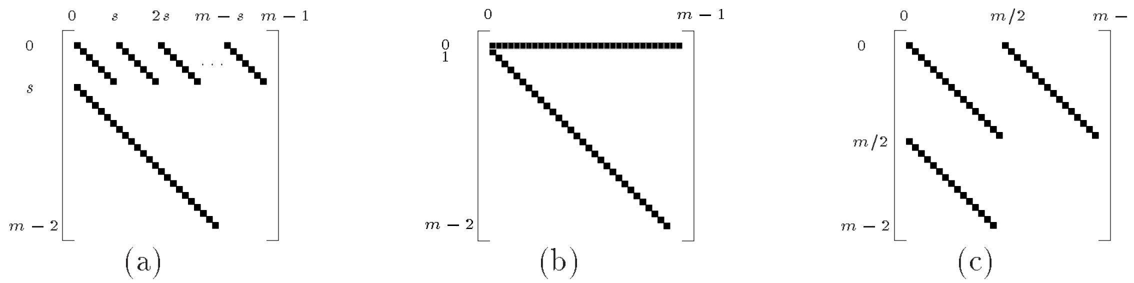


Figure 4: Graphical representations of the locations of non-zero entries of $\mathbf{Q}$ for s-ESP $P(x) = x^{ns} + x^{(n-1)s} + \cdots + x^s + 1$, $m = ns$. (a) $1 < s < \frac{m}{2}$ (b) $s = 1$ (AOP) (c) $s = \frac{m}{2}$ (trinomial).

Thus, using (24) and (25), the exact XOR gate count for an s-ESP based multiplier is $N_X = m^2 - s$. Referring to Figure 2, note that the gate delays to generate d_j, $0 \le j \le m-1$, and e_i, $0 \le i \le m-2$, are $T_A + \lceil \log_2(j+1) \rceil T_X$, and $T_A + \lceil \log_2(m-i-1) \rceil T_X$, respectively. Thus, d'_j of (25) can be generated with a maximum delay of $T_A + + \lceil \log_2 m \rceil T_X$. Although, this changes the architecture for the LCBP multiplier slightly, now each c_j, $0 \le j \le m-1$, has a maximum delay of $T_A + (1 + \lceil \log_2 m \rceil) T_X$.

It is worth mentioning that the resultant number of bus lines on IB reduces from $m-1$ to s. This corresponds to e_0 up to e_{s-1} as used in (24). It is noted that e_j for $s \le j \le m-2$ is not considered as a bus line because it is used only once in the multiplication formulations, i.e., (24) and (25). Thus, the total number of lines on the buses for the multiplier is $2m + s$.

$\square$

Reference	#AND	#XOR	Time delay
Itoh-Tsujii [10]	$(m+s)^2$	$(m+s)^2 - s$	$T_A + (\lceil \log_2 m \rceil + \lceil \log_2(m+s+1) \rceil) T_X$
Hasan et al. [9]	m^2	$m^2 + m - 2s$	$T_A + \left(\frac{m}{s} + \lceil \log_2 m \rceil\right) T_X$
Mastrovito [13], [12]	m^2	$\frac{2s+1}{2s} m^2 - \frac{3}{2} m$	$T_A + (1 + \lceil \log_2 m \rceil) T_X$
Halbutogullari-Koc [8]	m^2	$m^2 - s$	$T_A + (1 + \lceil \log_2 m \rceil) T_X$
Zhang-Parhi [27]	m^2	$m^2 - s$	$T_A + (1 + \lceil \log_2 m \rceil) T_X$
Presented Here	m^2	$m^2 - s$	$T_A + (1 + \lceil \log_2 m \rceil) T_X$

Table 1: Comparison of related s-ESP based polynomial basis multipliers.

Table 1 compares the proposed ESP based multiplier with a number of existing multipliers of the same kind. As seen in the table, our gate count and time delay match the best ones available in the literature.

5 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 $1 \leq k_1 < k_2 < \cdots < k_t \leq \frac{m}{2}$. 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 [15].

In order to apply the general formulation stated in Section 3 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}, $0 \leq i \leq m-2$, 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, row 0 of $\mathbf{Q}$ has 1's in these $t+1$ columns: 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 number of 1's in rows 0 to $m - k_t - 1$ is $t+1$. For the purpose of illustration, the $\mathbf{Q}$ matrices for $t = 1$ and $t = 3$ (i.e., trinomials and pentanomials, respectively) are shown in Figure 5.

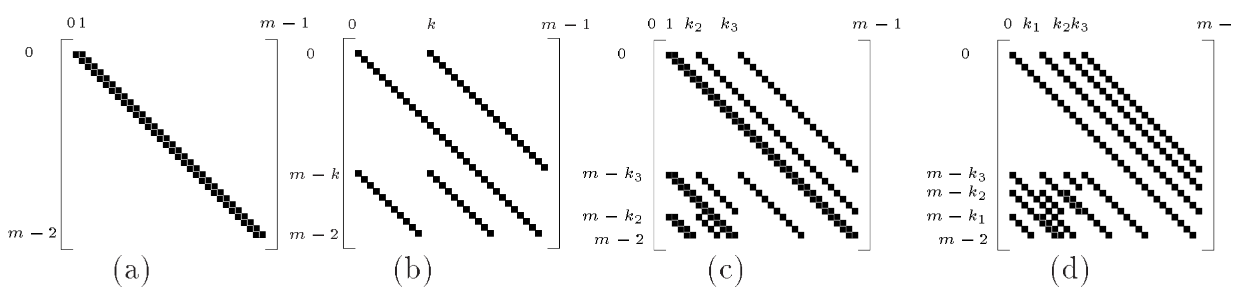


Figure 5: Graphical representations of the reduction matrix $\mathbf{Q}$ for a trinomial ($t = 1$): (a) $k = k_1 = 1$ (b) $1 < k < \frac{m}{2}$ (see Figure 4(c) for $k_1 = \frac{m}{2}$) and a pentanomial ($t = 3$): (c) $k_1 = 1$ (d) $1 < k_1 \leq \frac{m}{2}$.

As shown above, row i, $0 \leq i \leq m - k_t - 1$ of $\mathbf{Q}$ has $t+1$ 1's which correspond to the $t+1$ segmented lines. The last column of $\mathbf{Q}$ contains 1 in rows $i = m - k_j - 1$, $j = t, \cdots, 2, 1$. When a row ends with a 1, the following row originates new $t+1$ lines in columns: 0, k_1, k_2, up to k_t provided that three is no previous lines that pass these columns. If there exists a previous line that passes the column of 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 4(c) for trinomials when $k_1 = \frac{m}{2}$. This is also the case for pentanomials where $t = 3$ and it is shown in Figure 5(c) and 5(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 6 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 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 1's in each column of $\mathbf{Q}_i$, $0 \leq i \leq t$ is at most $t+1$ if $k_1 > 1$, and t if $k_1 = 1$.

