Brief Contributions

Mastrovito Multiplier for All Trinomials

B. Sunar and Ç.K. Koç, *Member, IEEE*

Abstract—An efficient algorithm for the multiplication in $GF(2^m)$ was introduced by Mastrovito. The space complexity of the Mastrovito multiplier for the irreducible trinomial $x^m + x + 1$ was given as $m^2 - 1$ XOR and m^2 AND gates. In this paper, we describe an architecture based on a new formulation of the multiplication matrix and show that the Mastrovito multiplier for the generating trinomial $x^m + x^n + 1$, where $m \neq 2n$, also requires $m^2 - 1$ XOR and m^2 AND gates. However, $m^2 - m/2$ XOR gates are sufficient when the generating trinomial is of the form $x^m + x^{m/2} + 1$ for an even m. We also calculate the time complexity of the proposed Mastrovito multiplier and give design examples for the irreducible trinomials $x^7 + x^4 + 1$ and $x^6 + x^3 + 1$.

Index Terms—Finite fields, multiplication, standard basis, irreducible trinomial.

◆

1 INTRODUCTION

SOFTWARE and hardware implementations of the basic arithmetic operations (addition, multiplication, and inversion) in the Galois field $GF(2^m)$ are desired in coding theory, computer algebra, and cryptography [7], [4]. The cryptographic applications include elliptic curve cryptosystems [8], [2] in which m is quite large, usually around several hundred. The efficiency of an algorithm is often measured by the number of bit-level or word-level operations. In the hardware implementations, it is often desirable to reduce the total number of gates (space complexity) and the total gate delay (time complexity) of the algorithm. The representation of the field elements has a crucial role in determining the space and time complexity of the arithmetic operations, particularly the field multiplication. In this paper, we are interested in space and time complexity of the finite field multiplication operation, where the field elements are represented using the standard basis.

The standard basis multiplication operation in $GF(2^m)$ is often accomplished in two steps: polynomial multiplication and modular reduction. Let $a(x), b(x), c(x) \in GF(2^m)$ and $p(x)$ be the irreducible polynomial generating $GF(2^m)$. In order to compute $c(x) = a(x)b(x) \bmod p(x)$, we first obtain the product polynomial $d(x)$ which is of degree (at most) $2m - 2$ as

$$d(x) = a(x)b(x) = \left(\sum_{i=0}^{m-1} a_i x^i \right) \left(\sum_{i=0}^{m-1} b_i x^i \right). \qquad (1)$$

The next step is then the reduction operation $c(x) = d(x) \bmod p(x)$ to obtain the $m - 1$ degree polynomial $c(x)$. In practice, the multiplication and the reduction steps are often combined for efficiency reasons. An architecture for performing the field multiplication was proposed by Mastrovito [5], [6]. In this method, we represent the computation of $d(x)$ as a matrix-vector product $d = Mb$, where $(2m - 1) \times m$ dimensional matrix M consists of the coefficients of the polynomial $a(x)$. We then obtain an $m \times m$ dimensional matrix Z by reducing the matrix M using the generating polynomial $p(x)$. The product $c(x)$ is computed using the matrix-vector product $c = Zb$.

● *The authors are with the Electrical and Computer Engineering Department, Oregon State University, Corvallis, OR 97331.*
E-mail: koc@ece.orst.edu.

The space complexity of the multiplier for the special generating trinomial $x^m + x + 1$ is shown to be $m^2 - 1$ XOR and m^2 AND gates [5], [6], [9], [10]. Paar [11] conjectured that the space complexity of the Mastrovito multiplier would be the same for all trinomials $x^m + x^n + 1$, where $1 \leq n \leq m - 1$. In this paper, we describe an architecture for the Mastrovito type multiplier using a general trinomial of the form $x^m + x^n + 1$ and show that the proposed architecture requires $m^2 - 1$ XOR and m^2 AND gates when $n \neq m/2$. However, when m is even and $n = m/2$ there is further reduction: The proposed architecture requires only $m^2 - m/2$ XOR gates.

A few examples of irreducible polynomials of the form $x^m + x^n + 1$ are given in Table 1. Furthermore, it is known [7] that a trinomial of the form $x^m + x^{m/2} + 1$ is irreducible over $GF(2)$ if m is of the form $m = 2 \cdot 3^r$ for some $r \geq 0$.

In the following sections, we give a formulation of the Mastrovito matrix Z and describe an architecture to compute Z. We show that it is sufficient to compute Z_n (the nth row of Z). The remaining elements can be obtained by rewiring, i.e., without using any gates. We then give an analysis of the multiplier architecture and calculate its space and time complexities.

2 THE REDUCTION PROCESS

The entries of the Mastrovito matrix Z are functions of the coefficients of the generating polynomial $p(x)$ and the elements of the original multiplication matrix M, which consists of the coefficients of $a(x)$. The matrix M gives the relationship between the coefficients of $b(x)$ and $d(x)$ in terms of the coefficients of $a(x)$, as follows:

