Toeplitz matrix-vector product based $GF(2^n)$ shifted polynomial basis multipliers for all irreducible pentanomials

Jiangtao Han and Haining Fan

Abstract

Besides Karatsuba algorithm, optimal Toeplitz matrix-vector product (TMVP) formulae is another approach to design $GF(2^n)$ subquadratic multipliers. However, when $GF(2^n)$ elements are represented using a shifted polynomial basis, this approach is currently appliable only to $GF(2^n)$s generated by all irreducible trinomials and a special type of irreducible pentanomials, not all general irreducible pentanomials. The reason is that no transformation matrix, which transforms the Mastrovito matrix into a Toeplitz matrix, has been found. In this article, we propose such a transformation matrix and its inverse matrix for an arbitrary irreducible pentanomial. Because there is no known value of n for which either an irreducible trinomial or an irreducible pentanomial does not exist, this transformation matrix makes the TMVP approach a universal tool, i.e., it is applicable to all practical $GF(2^n)$s.

Index Terms

Finite field, subquadratic space complexity multiplier, shifted polynomial basis, Toeplitz matrix, irreducible pentanomial.

I. Introduction

Finite field multiplication plays an important role in modern cryptographic systems. The existing $GF(2^n)$ multipliers can roughly be classified into two categories according to their space complexities, namely quadratic and subquadratic multipliers. Due to its simplicity, the polynomial version of Karatsuba

Jiangtao Han and Haining Fan are with the School of Software, Tsinghua University, Beijing, China. E-mails: hjt10@mails.tsinghua.edu.cn and fhn@tsinghua.edu.cn

algorithm is widely adopted to design $GF(2^n)$ subquadratic multipliers [1], see for example, [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], etc.

A Toeplitz matrix is a matrix in which each descending diagonal from left to right is constant. In 2007, $GF(2^n)$ subquadratic multipliers using optimal Toeplitz matrix-vector product (TMVP) formulae was introduced in reference [15]. It takes advantage of the shifted polynomial basis [16] and applies the coordinate transformation technique of [17] and [18]. The TMVP approach consists of two steps:

1) Converting the Mastrovito matrix into a Toeplitz matrix using a transformation matrix;
2) Computing the TMVP using optimal TMVP formulae.

Since both space and time complexities of optimal TMVP formulae in the second step are lower than those of the original Karatsuba algorithm, both complexities of the resulting multipliers are less than those of the best Karatsuba-based subquadratic multipliers proposed before 2007. Specially, the theoretical time complexity is reduced significantly. For example, it is reduced by about 33% and 25% for $n = 2^t$ and $n = 3^t$ $(t > 1)$ respectively. Recently, some further research in TMVP approach has been conducted in [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], etc. These improvements and generalizations make the TMVP approach even more attractive.

However, when $GF(2^n)$ elements are represented using a shifted polynomial basis (SPB), the TMVP approach is currently applicable only to $GF(2^n)$s generated by all irreducible trinomials and a special type of irreducible pentanomials, namely $f(u) = u^n+u^{p+1}+u^p+u^{p-1}+1$ $(1 < p < n-1)$, not all general irreducible pentanomials. The reason is that no transformation matrix in the first step has been found for an arbitrary irreducible pentanomial, and therefore the Mastrovito matrix can not be transformed into a Toeplitz matrix. In this article, we will propose such a transformation matrix and its inverse matrix for an arbitrary irreducible pentanomial $f(u) = u^n + u^p + u^q + u^r + 1$, where $n > p > q > r > 1$. Because there is no known value of n for which either an irreducible trinomial or an irreducible pentanomial does not exist [30], this transformation matrix makes it possible for the MVP approach to be used for all practical $GF(2^n)$s. Therefore, it is of particular importance for both theoretical and practical purposes.

The paper is organized as follows. In section II, we present the transformation matrix and its inverse matrix. Two examples are given in section III. Finally, concluding remarks are made in section IV.

II. TMVP-based SPB Subquadratic Multipliers for General Irreducible Pentanomials

A. TMVP-based SPB Subquadratic Multipliers

We first introduce TMVP-based $GF(2^n)$ subquadratic multipliers briefly. For more details, please refer to reference [15]. Let $f(u) \in GF(2)[u]$ be the irreducible polynomial defining $GF(2^n)$, and x be a root

of $f(u)$. A shifted polynomial basis of $GF(2^n)$ over $GF(2)$ is defined as follows [16]:

Definition Let v be an integer and the ordered set $W = \{x^i | 0 \leq i \leq n-1\}$ be a polynomial basis of $GF(2^n)$ over $GF(2)$. The ordered set $x^{-v}W := \{x^{i-v} | 0 \leq i \leq n-1\}$ is called a shifted polynomial basis with respect to W.

Let $X = (x^{-v}, x^{-v+1}, \ldots, x^{n-v-1})^T$ be the column vector of SPB basis elements, $A = (a_0, a_1, \ldots, a_{n-1})^T$ be the coordinate column vector of the $GF(2^n)$ element $a = X^T A = x^{-v} \sum_{i=0}^{n-1} a_i x^i$, and B and C are defined similarly. The product $c = X^T C = x^{-v} \sum_{i=0}^{n-1} c_i x^i$ of a and b in SPB can be expressed as follows [15]:

$$\begin{aligned} c &= ab = X^T C = \sum_{i=0}^{n-1} a_i x^{i-v} b \\ &= \left(x^{-v}b, \ldots, x^{-1}b, b, xb, \ldots, x^{n-v-1}b\right) A \quad (1) \\ &= X^T \left(M_{*,0}, M_{*,1}, \ldots, M_{*,n-1}\right) A \quad (2) \\ &= X^T M A, \quad (3) \end{aligned}$$

where $n \times n$ matrix M in (3) is often called the Mastrovito matrix, and column vector $M_{*,j}$ in (2) denotes the j-th column of M. In the following, we will also use $M_{i,*}$ to denote the i-th row of matrix M.

The matrix-vector product MA in (3) is just the the coordinate column vector of the product c, i.e., $C = MA$. In order to adopt the TMVP approach to compute C, Mastrovito matrix M must be transformed into a Toeplitz matrix first, i.e., we must find an $n \times n$ invertible matrix H over $GF(2)$ such that $T = HM$ is a Toeplitz matrix. Then the coordinate column vector C of c equals to

$$C = MA = (H^{-1}H)MA = H^{-1}((HM)A) = H^{-1}(TA) = H^{-1}V, \quad (4)$$

where the TMVP $V = TA$ is computed using some optimal TMVP formulae.

