# Fast Bit Parallel Shifted Polynomial Basis Multipliers in $GF(2^n)$

Haining Fan and M. Anwar Hasan *Senior Member, IEEE,*

**Abstract**

A new bit parallel shifted polynomial basis multiplier for $GF(2^n)$ is presented. For some irreducible trinomials, the space complexity of the multiplier matches the best results avaliable in the literture, and its gate delay is equal to $T_A + \lceil \log_2 n \rceil T_X$, where $T_A$ and $T_X$ are the delay of one 2-input AND and XOR gates, respectively. To the best of our knowledge, this is the first time that the gate delay bound $T_A + \lceil \log_2 n \rceil T_X$ is reached. For some irreducible pentanomials, its gate delay is equal to $T_A + (1 + \lceil \log_2 n \rceil)T_X$. NIST has recommended five binary fields for the ECDSA (Elliptic Curve Digital Signature Algorithm) applications: $GF(2^{163})$, $GF(2^{233})$, $GF(2^{283})$, $GF(2^{409})$ and $GF(2^{571})$, but no irreducible trinomials exist for three degrees, viz., 163, 283 and 571. For the three corresponding binary fields, we show that the gate delay of the proposed multiplier is $T_A + (1 + \lceil \log_2 n \rceil)T_X$. This result outperforms the previously known results.

**Index Terms**

Finite field, multiplication, polynomial basis, shifted polynomial basis, irreducible polynomial.

## I. Introduction

Efficient VLSI implementation of high speed multipliers over $GF(2^n)$ is important for some cryptosystems. To this end, several bit parallel polynomial basis (PB) multipliers using low Hamming weight irreducible polynomials, such as trinomials and pentanomials, have been proposed. In [1], it has been shown that irreducible trinomials exist for 5148 values of $n$ in the range $1 < n < 10001$. For each of the other 4851 values of $n$ in the same range, where no such irreducible trinomial of degree $n$ exist, an irreducible pentanomial has been listed. In fact, there is no known value of $n$ for which an irreducible polynomial of weight $w < 6$ does not exist [1]. Therefore, we need only to consider irreducible trinomials and pentanomials for practical purposes.

In hardware, since a two-input XOR (respectively AND) gate can be used to realize an addition (respectively multiplication) operation over the ground field $GF(2)$, the space complexity of bit parallel multipliers in the extension field $GF(2^n)$ is often represented in terms of the total number of XOR and AND gates used. The corresponding time complexity is given in terms of the maximum delay faced by a signal due to these XOR and

Affiliation of authors: Haining Fan and M. Anwar Hasan are with the Department of Electrical and Computer Engineering University of Waterloo, Waterloo, Canada. E-mails: hfan@vlsi.uwaterloo.ca and ahasan@ece.uwaterloo.ca

AND gates. If $T_A$ and $T_X$ correspond to the delay due to one 2-input AND and XOR gates, respectively, then the total delay due to gates can be expressed as $c_A T_A + c_X T_X$, where $c_A$ and $c_X$ are two positive integers. For a given VLSI technology, the values of $c_A$ and $c_X$ can not be easily changed and hence in order to reduce the total gate delay, AND and XOR gates used in the multiplier are carefully organized, for example, XOR gates are often connected in the form of a binary tree. For most of the recently proposed multipliers, $c_A = 1$ and $c_X$ depends on $n$. For the special irreducible trinomials $f(u) = u^n + u^{n/2} + 1$ and $f(u) = u^n + u + 1$, the gate delay of multipliers in [2], [3] and [4] is $T_A + (1 + \lceil \log_2 n \rceil) T_X$. When $n = 2^j + 1$ for some $j > 0$, the gate delay of the multipliers in [5] and [6] is also $T_A + (1 + \lceil \log_2 n \rceil) T_X$. But for the general irreducible trinomial $f(u) = u^n + u^k + 1$ ($n-1$ is not a power of 2, $k \neq 1$ and $2k \neq n$), the gate delay of multipliers in [2]-[6] is $T_A + (2 + \lceil \log_2 n \rceil) T_X$. For the irreducible trinomial $f(u) = u^n + u^k + 1$, the gate delay of the PB multiplier of [11] is $T_A + (1 + \lceil \log_2 (n - 1 + \lceil k/2 \rceil) \rceil)\, T_X$, but it requires more XOR gates for $k > 2$. Gate delays of these irreducible trinomial-based PB multipliers are at least $T_A + (1 + \lceil \log_2 n \rceil) T_X$.

The time complexity of the pentanomial-based multiplier depends on the form of the field generating irreducible pentanomial. Multipliers for special types of the irreducible pentanomials have been proposed in [3], [4], [5] and [13]. Gate delays of these multipliers are at least $T_A + (3 + \lceil \log_2 (n-1) \rceil) T_X$. In [14], a redundant representation is used to design the bit parallel multiplier. Although the space complexity of this multiplier is slightly greater than other architectures, its gate delay is $T_A + \lceil 2 + \log_2 (n+1) \rceil\, T_X$.