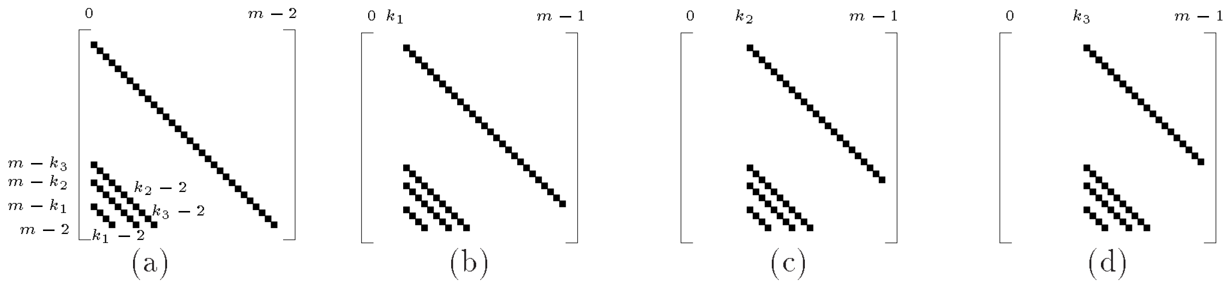


Figure 6: Graphical representations of submatrices of $\mathbf{Q} = \mathbf{Q}_0 + \mathbf{Q}_1 + \mathbf{Q}_2 + \mathbf{Q}_3$ for pentanomials $P(x) = x^m + x^{k_3} + x^{k_2} + x^{k_1} + 1$, where $1 < k_1 < k_2 < k_3 \le \frac{m}{2}$, (see Figure 5(d) for $\mathbf{Q}$). (a) $\mathbf{Q}_0$, (b) $\mathbf{Q}_1$, (c) $\mathbf{Q}_2$, (d) $\mathbf{Q}_3$.

Theorem 4. *The number of XOR gates, time delay, and the number of lines on the buses of the multiplier based on the irreducible polynomial* $P(x) = x^m + x^{k_t} + \cdots + x^{k_2} + x^{k_1} + 1$, $1 \le k_1 < k_2 < \cdots < k_t \le \frac{m}{2}$ *are* $N_X = (m+t)(m-1)$,

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

and $N_L = 3m + k_t - k_1 - 2$, *respectively.*

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 C as

$$\mathbf{c} = \mathbf{d} + \mathbf{e}^{(0)} + \mathbf{e}^{(1)} + \mathbf{e}^{(2)} + \cdots + \mathbf{e}^{(t)}. \tag{26}$$

First, let us assume that $k_1 \ne 1$. Using $\mathbf{Q}_0$ (see Figure 6(a) for $t = 3$), the elements of $\mathbf{e}^{(0)}$ can be written as follows:

$$e_j^{(0)} = \begin{cases} e_j + e_{j+m-k_t} + \cdots + e_{j+m-k_2} + e_{j+m-k_1}, & \text{if } 0 \le j \le k_1 - 2 \\ e_j + e_{j+m-k_t} + \cdots + e_{j+m-k_2} & \text{if } k_1 - 1 \le j \le k_2 - 2 \\ \vdots & \vdots \\ e_j + e_{j+m-k_t} & \text{if } k_{t-1} - 1 \le j \le k_t - 2 \\ e_j & \text{if } k_t - 1 \le j \le m-2 \\ 0 & \text{if } j = m-1. \end{cases} \tag{27}$$

For $0 \le j \le k_t - 2$ the total number of XOR gates to form $e_j^{(0)}$'s, 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 the gates to generate $e_j^{(0)}$. As seen in (27), the longest delay is due to $e_0^{(0)} = e_0 + e_{m-k_t} + \cdots + e_{m-k_2} + e_{m-k_1}$, 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., $e_{m-k_j} + e_{m-k_i}$, $1 \le i, j \le t$, $i \ne j$. Then add these $\lceil \frac{t}{2} \rceil$ terms/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 $T(e_{m-k_j} + e_{m-k_i}) \le$

$T_X + T(e_{m-k_t}) = T_A + (1 + \lceil \log_2(k_t - 1) \rceil)T_X \leq T_A + \lceil \log_2(m-1) \rceil T_X$, where the last inequality is due to $k_t \leq \frac{m}{2}$. Thus, we have

$$T(e_j^{(0)}) \leq \begin{cases} T_A + \left(\lceil \log_2(\lceil \frac{t}{2} \rceil + 1) \rceil + \lceil \log_2(m-1) \rceil \right) T_X, & \text{if } 0 \leq j \leq k_t - 2 \\ T_A + \lceil \log_2(m-1) \rceil T_X & \text{if } k_t - 1 \leq j \leq m-2. \end{cases} \tag{28}$$

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

$$e_j^{(i)} = \begin{cases} 0, & \text{if } 0 \leq j \leq k_i - 1 \\ e_{j-k_i}^{(0)} & \text{otherwise.} \end{cases} \tag{29}$$

Equations (29) and (26) result in the following:

$$c_j = d_j + \begin{cases} e_j^{(0)} & \text{if } 0 \leq j \leq k_1 - 1 \\ e_j^{(0)} + e_j^{(1)} & \text{if } k_1 \leq j \leq k_2 - 1 \\ \vdots & \vdots \\ e_j^{(0)} + e_j^{(1)} + \cdots + e_j^{(t-1)} & \text{if } k_{t-1} \leq j \leq k_t - 1 \\ e_j^{(0)} + e_j^{(1)} + \cdots + e_j^{(t)} & \text{if } k_t \leq j \leq m-2 \\ e_j^{(1)} + e_j^{(2)} + \cdots + e_j^{(t)} & \text{if } j = m-1. \end{cases} \tag{30}$$

To realize (30) 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 number 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 assume a binary tree of XOR gates for each coordinate in (30). For $j \notin [k_t, m-2]$, it can be seen from (30) that $T_C \leq \lceil \log_2(t+1) \rceil T_X + T(e_0^{(0)})$ and the proof is complete by using (28).

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

$$T(d_j + e_j^{(0)}) \leq T_A + (1 + \lceil \log_2(m-1) \rceil)T_X \leq T_A + \left(\left\lceil \log_2(\left\lceil \frac{t}{2} \right\rceil + 1) \right\rceil + \lceil \log_2(m-1) \rceil \right) T_X. \tag{31}$$

Also, using (29) and (28), one can see $T(e_j^{(t)}) \leq T_A + \left(\lceil \log_2(\lceil \frac{t}{2} \rceil + 1) \rceil + \lceil \log_2(m-1) \rceil \right) T_X$ which implies that $T_C \leq T_A + \left(\lceil \log_2(t+1) \rceil + \lceil \log_2(\lceil \frac{t}{2} \rceil + 1) \rceil + \lceil \log_2(m-1) \rceil \right) T_X$ and the proof is complete.

In addition to the three buses shown in Figure 2, now there will be another bus in the middle of the **Q**-network for signals $e_j^{(0)}$, $0 \leq j \leq k_t - 2$. Also note that the signal e_j, $0 \leq j \leq k_1 - 1$, is used once in (27) and (30). Thus, the total number of bus lines is $3m + k_t - k_1 - 2$.

□

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

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

For this special case of irreducible polynomials, our multiplier has the same gate complexities with shorter time delay compared to the Mastrovito multiplier reported in [27]. This comparison is shown in Table 2.

Reference	#AND	#XOR	Time delay
Zhang-Parhi[27]	m^2	$(m+t)(m-1)$	$T_A + (2t + \lceil \log_2 m \rceil)\, T_X$
Presented here	m^2	$(m+t)(m-1)$	$T_A + (\lceil \log_2(t+1) \rceil + \lceil \log_2(\lceil \frac{t}{2} \rceil + 1) \rceil + \lceil \log_2(m-1) \rceil)\, T_X$

Table 2: Comparison of related polynomial basis multipliers for $P(x) = x^m + x^{k_t} + \cdots + x^{k_2} + x^{k_1} + 1$, $1 \leq k_1 < k_2 < \cdots < k_t \leq \frac{m}{2}$.