In Reference [15], invertible transformation matrices Hs and their inverses were presented for all irreducible trinomials $f(u) = u^n + u^k + 1$ $(0 < k < n)$ and a special type of irreducible pentanomials, namely $f(u) = u^n + u^{p+1} + u^p + u^{p-1} + 1$ $(1 < p < n-1)$. In the following, we will propose a transformation matrix H and its inverse matrix for an arbitrary irreducible pentanomial $f(u) = u^n + u^p + u^q + u^r + 1$, where $n > p > q > r > 1$.

B. Transformation Matrices for General Irreducible Pentanomials

Upper shift matrix U^k and lower shift matrix L^k are two Toeplitz matrices defined by

$$U^k_{m \times m} = (\delta_{i+k,j})_{m \times m} \text{ and } \; L^k_{m \times m} = (\delta_{i,j+k})_{m \times m}, \quad (5)$$

where $0 \leq k < m$ is an integer and $\delta_{i,j}$ is the Kronecker delta symbol. For example,

$$U^1_{m\times m} = (\delta_{i+1,j}) = \begin{pmatrix} 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & \ddots & & \vdots \\ 0 & 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 1 & 0 \\ \vdots & & \ddots & 0 & 0 & 1 \\ 0 & \cdots & \cdots & 0 & 0 & 0 \end{pmatrix}, \quad L^1_{m\times m} = (\delta_{i,j+1}) = \begin{pmatrix} 0 & 0 & 0 & \cdots & \cdots & 0 \\ 1 & 0 & 0 & \ddots & & \vdots \\ 0 & 1 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 & 0 \\ \vdots & & \ddots & 1 & 0 & 0 \\ 0 & \cdots & \cdots & 0 & 1 & 0 \end{pmatrix}.$$

The transformation matrix H for an arbitrary irreducible pentanomial is given in the following proposition:

Proposition 2.1: Let $f(u) = u^n + u^p + u^q + u^r + 1$ $(n > p > q > r > 1)$ be an irreducible pentanomial over $GF(2)$, and M be the Mastrovito matrix defined in (3). Define two integers k_U and k_L by $k_U = \left\lceil \frac{n-q}{n-p} \right\rceil - 1$ and $k_L = \lceil \frac{q}{r} \rceil - 1$. Define three matrices $\bar{U}$, $\bar{L}$ and H by

$$\begin{aligned} \bar{U} &= \sum_{k=0}^{k_U} U^{k(n-p)}_{(n-q)\times(n-q)}, \\ \bar{L} &= \sum_{k=0}^{k_L} L^{kr}_{q\times q}, \\ H &= \begin{pmatrix} \mathbf{0}_{(n-q)\times q} & \bar{U} \\ \bar{L} & \mathbf{0}_{q\times(n-q)} \end{pmatrix}_{n\times n}. \end{aligned} \tag{6}$$

Then $T = HM$ is a Toeplitz matrix.

Proof:

Let $g = x^{j-v}b = x^{-v}\sum_{i=0}^{n-1} g_i x^i$ be the j-th element in the row vector $\left(x^{-v}b, \ldots, x^{-1}b, b, xb, \ldots, x^{n-v-1}b\right)$ in (1), where $0 \leq j \leq n-2$. Thus the $(j+1)$-th element in this row vector is $xg = x^{j-v+1}b$. Since this row vector is equal to the row vector $X^T(M_{*,0}, M_{*,1}, \ldots, M_{*,n-1})$ in (2), we know that equation $g = x^{-v}\sum_{i=0}^{n-1} g_i x^i = X^T M_{*,j}$ holds. Because X^T is the row vector of SPB basis elements, it is clear that the j-th column of matrix M, i.e., $M_{*,j}$, is just the SPB coordinate column vector of element g, i.e.,

$$M_{*,j} = (g_0, g_1, \ldots, g_{n-1})^T. \tag{7}$$

Now we derive the SPB coordinate column vectors of element xg, which is the $(j+1)$-th column of matrix M, i.e., $M_{*,j+1}$. Since x is a root of the irreducible pentanomial $f(u) = u^n + u^p + u^q + u^r + 1$,

i.e., $x^n + x^p + x^q + x^r + 1 = 0$, we have $x^{n-v} = x^{p-v} + x^{q-v} + x^{r-v} + x^{-v}$. Thus we obtain

$$\begin{aligned} xg &= x^{j-v+1}b = x^{-v+1}\sum_{i=0}^{n-1} g_i x^i \\ &= \left(\sum_{i=0}^{n-2} g_i x^{i-v+1}\right) + g_{n-1}x^{n-v} \\ &= X^T \cdot (0, g_0, \ldots, g_{n-2})^T + g_{n-1}\left(x^{p-v} + x^{q-v} + x^{r-v} + x^{-v}\right), \end{aligned} \tag{8}$$

where $0 \le j \le n-2$.

In order to represent the SPB coordinate column vectors of elements x^{p-v}, x^{q-v}, x^{r-v} and x^{-v} in the above equation, we introduce notation

$$\vec{e}_v = (e_0, \ldots, e_v, \ldots, e_{n-1}) \tag{9}$$

to represent a unit row vector, where $e_v = 1$ and $e_i = 0$ for all $i \neq v$. For example, $\vec{e}_1 = (0, 1, 0, \ldots, 0)$. Thus the SPB coordinate column vector of element x^{-v} is $(\vec{e}_0)^T$ because $x^{-v} = (x^{-v}, x^{-v+1}, \ldots, x^{n-v-1}) \cdot (1, 0, \ldots, 0)^T$. Similarly, the SPB coordinate column vectors of elements x^{p-v}, x^{q-v} and x^{r-v} are $(\vec{e}_p)^T$, $(\vec{e}_q)^T$ and $(\vec{e}_r)^T$ respectively.