In this report, we present a straightforward architecture of a bit parallel multiplier using the shift polynomial basis (SPB). For all irreducible trinomials, the space complexity of the new multiplier matches the best results. The main contribution of the new multiplier is that its gate delay is equal to $T_A + \lceil \log_2 n \rceil\, T_X$ for certain irreducible trinomials. To the best of our knowledge, this is the first time that the gate delay bound $T_A + \lceil \log_2 n \rceil\, T_X$ is achieved. For a special type of the irreducible pentanomials, namely, $f(u) = u^n + u^{v+1} + u^v + u^{v-1} + 1$ ($3 < v < (n-3)/2$), we present a closed form formulae for the multiplier. Please note that this special type of pentanomials have been studied in [13], where the gate delay of the multiplier is $T_A + (3 + \lceil \log_2 n \rceil) T_X$. NIST has recommended five binary fields for the ECDSA (Elliptic Curve Digital Signature Algorithm) applications: $GF(2^{163})$, $GF(2^{233})$, $GF(2^{283})$, $GF(2^{409})$ and $GF(2^{571})$, but no irreducible trinomials exist for three degrees, viz., 163, 283 and 571. For the three corresponding binary fields, we show that the gate delay of the proposed multiplier is $T_A + (1 + \lceil \log_2 n \rceil) T_X$. This result outperforms the previously known results.

The remainder of this report is organized as follows: In Section II, we introduce notations used in the report. The new multipliers for the irreducible trinomials and pentanomials are presented in Section III and IV, respectively. Finally, concluding remarks are made in Section V.

## II. Notations and Preliminaries

Let $f(u)$ be an irreducible polynomial over $GF(2)$ and $GF(2^n) = GF(2)[u]/(f(u))$. A SPB of $GF(2^n)$ over $GF(2)$ is defined as follows [12]:

*Definition 1:* Let $v$ be an integer and the ordered set $M = \{x^i | 0 \leq i \leq m-1\}$ be a polynomial basis of $GF(2^m)$

over $GF(2)$. The ordered set $x^{-v}M := \{x^{i-v} | 0 \leq i \leq m-1\}$ is called a shifted polynomial basis (SPB) with respect to $M$.

In Sections II and III, we assume that $f(u) = u^n + u^k + 1$ ($n > 2$) is an irreducible trinomial over $GF(2)$ and $x$ is a root of $f$. In [12], it is shown that the best values of $v$ are $k$ and $k-1$ when the SPB is used to design parallel multipliers. Given two field elements $A$ and $B$, let $A = (a_0, a_1, ..., a_{n-1})^T = x^{-v} \sum_{i=0}^{n-1} a_i x^i$ and $B = (b_0, b_1, ..., b_{n-1})^T = x^{-v} \sum_{i=0}^{n-1} b_i x^i$ be their SPB representations. In [15], the structures to compute the product of $A$ and $B$ using SPB have been grouped into two types. The type-I multiplier computes the product $C = (c_0, c_1, ..., c_{n-1})^T = x^{-v} \sum_{i=0}^{n-1} c_i x^i$ of $A$ and $B$ using the following two steps.

(i) Perform the conventional polynomial multiplication:

$$S = AB = x^{-2v} \sum_{t=0}^{2n-2} s_t x^t = \sum_{t=-2v}^{2n-2-2v} s_{t+2v} x^t = r_- + r + r_+, \text{ where}$$

$r = \sum_{t=-v}^{n-1-v} s_{t+2v} x^t$, $r_- = \sum_{t=-2v}^{-1-v} s_{t+2v} x^t$, $r_+ = \sum_{t=n-v}^{2(n-1-v)} s_{t+2v} x^t$ and

$$s_t = \sum_{\substack{i+j=t \\ 0 \leq i,j \leq n-1}} a_i b_j = \begin{cases} \sum_{i=0}^{t} a_i b_{t-i} & 0 \leq t \leq n-1 \\ \sum_{i=t+1-n}^{n-1} a_i b_{t-i} & n \leq t \leq 2n-2 \end{cases}. \quad (1)$$

(ii) Reduce $r_+$ and $r_-$ using the following two reduction formulae, respectively:

$$\begin{aligned} x^i &= x^{k+i-n} + x^{i-n}, \text{ where } n - v \leq i \leq 2n-2-2v, \\ x^i &= x^{n+i} + x^{k+i}, \text{ where } -2v \leq i \leq -(v+1). \end{aligned}$$

The reduced results $\widetilde{r}_+$ and $\widetilde{r}_-$ are defined as

$$\begin{aligned} \widetilde{r}_- &= \sum_{t=n-2v}^{n-1-v} s_{t+2v-n} x^t + \sum_{t=k-2v}^{k-1-v} s_{t+2v-k} x^t \text{ and} \\ \widetilde{r}_+ &= \sum_{t=k-v}^{k+n-2-2v} s_{t+2v+n-k} x^t + \sum_{t=-v}^{n-2-2v} s_{t+n+2v} x^t. \end{aligned}$$

The product of $A$ and $B$ is $C = \sum_{i=0}^{n-1} c_i x^{i-v} = x^{-v} \sum_{i=0}^{n-1} c_i x^i = r + \widetilde{r}_- + \widetilde{r}_+$.

The type-II SPB multiplier combines the two steps into a single matrix-vector product, i.e., $C = (c_0, c_1, ..., c_{n-1})^T = Z(a_0, a_1, ..., a_{n-1})^T$, where the $n \times n$ matrix $Z = (z_{i,j})_{0 \leq i,j \leq n-1}$ is called the Mastrovito matrix and it depends on both $B$ and $f$. In order to compute $C = Z(a_0, a_1, ..., a_{n-1})^T$, $Z$ is computed first, then $c_t (0 \leq t \leq n-1)$ is computed in a vector inner-product module whose output is $c_t = \sum_{i=0}^{n-1} a_i z_{t,i}$.

## III. SPB Multiplier for Irreducible Trinomials

### A. Architectures

We now present a straightforward design of the SPB parallel multiplier. Instead of computing $c_t (0 \leq t \leq n-1)$ by a vector inner-product module, the new multiplier calculates $c_t$ using a binary XOR tree of the smallest height.