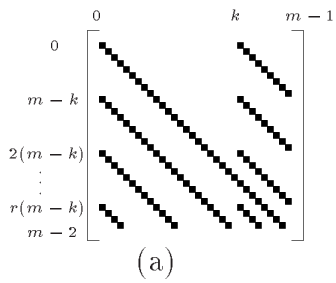
6 Trinomials

Let $P(x) = x^m + x^k + 1$ be an irreducible trinomial generating $GF(2^m)$. Trinomial $P(x)$ has only three non-zero coefficients and no binary irreducible polynomial can have any fewer non-zero coefficients. Since low Hamming weight polynomials can potentially reduce the space and time complexities of a finite field multiplier, irreducible trinomials have drawn significant attention in the past. Reference [21] lists an irreducible trinomial for every degree m $(\leq 10,000)$ for which such a polynomial exists.

Now we derive $\mathbf{Q}$ for the trinomial to obtain the complexities of the LCBP multiplier. The graphical representations of the locations of the non-zeros of $\mathbf{Q}$ for irreducible trinomials with $k = 1$ and $1 < k < \frac{m}{2}$ have been already shown in Figure 5(a) and Figure 5(b), respectively. Similarly, for $\frac{m}{2} < k < m$ and $k = m-1$, $\mathbf{Q}$ can be obtained and their graphical representation of the locations of the non-zeros are shown in Figure 7(a) and Figure 7(b), respectively. Now, using the representation of $\mathbf{Q}$, we can state the following theorem.

Theorem 5. *The number of XOR gates and the time delay of the LCBP multiplier based on the trinomial $x^m + x^k + 1$ are*

$$N_X = \begin{cases} m^2 - \frac{m}{2}, & for\, k = \frac{m}{2} \\ m^2 - 1, & otherwise \end{cases}$$



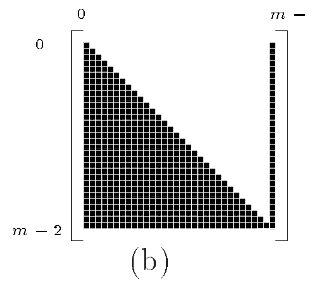


Figure 7: Graphical representations of the reduction matrix $\mathbf{Q}$ for trinomial $P(x) = x^m + x^k + 1$. (a) $\frac{m}{2} < k < m-1$, $r = \left\lfloor \frac{m-2}{m-k} \right\rfloor$, (b) $k = m-1$ (see Figures 5(a), 5(b), and 4(c) for $k = 1$, $1 < k < \frac{m}{2}$, and $k = \frac{m}{2}$, respectively).

and

$$T_C = \begin{cases} T_A + (2 + \lceil \log_2(m-1) \rceil) T_X, & \textit{for } 1 \leq k < \frac{m}{2}, \\ T_A + (1 + \lceil \log_2 m \rceil) T_X, & \textit{for } k = \frac{m}{2}, \\ T_A + \left(1 + \left\lfloor \frac{m-2}{m-k} \right\rfloor + \left\lceil \log_2 \left(m - 1 - \left\lfloor \frac{k-2}{m-k} \right\rfloor (m-k) \right) \right\rceil \right) T_X, & \textit{for } \frac{m}{2} < k < m. \end{cases}$$

Proof. Based on the results obtained in Section 5, one can obtain the time delay and the number of XOR gates by substituting $t = 1$ in Theorem 4, for $1 \leq k < \frac{m}{2}$. Since the trinomial with $k = \frac{m}{2}$, i.e., $P(x) = x^m + x^{\frac{m}{2}} + 1$, is an $\frac{m}{2}$-ESP, the complexities of the multiplier based on this type of trinomials can also be obtained from Theorem 3 with $s = \frac{m}{2}$.

Below, we discuss trinomials with $k > \frac{m}{2}$.

Case: $\frac{m}{2} < k \leq m-1$

Using Figure 7(a) and Theorem 5, one can generate the coordinates of C as

$$c_j = d_j + \begin{cases} e'_j & \text{for } 0 \leq j \leq k-2 \\ e_{k-1} & \text{for } j = k-1 \\ e_j + e'_{j-k} & \text{for } k \leq j \leq 2k-2 \\ e_j + e_{j-k} & \text{for } 2k-1 \leq j \leq m-2 \\ e_{m-k-1} & \text{for } j = m-1. \end{cases} \tag{32}$$

where e'_j can be obtained recursively from $j = k-2$ down to $j = 0$ as follows:

$$e'_j = \begin{cases} e_j + e_{j+m-k}, & \text{for } k-2 \geq j \geq 2k-m-1, \\ e_j + e'_{j+m-k,} & \text{for } 2k-m-2 \geq j \geq 0. \end{cases} \tag{33}$$

These require the same number of XOR gates as in the case of $1 \leq k < \frac{m}{2}$, which is $m^2 - 1$. Also, the time delay of the multiplier is determined by

$$c_k = ((d_k + e_k) + (e_0 + (e_{m-k} + \cdots + (e_{(r-1)(m-k)} + e_{r(m-k)}) \cdots))),$$

where $r = \left\lfloor \frac{m-2}{m-k} \right\rfloor$. Thus, $T_C = (r+1)T_X + T(e_{(r-1)(m-k)})$ and using (15), the total time delay of the multiplier is $T_C = T_A + \left(1 + \left\lfloor \frac{m-2}{m-k} \right\rfloor + \left\lceil \log_2 \left(m - 1 - \left\lfloor \frac{k-2}{m-k} \right\rfloor (m-k)\right) \right\rceil \right) T_X$.

Note that for $k = m-1$, (33) becomes $e'_j = \begin{cases} \sum_{i=j}^{m-2} e_i, & \text{for } 0 \leq j \leq m-2, \\ e'_0, & \text{for } j = m-1, \end{cases}$ which requires the same number of XOR gates and the corresponding delay is $T_A + mT_X$.

$\square$

In [24], a trinomial based multiplier for the cases of $1 \leq k \leq \frac{m}{2}$ has been proposed. For these values of k, the above results match those reported in [24]. Table 3 compares the presented multiplier with other trinomial-based multipliers. As shown in this table, the proposed multiplier has the same gate complexities as the Mastrovito multiplier. For $k = 1$, the proposed multiplier has a time delay which is longer by T_X than the Mastrovito multiplier. However, for the other values of k, i.e., $1 < k < m$, it has the same or shorter delay compared to the Mastrovito multiplier.

To reduce the time delay of the Mastrovito multiplier for $\frac{m}{2} < k < m$, a hybrid tree structure is used in [27]. One can also use a similar technique to the proposed multiplier by applying a hybrid tree to generate e'_j in (33).

If one attempts to apply Theorem 5 to the multiplier in Figure 3, the $\mathbf{Q}$-network should be modified by reusing signals $(e'_0,\ e'_1,\ e'_2)$ instead of signals $(e_0,\ e_1,\ e_2)$. The coordinates of C can be obtained as $c_j = d_j + e'_j$, $0 \leq j \leq 3$, where $e'_0 = e'_3 = e_0 + e'_1$, $e'_1 = e_1 + e_2$, $e'_2 = e_2$.

7 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 irreducible property needed to define the representation of 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 [27].

7.1 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 5. This yields the following.