$$
\begin{bmatrix}
d_0 \\
d_1 \\
d_2 \\
\vdots \\
d_{m-2} \\
d_{m-1} \\
d_m \\
d_{m+1} \\
\vdots \\
d_{2m-3} \\
d_{2m-2}
\end{bmatrix}
=
\begin{bmatrix}
a_0 & 0 & 0 & \cdots & 0 & 0 \\
a_1 & a_0 & 0 & \cdots & 0 & 0 \\
a_2 & a_1 & a_0 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
a_{m-2} & a_{m-3} & a_{m-4} & \cdots & a_0 & 0 \\
a_{m-1} & a_{m-2} & a_{m-3} & \cdots & a_1 & a_0 \\
0 & a_{m-1} & a_{m-2} & \cdots & a_2 & a_1 \\
0 & 0 & a_{m-1} & \cdots & a_3 & a_2 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & a_{m-1} & a_{m-2} \\
0 & 0 & 0 & \cdots & 0 & a_{m-1}
\end{bmatrix}
\begin{bmatrix}
b_0 \\
b_1 \\
b_2 \\
\vdots \\
b_{m-2} \\
b_{m-1}
\end{bmatrix}.
$$

$$(2)$$

The product polynomial $d(x)$ contains terms with degrees larger than $m - 1$. These terms need to be reduced using the modulus polynomial $p(x)$ in order to obtain the polynomial representation of the field element in $GF(2^m)$. Since we are considering the generating polynomial $p(x) = x^m + x^n + 1$, we use the identity $x^m = x^n + 1$ to reduce the higher order terms in $d(x)$. A particular term x^i for $i \geq m$ may need to be reduced several times. For example, let $m = 5$ and $p(x) = x^5 + x^3 + 1$. The terms x^5 and x^6 need to be reduced only once: $x^5 = x^3 + 1$ and $x^6 = x^4 + x$. However, the term x^7 will need two reductions $x^7 = x^5 + x^2 = x^3 + 1 + x^2$. For a specific element, the number of reductions depends solely on the degree of the element and on the order of the middle term of the generating trinomial. The maximum number of reductions are performed on the highest order element x^{2m-2}. Let k be the number of reductions required to bring this element to its proper range $[0, m - 1]$. This integer k has the property $2m - 2 - k(m - n) < m$, which implies $k > \frac{m-2}{m-n}$. Therefore, we have

TABLE 1
Examples of Irreducible Polynomials

irreducible $x^m + x^n + 1$ encoded as (m, n)	
(4,3), (4,1)	(10,7), (10,3)
(5,3), (5,2)	(11,9), (11,2)
(6,5), (6,3), (6,1)	(12,9), (12,7), (12,5), (12,3)
(7,6), (7,4), (7,3)	(14,9), (14,5)
(9,8), (9,5), (9,4), (9,1)	(15,14), (15,11), (15,8), (15,7), (15,4), (15,1)

$$k = \left\lfloor \frac{m-2}{m-n} \right\rfloor + 1. \qquad (3)$$

Our objective is to obtain the $m \times m$ matrix Z by systematically reducing the last $m-1$ rows of the $(2m-1) \times m$ matrix M using the generating trinomial $x^m + x^n + 1$. In order to accomplish this task, we define *the reduction array*, which is the array of $(m-1)$ rows produced by the reduction of the higher order elements $x^m, x^{m+1}, \ldots, x^{2m-2}$, as shown in Table 2.

The rows defined by the reduction array are added to the rows of M in order to eliminate the last $m-1$ rows of M. The exponent on the left-hand side provides the index to the source row, which will be added to the rows determined by the exponents on the right-hand side. Initially, we take the first m rows of M as the Z matrix and use the rows above to add certain rows of M to certain other rows of Z in order to obtain the final Z matrix. Let Z_i and M_j denote the ith and jth rows of the matrices Z and M, respectively. The first reduction is determined by the first row of the reduction array as adding M_m to Z_0 and Z_n, since $x^m = 1 + x^n$. The reduction array is given in Table 2. The rows of the reduction array can be divided into groups consisting of rows with equal number of reductions. Since the number of reductions is k, there are k partitions in the array. Since the degree of a term decreases by $m-n$ after each reduction, the first $m-n$ rows, which have degrees ranging from m to $2m-n-1$, are reduced only once. Thus, the first $m-n$ rows form the first partition. The next partition is the next set of $m-n$ rows. This continues in the same fashion until the kth partition which will have $m-n$ or fewer rows. We enumerate the partitions in increasing order, beginning from the topmost as the 0th partition. In general, the ith partition consists of the rows starting with the term $x^{m+i(m-n)}$ and ending with the term $x^{m+(i+1)(m-n)-1}$.

Also, the columns of the reduction array possess certain properties. The first column on the right-hand side is special: It is the sequence of increasing powers of x as $1, x, x^2, \ldots, x^{m-2}$. The second columns contains two sequences: The sequence $x^n, x^{n+1}, \ldots, x^{m-1}$ followed by the sequence $1, x^{m-n-1}, x^{m-n}, \ldots, x^{n-2}$. The third column is obtained by shifting down the second column $m-n$ positions. The fourth column is obtained by shifting down the third column $m-n$ positions, and so on.

Following the construction method proposed in [3], we decompose the Mastrovito matrix Z as the sum of two $m \times m$ matrices X and Y, i.e., $Z = X + Y$, where X is the upper m rows of the matrix M. The matrix X is an $m \times m$ Toeplitz matrix, i.e., a matrix whose entries are constant along each diagonal [1]. Furthermore, X is lower triangular. On the other hand, the $m \times m$ matrix Y represents the terms obtained through reduction and is constructed using the reduction array. We will show that the matrix Y is made of two Toeplitz matrices.