Therefore, we can obtain the following SPB coordinate column vector of element xg from (8):

$$M_{*,j+1} = (0, g_0, \ldots, g_{n-2})^T + g_{n-1} \cdot (\vec{e}_0 + \vec{e}_r + \vec{e}_q + \vec{e}_p)^T . \tag{10}$$

Comparing column vectors $(0, g_0, \ldots, g_{n-2})^T$ in (10) to $M_{*,j} = (g_0, g_1, \ldots, g_{n-1})^T$ in (7), we see that the former is obtained by shifting the later down once and then filling a 0 in the 0-th position. In the following, we will use a down arrow to denote this transformation, i.e., $(0, g_0, \ldots, g_{n-2})^T = (M_{*,j} \downarrow 1)$. Similarly, we will use left and right arrows to denote left and right shifts of a row vector respectively. For example, $(M_{i,*} \rightarrow 1)$ denotes right shift of row vector $M_{i,*}$ once and then filling a 0 in the 0-th position. Using these notations, equation (10) can be rewritten as

$$M_{*,j+1} = (M_{*,j} \downarrow 1) + g_{n-1} \cdot (\vec{e}_0 + \vec{e}_r + \vec{e}_q + \vec{e}_p)^T . \tag{11}$$

In order to prove that $T = HM$ in (6) is a Toeplitz matrix, i.e., $T_{i,j} = T_{i+1,j+1}$ for $0 \le i, j \le n-2$, we first analyse the structure of the proposed transformation matrix H in (6).

Matrix H can be split into two parts: the upper $(n-q) \times n$ submatrix $\left(\mathbf{0}_{(n-q)\times q}, \bar{U}\right)$ and the lower $q \times n$ submatrix $\left(\bar{L}, \mathbf{0}_{q\times(n-q)}\right)$. Therefore, the matrix product $T = HM$ is equal to

$$T = HM = \begin{pmatrix} \left(\mathbf{0}_{(n-q)\times q}, \bar{U}\right) \cdot M \\ \left(\bar{L}, \mathbf{0}_{q\times(n-q)}\right) \cdot M \end{pmatrix}_{n\times n},$$

and matrix T is a Toeplitz matrix if we can prove the following 3 claims:

1) the upper $(n-q)\times n$ submatrix $\left(\mathbf{0}_{(n-q)\times q}, \bar{U}\right)\cdot M$ of T is an $(n-q)\times n$ Toeplitz matrix;
2) the lower $q\times n$ submatrix $\left(\bar{L}, \mathbf{0}_{q\times(n-q)}\right)\cdot M$ of T is a $q\times n$ Toeplitz matrix;
3) The last row of $\left(\mathbf{0}_{(n-q)\times q}, \bar{U}\right)\cdot M$ and the first row of $\left(\bar{L}, \mathbf{0}_{q\times(n-q)}\right)\cdot M$, which are two succesive rows of matrix T, satify the definition of a Toeplitz matrix.

Now we prove equation $T_{i,j} = T_{i+1,j+1}$ for $0 \le i, j \le n-2$ by showing that the above 3 claims are true.

1) CASE $0 \le i \le n-q-2$:

   This case corresponds to claim 1. We consider the first row $H_{0,*}$ of H, which is also the first row of $\left(\mathbf{0}_{(n-q)\times q}, \bar{U}\right)$. By the definition of matrix $\bar{U} = \sum_{k=0}^{k_U} U^{k(n-p)}_{(n-q)\times(n-q)}$ in (6), where upper shift matrix $U^k_{(n-q)\times(n-q)} = (\delta_{i+k,j})_{(n-q)\times(n-q)}$ and $k_U = \left\lceil \frac{n-q}{n-p} \right\rceil - 1$, we know that element 1s in $H_{0,*}$ appear only at positions $q + k(n-p)$, where $0 \le k \le k_U$. Therefore, using notation $\vec{e}_v$ defined in (9), we may rewrite the first row $H_{0,*}$ of H as follows:

$$H_{0,*} = \sum\nolimits_{k=0}^{k_U} \vec{e}_{q+k(n-p)}.$$

   It is clear that matrix $\bar{U}$ is a Toeplitz matrix, for the summation of two Toeplitz matrices is still a Toeplitz matrix. Thus we have

$$H_{i+1,*} = (H_{i,*} \to 1) \tag{12}$$

   and

$$H_{i,*} = (H_{0,*} \to i) = \sum\nolimits_{k=0}^{\hat{k}} \vec{e}_{i+q+k(n-p)}, \tag{13}$$

   where $\hat{k} = \left\lceil \frac{n-q-i}{n-p} \right\rceil - 1$. The reason that $\hat{k}$ is defined in this way is that subscript $i+q+k(n-p)$ in (13) must be less than n, i.e., $i+q+k(n-p) < n$. Thus we have $k < \frac{n-q-i}{n-p}$, and the maximal value $\hat{k}$ of integer k is $\hat{k} = \left\lceil \frac{n-q-i}{n-p} \right\rceil - 1$.

   Equation (13) shows that elements 1s in $H_{i,*}$ appear only at positions $i+q+k(n-p)$, where $0 \le k \le \hat{k}$. By (13) and the definition $M_{*,j} = (g_0, g_1, \ldots, g_{n-1})^T$ in (7), element $T_{i,j}$ of matrix $T = HM$ can be expressed as

$$T_{i,j} = H_{i,*}\cdot M_{*,j} = \sum\nolimits_{k=0}^{\hat{k}} \vec{e}_{i+q+k(n-p)}\cdot (g_0, g_1, \ldots, g_{n-1})^T = \sum_{k=0}^{\hat{k}} g_{i+q+k(n-p)}. \tag{14}$$

   By (12) and the expression of $M_{*,j+1}$ in (11), we know that element $T_{i+1,j+1}$ is

$$\begin{aligned} T_{i+1,j+1} &= H_{i+1,*}\cdot M_{*,j+1} = H_{i+1,*}\cdot\left[(M_{*,j}\downarrow 1) + g_{n-1}\left(\vec{e}_0+\vec{e}_r+\vec{e}_q+\vec{e}_p\right)^T\right] \\ &= (H_{i,*}\to 1)\cdot(M_{*,j}\downarrow 1) + g_{n-1}\left[H_{i+1,*}\cdot\left(\vec{e}_0+\vec{e}_r+\vec{e}_q+\vec{e}_p\right)^T\right] \end{aligned} \tag{15}$$

We now prove equation $T_{i,j} = T_{i+1,j+1}$ according to the following two subcases.

a) SUBCASE The last element of $H_{i,*}$ is 1, i.e., $H_{i,n-1} = 1$:

We need to compute the two inner products in (15). Because the last element of $H_{i,*}$ is 1 in this subcase and this 1 will be discarded in vector $(H_{i,*} \to 1)$, only the last term $g_{i+q+\hat{k}(n-p)}$ in (14) will not appear in the expression of the first inner product $(H_{i,*} \to 1) \cdot (M_{*,j} \downarrow 1)$. Thus, by (14), we have

$$(H_{i,*} \to 1) \cdot (M_{*,j} \downarrow 1) = \sum_{k=0}^{\hat{k}-1} g_{i+q+k(n-p)}. \tag{16}$$