In [12], the detailed design of the type-II SPB multiplier is presented for the case $v = k$, $n+1 \le 2v$ and $v \le n-2$. We now use this special case to illustrate the new multiplier. The product $C = AB$ is given as follows [12]:

$$\begin{aligned} C &= \sum_{t=-v}^{n-v-1} c_{v+t}x^t = \sum_{t=-v}^{n-2v-1}\left(\sum_{i=0}^{2v+t} a_i b_{2v+t-i}\right)x^t + \sum_{t=n-2v}^{n-v-1}\left(\sum_{i=2v-n+t+1}^{n-1} a_i b_{2v+t-i}\right)x^t \\ &\quad + \sum_{t=n-2v}^{n-v-1}\left(\sum_{i=0}^{2v-n+t} a_i b_{2v-n+t-i}\right)x^t + \sum_{t=-v}^{-1}\left(\sum_{i=0}^{v+t} a_i b_{v+t-i}\right)x^t \\ &\quad + \sum_{t=0}^{n-v-2}\left(\sum_{i=v+t+1}^{n-1} a_i b_{v+n+t-i}\right)x^t + \sum_{t=-v}^{n-2v-2}\left(\sum_{i=2v+t+1}^{n-1} a_i b_{2v+n+t-i}\right)x^t. \end{aligned}$$

Comparing the coefficients of $x^t$ in this formula, we may obtain explicit expressions of the coordinate $c_{v+t}$ for $-v \le t \le n-1-v$. For example, for the case $t = n-2v-1$, we have

$$c_{n-v-1} = \sum_{i=0}^{n-v-1} a_i(b_{n-v-1-i} + b_{n-1-i}) + \sum_{i=n-v}^{n-1} a_i b_{n-1-i}. \tag{2}$$

In order to compute the coordinate $c_{n-v-1}$, the new multiplier defines terms $y_i$'s for $0 \le i \le n-v-1$ as $y_i = a_i(b_{n-v-1-i} + b_{n-1-i})$. Obviously, computing each $y_i$ requires a gate delay of $T_A + T_X$. Since computing $a_i b_{n-1-i}$ $(n-v \le i \le n-1)$ in (2) requires a delay of $T_A$ only, we may define terms $y_i$'s for $n-v \le i \le n-v+\lceil v/2 \rceil - 1$ as the pairwise summation of the expression $\sum_{i=n-v}^{n-1} a_i b_{n-1-i}$ in (2), i.e.,

$$y_i = \begin{cases} a_{2i-(n-v)}b_{2n-v-1-2i} + a_{1+2i-(n-v)}b_{2n-v-2-2i}, & \text{if } v \text{ is even,} \\ \begin{cases} a_{2i-(n-v)}b_{2n-v-1-2i} + a_{1+2i-(n-v)}b_{2n-v-2-2i}, & n-v \le i \le n-(v+3)/2 \\ a_{n-1}b_0, & i = n-(v+1)/2 \end{cases} & \text{if } v \text{ is odd.} \end{cases}$$

Due to the parallelism, it is easy to see that computing all $y_i$'s $(0 \le i \le n-v+\lceil v/2 \rceil - 1)$ requires a gate delay of $T_A + T_X$. The coordinate $c_{n-v-1}$ is then obtained by adding all $y_i$'s using a binary XOR tree, which requires $\lceil \log_2(n-v+\lceil v/2 \rceil) \rceil T_X$ gate delay. Therefore, the total delay due to gates for computing $c_{n-v-1}$ is $T_A + (1 + \lceil \log_2(\lceil (2n-v)/2 \rceil) \rceil) T_X = T_A + \lceil \log_2(2n-v) \rceil T_X$. Please note that the equality $1 + \lceil \log_2 \lceil i/2 \rceil \rceil = \lceil \log_2 i \rceil$ holds for integer $i > 1$. Other coordinates of $C$ are computed similarly.

Based on the coordinate expressions in [12], we may obtain the gate delay to compute each coordinate. Table I summarizes the total XOR gate delays required to compute each coordinate for $n+1 \le 2v$ and $v \le n-2$. The delay due to gates of the multiplier corresponds to the maximal one $(t = -1)$, which is found to be $T_A + (1 + \lceil \log_2(\lceil (n+v)/2 \rceil) \rceil) T_X = T_A + \lceil \log_2(n+v) \rceil T_X$.

TABLE I

DELAYS DUE TO XOR GATES TO COMPUTE $c_{v+t}$ FOR $n+1 \leq 2v$ AND $v \leq n-2$.

| $t$ | Formula of $c_{v+t}$ | Total XOR delays |
|---|---|---|
| $-v \leq t \leq n-2v-2$ | $\sum_{i=0}^{v+t} a_i(b_{v+t-i}+b_{2v+t-i})+$ $\sum_{i=v+t+1}^{2v+t} a_i b_{2v+t-i} + \sum_{i=2v+t+1}^{n-1} a_i b_{2v+n+t-i}$ | $\lceil \log_2(n+v+t+1) \rceil T_x$ |
| $t = n-2v-1$ | $\sum_{i=0}^{n-v-1} a_i(b_{n-v-1-i}+b_{n-1-i}) + \sum_{i=n-v}^{n-1} a_i b_{n-1-i}$ | $\lceil \log_2(2n-v) \rceil T_x$ |
| $n-2v \leq t \leq -1$ | $\sum_{i=0}^{2v-n+t} a_i(b_{2v-n+t-i}+b_{v+t-i})+$ $\sum_{i=2v-n+t+1}^{v+t} a_i(b_{v+t-i}+b_{2v+t-i})+$ $\sum_{i=v+t+1}^{n-1} a_i b_{2v+t-i}$ | $\lceil \log_2(n+v+t+1) \rceil T_x$ |
| $0 \leq t \leq n-v-2$ | $\sum_{i=v+t+1}^{n-1} a_i(b_{v+n+t-i}+b_{2v+t-i})+$ $\sum_{i=2v-n+t+1}^{v+t} a_i b_{2v+t-i} + \sum_{i=0}^{2v-n+t} a_i b_{2v-n+t-i}$ | $\lceil \log_2(2n-1-v-t) \rceil T_x$ |
| $t = n-v-1$ | $\sum_{i=v}^{n-1} a_i b_{n+v-1-i} + \sum_{i=0}^{v-1} a_i b_{v-1-i}$ | $\lceil \log_2 n \rceil T_x$ |