Theorem 1. *The $m \times m$ dimensional matrix Y is partitioned into two Toeplitz matrices. The upper n rows form an $n \times m$ Toeplitz matrix, while the lower $m-n$ rows form an $(m-n) \times m$ Toeplitz matrix.*

Proof. The first column of the reduction array is the sequence $1, x, \ldots, x^{m-2}$ corresponding to the left-hand side $x^m, x^{m+1}, \ldots, x^{2m-2}$. This implies that we add the rows $M_m, M_{m+1}, \ldots, M_{2m-2}$ to the rows $Z_0, Z_1, \ldots, Z_{m-2}$, respectively. We represent this computation using the $m \times m$ matrix T given as

$$T = \begin{bmatrix} 0 & a_{m-1} & a_{m-2} & a_{m-3} & \cdots & a_2 & a_1 \\ 0 & 0 & a_{m-1} & a_{m-2} & & a_3 & a_2 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & a_{m-1} & a_{m-2} \\ 0 & 0 & 0 & 0 & \cdots & 0 & a_{m-1} \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 \end{bmatrix}, \qquad (4)$$

obtained from the matrix M in (2). The matrix T, which is an $m \times m$ Toeplitz matrix, is the initial value of the matrix Y as $Y := T$. After this computation, we need to accumulate the contributions of the remaining columns of the reduction array. We first consider the contribution of the sequence $x^n, x^{n+1}, \ldots, x^{m-1}$, which is the starting sequence in the second column of the reduction array (and, also, all columns thereafter). This sequence implies that we add the rows $M_m, M_{m+1}, \ldots, M_{2m-n-1}$ to the rows $Z_n, Z_{n+1}, \ldots, Z_{m-1}$, respectively. This contribution to the matrix Y is represented using the $m \times m$ matrix U as $Y := Y + U$. The matrix U is obtained from the matrix T by shifting down n rows as follows:

$$U = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 \\ 0 & a_{m-1} & a_{m-2} & \cdots & a_n & \cdots & a_2 & a_1 \\ 0 & 0 & a_{m-1} & \cdots & a_{n+1} & \cdots & a_3 & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_{m-1} & \cdots & a_{m-n+1} & a_{m-n} \end{bmatrix} \begin{matrix} 0 \\ \vdots \\ n-1 \\ n \\ n+1 \\ \vdots \\ m-1 \end{matrix} \qquad (5)$$

Note that the matrix U is composed of two matrices. Its upper n rows constitute an $n \times m$ zero matrix and its lower $m-n$ rows constitute an $(m-n) \times m$ Toeplitz matrix.

Let $T[\uparrow i]$ represent the matrix T shifted up i rows by feeding i rows of zeros from bottom. Also, let $U[\rightarrow i]$ represent the matrix U shifted right i columns by feeding i columns of zeros from left. The contribution of the first column of the reduction array (i.e., the sequence $1, x, x^2, \ldots, x^{m-2}$ to the Y matrix is given as $T[\uparrow 0] = T$. The contribution of the second column of the reduction array has two components: The starter sequence $x^n, x^{n+1}, \ldots, x^{m-1}$ contributes the U matrix and the remainder sequence $1, x^{m-n-1}, x^{m-n}, \ldots, x^{n-2}$ contributes the matrix T shifted up $m-n$ rows, i.e., the matrix $T[\uparrow (m-n)]$. Similarly,

TABLE 2
The Reduction Array

x^m	$=$	1	$+x^n$			
x^{m+1}	$=$	x	$+x^{n+1}$			
$\vdots$	$\vdots$					
x^{2m-n-1}	$=$	x^{m-n-1}	$+x^{m-1}$			
x^{2m-n}	$=$	x^{m-n}	$+1$	$+x^n$		
$\vdots$	$\vdots$					
$x^{3m-2n-1}$	$=$	$x^{2m-2n-1}$	$+x^{m-n-1}$	$+x^{m-1}$		
x^{3m-2n}	$=$	x^{2m-2n}	$+x^{m-n}$	$+1$	$+x^n$	
$\vdots$	$\vdots$					
$x^{4m-3n-1}$	$=$	$x^{3m-3n-1}$	$+x^{2m-2n-1}$	$+x^{m-n-1}$	$+x^{m-1}$	
$\vdots$	$\vdots$					
$x^{km-(k-1)n}$	$=$	$x^{(k-1)m-(k-1)n}$	$+x^{(k-2)m-(k-2)n}$	$+\cdots$	$+x^0$	$+x^n$
$\vdots$	$\vdots$					
x^{2m-2}	$=$	x^{m-2}	$+x^{n-2}$	$+\cdots$	$+x^{(k-1)n-(k-2)m-2}$	$+x^{kn-(k-2)m-2}$

the starter sequence in the third column contributes the matrix $U[\rightarrow (m-n)]$, while the remainder the sequence contributes $T[\uparrow 2(m-n)]$. Adding these contributions for $i = 0$ to $k-1$, we obtain

$$Y = \sum_{i=0}^{k-1} T[\uparrow i(m-n)] + \sum_{i=0}^{k-1} U[\rightarrow i(m-n)]. \qquad (6)$$

Note that T and, thus, $T[\uparrow i]$ for all $i \geq 0$ are Toeplitz matrices. Their sum is also a Toeplitz matrix. The first n rows of the matrix U are zero, as are the first n rows of $U[\rightarrow i]$ for $i \geq 0$. Therefore, we conclude that the upper n rows of the matrix Y form an $n \times m$ Toeplitz matrix. Furthermore, the last $m-n$ rows the matrix U form an $(m-n) \times m$ Toeplitz matrix. Similarly, the last $m-n$ rows of all $U[\rightarrow i]$ are $(m-n) \times m$ Toeplitz matrices. Therefore, the last $m-n$ rows of the matrix Y form an $(m-n) \times m$ Toeplitz matrix. □

3   THE MULTIPLIER ARCHITECTURE

Since X is an $m \times m$ Toeplitz matrix and Y can be partitioned into two Toeplitz matrices, and $Z = X + Y$, we conclude that Z matrix can also be partitioned into two Toeplitz matrices. In other words, the upper n rows and the lower $m-n$ rows form two Toeplitz matrices of dimension $n \times m$ and $(m-n) \times m$, respectively. We will use this fact in the design of our multiplier.