Before computing the second inner product, we first derive the expression of $H_{i+1,*}$. By (12), we know that $H_{i+1,*}$ is obtained by right shifting of row vector $H_{i,*}$ once. In this subcase, the last element of $H_{i,*}$ is 1. Therefore, the number of 1s in $H_{i+1,*}$ is 1 less than that in $H_{i,*}$. By (12) and the expression of $H_{i,*}$ in (13), we can get the following expression of $H_{i+1,*}$

$$H_{i+1,*} = (H_{i,*} \to 1) = \sum\nolimits_{k=0}^{\hat{k}-1} \vec{e}_{(i+1)+q+k(n-p)}. \tag{17}$$

The minimal value of subscript $(i+1)+q+k(n-p)$ in (17) is $(i+1)+q$ when $k=0$, which is greater than q. By the definition of $\vec{e}_i$, we know that $\vec{e}_i \cdot (\vec{e}_j)^T = \delta_{i,j}$, where $\delta_{i,j}$ is the Kronecker delta symbol. Thus we have

$$H_{i+1,*} \cdot (\vec{e}_0 + \vec{e}_r + \vec{e}_q)^T = \sum\nolimits_{k=0}^{\hat{k}-1} \vec{e}_{(i+1)+q+k(n-p)} \cdot (\vec{e}_0 + \vec{e}_r + \vec{e}_q)^T = 0. \tag{18}$$

In this subcase, the last element $H_{i,n-1}$ of $H_{i,*}$ is 1. This means that the position of the last 1 in $H_{i,*}$ is $n-1$. Thus by the expression of $H_{i,*}$ in (13), we have

$$i + q + \hat{k}\,(n-p) = n-1. \tag{19}$$

This equation can be transformed to:

$$(i+1) + q + (\hat{k}-1)(n-p) = p.$$

The maximal value of subscript $(i+1)+q+k(n-p)$ in (17) is $(i+1)+q+(\hat{k}-1)(n-p)$ when $k = \hat{k}-1$, and it is equal to p by the above equation. Thus we have

$$\vec{e}_{(i+1)+q+(\hat{k}-1)(n-p)} = \vec{e}_p$$

and, by (17), inner product $H_{i+1,*} \cdot (\vec{e}_p)^T$ equals to

$$\begin{aligned} H_{i+1,*} \cdot (\vec{e}_p)^T &= \left(\sum_{k=0}^{\hat{k}-1} \vec{e}_{(i+1)+q+k(n-p)} \right) \cdot (\vec{e}_p)^T \\ &= \left(\sum_{k=0}^{\hat{k}-2} \vec{e}_{(i+1)+q+k(n-p)} \right) \cdot (\vec{e}_p)^T + (\vec{e}_{(i+1)+q+(\hat{k}-1)(n-p)}) \cdot (\vec{e}_p)^T \\ &= 0 + (\vec{e}_p) \cdot (\vec{e}_p)^T = 1. \end{aligned} \tag{20}$$

Based on (18) and (20), we see that the value of the second inner product in (15) is

$$H_{i+1,*} \cdot (\vec{e}_0 + \vec{e}_r + \vec{e}_q + \vec{e}_p)^T = \left[H_{i+1,*} \cdot (\vec{e}_0 + \vec{e}_r + \vec{e}_q)^T \right] + \left[H_{i+1,*} \cdot (\vec{e}_p)^T \right] = 0 + 1 = 1.$$

We know that $g_{n-1} = g_{i+q+\hat{k}(n-p)}$ by (19). Thus, by (16), the value of $T_{i+1,j+1}$ in (15) is equal to

$$\begin{aligned} T_{i+1,j+1} &= (H_{i,*} \to 1) \cdot (M_{*,j} \downarrow 1) + g_{n-1} \left[H_{i+1,*} \cdot (\vec{e}_0 + \vec{e}_r + \vec{e}_q + \vec{e}_p)^T \right] \\ &= \left[\sum_{k=0}^{\hat{k}-1} g_{i+q+k(n-p)} \right] + g_{n-1} \cdot 1 \\ &= \left[\sum_{k=0}^{\hat{k}-1} g_{i+q+k(n-p)} \right] + g_{i+q+\hat{k}(n-p)} \\ &= \sum_{k=0}^{\hat{k}} g_{i+q+k(n-p)}, \end{aligned}$$

which is equal to the value of $T_{i,j}$ in (14).

b) SUBCASE The last element of $H_{i,*}$ is 0, i.e., $H_{i,n-1} = 0$:

We also compute the two inner products in (15) one by one. Since the last element of $H_{i,*}$ is 0, it is clear that the first inner product, i.e., $(H_{i,*} \to 1) \cdot (M_{*,j} \downarrow 1)$, equals to inner product $(H_{i,*}) \cdot (M_{*,j}) = T_{i,j}$. Thus we need only to show that the second inner product in (15) is 0. Because the last element of row vector $H_{i,*}$ is 0 in this subcase and $H_{i+1,*} = (H_{i,*} \to 1)$, by the expression of $H_{i,*}$ in (13), we get the following expression of $H_{i+1,*}$

$$H_{i+1,*} = (H_{i,*} \to 1) = \sum\nolimits_{k=0}^{\hat{k}} \vec{e}_{(i+1)+q+k(n-p)}. \tag{21}$$

The minimal value of subscript $(i+1)+q+k(n-p)$ in (21) is $(i+1)+q$ when $k=0$, which is also greater than q. By the definition of $\vec{e}_i$, we have

$$H_{i+1,*} \cdot (\vec{e}_0 + \vec{e}_r + \vec{e}_q)^T = 0.$$

Therefore the second inner product $H_{i+1,*} \cdot (\vec{e}_0 + \vec{e}_r + \vec{e}_q + \vec{e}_p)^T$ in (15) is 0 if we can prove that inner product $H_{i+1,*} \cdot (\vec{e}_p)^T = 0$.