Since we have only reorganized the computational sequence of the coordinate formulae of $C = (c_0, c_1, ..., c_{n-1})^T$, the AND and XOR gate complexities of the proposed multiplier are the same as those of the type-II SPB multiplier. For the irreducible trinomial $f(u) = u^n + u^k + 1$ with $v = k$ and $v = k-1$ [12], these complexities are:

AND gates = $n^2$;

XOR gates = $\begin{cases} n^2 - 1 & 2k \neq n, \\ n^2 - n/2 & 2k = n. \end{cases}$

For simplicity, we do not present detailed computational procedures of gate delays for the other cases here. But we note that we have obtained these values for all irreducible trinomials $f(u) = u^n + u^k + 1$. We summarize gate delays of the proposed multiplier in Table II.

TABLE II

GATE DELAYS FOR $f(u) = u^n + u^k + 1$-BASED SPB MULTIPLIERS FOR $v = k$ OR $k-1$

| $v$ | Gate delay |
|---|---|
| $n \leq 2v$ | $T_A + \lceil \log_2(n+v) \rceil T_X$ |
| $2v \leq n-1$ | $T_A + \lceil \log_2(2n-v-1) \rceil T_X$ |

For $2 < n < 1000$, now we list pairs $(n, k)$ such that $f(u) = u^n + u^k + 1$ is irreducible and the gate delay of the presented multiplier equals to $T_A + \lceil \log_2 n \rceil T_X$.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $(3,1)$ | $(5,2)$ | $(9,4)$ | $(10,3)$ | $(17,6)$ | $(18,9)$ | $(33,13)$ | $(34,7)$ |
| $(36,15)$ | $(39,14)$ | $(41,20)$ | $(65,32)$ | $(66,3)$ | $(68,33)$ | $(71,35)$ | $(73,31)$ |
| $(74,35)$ | $(81,35)$ | $(84,39)$ | $(129,46)$ | $(130,3)$ | $(132,29)$ | $(134,57)$ | $(135,29)$ |
| $(137,57)$ | $(140,65)$ | $(145,69)$ | $(146,71)$ | $(147,49)$ | $(150,73)$ | $(151,70)$ | $(155,62)$ |
| $(156,65)$ | $(162,81)$ | $(167,77)$ | $(169,84)$ | $(257,65)$ | $(258,83)$ | $(260,105)$ | $(263,93)$ |
| $(265,127)$ | $(266,47)$ | $(268,61)$ | $(270,133)$ | $(271,70)$ | $(273,113)$ | $(274,135)$ | $(276,91)$ |
| $(279,125)$ | $(281,99)$ | $(282,63)$ | $(284,141)$ | $(286,73)$ | $(287,125)$ | $(289,84)$ | $(292,97)$ |
| $(294,81)$ | $(295,147)$ | $(297,137)$ | $(300,147)$ | $(305,102)$ | $(313,121)$ | $(316,135)$ | $(319,129)$ |
| $(321,155)$ | $(324,149)$ | $(327,152)$ | $(513,242)$ | $(514,103)$ | $(516,91)$ | $(518,113)$ | $(519,79)$ |
| $(521,168)$ | $(522,259)$ | $(524,195)$ | $(526,97)$ | $(527,239)$ | $(529,157)$ | $(532,81)$ | $(534,261)$ |
| $(537,94)$ | $(538,195)$ | $(540,211)$ | $(543,235)$ | $(545,122)$ | $(550,193)$ | $(551,240)$ | $(553,258)$ |
| $(556,273)$ | $(559,210)$ | $(561,155)$ | $(564,163)$ | $(566,273)$ | $(567,275)$ | $(569,210)$ | $(570,143)$ |
| $(575,258)$ | $(577,231)$ | $(580,237)$ | $(582,261)$ | $(585,256)$ | $(588,253)$ | $(593,177)$ | $(594,195)$ |
| $(596,273)$ | $(599,210)$ | $(601,202)$ | $(602,215)$ | $(607,273)$ | $(609,233)$ | $(612,297)$ | $(615,238)$ |
| $(618,295)$ | $(622,297)$ | $(623,311)$ | $(626,251)$ | $(628,289)$ | $(631,307)$ | $(633,292)$ | $(634,315)$ |
| $(636,315)$ | $(639,305)$ | $(641,287)$ | $(647,312)$ | $(649,321)$ | $(657,292)$ | $(663,307)$ | $(665,317)$ |

For the range $2 < n < 1001$, there are 128 values of $n$ for which the gate delay of the proposed multiplier is equal to $T_A + \lceil \log_2 n \rceil T_X$. We note that for a fixed degree $n$, more than one irreducible trinomial of degree $n$ may exist such that the gate delay of the proposed multiplier equals to $T_A + \lceil \log_2 n \rceil T_X$, e.g., pairs (9, 4) and (9, 1).