First, we make three important observations about the construction of Z_i for $0 \leq i \leq m-1$ and $k \neq n$ using the row Z_n without using any gates:

1. The rows Z_i for $1 \leq i \leq n-1$ can be obtained from Z_0 by rewiring.
2. The rows Z_i for $n+1 \leq i \leq m-1$ can be obtained from Z_n by rewiring.
3. The row Z_0 can be obtained from (an intermediate step of) Z_n by rewiring.

The proof of Property 1 is straightforward. Since the first n rows of Z form an $n \times m$ Toeplitz matrix, each position in the upper triangular region contains diagonally the same value. We first

implement the first row and, then, obtain the other values in the upper triangular region of the $n \times m$ matrix by rewiring the values from the first row. On the other hand, the lower triangular part of Y corresponding to the first $n-1$ rows is filled with zeros and, thus, the only contribution to that part of Z comes from X, which consists of single terms. Therefore, the input bits will simply be wired to obtain the first $n-1$ rows of Z.

In order to prove Property 2, we note that the last $m-n$ rows of Z form an $(m-n) \times m$ dimensional Toeplitz matrix. The elements in the upper triangular region of this submatrix are diagonally the same and, therefore, they can be obtained from Z_n by rewiring. All the remaining entries (in the lower triangular region) contain single terms coming from X, which are obtained from the inputs by rewiring.

Property 3 is proven as follows: On the right-hand side of the reduction array, whenever there is the term 1 in a particular row, there is also the term x^n, which shows that the set of contributions from the reduction array to Z_n covers the set of contributions to Z_0. The remaining terms come from X. However, X_0 contains all zero entries except the single term a_0 in the leftmost position. Since this position in Y contains a zero, this term is from the input. The other entries of Z_0 are obtained from Z_n.

The complexity of the multiplier solely depends on Z_n, which is explicitly given as

$$Z_n = (a_n a_{n-1} \cdots a_1 a_0 0 \cdots 0) + (0 \cdots 0 a_{m-1} \cdots a_{n+1})$$
$$+ \sum_{i=0}^{k-1} M_m[\rightarrow i(m-n)].$$

The first term (vector) in (7) is the nth row of X. The second term (vector) comes from the x^n term in the first column on the right-hand side of the reduction array. The other terms (the terms inside the summation) come from the x^n terms on the top of each column. Let the sum of the first two vectors be denoted as

$$W = (a_n a_{n-1} \cdots a_1 a_0 a_{m-1} \cdots a_{n+1}),$$

then, we can write Z_n as

$$Z_n = W + \sum_{i=0}^{k-1} M_m[\to i(m-n)]. \tag{7}$$

The summation (7) has important properties which we will use to construct the proposed architecture. In the addition of $W + M_m[\to 0]$, the element a_i in W and the element a_{i+m-n} in $M_m[\to 0]$ are aligned for $i = n-1, n-2, \ldots, 1$ as

$$
\begin{array}{ccccccccc}
a_n & a_{n-1} & a_{n-2} & \cdots & a_1 & a_0 & a_{m-1} & \cdots & a_{n+1} \\
0 & a_{m-1} & a_{m-2} & \cdots & a_{m-n+1} & a_{m-n} & a_{m-n-1} & \cdots & a_1
\end{array}
$$

Furthermore, in the addition of $M_m[\to 0] + M_m[\to (m-n)]$, the element a_i in $M_m[\to 0]$ and the element a_{i+m-n} in $M_m[\to (m-n)]$ are aligned for $i = n-1, n-2, \ldots, 1$ as

$$
\begin{array}{ccccccccc}
0 & a_{m-1} & \cdots & a_n & a_{n-1} & a_{n-2} & \cdots & a_1 \\
0 & 0 & \cdots & 0 & a_{m-1} & a_{m-2} & \cdots & a_{m-n+1}
\end{array}
$$

Therefore, the addition of the subvector $(a_{n-1}a_{n-2}\cdots a_1)$ of W to the corresponding part in $M_m[\to 0]$ is contained in the sum $M_m[\to 0] + M_m[\to (m-n)]$. Hence, this part of W need not be separately added. It can be obtained from the summation term in (7) by rewiring.