In this subcase, the last element $H_{i,n-1}$ of $H_{i,*}$ is 0. This condition means that the position of the last 1 in $H_{i,*}$ is less than $(n-1)$. Thus by the expression of $H_{i,*}$ in (13), we have

$$i + q + \hat{k}\,(n-p) < n-1,$$

and it is equivalent to

$$(i+1) + q + (\hat{k}-1)(n-p) < p. \tag{22}$$

Moreover, this condition also means that if we set $k = \hat{k}+1$ in (13), then the value of subscript $i + q + k(n-p)$ will exceed $(n-1)$, i.e.,

$$i + q + (\hat{k}+1)\,(n-p) > n-1,$$

which is equivalent to

$$(i+1) + q + \hat{k}(n-p) > p.$$

Combining this inequality with (22) together, we have the following chain of inequalities:

$$(i+1) + q + \hat{k}(n-p) > p > (i+1) + q + (\hat{k}-1)(n-p).$$

By (21), there are $\hat{k}+1$ element 1s in vector $H_{i+1,*}$, and any two adjacent 1s have the same fixed interval $n-p$. The last two adjacent 1s appear at positions $(i+1)+q+(\hat{k}-1)(n-p)$ and $(i+1)+q+\hat{k}(n-p)$ respectively. Thus, the above chain of inequalities shows that the p-th element in $H_{i+1,*}$, i.e., $H_{i+1,p}$ must be 0. Thus we have

$$H_{i+1,*} \cdot (\vec{e}_p)^T = H_{i+1,p} \cdot 1 = 0.$$

2) CASE $n - q \le i < n-1$:

This case corresponds to claim 2. First we consider the last row $H_{n-1,*}$ of H, which is also the last row of $\left(\bar{L}, \mathbf{0}_{q\times(n-q)}\right)$. By the definition of matrix $\bar{L} = \sum_{k=0}^{k_L} L_{q\times q}^{kr}$ in (6), where $L_{q\times q}^{k} = (\delta_{i,j+k})_{q\times q}$ and $k_L = \left\lceil \frac{q}{r} \right\rceil - 1$, we know that element 1s of $H_{n-1,*}$ appear only at positions $q-1-kr$, where $0 \le k \le k_L$. Therefore, we obtain the following expression of the last row $H_{n-1,*}$:

$$H_{n-1,*} = \sum\nolimits_{k=0}^{k_L} \vec{e}_{q-1-kr}. \tag{23}$$

Since matrix $\left(\bar{L}, \mathbf{0}_{q\times(n-q)}\right)$ is a Toeplitz matrix, we have

$$H_{i,*} = (H_{i+1,*} \leftarrow 1) = (H_{n-1,*} \leftarrow (n-1-i))\,. \tag{24}$$

We now prove that inner product $H_{i+1,*} \cdot (\vec{e}_0 + \vec{e}_r)^T$ is 0 by considering the distribution pattern of element 1s in row $H_{i+1,*}$. The expression of the last row in (23) reveals that element 1s are distributed evenly at a fixed interval of r. The last 1 of $H_{n-1,*}$ is at position $q-1$ when $k=0$. We claim that the position of the first 1 of $H_{n-1,*}$ is less than r. The position of the first 1 is $q-1-k_L r$ when $k=k_L$, where $k_L = \lceil \frac{q}{r} \rceil - 1$ is define in (6). Equation $k_L = \lceil \frac{q}{r} \rceil - 1$ implies that $k_L \geq \frac{q}{r} - 1$, thus we have $q-1-k_L r \leq q-1-(\frac{q}{r}-1)r = r-1$. Therefore, the claim is true. Based on this distribution pattern and the fact that row $H_{i+1,*}$ is obtained by shifting the last row $H_{n-1,*}$ left $(n-2-i)$ times (see (24)), we conclude that the two elements $H_{i+1,0}$ and $H_{i+1,r}$ are equal. Therefore, we have

$$H_{i+1,*} \cdot (\vec{e}_0 + \vec{e}_r)^T = H_{i+1,0} + H_{i+1,r} = 0. \tag{25}$$

We note that $1+1=0+0=0$ in fields of characteristic 2.

Row $H_{i+1,*}$ is a row of the $q \times n$ submatrix $\left(\bar{L}, \mathbf{0}_{q\times(n-q)}\right)$, and its last $(n-q)$ elements are all 0s. Thus we have

$$H_{i+1,*} \cdot (\vec{e}_q + \vec{e}_p)^T = 0.$$

This equation and (25) imply that

$$H_{i+1,*} \cdot (\vec{e}_0 + \vec{e}_r + \vec{e}_q + \vec{e}_p)^T = H_{i+1,*} \cdot (\vec{e}_0 + \vec{e}_r)^T + H_{i+1,*} \cdot (\vec{e}_q + \vec{e}_p)^T = 0 + 0 = 0. \tag{26}$$

We now prove equation $T_{i,j} = T_{i+1,j+1}$ according to the following two subcases.

a) SUBCASE The first element of $H_{i+1,*}$ is 1, i.e., $H_{i+1,0} = 1$:

The first element of $H_{i+1,*}$ is 1 in this subcase. Because $H_{i,*} = (H_{i+1,*} \leftarrow 1)$, we know that this first 1 of row vector $H_{i+1,*}$ will be discarded in $H_{i,*}$. Thus, we have

$$H_{i+1,*} = (H_{i,*} \rightarrow 1) + \vec{e}_0. \tag{27}$$

Thus by (26), (27) and the expression $M_{*,j+1}$ in (11), we obtain

$$\begin{aligned} T_{i+1,j+1} &= H_{i+1,*} \cdot M_{*,j+1} \\ &= H_{i+1,*} \cdot \left[(M_{*,j} \downarrow 1) + g_{n-1} \left(\vec{e}_0 + \vec{e}_r + \vec{e}_q + \vec{e}_p\right)^T \right] \\ &= \left[(H_{i,*} \rightarrow 1) + \vec{e}_0 \right] \cdot (M_{*,j} \downarrow 1) + g_{n-1} \left[H_{i+1,*} \cdot \left(\vec{e}_0 + \vec{e}_r + \vec{e}_q + \vec{e}_p\right)^T \right] \\ &= (H_{i,*} \rightarrow 1) \cdot (M_{*,j} \downarrow 1) + \vec{e}_0 \cdot (M_{*,j} \downarrow 1) + 0 \end{aligned} \tag{28}$$

Because the first element in $(M_{*,j} \downarrow 1)$ is 0, we know that $\vec{e}_0 \cdot (M_{*,j} \downarrow 1)$ equals to 0. Furthermore, because row $H_{i,*}$ is a row of matrix $\left(\bar{L}, \mathbf{0}_{q\times(n-q)}\right)$, we know the last $(n-q)$

elements in $H_{i,*}$ are all 0. Thus, inner product $(H_{i,*} \to 1)\cdot(M_{*,j} \downarrow 1)$ is equal to inner product $T_{i,j} = (H_{i,*}) \cdot (M_{*,j})$. Thus equation (28) can be written as $T_{i+1,j+1} = T_{i,j} + 0 + 0 = T_{i,j}$.