### *B. Comparison*

Reference [12] compares gate delays of the type-I and type-II SPB multipliers with those of a number of other multipliers published earlier. Since the AND and XOR gates complexities of the proposed SPB parallel multiplier match the best results known to date, we now compare the gate delay of the proposed multiplier with those of some recently published multipliers. We note that the XOR gate complexity of the PB multiplier in [11] is $n^2+(k^2-3k)/2$. As shown in the table, the gate delay of the proposed SPB multiplier matches or outperforms the previously known best results for the same class of fields.

TABLE III

COMPARISONS OF GATE DELAYS FOR $f(u) = u^n + u^k + 1$-BASED MULTIPLIERS FOR $v = k$ OR $k-1$

| Multiplier | Gate delay |
|---|---|
| PB [11] | $T_A + \lceil \log_2(2n + k - 2) \rceil T_X$ |
| Type-I SPB[12] | $\leq T_A + \lceil \log_2 4n \rceil T_X$ |
| Type-II SPB [12] | $T_A + \lceil \log_2 2n \rceil T_X$ |
| Presented Here | $T_A + \lceil \log_2(n + v) \rceil T_X$, for $n \leq 2v$ |
| | $T_A + \lceil \log_2(2n - v - 1) \rceil T_X$, for $2v \leq n - 1$ |

### C. An Example

As an example, we now construct the proposed multipliers for $f(u) = u^3 + u + 1$ . Let $v = k = 1$. The SPB is $\{x^{i-1} | 0 \le i \le 2\} = \{x^{-1}, 1, x^1\}$. The SPB Mastrovito matrix $Z$ is given as

$$Z = \begin{pmatrix} b_1 & b_0 & b_2 \\ b_0 + b_2 & b_1 & b_0 \\ b_0 & b_2 & b_1 + b_2 \end{pmatrix}.$$

The coordinate formulae of $C = (c_0, c_1, c_2)^T$ are

$c_0 = [b_1 a_0 + b_0 a_1] + b_2 a_2$,

$c_1 = [(b_0 + b_2) a_0] + [b_1 a_1 + b_0 a_2]$, and

$c_2 = [b_0 a_0 + b_2 a_1] + [(b_1 + b_2) a_2]$.

Terms in square brackets are computed in parallel. So the gate delay of the proposed multiplier is $T_A + 2T_X$. The multiplier requires 9 AND gates and 8 XOR gates.

## IV. SPB Multiplier for Special Irreducible Pentanomials

### A. Architectures

Let $g(u) = u^n + u^e + u^h + u^k + 1$ be an irreducible pentanomial $(n > e > h > k > 0)$ and $x$ be a root of $g(u) = 0$. We use the SPB $\{x^{i-v} | 0 \le i \le n-1\}$ $(0 < v < n)$ to represent field elements, i.e., $A = x^{-v} \sum_{i=0}^{n-1} a_i x^i$. To obtain the formulae of coordinates of *C=AB* for this case, we first compute:

$$S = AB = \sum_{t=-2v}^{2(n-v-1)} s_{t+2v} x^t = r_- + r + r_+, \tag{3}$$

where $r = \sum_{t=-v}^{n-1-v} s_{t+2v} x^t$, $r_- = \sum_{t=-2v}^{-v-1} s_{t+2v} x^t$, $r_+ = \sum_{t=n-v}^{2(n-v-1)} s_{t+2v} x^t$ and $s_{t+2v}$ is defined in (1).

In (3), terms $r_-$ and $r_+$ are reduced by the following reduction formulae:

$$x^i = x^{e+i-n} + x^{h+i-n} + x^{k+i-n} + x^{i-n}, \text{where } n - v \le i \le 2n - 2v - 2, \tag{4}$$

and

$$x^i = x^{n+i} + x^{e+i} + x^{h+i} + x^{k+i}, \text{where } -2v \le i \le -(v+1). \tag{5}$$

The reduced results $\widetilde{r}_+$ and $\widetilde{r}_-$ are defined as follows:

$$\begin{aligned} \widetilde{r}_+ &:= \sum_{t=n-v}^{2n-2v-2} s_{t+2v} x^{t+e-n} + \sum_{t=n-v}^{2n-2v-2} s_{t+2v} x^{t+h-n} + \sum_{t=n-v}^{2n-2v-2} s_{t+2v} x^{t+k-n} + \sum_{t=n-v}^{2n-2v-2} s_{t+2v} x^{t-n} \\ &= \sum_{t=e-v}^{e+n-2v-2} s_{t+2v+n-e} x^t + \sum_{t=h-v}^{h+n-2v-2} s_{t+2v+n-h} x^t + \sum_{t=k-v}^{k+n-2v-2} s_{t+2v+n-k} x^t + \sum_{t=-v}^{n-2v-2} s_{t+n+2v} x^t, \end{aligned} \tag{6}$$

and

$$\widetilde{r}_{-} := \sum_{t=-2v}^{-v-1} s_{t+2v}x^{n+t} + \sum_{t=-2v}^{-v-1} s_{t+2v}x^{e+t} + \sum_{t=-2v}^{-v-1} s_{t+2v}x^{h+t} + \sum_{t=-2v}^{-v-1} s_{t+2v}x^{k+t}$$

$$= \sum_{t=n-2v}^{n-v-1} s_{t+2v-n}x^{t} + \sum_{t=e-2v}^{e-v-1} s_{t+2v-e}x^{t} + \sum_{t=h-2v}^{h-v-1} s_{t+2v-h}x^{t} + \sum_{t=k-2v}^{k-v-1} s_{t+2v-k}x^{t}. \quad (7)$$