We stack the m-dimensional row vectors $M_m[\to i(m-n)]$ on top of one another to obtain the $k \times m$ matrix C as

$$
C = \begin{bmatrix}
M_m[\to 0] \\
M_m[\to (m-n)] \\
M_m[\to 2(m-n)] \\
\vdots \\
M_m[\to (k-1)(m-n)]
\end{bmatrix}. \tag{8}
$$

The computation of the sum in (7) is equivalent to the summation of the *columns* of the matrix C. Let $C_i = (C_{0,i}C_{1,i}\cdots C_{k-1,i})^T$ be the ith column of C indexed from left to right as $i = 0, 1, \ldots, m-1$. Since the matrix C is obtained by first writing M_m to the first row and, then, shifting this row $(m-n)$ times to the right to obtain the remaining rows, the sum $\sum_{j=0}^{k-1} C_{j,i}$ is fully contained in the sum $\sum_{j=0}^{k-1} C_{j,i+(m-n)}$. Therefore, it suffices to obtain the individual sums of the last $m-n$ rows of the matrix C. The remaining column sums are obtained as byproducts. Also, the first element a_n of W need not be added either, since the first column C_0 is zero column; we simply rewire this element from the input.

Furthermore, among the last $m-n$ columns, some C_i columns are of length k, while some other are of length $k-1$. This is because, when M_m is shifted $(k-1)(m-n)$ times to the right, the leftmost side of $M_m[\to (k-1)(m-n)]$ is filled with zeros; only the last $\alpha = (m-1) - (k-1)(m-n)$ entries will be the individual a_i terms. Therefore, the last α columns are of length k and the remaining $(m-n) - \alpha$ columns are of length $k-1$.

4 SPACE AND TIME COMPLEXITY

It follows from the analysis in the preceding section that we need to compute the individual sum of the last α columns C_i for $i = m-1-\alpha+1, m-1-\alpha, \ldots, m-1$, which are of length k. A single column sum requires $k-1$ XOR gates. All α columns require $\alpha(k-1)$ XOR gates. The remaining $(m-n) - \alpha$ columns are of length $k-1$, which requires $k-2$ XOR gates to obtain each column sum. Therefore, we need $((m-n) - \alpha)(k-2)$ XOR gates to obtain these column sums. Hence, the computation of the individual sums of the last $m-n$ columns of C requires a total of

$$\alpha(k-1) + ((m-n) - \alpha)(k-2) = n-1$$

XOR gates. The rest of the column sums are obtained from these $m-n$ column sums as byproducts. We then need to add the vector

W except its subvector $(a_{n-1}a_{n-2}\cdots a_1)$. Also, the first element a_n of W need not be added; it can be rewired form the input. Since W is of length m, we need $m - (n-1) - 1$ XOR gates to add the row vector W to the final sum. This gives the total number of XOR gates to compute Z_n as

$$n - 1 + m - (n-1) - 1 = m - 1.$$

Therefore, the generation of the matrix Z requires a total of $m-1$ XOR gates. The matrix multiplication $c = Zb$, where b is of dimension $m \times 1$ and Z is of dimension $m \times m$, requires m^2 two-input AND gates and $m(m-1)$ XOR gates. This gives the total number of AND and XOR gates to obtain the product $c(x) = a(x)b(x)x^m + x^n + 1$ as

$$\text{AND} = m^2$$
$$\text{XOR} = (m-1) + m(m-1) = m^2 - 1.$$

It is interesting to notice that the space complexity is not a function of n. On the other hand, the time complexity depends on n, as we will show now. The longest signal path in the architecture is defined as the time complexity of the multiplier. We will denote the delay of a 2-input AND and XOR gates by T_A and T_X, respectively. The longest delay occurs in the calculation of the last element Z_n, which requires the sum of the last element of W, and all k elements of the column vector C_{m-1}. Since some of the suffix (or prefix) elements of the summation are needed, we use a length k linear XOR chain to compute this sum, using a total of kT_X delays to compute the sum. The remaining elements of Z_n and, also, the entire Z matrix require no additional delays.

In order to compute the matrix-vector product $c = Zb$, we first use m^2 AND gates to compute all products in parallel using a single T_A delay. A single element of c is then computed by summing a vector of length m using a binary XOR tree, which requires $\lceil \log_2(m) \rceil T_X$ delays. Therefore, the total delay of the circuit to obtain the product c is obtained as

$$
kT_X + T_A + \lceil \log_2(m) \rceil T_X = \\
T_A + \left(\left\lfloor \frac{m-2}{m-n} \right\rfloor + 1 + \lceil \log_2(m) \rceil \right) T_X. \tag{9}
$$

5 AN EXAMPLE

In this section, we construct the Mastrovito multiplier for the irreducible trinomial $x^7 + x^4 + 1$. We use this example to illustrate the proposed architecture. First, we calculate the number of reductions using (3) as

$$k = \left\lfloor \frac{m-2}{m-n} \right\rfloor + 1 = \left\lfloor \frac{7-2}{7-4} \right\rfloor + 1 = 2.$$

Since $2m - 2 = 12$, the reduction array contains $2m - 2 - m + 1 = 6$ rows for reducing the powers $x^7, x^8, \ldots, x^{12}$. The rows of the reduction array are partitioned into $k = 2$ groups, where the two groups contain $m - n = 7 - 4 = 3$ rows each. The first group of three rows contains one reduction for each expression:

$$x^7 = 1 + x^4$$
$$x^8 = x + x^5$$
$$x^9 = x^2 + x^6.$$

The second group of three rows contains two reductions for each expression:

$$x^{10} = x^3 + x^7 = x^3 + 1 + x^4$$
$$x^{11} = x^4 + x^8 = x^4 + x + x^5$$
$$x^{12} = x^5 + x^9 = x^5 + x^2 + x^6.$$