b) SUBCASE The first element of $H_{i+1,*}$ is 0, i.e., $H_{i+1,0} = 0$:

As we have just discussed in the above paragraph, inner product $T_{i,j} = H_{i,*} \cdot M_{*,j}$ equals to

$$T_{i,j} = H_{i,*} \cdot M_{*,j} = (H_{i,*} \to 1) \cdot (M_{*,j} \downarrow 1). \tag{29}$$

Thus by (26) and (29), we have

$$\begin{aligned} T_{i+1,j+1} &= H_{i+1,*} \cdot M_{*,j+1} = H_{i+1,*} \cdot \left[(M_{*,j} \downarrow 1) + g_{n-1}\left(\vec{e}_0 + \vec{e}_r + \vec{e}_q + \vec{e}_p\right)^T\right] \\ &= (H_{i,*} \to 1) \cdot (M_{*,j} \downarrow 1) + g_{n-1}\left[H_{i+1,*} \cdot \left(\vec{e}_0 + \vec{e}_r + \vec{e}_q + \vec{e}_p\right)^T\right] \\ &= H_{i,*} \cdot M_{*,j} + 0 \\ &= T_{i,j}. \end{aligned}$$

3) CASE $i = n - q - 1$:

This case corresponds to claim 3. The expression of $T_{i,j}$ is $T_{i,j} = H_{i,*} \cdot M_{*,j} = H_{n-q-1,*} \cdot M_{*,j}$, where $H_{n-q-1,*}$ is the last row of submatrix $\left(\mathbf{0}_{(n-q)\times q}, \bar{U}\right)$. We first show that $H_{n-q-1,*} = \vec{e}_{n-1}$. The expression of $\bar{U}$ in (6) can be rewritten as $\bar{U} = \sum_{k=0}^{k_U} U^{k(n-p)}_{(n-q)\times(n-q)} = U^0_{(n-q)\times(n-q)} + \sum_{k=1}^{k_U} U^{k(n-p)}_{(n-q)\times(n-q)}$, where $k_U = \left\lceil \frac{n-q}{n-p} \right\rceil - 1 \geq 1$. It is clear that $U^0_{(n-q)\times(n-q)}$ is the $(n-q) \times (n-q)$ identity matrix and the last row of $\sum_{k=1}^{k_U} U^{k(n-p)}_{(n-q)\times(n-q)}$ is the zero vector $(0, 0, \ldots, 0)$. Thus the last element $H_{n-q-1,n-1}$ is the only 1 in row $H_{n-q-1,*}$, i.e.,

$$H_{n-q-1,*} = \vec{e}_{n-1}. \tag{30}$$

Therefore, element $T_{i,j} = H_{n-q-1,*} \cdot M_{*,j} = \vec{e}_{n-1} \cdot M_{*,j}$ is equal to the $(n-1)$-th element in the column vector $M_{*,j}$, which is g_{n-1} by (7).

Now we show that $T_{i+1,j+1}$ is also g_{n-1}. Similar to the proof of (30), by the definition of $\bar{L}$ in (6) we can obtain that $H_{n-q,*} = \vec{e}_0$. Therefore, Element $T_{i+1,j+1} = H_{n-q,*} \cdot M_{*,j+1} = \vec{e}_0 \cdot M_{*,j+1}$ is equal to the 0-th element in the column vector $M_{*,j+1}$, which is also g_{n-1} by (11).

Thus, we conclude that $T_{i,j} = g_{n-1} = T_{i+1,j+1}$ for this case.

In summary, the three claims are all true. Therefore, T is a Toeplitz matrix. ■

We have proved that matrix

$$H = \begin{pmatrix} \mathbf{0}_{(n-q)\times q} & \bar{U} \\ \bar{L} & \mathbf{0}_{q\times(n-q)} \end{pmatrix}_{n\times n}$$

can transform the Mastrovito matrix M into a Toeplitz matrix T. Because H is a block matrix, its inverse matrix can be derived using the following lemma.

Lemma 2.2: Let integers $m = n - q$ and $d = n - p$. Then the inverse matrix of $\bar{U} = \sum_{i=0}^{\lceil \frac{m}{d} \rceil - 1} U_{m\times m}^{i\cdot d}$ is $\bar{U}^{-1} = I_{m\times m} + U_{m\times m}^{d}$, and the inverse matrix of $\bar{L} = \sum_{i=0}^{\lceil \frac{q}{r} \rceil - 1} L_{q\times q}^{i\cdot r}$ is $\bar{L}^{-1} = I_{q\times q} + L_{q\times q}^{r}$.

Proof:

Because $\lceil \frac{m}{d} \rceil d \geq m$, by the definition of upper shift matrix $U_{m\times m}^{k}$ in (5), we have

$$U_{m\times m}^{\lceil \frac{m}{d} \rceil d} = 0_{m\times m}. \tag{31}$$

Here $U_{m\times m}^{k}$ is not merely a symbol, in fact, it is equal to the k-th power of matrix $U_{m\times m}^{1}$, i.e., $U_{m\times m}^{k} = (U_{m\times m}^{1})^{k}$. Therefore, it is easy to prove that

$$U_{m\times m}^{i\cdot d} \cdot U_{m\times m}^{d} = U_{m\times m}^{(i+1)\cdot d},$$

where $0 \leq i \leq \lceil \frac{m}{d} \rceil - 1$.

By this equation and (31), we have

$$\begin{aligned}
\bar{U} \cdot \bar{U}^{-1} &= \left(\sum_{i=0}^{\lceil \frac{m}{d} \rceil - 1} U_{m\times m}^{i\cdot d} \right) \left(I_{m\times m} + U_{m\times m}^{d} \right) \\
&= \sum_{i=0}^{\lceil \frac{m}{d} \rceil - 1} U_{m\times m}^{i\cdot d} + \sum_{i=1}^{\lceil \frac{m}{d} \rceil} U_{m\times m}^{i\cdot d} \\
&= \left[U_{m\times m}^{0} + \sum_{i=1}^{\lceil \frac{m}{d} \rceil - 1} U_{m\times m}^{i\cdot d} \right] + \left[\sum_{i=1}^{\lceil \frac{m}{d} \rceil - 1} U_{m\times m}^{i\cdot d} + U_{m\times m}^{\lceil \frac{m}{d} \rceil d} \right] \\
&= U_{m\times m}^{0} + \left[\sum_{i=1}^{\lceil \frac{m}{d} \rceil - 1} U_{m\times m}^{i\cdot d} + \sum_{i=1}^{\lceil \frac{m}{d} \rceil - 1} U_{m\times m}^{i\cdot d} \right] + U_{m\times m}^{\lceil \frac{m}{d} \rceil d} \\
&= I_{m\times m} + 0_{m\times m} + U_{m\times m}^{\lceil \frac{m}{d} \rceil d} \\
&= I_{m\times m}.
\end{aligned}$$

Therefore the first part of the lemma is true.