Multiplier	Reference	#AND	#XOR	Time delay
$P(x) = x^m + x + 1$				
Mastrovito	[13, 23, 8, 27]	m^2	$m^2 - 1$	$T_A + (1 + \lceil \log_2 m \rceil) T_X$
Non-Mastrovito	[24], Presented here	m^2	$m^2 - 1$	$T_A + (2 + \lceil \log_2 (m-1) \rceil) T_X$
$P(x) = x^m + x^k + 1,\ 1 < k < \frac{m}{2}$				
Mastrovito	[13, 23, 8, 27]	m^2	$m^2 - 1$	$T_A + (2 + \lceil \log_2 m \rceil) T_X$
Non-Mastrovito	[24], Presented here	m^2	$m^2 - 1$	$T_A + (2 + \lceil \log_2 (m-1) \rceil) T_X$
$P(x) = x^m + x^{\frac{m}{2}} + 1$				
Mastrovito	[13, 23, 8, 27]	m^2	$m^2 - \frac{m}{2}$	$T_A + (1 + \lceil \log_2 m \rceil) T_X$
Non-Mastrovito	[24], Presented here	m^2	$m^2 - \frac{m}{2}$	$T_A + (1 + \lceil \log_2 m \rceil) T_X$
$P(x) = x^m + x^k + 1,\ \frac{m}{2} < k < m$				
Mastrovito	[23, 27]	m^2	$m^2 - 1$	$T_A + \left(1 + \left\lfloor \frac{m-2}{m-k} \right\rfloor + \lceil \log_2 m \rceil\right) T_X$
Mastrovito	[8]	m^2	$m^2 - 1$	$T_A + \left(\left\lceil \frac{m-1}{m-k} \right\rceil + \lceil \log_2 m \rceil\right) T_X$
Non-Mastrovito	Presented here	m^2	$m^2 - 1$	$\leq T_A + \left(1 + \left\lceil \frac{m-2}{m-k} \right\rceil + \lceil \log_2 (m-1) \rceil\right) T_X$
$P(x) = x^m + x^{m-1} + 1$				
Mastrovito	[23, 8, 27]	m^2	$m^2 - 1$	$T_A + (m - 1 + \lceil \log_2 m \rceil) T_X$
Non-Mastrovito	Presented here	m^2	$m^2 - 1$	$T_A + m T_X$

Table 3: Comparison of related polynomial basis multipliers based on trinomials.

Corollary 2. *The gate counts and time delay of the multiplier for the pentanomial* $P(x) = x^m + x^{k_3} + x^{k_2} + x^{k_1} + 1$, *where* $k_1 < k_2 < k_3 \leq \frac{m}{2}$, *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 $N_L = 3m + k_3 - k_1 - 2$.

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 intermediate terms/signals

$$e'_j = e_{j+m-k_3} + e_{j+m-k_2}, \quad 0 \leq j \leq k_2 - 2. \tag{34}$$

Equation (34) can be used to generate $e_j^{(0)}$, $0 \leq j \leq k_2 - 2$, by substituting $t = 3$ in (27) as follows

$$e_j^{(0)} = \begin{cases} e_j + e'_j + e_{j+m-k_1}, & \text{if } 0 \le j \le k_1 - 2 \\ e_j + e'_j & \text{if } k_1 - 1 \le j \le k_2 - 2 \\ e_j + e_{j+m-k_3} & \text{if } k_2 - 1 \le j \le k_3 - 2 \\ e_j & \text{if } k_3 - 1 \le j \le m - 2 \\ 0 & \text{if } j = m - 1. \end{cases} \tag{35}$$

The total number of XOR gates needed to generate $e_j^{(0)}$'s (see (35)) is $N_1 = k_1 + k_2 + k_3 - 3$ in which (34) contributes $k_2 - 1$. Also, the maximum delay due to gates in (35) is

$$T(e_j^{(0)}) \le \begin{cases} T_A + (2 + \lceil \log_2(m-1) \rceil)\, T_X & \text{if } 0 \le j \le k_1 - 2 \\ T_A + (1 + \lceil \log_2(m-1) \rceil)\, T_X & \text{if } k_1 - 1 \le j \le k_3 - 2 \\ T_A + \lceil \log_2(m-1) \rceil\, T_X & \text{if } k_3 - 1 \le j \le m - 1. \end{cases} \tag{36}$$

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

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

Proof. Since $k_3 \le \frac{m}{2}$, one can easily verify that for all j's $k_3 - 1 \le j - k_1$ (and hence $k_3 - 1 \le j$). Thus, using (35) and (29), one can simply obtain

$$\begin{aligned} e_j^{(0)} + e_j^{(1)} &= e_j^{(0)} + e_{j-k_1}^{(0)} \\ &= e_j + e_{j-k_1} \\ &= e'_{j+k_2-m}, \text{ for } m - k_2 \le j \le m - 2. \end{aligned}$$

Similarly, the second equation can be proved by using (35), (29) and $k_2 = k_3 - k_1$ as follows:

$$\begin{aligned} e_j^{(2)} + e_j^{(3)} &= e_{j-k_2}^{(0)} + e_{j-k_3}^{(0)} \\ &= e_{j-k_2}^{(0)} + e_{j+k_1-k_3}^{(1)} \\ &= e_{j-k_2}^{(0)} + e_{j-k_2}^{(1)}, \text{ for } k_3 \le j \le m - 1. \end{aligned}$$

□

Let us represent $e_j^{(01)}$, $0 \le j \le m-1$, 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 6(a) and Figure 6(b), respectively. Then substituting $t = 3$ in the general case given in (30) and using the above lemma, we can obtain the coordinates of

$C = AB$ as follows:

$$c_j = d_j + e_j^{(01)} + e_{j-k_2}^{(01)},\ 0 \le j \le m-1, \tag{37}$$

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

$$e_j^{(01)} = \begin{cases} e_j^{(0)} & \text{if } 0 \le j \le k_1 - 1 \\ e_j^{(0)} + e_j^{(1)} & \text{if } k_1 \le j \le m - k_2 - 1 \\ e'_{j+k_2-m} & \text{if } m - k_2 \le j \le m-2 \\ e_j^{(1)} & \text{if } j = m-1. \end{cases} \tag{38}$$

As seen in (38), 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 (37) 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 $\mathbf{Q}$-network are $(k_2 - 1)$ and $(m - k_1 - k_2)$, respectively. Thus, the total number of lines on the buses is increased to $4m + k_2 - k_1 - 3$.

To obtain the time delay of the proposed multiplier, we use Table 4 which shows the maximum delay of the signals in (37) for the given ranges of j in each row. In this table, the parameter $t(i)$, $0 \le i \le 4$, represents the time delay of $t(i) = T_A + (i + \lceil \log_2(m-1) \rceil)\, T_X$, and the numbers inside square brackets are for $k_1 = 1$. Also, x determines whether $e_j^{(01)}$ or $e_{j-k_2}^{(01)}$ to be added to d_j first to obtain c_j. For example, using the fifth row of this table, c_{k_3} can be obtained as $c_{k_3} = (d_{k_3} + e_{k_3}^{(01)}) + e_{k_1}^{(01)}$. 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.

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

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

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

Theorem 6. *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* $k_1 < k_2 < k_3 \leq \frac{m}{2}$*, and* $k_3 - k_2 = k_1$ *are*

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

and the number of lines on the buses is $N_L = 4m + k_2 - k_1 - 3$.