The reduction array in its final form is as follows:

$$x^7 = 1 + x^4$$
$$x^8 = x + x^5$$
$$x^9 = x^2 + x^6$$
$$x^{10} = x^3 + 1 + x^4$$
$$x^{11} = x^4 + x + x^5$$
$$x^{12} = x^5 + x^2 + x^6.$$

In order to obtain the 7×7 matrix Y, we write the expression

$$Y = \sum_{i=0}^{1} T[\uparrow i(7-4)] + \sum_{i=0}^{1} U[\rightarrow i(7-4)]$$
$$= T[\uparrow 0] + T[\uparrow 3] + U[\rightarrow 0] + U[\rightarrow 3].$$

We first obtain the 7×7 matrices $T[\uparrow 3i]$ for $i = 0, 1$ as

$$T = \begin{bmatrix} 0 & a_6 & a_5 & a_4 & a_3 & a_2 & a_1 \\ 0 & 0 & a_6 & a_5 & a_4 & a_3 & a_2 \\ 0 & 0 & 0 & a_6 & a_5 & a_4 & a_3 \\ 0 & 0 & 0 & 0 & a_6 & a_5 & a_4 \\ 0 & 0 & 0 & 0 & 0 & a_6 & a_5 \\ 0 & 0 & 0 & 0 & 0 & 0 & a_6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$T[\uparrow 3] = \begin{bmatrix} 0 & 0 & 0 & 0 & a_6 & a_5 & a_4 \\ 0 & 0 & 0 & 0 & 0 & a_6 & a_5 \\ 0 & 0 & 0 & 0 & 0 & 0 & a_6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Similarly, we obtain the 7×7 matrices $U[\rightarrow 3i]$ for $i = 0, 1$ as

$$U = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & a_6 & a_5 & a_4 & a_3 & a_2 & a_1 \\ 0 & 0 & a_6 & a_5 & a_4 & a_3 & a_2 \\ 0 & 0 & 0 & a_6 & a_5 & a_4 & a_3 \end{bmatrix},$$

$$U[\rightarrow 3] = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a_6 & a_5 & a_4 \\ 0 & 0 & 0 & 0 & 0 & a_6 & a_5 \\ 0 & 0 & 0 & 0 & 0 & 0 & a_6 \end{bmatrix}.$$

Finally, we obtain the 7×7 matrices X and Y as

$$X = \begin{bmatrix} a_0 & 0 & 0 & 0 & 0 & 0 & 0 \\ a_1 & a_0 & 0 & 0 & 0 & 0 & 0 \\ a_2 & a_1 & a_0 & 0 & 0 & 0 & 0 \\ a_3 & a_2 & a_1 & a_0 & 0 & 0 & 0 \\ a_4 & a_3 & a_2 & a_1 & a_0 & 0 & 0 \\ a_5 & a_4 & a_3 & a_2 & a_1 & a_0 & 0 \\ a_6 & a_5 & a_4 & a_3 & a_2 & a_1 & a_0 \end{bmatrix},$$

$$Y = \begin{bmatrix} 0 & a_6 & a_5 & a_4 & a_3 + a_6 & a_2 + a_5 & a_1 + a_4 \\ 0 & 0 & a_6 & a_5 & a_4 & a_3 + a_6 & a_2 + a_5 \\ 0 & 0 & 0 & a_6 & a_5 & a_4 & a_3 + a_6 \\ 0 & 0 & 0 & 0 & a_6 & a_5 & a_4 \\ 0 & a_6 & a_5 & a_4 & a_3 + a_6 & a_6 + a_2 + a_5 & a_5 + a_1 + a_4 \\ 0 & 0 & a_6 & a_5 & a_4 & a_3 + a_6 & a_6 + a_2 + a_5 \\ 0 & 0 & 0 & a_6 & a_5 & a_4 & a_3 + a_6 \end{bmatrix}.$$

We proved that Z_i for $i = 1, 2, 3$ can be obtained from Z_0 and from the input by rewiring, since the computed terms in Z_0 cover all other computed terms, as easily seen below:

$$
\begin{array}{ccccccc}
Z_0: & a_0 & a_6 & a_5 & a_4 & a_3 + a_6 & a_2 + a_5 & a_1 + a_4 \\
Z_1: & a_1 & a_0 & a_6 & a_5 & a_4 & a_3 + a_6 & a_2 + a_5 \\
Z_2: & a_2 & a_1 & a_0 & a_6 & a_5 & a_4 & a_3 + a_6 \\
Z_3: & a_3 & a_2 & a_1 & a_0 & a_6 & a_5 & a_4
\end{array}
$$

We also proved that Z_i for $i = 5, 6$ can be obtained from Z_4 and from the input by rewiring, which is seen as

$$
\begin{array}{l}
Z_4: \quad a_4 \qquad\qquad a_3 + a_6 \qquad a_2 + a_5 \quad a_1 + a_4 \quad a_0 + a_3 + a_6 \\
\qquad a_6 + a_2 + a_5 \quad a_5 + a_1 + a_4 \\
Z_5: \quad a_5 \qquad\qquad a_4 \qquad\qquad a_3 + a_6 \quad a_2 + a_5 \quad a_1 + a_4 \\
\qquad a_0 + a_3 + a_6 \quad a_6 + a_2 + a_5 \\
Z_6: \quad a_6 \qquad\qquad a_5 \qquad\qquad a_4 \qquad\quad a_3 + a_6 \quad a_2 + a_5 \\
\qquad a_1 + a_4 \qquad\quad a_0 + a_3 + a_6
\end{array}
$$