Toeplitz matrix $L_{q\times q}^{k}$ is a lower shift matrix, and its transpose $(L_{q\times q}^{k})^{T}$ is an upper shift matrix. By the equation $\bar{L}^{-1} = \left(\left(\bar{L}^{T} \right)^{-1} \right)^{T}$ and the above result, the second part of the lemma is true. ■

The above lemma implies the following result:

Proposition 2.3: The inverse matrix of H defined in (6) is

$$H^{-1} = \begin{pmatrix} 0 & \bar{L}^{-1} \\ \bar{U}^{-1} & 0 \end{pmatrix}_{n\times n} = \begin{pmatrix} 0 & I_{q\times q} + L^{r}_{q\times q} \\ I_{(n-q)\times(n-q)} + U^{n-p}_{(n-q)\times(n-q)} & 0 \end{pmatrix}_{n\times n}. \tag{32}$$

C. Two Examples

The first example is the transformation matrix for a special irreducible pentanomial $f(u) = u^n + u^{p+1} + u^p + u^{p-1} + 1$ $(1 < p < n-1)$. We have verified that H is the same as the transformation matrix presented in reference [15].

The second example demonstrates the transformation matrix H and its inverse H^{-1}. Let $X = \{x^{-6}, x^{-5}, \ldots, x^0\}$ be a shifted polynomial basis of $GF(2^7)$ generated by irreducible pentanomial $f(u) = u^7+u^6+u^4+u^2+1$. Matrices H, H^{-1}, M and T are as follows:

$$H = \begin{pmatrix} 0&0&0&0&1&1&1 \\ 0&0&0&0&0&1&1 \\ 0&0&0&0&0&0&1 \\ 1&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0 \\ 1&0&1&0&0&0&0 \\ 0&1&0&1&0&0&0 \end{pmatrix}, H^{-1} = \begin{pmatrix} 0&0&0&1&0&0&0 \\ 0&0&0&0&1&0&0 \\ 0&0&0&1&0&1&0 \\ 0&0&0&0&1&0&1 \\ 1&1&0&0&0&0&0 \\ 0&1&1&0&0&0&0 \\ 0&0&1&0&0&0&0 \end{pmatrix},$$

$$M = \begin{pmatrix} b_4+b_6 & b_3+b_5 & b_2+b_4 & b_1+b_3 & b_0+b_2 & b_1 & b_0 \\ b_0+b_5 & b_4+b_6 & b_3+b_5 & b_2+b_4 & b_1+b_3 & b_0+b_2 & b_1 \\ b_0+b_1+b_4 & b_0+b_3 & b_2+b_6 & b_1+b_5 & b_0+b_4 & b_3 & b_2 \\ b_0+b_1+b_2+b_5 & b_0+b_1+b_4 & b_0+b_3 & b_2+b_6 & b_1+b_5 & b_0+b_4 & b_3 \\ b_1+b_2+b_3+b_4 & b_0+b_1+b_2+b_3 & b_0+b_1+b_2 & b_0+b_1 & b_0+b_6 & b_5 & b_4 \\ b_2+b_3+b_4+b_5 & b_1+b_2+b_3+b_4 & b_0+b_1+b_2+b_3 & b_0+b_1+b_2 & b_0+b_1 & b_0+b_6 & b_5 \\ b_3+b_5 & b_2+b_4 & b_1+b_3 & b_0+b_2 & b_1 & b_0 & b_6 \end{pmatrix},$$

and

$$T = \begin{pmatrix} b_1+b_3 & b_0+b_2 & b_1 & b_0 & b_6 & b_5+b_6 & b_4+b_5+b_6 \\ b_2+b_4 & b_1+b_3 & b_0+b_2 & b_1 & b_0 & b_6 & b_5+b_6 \\ b_3+b_5 & b_2+b_4 & b_1+b_3 & b_0+b_2 & b_1 & b_0 & b_6 \\ b_4+b_6 & b_3+b_5 & b_2+b_4 & b_1+b_3 & b_0+b_2 & b_1 & b_0 \\ b_0+b_5 & b_4+b_6 & b_3+b_5 & b_2+b_4 & b_1+b_3 & b_0+b_2 & b_1 \\ b_0+b_1+b_6 & b_0+b_5 & b_4+b_6 & b_3+b_5 & b_2+b_4 & b_1+b_3 & b_0+b_2 \\ b_1+b_2 & b_0+b_1+b_6 & b_0+b_5 & b_4+b_6 & b_3+b_5 & b_2+b_4 & b_1+b_3 \end{pmatrix}.$$

III. Conclusion

In this paper, we have first presented a matrix H to transform the Mastrovito matrix M into a Toeplitz matrix T for an arbitrary irreducible pentanomial $f(u) = u^n + u^p + u^q + u^r + 1$ $(n > p > q > r > 1)$ when $GF(2^n)$ elements are represented using a shifted polynomial basis. This makes it possible for the MVP approach to be used for all practical $GF(2^n)$s.

In order to derive the exact explicit formulae for the complexities of the matrix transformation step, we had examined expressions for elements of Toeplitz matrix T, but no straightforward regularity was found among these expressions. Moreover, there are common subexpressions in the Toeplitz matrix T, e.g., $b_5 + b_6$ appears in both $T_{0,5}$ and $T_{0,6}$ in the above example. These factors make it hard to obtain our desired explicit complexity formulae. Fortunately, it is clear that the number of XOR gates used in this step is linear to n, which is much smaller than that in the TMVP step. Furthermore, for a given finite field $GF(2^n)$ in some practical application, we can test different irreducible pentanomials and select a proper $f(u)$ to construct subquadratic multipliers.

References

[1] A. Karatsuba and Y. Ofman, "Multiplication of multidigit numbers on automata," *Sov. Phys.-Dokl. (English translation)*, vol. 7, pp. 595–196, 1963.