In this section, we present architecture of the new multiplier for the special type of the irreducible pentanomials $g(u) = u^n + u^{v+1} + u^v + u^{v-1} + 1$, i.e., $e = v+1$, $h = v$ and $k = v+1$. Therefore, only the last term in (7) will be reduced again, i.e.,

$$\sum_{t=k-2v}^{k-v-1} s_{t+2v-k}x^{t} = \sum_{t=-v}^{k-1-v} s_{t+2v-k}x^{t} + \sum_{t=k-2v}^{-v-1} s_{t+2v-k}x^{t}$$

$$= \sum_{t=-v}^{-2} s_{t+v+1}x^{t} + s_0x^{n-v-1} + s_0x^0 + s_0x^{-1} + s_0x^{-2}$$

The product of $A$ and $B$ is then computed by the formula

$$C = \sum_{i=0}^{n-1} c_i x^{i-v} = x^{-v} \sum_{i=0}^{n-1} c_i x^i = r + \widetilde{r}_{-} + \widetilde{r}_{+}. \quad (8)$$

For this special type of the irreducible pentanomials, the formula for $C = AB$ obtained by applying (1), (6), (7) to (8) may be simplified as follows:

$$\begin{aligned} C = & \sum_{t=-v}^{n-1-v} c_{v+t}x^t = \sum_{t=-v}^{n-2v-1} \left( \sum_{i=0}^{2v+t} a_i b_{2v+t-i} \right) x^t + \sum_{t=n-2v}^{n-v-1} \left( \sum_{i=2v-n+t+1}^{n-1} a_i b_{2v+t-i} \right) x^t \\ & + \sum_{t=1}^{n-v-1} \left( \sum_{i=t+v}^{n-1} a_i b_{v+n-1+t-i} \right) x^t + \sum_{t=0}^{n-v-2} \left( \sum_{i=t+v+1}^{n-1} a_i b_{v+n+t-i} \right) x^t \\ & + \sum_{t=-1}^{n-v-3} \left( \sum_{i=t+v+2}^{n-1} a_i b_{v+n+1+t-i} \right) x^t + \sum_{t=-v}^{n-2v-2} \left( \sum_{i=t+2v+1}^{n-1} a_i b_{n+2v+t-i} \right) x^t \\ & + \sum_{t=n-2v}^{n-v-1} \left( \sum_{i=0}^{t+2v-n} a_i b_{2v-n+t-i} \right) x^t + \sum_{t=1-v}^{0} \left( \sum_{i=0}^{t+v-1} a_i b_{v-1+t-i} \right) x^t \\ & + \sum_{t=-v}^{-1} \left( \sum_{i=0}^{t+v} a_i b_{v+t-i} \right) x^t + \sum_{t=-v}^{-2} \left( \sum_{i=0}^{t+v+1} a_i b_{v+1+t-i} \right) x^t \\ & + a_0b_0x^{n-v-1} + a_0b_0 + a_0b_0x^{-1} + a_0b_0x^{-2}. \end{aligned}$$

Comparing the coefficients of $x^t$ in this formula, we can obtain explicit expressions of the coordinate $c_{v+t}$ for $-v \le t \le n-1-v$. Expressions are different according to the value of $v$. For three of the five NIST recommended values of $n$ for ECDSA, namely, $n$=163, 283 and 571, all pairs of $(n, v)$, for which $g(u) = u^n+u^{v+1}+u^v+u^{v-1}+1$ is irreducible, are as follows: (163, 67), (163, 69), (163, 71), (163, 92), (163, 94), (163, 96), (283, 24), (283, 133), (283, 150), (283, 259), (571, 104), (571, 230), (571, 341) and (571, 467). These values of $v$ are in the range of $3 < v < (n-3)/2$ and we can now present explicit expressions of the coordinate $c_{v+t}$. To this end, the

corresponding values of $t$ are divided into ten segments/cases. Below we present **Case 1** only and leave the rest for the appendix.

**Case 1:** $t = -v$

$$\begin{aligned} c_0 &= \sum_{i=0}^{v} a_i b_{v-i} + \sum_{i=v+1}^{n-1} a_i b_{n+v-i} + a_0 b_0 + a_0 b_1 + a_1 b_0 \\ &= a_0(b_0 + b_1 + b_v) + \left\{ a_1(b_0 + b_{v-1}) + \left[ \sum_{i=2}^{v} a_i b_{v-i} + \sum_{i=v+1}^{n-1} a_i b_{n+v-i} \right] \right\} \end{aligned} \tag{9}$$

The expressions of the corresponding row of the Mastrovito matrix is

$$z_{0,i} = \begin{cases} b_0 + b_1 + b_v & i = 0 \\ b_0 + b_{v-1} & i = 1 \\ b_{v-i} & 2 \le i \le v \\ b_{n+v-i} & v+1 \le i \le n-1. \end{cases}$$

There are $n-2$ terms in the square brackets in (9), and they are added pairwise first. Then the $\lceil (n-2)/2 \rceil$ summations and the term $a_1(b_0 + b_{v-1})$ in the curly brackets are added pairwise. Finally, the $\lceil (1 + \lceil (n-2)/2 \rceil)/2 \rceil$ summations obtained in the second step and the term $a_0(b_0 + b_1 + b_v)$ are added pairwise using a binary XOR tree. We note that the square and curly brackets have the similar computation sequence in the following cases. The AND gate delay in this case and the following cases are the same, namely, $T_A$. So we only consider the XOR gate delay. Due to the parallelism, the XOR gate delay for computing $c_0$ is $2 + \lceil \log_2 (1 + \lceil (1 + \lceil (n-2)/2 \rceil)/2 \rceil) \rceil = 2 + \lceil \log_2 (1 + \lceil n/4 \rceil) \rceil$.

Using the formula for each coordinate of $C$ as given above and in the appendix, we now compute complexities of the proposed multiplier. The maximal gate delay occurs in **Case 5** ($t = 0$), which is found to be $T_A + (1 + \lceil \log_2 (2n - v - 1) \rceil) T_X$.