Remark 3. *To verify that class 1 irreducible pentanomials exist, we have used a Maple*^{TM} *program for* $m \in [160, 600]$ *and have found that at least one such irreducible pentanomial exists for every* 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. This is shown in Tables 5 and 6. As can be seen from the table,* k *is less than or equal to 6 for any* m *in the above mentioned range.*

It is noted that the pentanomial presented in [19] is the special case of $k_1 = 1$.

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

We refer to polynomials $P(x) = x^m + x^{k_3} + x^{k_2} + x^{k_1} + 1$, where $1 \leq k_1 < k_2 < k_3 \leq m - 1$, and $m - k_3 = k_3 - k_2 = k_2 - k_1 = s$ as class 2 type pentanomials. 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. Here, only three of them are presented. These $\mathbf{Q}$ matrices for $\frac{m-1}{8} \leq s \leq \frac{m-1}{3}$ (or $1 \leq k_1 \leq 5s + 1$) are shown in Figure 8. Based on this figure, we can state the following theorem.

Theorem 7. *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* $N_A = m^2$,

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

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

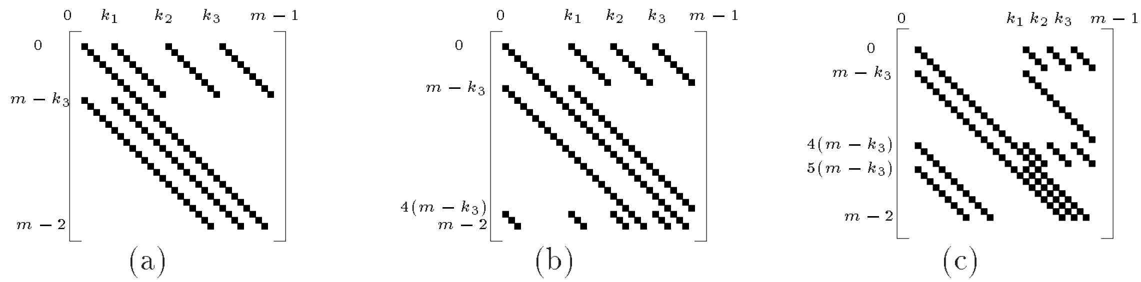


Figure 8: Graphical representations of the reduction matrix $\mathbf{Q}$ for class 2 pentanomials $P(x) = x^m + x^{k_3} + x^{k_2} + x^{k_1} + 1$, where $m - k_3 = k_3 - k_2 = k_2 - k_1 = s$. (a) $\frac{m-1}{4} \leq s \leq \frac{m-1}{3}$ or $1 \leq k_1 \leq s+1$ (see Figure 4(a) for $k_1 = s$), (b) $\frac{m-1}{5}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

and

$$N_L = \begin{cases} 4m-2, & \textit{if } \frac{m-1}{4} \leq s \leq \frac{m-1}{3} \\ 5m-4s-3 & \textit{if } \frac{m-1}{5} \leq s < \frac{m-1}{4} \\ 5k_3 - 3 & \textit{if } \frac{m-1}{8} \leq s < \frac{m-1}{5} \end{cases}$$

Proof. Case I: $1 \leq k_1 \leq s+1$, $\frac{m-1}{4} \leq s \leq \frac{m-1}{3}$

Using (9) and Figure 8(a), one can compute the coordinates of C as

$$c_j = d_j + \begin{cases} e_j + e_{j+s} & \text{if } 0 \leq j \leq k_1 - 1 \\ e_{j-k_1} + e_j + e_{j-k_1+s} + e_{j+s} & \text{if } k_1 \leq j \leq k_2 - 1 \\ e_{j-k_2} + e_j + e_{j-k_1+s} + e_{j+s} & \text{if } k_2 \leq j \leq k_3 - 2 \\ e_{j-k_2} + e_j + e_{j-k_1+s} & \text{if } j = k_3 - 1 \\ e_{j-k_3} + e_j + e_{j-k_1+s} & \text{if } k_3 \leq j \leq k_1 + k_3 - 2 \\ e_{j-k_3} + e_j & \text{if } k_1 + k_3 - 1 \leq j \leq m-2 \\ e_{j-k_3} & \text{if } j = m-1. \end{cases} \tag{39}$$

In order to reduce the number of XOR gates needed for implementing (39), one can pre-compute

$$\begin{aligned} e'_j &= \quad e_j + e_{j+s}, \quad \text{for } 0 \leq j \leq k_2 - 1, \\ e''_{j-k_2} &= \quad e_{j-k_2} + e_{j+s}, \quad \text{for } k_2 \leq j < k_3 - 1. \end{aligned}$$

The pre-computation requires a total of $k_3 - 1$ XOR gates with a maximum time delay of $T_A + (1 + \lceil \log_2(m-1) \rceil) T_X$. Then, by reusing the first s terms of e'_j's and all signals of

e''_{j-k_2}'s, i.e., e'_0, e'_1, $\cdots$, e'_{s-1}, e''_0, e''_1, $\cdots$, e''_{k_3-2}, one can simplify (39) as

$$c_j = d_j + \begin{cases} e'_j & \text{if } 0 \le j \le k_1 - 1 \\ e'_j + e'_{j-k_1} & \text{if } k_1 \le j \le k_2 - 1 \\ e''_{j-k_2} + e_j + e_{j-k_1+s} & \text{if } k_2 \le j \le k_3 - 2 \\ e_{j-k_2} + e_j + e_{j-k_1+s} & \text{if } j = k_3 - 1 \\ e''_{j-k_3} + e_{j-k_1+s} & \text{if } k_3 \le j \le k_1 + k_3 - 2 \\ e''_{j-k_3} & \text{if } k_1 + k_3 - 1 \le j \le m - 2 \\ e_{j-k_3} & \text{if } j = m - 1. \end{cases} \tag{40}$$

Equation (40) requires $m+(k_2-k_1)+2(k_3-k_2-1)+2+(k_1-1) = m+2k_3-k_2-1 = 2m-1$ XOR gates with a time delay of $2T_X$. Thus, the total number of XOR gates required for the whole multiplier is $(m-1)^2 + k_3 - 1 + 2m - 1 = m^2 + k_3 - 1 = m^2 + m - s - 1$ with a time delay of $T_C = T_A + (3 + \lceil \log_2(m-1) \rceil)T_X$. The number of lines on the buses has now increased by the number of reused e'_j's and e''_{j-k_2}'s, i.e., $3m - 1 + s + k_3 - 1 = 4m - 2$.

It is noted that for the special case of $k_1 = 1$, equation (40) should be modified by simply removing the fifth line with condition $k_3 \le j \le k_1 + k_3 - 2$. This does not affect the complexities of the whole multiplier structure.