[2] V. Afanasyev, "Complexity of VLSI implementation of finite field arithmetic," in *Proc. II. Intern. Workshop on Algebraic and Combinatorial Coding Theory*, vol. 2, 1990, pp. 6–7.

[3] C. Paar, "A new architecture for a parallel finite field multiplier with low complexity based on composite fields," *IEEE Transactions on Computers*, vol. 45, no. 7, pp. 856–861, 1996.

[4] M. Elia, M. Leone, and C. Visentin, "Low complexity bit-parallel multipliers for $GF(2^m)$ with generator polynomial $x^m + x^k + 1$," *IEE Electronics Letters*, vol. 35, no. 7, pp. 551–552, 1999.

[5] C. Grabbe, M. Bednara, J. Teich, J. Von Zur Gathen, and J. Shokrollahi, "FPGA designs of parallel high performance $GF(2^{233})$ multipliers," in *Proc. Int'l Symp. Circuits and Systems (ISCAS 03)*, vol. 2, 2003, pp. 268–271.

[6] F. Rodríguez-Henríquez and Ç. K. Koç, "On fully parallel Karatsuba multipliers for $GF(2^m)$," in *Computer Science and Technology*. ACTA Press, 2003, pp. 405–410.

[7] B. Sunar, "A generalized method for constructing subquadratic complexity $GF(2^k)$ multipliers," *IEEE Transactions on Computers*, vol. 53, no. 9, pp. 1097–1105, 2004.

[8] N. S. Chang, C. H. Kim, Y. H. Park, and J. Lim, "A non-redundant and efficient architecture for Karatsuba-Ofman algorithm," in *8th International Conf. on Information Security (ISC 2005), LNCS 3650*, 2005, pp. 288–299.

[9] J. von zur Gathen and J. Shokrollahi, "Efficient FPGA-based karatsuba multipliers for polynomials over $\mathbb{F}_2$," in *Selected Areas in Cryptography*. Springer, 2006, pp. 359–369.

[10] H. Fan, J. Sun, M.Gu, and K.-Y. Lam, "Overlap-free Karatsuba-Ofman polynomial multiplication algorithms," *IET Information Security*, vol. 4, no. 1, pp. 8–14, 2010.

[11] D. J. Bernstein, "Batch binary edwards," in *Proc. CRYPTO 2009, LNCS-5677*, 2009, pp. 317–336.

[12] G. Zhou and H. Michalik, "Comments on "a new architecture for a parallel finite field multiplier with low complexity based on composite field"," *IEEE Transactions on Computers*, vol. 59, no. 7, pp. 1007–1008, 2010.

[13] C. Negre, "Efficient binary polynomial multiplication based on optimized Karatsuba reconstruction," in *Technical Report hal-00724778, Team DALI/LIRMM, on Hyper Articles en Ligne (HAL)*, 2012.

[14] ——, "Improved three-way split approach for binary polynomial multiplication based on optimized reconstruction," in *Technical Report hal-00788646, Team DALI/LIRMM, on Hyper Articles en Ligne (HAL)*, 2013.

[15] H. Fan and M. A. Hasan, "A new approach to subquadratic space complexity parallel multipliers for extended binary fields," *IEEE Transactions on Computers*, vol. 56, no. 2, pp. 224–233, 2007.

[16] H. Fan and Y. Dai, "Fast bit-parallel $GF(2^n)$ multiplier for all trinomials," *IEEE Transactions on Computers*, vol. 54, no. 4, pp. 485–490, 2005.

[17] M. A. Hasan and V. K. Bhargava, "Division and bit-serial multiplication over $GF(q^m)$," *IEE Proceedings-E, Computers and Digital Techniques*, vol. 139, no. 3, pp. 230–236, May 1992.

[18] ——, "Architecture for low complexity rate-adaptive Reed-Solomon encoder," *IEEE Transactions on Computers*, vol. 44, no. 7, pp. 938–942, July 1995.

[19] H. Fan and M. A. Hasan, "Subquadratic computational complexity schemes for extended binary field multiplication using optimal normal bases," *IEEE Transactions on Computers*, vol. 56, no. 10, pp. 1435–1437, 2007.

[20] M. A. Hasan, "On matrix-vector product based sub-quadratic arithmetic complexity schemes for field multiplication," in *SPIE 6697, 669702*, 2007.

[21] C. Lee, "Low-complexity parallel systolic montgomery multipliers over $GF(2^m)$ using Toeplitz matrix-vector representation," *IEICE Trans. Fund.*, vol. E91-A, pp. 1470–1477, 2008.

[22] M. A. Hasan and C. Negre, "Subquadratic space complexity multiplier for a class of binary fields using Toeplitz matrix approach," in *19th IEEE Symposium on Computer Arithmetic, ARITH 2009*. IEEE, 2009, pp. 67–75.

[23] ——, "Low space complexity multiplication over binary fields with Dickson polynomial representation," *IEEE Transactions on Computers*, vol. 60, no. 4, pp. 602–607, 2011.

[24] C. Lee and C. Chiou, "Scalable Gaussian normal basis multipliers over $GF(2^m)$ using Hankel matrix-vector representation," *J Sign Process Syst*, vol. 69, pp. 197–211, 2012.

[25] M. A. Hasan, N. Meloni, A. H. Namin, and C. Negre, "Block recombination approach for subquadratic space complexity binary field multiplication based on Toeplitz matrix-vector product," *IEEE Transactions on Computers*, vol. 61, no. 2, pp. 151–163, 2012.

[26] M. Cenk, C. Negre, and M. A. Hasan, "Improved three-way split formulas for binary polynomial and Toeplitz matrix vector products," *IEEE Transactions on Computers*, vol. 62, no. 7, pp. 1345–1361, 2013.

[27] J. Pan, R. Azarderakhsh, M. Kermani, C. Lee, W. Lee, C. Chiou, and J. Lin, "Low-latency digit-serial systolic double basis multiplier over $GF(2^m)$ using subquadratic Toeplitz matrix-vector product approach," *IEEE Transactions on Computers accepted*.

[28] J. Adikari, A. Barsoum, M. A. Hasan, A. H. Namin, and C. Negre, "Improved area-time trade-offs for field multiplication using optimal normal bases," *IEEE Transactions on Computers accepted*.

[29] M. A. Hasan and C. Negre, "Multiway splitting method for Toeplitz matrix vector product," *IEEE Transactions on Computers*, vol. 62, no. 7, pp. 1467–1471, 2013.

[30] G. Seroussi, "Table of low-weight binary irreducible polynomials," *HP Labs Technical Reports HPL-98-135*, 1998.