Furthermore, we proved that Z_0 can be obtained from an intermediate step of Z_4 by rewiring:

$$
\begin{array}{l}
Z_0: \quad a_0 \qquad\qquad a_6 \qquad\qquad a_5 \qquad\quad a_4 \qquad\quad a_3 + a_6 \\
\qquad a_2 + a_5 \qquad a_1 + a_4 \\
Z_4: \quad a_4 \qquad\qquad a_3 + a_6 \qquad a_2 + a_5 \quad a_1 + a_4 \quad a_0 + \underline{a_3 + a_6} \\
\qquad a_6 + \underline{a_2 + a_5} \quad a_5 + \underline{a_1 + a_4}
\end{array}
$$

In order to illustrate the computation of $Z_n = Z_4$, we write the sum (7) by expanding into individual terms:

$$
\begin{array}{lccccccc}
W: & a_4 & a_3 & \underline{a_2} & \underline{a_1} & \underline{a_0} & a_6 & a_5 \\
M_m[\rightarrow 0]: & 0 & a_6 & a_5 & a_4 & \underline{a_3} & \underline{a_2} & \underline{a_1} \\
M_m[\rightarrow 3]: & 0 & 0 & 0 & 0 & a_6 & a_5 & a_4
\end{array}
$$

As underlined above, the addition of the subvector $(a_3\ a_2\ a_1)$ of W to the corresponding part in $M_m[\rightarrow 0]$ is also present in the sum $M_m[\rightarrow 0] + M_m[\rightarrow 3]$. Hence, this part of W does not need to be separately computed. We need to compute the individual sums of the last $m - n = 3$ columns. These three columns are of length $k + 1 = 3$, as easily seen above. Therefore, the construction of Z_4 requires a total of six XOR gates.

The remaining vectors Z_i for $i \neq 4$ are obtained from Z_4, as we have shown. What remains is the computation of the matrix-vector product $c = Zb$, which requires $m^2 = 7^2 = 49$ AND gates and $m(m-1) = 7(7-1) = 42$ XOR gates. We conclude that the computation of $c(x) = a(x)b(x)(\mathrm{mod}\ x^7 + x^4 + 1)$ requires 49 AND gates and 48 XOR gates.

6   THE SPECIAL CASE OF $n = m/2$

In this section, we show that, when m is even and n is equal to $m/2$, the Mastrovito multiplier architecture described in this paper

further simplifies. When $n = m/2$, we find the number of reductions k as

$$k = \left\lfloor \frac{m-2}{m - m/2} \right\rfloor + 1 = \left\lfloor \frac{2-4}{m} \right\rfloor + 1 = 2. \tag{10}$$

Since $k = 2$, we write the vector $Z_n = Z_{m/2}$ from (7) as

$$Z_n = W + M[\to 0] + M[\to m/2],$$

which is explicitly given as

$$Z_n = Z_{m/2} =$$
$$(a_{m/2} \quad a_{m/2-1} \quad \cdots \quad a_1 \quad a_0 \quad a_{m-1} \quad \cdots \quad a_{m/2+1})+$$
$$(0 \qquad a_{m-1} \quad \cdots \quad a_{m/2+1} \quad a_{m/2} \quad a_{m/2-1} \quad \cdots \quad a_1 \quad)+$$
$$(0 \qquad 0 \qquad \cdots \quad 0 \qquad 0 \qquad a_{m-1} \quad \cdots \quad a_{m/2+1}).$$

We notice that last $m/2 - 1$ elements starting from a_{m-1} and ending with $a_{m/2+1}$ of the vectors W and $M[\to m/2]$ are exactly the same and, therefore, their sum is equal to zero. We remove these elements from the sum, and obtain

$$Z_n = Z_{m/2} =$$
$$(a_{m/2} \quad a_{m/2-1} \quad \cdots \quad a_1 \quad a_0 \quad 0 \qquad \cdots \quad 0 \ )+$$
$$(0 \qquad a_{m-1} \quad \cdots \quad a_{m/2+1} \quad a_{m/2} \quad a_{m/2-1} \quad \cdots \quad a_1)+$$
$$(0 \qquad 0 \qquad \cdots \quad 0 \qquad 0 \qquad 0 \qquad \cdots \quad 0 \ ).$$

In other words, $M_m[\to m/2]$ makes no contribution and can be removed from the sum to obtain Z_n. Therefore, the computation of $Z_{m/2}$ requires only the addition of the subvectors

$$(a_{m/2-1} \ \cdots \ a_1 \ a_0) + (a_{m-1} \ \cdots \ a_{m/2+1} \ a_{m/2}),$$

which requires only $m/2$ gates. Thus, we conclude that the construction of the vector Z_n in the case $n = m/2$ requires only $m/2$ XOR gates, instead of $m - 1$ XOR gates. This brings the total number of XOR gates required to perform the multiplication to $m(m-1) + m/2 = m^2 - m/2$. The number of AND gates is the same as before.