Case II: $s + 1 < k_1 \le 2s + 1$, $\frac{m-1}{5} \le s < \frac{m-1}{4}$

By comparing Figure 8(b) with Figure 8(a), one can see that the $\mathbf{Q}$ matrix in this case has four more small lines at the bottom of Figure 8(b). This results in more terms in the representations of the coordinates of C. In order to be consistent with the previous case and to use equation (40), one can introduce the following terms

$$e'_j = \begin{cases} e_j + e_{j+4s} + e_{j+s} & \text{for } 0 \le j \le m - 2 - 4s \\ e_j + e_{j+s} & \text{for } m - 1 - 4s \le j \le k_2 - 1, \end{cases} \tag{41}$$

and

$$e''_{j-k_2} = \begin{cases} e_{j-k_2} + e_{j-k_2+4s} + e_{j+s} & \text{for } k_2 \le j \le k_2 + m - 2 - 4s \\ e_{j-k_2} + e_{j+s} & \text{for } k_2 + m - 1 - 4s \le j < k_3 - 1. \end{cases} \tag{42}$$

These new terms cause case II require $m - 1 - 4s$ more XOR gates than case I. Note that the following terms: $e_j + e_{j+4s}$, $0 \le j \le m - 2 - 4s$ are common between (41) and (42). Thus, using (40) with new e'_j's and e''_{j-k_2}'s, i.e., (41) and (42), we have a total number of XOR gates as $m^2 + k_3 - 1 + m - 1 - 4s = m^2 + 2m - 5s - 2$ and the total number of lines on the buses is $4m - 2 + m - 1 - 4s = 5m - 4s - 3$. The maximum delays in (41) and (42) are due to e'_0 and e''_0, respectively and are equal to $T_A + (2 + \lceil \log_2(m-1) \rceil)T_X$ each. Compared to Case I, this delay is increased by T_X, however for an implementation similar to Case I, one can obtain $T_C = T_A + (3 + \lceil \log_2(m-1) \rceil)T_X$.

Case III $2s+1 < k_1 \leq 5s+1$ $\frac{m-1}{8} \leq s < \frac{m-1}{5}$

Let us introduce

$$e'_j = e_j + e_{j+4s}, \text{for } 0 \leq j \leq m-2-4s,$$

which requires $m-1-4s$ XOR gates and a delay of $T_A + (1 + \lceil \log_2(m-1) \rceil)T_X$. Let $\mathbf{Q}_0$ be a submatrix which contains all four lines starting from column 0 in Figure 8(c). Then, the coordinates of $\mathbf{e}^{(0)} = \mathbf{Q}_0^T \mathbf{e}$, can be obtained as

$$e_j^{(0)} = \begin{cases} e'_j + e'_{j+s} & \text{if } 0 \leq j \leq m-2-5s \\ e'_j + e_{j+s} & \text{if } m-1-5s \leq j \leq m-2-4s \\ e_j + e_{j+s} & \text{if } m-1-4s \leq j \leq k_3-2 \\ e_j & \text{if } k_3-1 \leq j \leq m-2 \\ 0 & \text{if } j = m-1, \end{cases} \tag{43}$$

which requires $k_3 - 1$ XOR gates and a maximum time delay of $T_A + (2 + \lceil \log_2(m-1) \rceil)T_X$. Thus, using Figure 8(c) and (9), the coordinates of C can be obtained as

$$c_j = d_j + \begin{cases} e_j^{(0)} & \text{if } 0 \leq j \leq k_1-1 \\ e_j^{(0)} + e_{j-k_1}^{(0)} & \text{if } k_1 \leq j \leq k_2-1 \\ e_j^{(0)} + e'_{j-k_2} + e'_{j+s-k_1} & \text{if } k_2 \leq j \leq k_3-1 \\ e_j^{(0)} + e'_{j-k_3} + e'_{j+s-k_1} & \text{if } k_3 \leq j \leq k_1+m-2-5s \\ e_j^{(0)} + e'_{j-k_3} + e_{j+s-k_1} & \text{others}, \end{cases} \tag{44}$$

To implement (44), one requires $3m - k_1 - k_2 - 1$ XOR gates with the time delay of $2T_X$. Thus, the total number of XOR gates and time delay of the multiplier are $(m-1)^2 + (m-1-4s) + (k_3-1) + (3m-k_1-k_2-1) = m^2+m-2$, and $T_A + (4 + \lceil \log_2(m-1) \rceil)T_X$, respectively. Also, similar to the previous cases, one can obtain the number of lines on the buses as $5k_3 - 3$.

□

A comparison of our newly obtained gate counts and delays as presented above with those of existing ones for pentanomial based multiplier is shown in Table 7. As seen in this table, for class 1 pentanomials with $k_3 - k_2 = k_1$, the proposed multiplier is faster than [27] and has fewer XOR gates. This proposed special case of class 1 covers the case of pentanomials reported in [19], where $k_1 = 1$. Compared to the multiplier proposed in [19], the proposed multiplier for the special case of $k_1 = k_3 - k_2 = 1$ has $2k_2$ fewer XOR gates and match the ones proposed in [19] which uses $k_1 = 1$ 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 [27].

Remark 4. *Using Maple^{TM}, we have found that there exists 147 values of m, as shown in Table 8, where $m \in [160, 600]$ such that polynomial $P(x) = x^m + x^{m-s} + x^{m-2s} + x^{m-3s} + 1$, $1 \le s \le \frac{m-1}{3}$ is irreducible. Among them only 23 have $1 \le s < \frac{m-1}{8}$.*

8 Concluding Remarks

In this report, new bit- parallel polynomial basis multipliers over $GF(2^m)$ have been proposed. 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 have given exact complexity analysis of the multiplier. In general, our results match or outperform the previously known best results in similar classes. We have also presented 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.

Moreover compared to the well known Mastrovito multiplier, the architectures discussed here have fewer number of lines on the buses. This is shown in Table 9. Fewer number of lines on the buses can be advantageous for VLSI implementation especially for cryptographic applications where m is usually very large.

Acknowledgement

The work is supported in part by an NSERC post-doctoral fellowship to A. Reyhani-Masoleh. A preliminary version of this report has appeared in [18] and to appear in [17].

References

[1] G. B. Agnew, T. Beth, R. C. Mullin, and S. A. Vanstone. "Arithmetic Operations in $GF(2^m)$". *Journal of Cryptology*, 6:3–13, 1993.

[2] 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.

[3] T. C. Bartee and D. I. Schneider. "Computation with Finite Fields". *Information and Computers*, 6:79–98, March 1963.

[4] E. R. Berlekamp. *Algebraic Coding Theory.* McGraw-Hill, 1968.

[5] R. E. Blahut. *Fast Algorithms for Digital Signal Processing.* Addison-Wesley, 1985.

[6] T. A. Gulliver, M. Serra, and V. K. Bhargava. "The generation of primitive polynomials in $GF(q)$ with independent roots and their application for power residue codes, VLSI

testing and finite field multipliers using normal bases". *Int. J. Electronics*, 71(4):559–576, 1991.

[7] J. H. Guo and C. L. Wang. "Systolic Array Implementation of Euclid's Algorithm for Inversion and Division in $GF(2^m)$". *IEEE Transactions on Computers*, 47(10):1161–1167, Oct. 1998.

[8] A. Halbutogullari and C. K. Koc. "Mastrovito Multiplier for General Irreducible Polynomials". *IEEE Transactions on Computers*, 49(5):503–518, May 2000.

[9] 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 Transactions on Computers*, 41(8):962–971, Aug. 1992.

[10] T. Itoh and S. Tsujii. "Structure of Parallel Mutipliers for a Class of Fields $GF(2^m)$". *Information and Computation*, 83:21–40, 1989.

[11] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge University Press, 1994.

[12] 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.

[13] E. D. Mastrovito. *VLSI Architectures for Computation in Galois Fields*. PhD thesis, Linkoping Univ., Linkoping Sweden, 1991.

[14] 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.

[15] National Institute of Standards and Technology. *Digital Signature Standard*. FIPS Publication 186-2, February 2000.

[16] I. S. Reed and X. Chen. *Error-Control Coding for Data Networks*. Kluwer Academic Publishers, 1999.

[17] A. Reyhani-Masoleh and M. A. Hasan. "On Low Complexity Bit Parallel Polynomial Basis Multipliers". In *Cryptographic Hardware and Embedded Systems - CHES 2003, LNCS No. xxxx, Springer Verlag, Berlin, Germany, 2003*, September.