From the discussions in **Case 3** and **Case 8**, which is given in the appendix, we know that the multiplier requires $n^2$ AND gates. Now we count the number of the XOR gates. First we need to compute the following summations of $b_i$'s. The number of the XOR gates used to compute the corresponding expression is listed in the curly brackets.

$$
\begin{aligned}
&b_{v-1}+b_{n-1}, && \{1\};\\
&b_{v}+b_{n-1}, && \{1\};\\
&b_{0}+b_{v-1}, && \{1\};\\
&b_{0}+b_{v}, && \{1\};\\
&b_{0}+b_{1}+b_{v}=(b_{0}+b_{v})+b_{1}, && \{1\};\\
&b_{v-1}+b_{n-2}+b_{n-1}=(b_{v-1}+b_{n-1})+b_{n-2}, && \{1\};\\
&b_{v-2}+b_{v-1}+b_{2v-1}+b_{0}=(b_{v-2}+b_{2v-1})+(b_{v-1}+b_{0}), && \{2\};\\
&b_{v-1}+b_{2v}+b_{0}=(b_{v-1}+b_{0})+b_{2v}, && \{1\};\\
&b_{j+v-1-n}+b_{j},\ \text{where } n-v+1\le j\le n-1, && \{v-1\};\\
&b_{j+v-1}+b_{j},\ \text{where } v+1\le j\le n-v, && \{n-2v\};\\
&b_{j+v+1}+b_{j},\ \text{where } 0\le j\le v-2, && \{v-2\};\\
&b_{j+v+1}+b_{j+1}+b_{j}=(b_{j+v+1}+b_{j})+b_{j+1},\ \text{where } 0\le j\le v-3, && \{v-2\};\\
&b_{j+v-n}+b_{j+1}+b_{j}=(b_{j+v-n}+b_{j+1})+b_{j},\ \text{where } n-v\le j\le n-2, && \{v-1\};\\
&b_{j+v}+b_{j+1}+b_{j}=(b_{j+v}+b_{j+1})+b_{j},\ \text{where } v+1\le j\le n-v-1, && \{n-2v-1\};\\
&b_{j+v+1}+b_{j+2}+b_{j+1}+b_{j}=(b_{j+v+1}+b_{j})+(b_{j+2}+b_{j+1}),\\
&\qquad\qquad \text{where } 0\le j\le v-3, && \{2v-4\};\\
&b_{j+1+v-n}+b_{j+2}+b_{j+1}+b_{j}=(b_{j+1+v-n}+b_{j+2})+(b_{j+1}+b_{j}),\\
&\qquad\qquad \text{where } n-v-1\le j\le n-3, && \{2v-2\};\\
&b_{j+1+v}+b_{j+2}+b_{j+1}+b_{j}=(b_{j+1+v}+b_{j+2})+(b_{j+1}+b_{j}),\\
&\qquad\qquad \text{where } v+1\le j\le n-v-2, && \{2(n-2v-2)\}.
\end{aligned}
$$

We note that a previous expression may be reused by a following one. For example, we need only $v-2$ XOR gates to compute $b_{j+v+1}+b_j$ $(0\le j\le v-2)$ since the term $(b_{v-2}+b_{2v-1})$ have been computed in the expression $b_{v-2}+b_{v-1}+b_{2v-1}+b_0=(b_{v-2}+b_{2v-1})+(b_{v-1}+b_0)$. Therefore, $4n-8$ XOR gates are required to calculate all expressions. Based on the discussions in **Case 3**, we know that the total number of the XOR gates of the multiplier is $n(n-1)+1+4n-8=n^2+3n-7$.

For simplicity, we do not present detailed computational procedures of gate delays for the other cases here. But we note that we have obtained these complexities for all irreducible pentanomials $g(u)=u^n+u^{v+1}+u^v+u^{v-1}+1$. We summarize the gate delay of the proposed multiplier as follows.

TABLE IV

GATE DELAYS FOR $g(u)=u^n+u^{v+1}+u^v+u^{v-1}+1$-BASED SPB MULTIPLIERS

| $v$ | Gate delay |
|---|---|
| $n+1<2v$ | $T_A+(1+\lceil\log_2(n+v-1)\rceil)T_X$ |
| $2v\le n+1$ | $T_A+(1+\lceil\log_2(2n-v-1)\rceil)T_X$ |

For $2<n<1000$, for which no irreducible trinomial of degree $n$ exists, we now list pairs $(n,v)$ such that

$g(u) = u^n + u^{v+1} + u^v + u^{v-1} + 1$ is irreducible and the gate delay of the presented multiplier equals to $T_A + \lceil 1 + \log_2 n \rceil T_X$.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $(19, 6)$ | $(38, 16)$ | $(40, 20)$ | $(67, 6)$ | $(70, 20)$ | $(133, 63)$ | $(139, 60)$ | $(149, 43)$ |
| $(157, 73)$ | $(160, 72)$ | $(163, 71)$ | $(164, 75)$ | $(259, 118)$ | $(262, 91)$ | $(269, 43)$ | $(275, 122)$ |
| $(277, 128)$ | $(283, 133)$ | $(290, 142)$ | $(298, 109)$ | $(299, 134)$ | $(301, 146)$ | $(307, 130)$ | $(326, 139)$ |
| $(331, 159)$ | $(515, 205)$ | $(523, 202)$ | $(533, 92)$ | $(535, 257)$ | $(536, 144)$ | $(541, 237)$ | $(542, 191)$ |
| $(547, 134)$ | $(548, 246)$ | $(554, 206)$ | $(557, 97)$ | $(560, 272)$ | $(562, 173)$ | $(563, 241)$ | $(565, 204)$ |
| $(568, 124)$ | $(571, 230)$ | $(572, 162)$ | $(578, 286)$ | $(581, 231)$ | $(584, 224)$ | $(586, 286)$ | $(587, 195)$ |
| $(589, 169)$ | $(592, 244)$ | $(595, 166)$ | $(598, 268)$ | $(605, 299)$ | $(611, 241)$ | $(638, 252)$ | $(644, 319)$ |
| $(661, 317)$ | $(667, 316)$ | $(680, 336)$ | | | | | |