Furthermore, the time complexity also simplifies since the construction of the vector Z_n now requires a single T_X delay instead of $k\, T_X$ delay. In the special case of the trinomial $x^m + x^{m/2} + 1$, the time complexity of the proposed architecture is found as

$$T_X + T_A + \lceil \log_2(m) \rceil T_X = T_A + (1 + \lceil \log_2(m) \rceil)T_X. \tag{11}$$

We exemplify this case using the irreducible trinomial $x^6 + x^3 + 1$ generating the field $GF(2^6)$ in the following. Since $m = 6$ and $n = 3$, we find the vector $Z_n = Z_3 = W + M[\to 0] + M[\to 3]$ as

$$Z_3 =$$
$$(a_3 \quad a_2 \quad a_1 \quad a_0 \quad a_5 \quad a_4) \ +$$
$$(0 \quad a_5 \quad a_4 \quad a_3 \quad a_2 \quad a_1) \ +$$
$$(0 \quad 0 \quad 0 \quad 0 \quad a_5 \quad a_4).$$

We remove the subvector $(a_{m-1} \cdots a_{m/2+1}) = (a_5 \ a_4)$ from the vectors W and $M[\to 3]$, and obtain

$$Z_3 =$$
$$(a_3 \quad a_2 \quad a_1 \quad a_0 \quad 0 \quad 0 \ ) \ +$$
$$(0 \quad a_5 \quad a_4 \quad a_3 \quad a_2 \quad a_1) \ +$$
$$(0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \ ).$$

Hence, we can obtain Z_3 using only $m/2 = 3$ XOR gates as

$$Z_3 = (a_3, a_2 + a_5, a_1 + a_4, a_0 + a_3, a_2, a_1).$$

Following the previous analysis, we conclude that the remaining Z_i vectors for $i \neq 3$ can be constructed from Z_3 without using any additional gates. The final reduction array and the required row operations in the 11×6 dimensional matrix M are illustrated below:

$$
\begin{array}{llll}
x^6 & = 1 + x^3 & \longrightarrow & M_0 := M_0 + M_6 \quad \text{and} \quad M_3 := M_3 + M_6 \\
x^7 & = x + x^4 & \longrightarrow & M_1 := M_1 + M_7 \quad \text{and} \quad M_4 := M_4 + M_7 \\
x^8 & = x^2 + x^5 & \longrightarrow & M_2 := M_2 + M_8 \quad \text{and} \quad M_5 := M_5 + M_8 \\
x^9 & = 1 & \longrightarrow & M_0 := M_0 + M_9 \\
x^{10} & = x & \longrightarrow & M_1 := M_1 + M_{10}.
\end{array}
$$

From these row operations, we obtain the final 6×6 dimensional Z matrix as follows:

$$
Z = \begin{bmatrix}
a_0 & a_5 & a_4 & a_3 & a_2 + a_5 & a_1 + a_4 \\
a_1 & a_0 & a_5 & a_4 & a_3 & a_2 + a_5 \\
a_2 & a_1 & a_0 & a_5 & a_4 & a_3 \\
a_3 & a_2 + a_5 & a_1 + a_4 & a_0 + a_3 & a_2 & a_1 \\
a_4 & a_3 & a_2 + a_5 & a_1 + a_4 & a_0 + a_3 & a_2 \\
a_5 & a_4 & a_3 & a_2 + a_5 & a_1 + a_4 & a_0 + a_3
\end{bmatrix}
$$

As seen in the matrix Z above, it is necessary and sufficient to to compute the terms

$$a_2 + a_5, a_1 + a_4, a_0 + a_3$$

in order to construct the entire 6×6 matrix Z. These operations require only three XOR gates. In order to perform the multiplication $c(x) = a(x)b(x) \bmod x^6 + x^3 + 1$, we need to perform the matrix vector product $c = Zb$, for which an additional $m(m-1) = 6(6-1) = 30$ XOR gates and $m^2 = 36$ AND gates are required. Therefore, the total number of XOR gates is $3 + 30 = 33$.

ACKNOWLEDGMENTS

REFERENCES

[1]   G.H. Golub and C.F. van Loan, *Matrix Computations, third ed.* Baltimore, Md.: Johns Hopkins Univ. Press, 1996.
[2]   J. Guajardo and C. Paar, "Efficient Algorithms for Elliptic Curve Cryptosystems," *Advances in Cryptology—CRYPTO 97*, B.S. Kaliski, ed., pp. 342-356, 1997.
[3]   Ç.K. Koç and B. Sunar, "Low-Complexity Bit-parallel Canonical and Normal Basis Multipliers for a Class of Finite Fields," *IEEE Trans. Computers*, vol. 47, no. 3, pp. 353-356, Mar. 1998.
[4]   R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, New York: Cambridge Univ. Press, 1994.
[5]   E.D. Mastrovito, "VLSI Architectures for Multiplication Over Finite Field GF(2^m)," *Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, Proc. Sixth Int'l Conf., AAECC-6*, T. Mora, ed., pp. 297-309, Rome, July 1988.
[6]   E.D. Mastrovito, "VLSI Architectures for Computation in Galois Fields," PhD thesis, Linköping Univ., Dept. of Electrical Eng., Linköping, Sweden, 1991.
[7]   *Applications of Finite Fields*, A.J. Menezes, ed. Boston: Kluwer Academic, 1993.
[8]   A.J. Menezes, *Elliptic Curve Public Key Cryptosystems*. Boston: Kluwer Academic, 1993.
[9]   C. Paar, "Efficient VLSI Architectures for Bit Parallel Computation in Galois Fields," PhD thesis, Universität GH Essen, VDI Verlag, 1994.
[10] C. Paar, "A New Architecture for a Parallel Finite Field Multiplier with Low Complexity Based on Composite Fields," *IEEE Tran. Computers*, vol. 45, no. 7, pp. 856-861, July 1996.
[11] C. Paar, private communication, 1997.