[18] 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.

[19] 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.

[20] P. A. Scott, S. J. Simmons, S. E. Tavares, and L. E. Peppard. "Architectures for Exponentiation in $GF(2^m)$". *IEEE J. Selected Areas in Communications*, 6(3):578–586, April 1988.

[21] Gadiel Seroussi. "Table of Low-Weight Binary Irreducible Polynomials". *HP Labs Tech. Report HPL-98-135*, August 1998.

[22] 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.

[23] B. Sunar and C. K. Koc. "Mastrovito Multiplier for All Trinomials". *IEEE Transactions on Computers*, 48(5):522–527, May 1999.

[24] H. Wu. "Bit-Parallel Finite Field Multiplier and Squarer Using Polynomial Basis". *IEEE Transactions on Computers*, 51(7):750–758, July 2002.

[25] H. Wu and M. A. Hasan. "Efficient Exponentiation of a Primitive Root in $GF(2^m)$". *IEEE Transactions on Computers*, 46(2):162–172, Feb. 1997.

[26] Y. Wu and M. I. Adham. "Scan-Based BIST Fault Diagnosis". *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 18(2):203–211, Feb. 1999.

[27] 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.

160, 18, 1	161, 15, 1	162, 15, 1	163, 59, 1	164, 13, 1	165, 30, 1
166, 5, 1	167, 34, 1	168, 15, 2	169, 21, 1	170, 7, 2	171, 18, 1
172, 12, 1	173, 57, 2	174, 15, 3	175, 4, 2	176, 15, 3	177, 84, 1
178, 11, 1	179, 33, 1	180, 36, 1	181, 6, 1	182, 27, 1	183, 52, 1
184, 73, 5	185, 30, 1	186, 22, 1	187, 57, 1	188, 20, 1	189, 31, 3
190, 17, 1	191, 8, 1	192, 27, 1	193, 14, 1	194, 15, 1	195, 9, 1
196, 2, 1	197, 61, 1	198, 45, 1	199, 45, 1	200, 41, 1	201, 16, 1
202, 25, 2	203, 7, 1	204, 73, 1	205, 29, 1	206, 28, 1	207, 72, 1
208, 11, 2	209, 66, 1	210, 32, 3	211, 45, 1	212, 22, 1	213, 7, 1
214, 48, 1	215, 75, 1	216, 23, 3	217, 11, 1	218, 7, 1	219, 18, 1
220, 14, 1	221, 34, 1	222, 87, 1	223, 32, 1	224, 30, 1	225, 24, 1
226, 57, 1	227, 45, 1	228, 72, 1	229, 63, 1	230, 45, 1	231, 18, 1
232, 99, 1	233, 25, 1	234, 49, 1	235, 9, 1	236, 4, 1	237, 25, 1
238, 63, 1	239, 13, 1	240, 5, 3	241, 84, 1	242, 41, 1	243, 75, 1
244, 39, 1	245, 85, 2	246, 34, 1	247, 21, 1	248, 63, 2	249, 35, 2
250, 99, 1	251, 10, 3	252, 34, 1	253, 6, 1	254, 18, 1	255, 93, 1
256, 99, 1	257, 44, 1	258, 121, 1	259, 14, 1	260, 20, 1	261, 63, 1
262, 96, 1	263, 12, 1	264, 9, 1	265, 14, 1	266, 6, 1	267, 85, 1
268, 15, 1	269, 6, 1	270, 7, 3	271, 53, 1	272, 107, 1	273, 6, 1
274, 26, 1	275, 22, 1	276, 88, 1	277, 69, 1	278, 4, 1	279, 4, 1
280, 41, 1	281, 94, 1	282, 7, 1	283, 59, 1	284, 36, 1	285, 105, 1
286, 80, 1	287, 76, 1	288, 10, 1	289, 71, 1	290, 10, 1	291, 58, 1
292, 87, 1	293, 95, 1	294, 43, 1	295, 12, 1	296, 33, 1	297, 4, 1
298, 29, 1	299, 46, 1	300, 42, 3	301, 65, 1	302, 50, 1	303, 28, 1
304, 45, 1	305, 12, 1	306, 15, 2	307, 115, 2	308, 28, 1	310, 15, 1
311, 30, 1	312, 9, 3	313, 113, 1	314, 63, 1	315, 9, 1	316, 80, 1
317, 95, 1	318, 114, 1	319, 128, 1	320, 3, 1	321, 13, 1	322, 21, 2
323, 10, 3	324, 5, 2	325, 75, 1	326, 12, 1	327, 94, 1	328, 91, 2
329, 74, 1	330, 15, 1	331, 82, 3	332, 12, 1	333, 53, 3	334, 26, 1
335, 41, 1	336, 81, 1	337, 132, 1	338, 3, 1	339, 91, 3	340, 44, 1
341, 23, 1	342, 84, 1	343, 20, 1	344, 61, 3	345, 15, 1	346, 29, 2
347, 125, 3	348, 22, 1	349, 11, 1	350, 114, 1	351, 118, 1	352, 75, 1
353, 58, 1	354, 15, 1	355, 5, 1	356, 20, 1	357, 69, 1	358, 38, 1
359, 169, 1	360, 25, 1	361, 44, 1	362, 26, 1	363, 7, 1	364, 8, 1
365, 71, 1	366, 24, 1	367, 11, 1	368, 37, 1	369, 79, 1	370, 83, 1
371, 15, 1	372, 22, 3	373, 99, 1	374, 63, 1	375, 7, 1	376, 141, 1
377, 17, 1	378, 165, 2	379, 113, 1	380, 17, 1	381, 183, 2	382, 174, 1
383, 22, 1	384, 163, 1	385, 65, 1	386, 85, 1	387, 7, 1	388, 68, 1
389, 153, 1	390, 93, 1	391, 21, 1	392, 14, 1	393, 96, 1	394, 66, 1
395, 183, 2	396, 57, 2	397, 66, 1	398, 97, 1	399, 49, 1	400, 117, 1

Table 5: Values $m \in [160, 400]$, k_2, and k_1 such that polynomial $P(x) = x^m + x^{k_1+k_2} + x^{k_2} + x^{k_1} + 1$, is irreducible.

401, 123, 1	402, 81, 2	403, 149, 1	404, 64, 1	405, 90, 7	406, 83, 1
407, 117, 1	408, 3, 2	409, 9, 2	410, 155, 1	411, 131, 5	412, 102, 1
413, 27, 3	414, 45, 1	415, 80, 1	416, 63, 1	417, 30, 1	418, 17, 1
419, 163, 3	420, 58, 1	421, 11, 6	422, 82, 1	423, 40, 1	424, 65, 1
425, 198, 1	426, 49, 1	427, 105, 1	428, 24, 1	429, 66, 4	430, 38, 1
431, 70, 1	432, 17, 3	433, 32, 1	434, 163, 1	435, 86, 5	436, 42, 1
437, 37, 1	438, 19, 1	439, 99, 1	440, 3, 1	441, 21, 1	442, 5, 2
443, 15, 1	444, 24, 1	445, 57, 1	446, 58, 1	447, 25, 1	448, 14, 1
449, 78, 1	450, 53, 3	451, 195, 1	452, 34, 1	453, 151, 1	454, 35, 1
455, 15, 1	456, 195, 3	457, 75, 1	458, 31, 2	459, 135, 1	460, 78, 1
461, 6, 1	462, 60, 1	463, 17, 1	464, 186, 1	465, 48, 1	466, 15, 1
467, 27, 3	468, 175, 1	469, 31, 3	470, 8, 1	471, 54, 1	472, 87, 1
473, 125, 1	474, 21, 1	475, 77, 3	476, 8, 1	477, 191, 2	478, 80, 1
479, 60, 1	480, 54, 3	481, 9, 1	482, 41, 1	483, 193, 3	484, 153, 1
485, 63, 1	486, 48, 1	487, 167, 1	488, 3, 1	489, 79, 1	490, 155, 1
491, 14, 1	492, 7, 1	493, 203, 1	494, 16, 1	495, 25, 1	496, 185, 1
497, 97, 1	498, 75, 1	499, 142, 2	500, 44, 1	501, 129, 5	502, 102, 1
503, 2, 1	504, 95, 2	505, 92, 1	506, 245, 1	507, 78, 4	508, 8, 1
510, 48, 1	511, 182, 1	512, 87, 1	513, 31, 1	514, 21, 1	515, 239, 1
516, 25, 1	517, 10, 2	518, 32, 1	519, 124, 1	520, 189, 1	521, 62, 1
522, 105, 2	523, 201, 1	524, 205, 1	525, 197, 2	526, 134, 1	527, 164, 1
528, 121, 1	529, 105, 1	530, 131, 1	531, 18, 1	532, 18, 3	533, 99, 1
534, 88, 1	535, 51, 1	536, 51, 1	537, 85, 1	538, 57, 2	539, 147, 3
540, 258, 1	541, 177, 3	542, 17, 1	543, 36, 1	544, 183, 3	545, 41, 1
546, 37, 1	547, 245, 2	548, 98, 1	549, 245, 2	550, 84, 1	551, 43, 1
552, 87, 1	553, 123, 1	554, 207, 2	555, 261, 2	556, 38, 1	557, 239, 1
558, 60, 1	559, 129, 1	560, 209, 1	561, 13, 1	562, 75, 1	563, 79, 1
564, 208, 1	565, 81, 1	566, 34, 1	567, 76, 1	568, 125, 1	569, 239, 1
570, 155, 2	571, 275, 2	572, 226, 1	573, 51, 1	574, 78, 1	575, 77, 1
576, 31, 1	577, 132, 1	578, 71, 1	579, 63, 1	580, 45, 1	581, 139, 1
582, 174, 1	583, 206, 1	584, 73, 1	585, 36, 1	586, 117, 1	587, 45, 1
588, 67, 1	589, 217, 2	590, 129, 1	591, 49, 1	592, 31, 2	593, 42, 1
594, 291, 1	595, 9, 1	596, 180, 1	597, 57, 1	598, 6, 1	599, 134, 1
600, 10, 1					

Table 6: Values $m \in [401, 600]$, k_2, and k_1 such that polynomial $P(x) = x^m + x^{k_1+k_2} + x^{k_2} + x^{k_1} + 1$, is irreducible.

Reference	Special Case	#XOR	Time delay
$P(x) = x^m + x^{k_3} + x^{k_2} + x^{k_1} + 1,\ 1 < k_1 < k_2 < k_3 \leq \frac{m}{2}$			
[27]	$k_1 \geq 1$	$m^2 + 2m - 3$	$T_A + (6 + \lceil \log_2 m \rceil) T_X$
LCBP	$k_1 > 1$	$m^2 + 2m - 3$	$T_A + (4 + \lceil \log_2 (m-1) \rceil) T_X$
LCBP	$k_1 = 1$	$m^2 + 2m - 3$	$T_A + (3 + \lceil \log_2 (m-1) \rceil) T_X$
LCBP	$k_3 - k_2 = k_1$	$m^2 + m + k_1 - 2$	$T_A + (4 + \lceil \log_2 (m-1) \rceil) T_X$
[19]	$k_3 - k_2 = k_1 = 1$	$m^2 + m + 2k_2$	$T_A + (3 + \lceil \log_2 (m-1) \rceil) T_X$
LCBP	$k_3 - k_2 = k_1 = 1$	$m^2 + m$	$T_A + (3 + \lceil \log_2 (m-1) \rceil) T_X$
LCBP,[19]	$k_i = i$	$m^2 + m$	$T_A + (3 + \lceil \log_2 (m-1) \rceil) T_X$
$P(x) = x^m + x^{m-s} + x^{m-2s} + x^{m-3s} + 1$			
[27]	$1 \leq s \leq \frac{m-1}{3}$	$m^2 + 4m - 5s - 5$	$T_A + \left(\lfloor \frac{d}{4} \rfloor + 4 + \lceil \log_2 (m-1) \rceil \right) T_X$
[27]	$s \leq \frac{m-1}{3}$	$\geq m^2 + 2.33m - 7$	$\geq T_A + (4 + \lceil \log_2 (m-1) \rceil) T_X$
LCBP	$\frac{m-1}{8} \leq s \leq \frac{m-1}{3}$	$\leq m^2 + m$	$\leq T_A + (4 + \lceil \log_2 (m-1) \rceil) T_X$

Table 7: Comparison of related pentanomial based multipliers.

161, 20	166, 43	167, 44	169, 45	170, 53	172, 57	175, 53	178, 49
182, 27	185, 48	191, 40	193, 40	194, 29	196, 43	199, 55	202, 49
209, 67	212, 35	214, 47	215, 64	217, 51	218, 69	220, 71	223, 63
233, 53	236, 77	238, 55	239, 27	241, 57	242, 49	244, 37	247, 55
250, 49	253, 69	257, 72	260, 75	263, 31	265, 46	266, 73	268, 81
271, 71	274, 69	278, 91	281, 33	284, 77	286, 71	287, 72	289, 28
292, 85	295, 61	302, 87	305, 34	308, 5	310, 31	313, 78	314, 5
316, 45	319, 89	322, 85	329, 93	332, 81	337, 94	340, 55	343, 53
346, 21	350, 99	353, 86	358, 19	359, 97	362, 85	364, 99	367, 57
370, 77	377, 112	380, 111	382, 27	383, 45	385, 81	386, 101	388, 53
391, 121	394, 45	401, 83	404, 113	406, 83	407, 112	409, 29	412, 49
415, 84	418, 73	422, 91	425, 78	428, 35	431, 77	433, 124	436, 55
439, 130	446, 51	449, 105	455, 139	457, 147	458, 85	460, 147	463, 83
470, 107	473, 91	476, 47	478, 119	479, 125	481, 77	484, 35	487, 131
490, 73	494, 159	497, 76	500, 135	503, 159	505, 58	506, 161	508, 133
511, 167	514, 149	518, 135	521, 163	524, 119	526, 143	527, 160	529, 124
532, 177	538, 65	545, 141	550, 119	551, 80	553, 153	556, 91	559, 175
566, 91	569, 164	574, 187	575, 143	577, 184	580, 79	583, 151	590, 31
593, 169	596, 91	599, 70					

Table 8: Values $m \in [160, 600]$ and s 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.

Multipliers	# Lines on the buses			
	trinomial	s-ESP	pentanomial	generic
Mastrovito [13]	$3m-1$	$\frac{m(m-s)}{2s}+2m$	$5m-3$	$(t+2)(m-1)+2$
This paper	$3m-1$	$2m+s$	$\leq 4m+k_2$	$3m+k_t-2$

Table 9: Comparison of the numbers of bus lines of Figure 2 with that of the Mastrovito multiplier.