For the range $2 < n < 1001$, there are 59 values of $n$ for which the gate delay of the proposed multiplier equals to $T_A + \lceil 1 + \log_2 n \rceil T_X$. Especially, for the binary fields $GF(2^{163})$, $GF(2^{283})$ and $GF(2^{571})$, which have been recommended by NIST for ECDSA applications but no irreducible trinomials exist for the degrees $n$ =163, 283 and 571, we have found pairs of $(n, v)$ for these values of $n$ such that the gate delay of the proposed SPB multipliers is $T_A + \lceil 1 + \log_2 n \rceil T_X$.

### *B. Comparison*

We now compare the gate delay of the proposed multiplier with some recently published multipliers. Please note that the multiplier proposed in [14] uses $n + 1$ bits to represent $GF(2^n)$ elements, therefore the width of the data-path is equal to $n + 1$ and its AND gate complexity is $(n + 1)^2$. Other multipliers in Table V do not use the redundant representation.

TABLE V

COMPARISONS OF SOME SELECTED MULTIPLIERS

| Polynomials | Bases | # XOR | Gate delay |
|---|---|---|---|
| $u^n + u^{v+1} + u^v + u^{v-1} + 1$ | Dual Basis [13] | $n^2 + \lceil 1.5n \rceil + 3v - 6$ | $T_A + \lceil 3 + \log_2 n \rceil T_X$ |
| $u^n + u^{v+1} + u^v + u + 1$ | PB [5] | $n^2 + n$ | $T_A + \lceil 3 + \log_2(n-1) \rceil T_X$ |
| $u^{n+1} + u^v + u^k + 1$ | Redundant [14] | $n^2 + 2n + v - k$ | $T_A + \lceil 2 + \log_2(n+1) \rceil T_X$ |
| $u^n + u^{v+1} + u^v + u^{v-1} + 1$ | SPB Proposed | $n^2 + 3n - 7$ | $T_A + \lceil 1 + \log_2(n+v-1) \rceil T_X$, if $n + 1 < 2v$ |
| | | | $T_A + \lceil 1 + \log_2(2n-v-1) \rceil T_X$, if $2v \leq n + 1$ |

For the purpose of illustration, in Table VI, we list the number of AND/XOR gates and the gate delay of some available bit parallel multipliers for fields $GF(2^{163})$, $GF(2^{283})$ and $GF(2^{571})$. Since existences of the suitable 4-term polynomials for $n$ =283 and 571 are unknown, the algorithm in [14] is not applicable for these two fields. From Table VI, we conclude the following:

For the field $GF(2^{163})$, the proposed design improves the gate delay of [14] by 10%; For the field $GF(2^{283})$, the proposed design improves the gate delay of [5] by 16.7% at the cost of 0.7% increase of the XOR gate number;

For the field $GF(2^{571})$, the proposed design improves the gate delay of [13] by 15.4% at the cost of 0.2% increase of the XOR gate number.

TABLE VI

COMPLEXITIES OF SOME PRACTICAL FIELDS

| Polynomials | Bases | Space complexity | | Gate delay |
|---|---|---|---|---|
| | | # AND | # XOR | |
| $u^{163}+u^{68}+u^{67}+u^{66}+1$ | Dual Basis [13] | 26569 | 27009 | $T_A+11T_X$ |
| $u^{163}+u^{60}+u^{59}+u+1$ | PB [5] | 26569 | 26732 | $T_A+11T_X$ |
| $u^{164}+u^{33}+u^{22}+1$ | Redundant [14] | 26896 | 26906 | $T_A+10T_X$ |
| $u^{163}+u^{72}+u^{71}+u^{70}+1$ | SPB Proposed | 26569 | 27051 | $T_A+9T_X$ |
| $u^{283}+u^{25}+u^{24}+u^{23}+1$ | Dual Basis [13] | 80089 | 80580 | $T_A+12T_X$ |
| $u^{283}+u^{60}+u^{59}+u+1$ | PB [5] | 80089 | 80372 | $T_A+12T_X$ |
| $u^{283}+u^{134}+u^{133}+u^{132}+1$ | SPB Proposed | 80089 | 80931 | $T_A+10T_X$ |
| $u^{571}+u^{105}+u^{104}+u^{103}+1$ | Dual Basis [13] | 326041 | 327204 | $T_A+13T_X$ |
| $u^{571}+u^{277}+u^{275}+u^{2}+1$ | PB [5] | 326041 | 326612 | $T_A+14T_X$ |
| $u^{571}+u^{231}+u^{230}+u^{229}+1$ | SPB Proposed | 326041 | 327747 | $T_A+11T_X$ |

## V. CONCLUSIONS

After reorganizing the computational procedure of the coordinate formulae of $C=AB=(c_0,c_1,...,c_{n-1})^T$, we have proposed a new SPB multiplier. For all irreducible trinomials, its space complexity matches the previously known best results, but for certain irreducible trinomials its gate delay reaches a new low value of $T_A+\lceil \log_2 n \rceil T_X$. For a special type of irreducible pentanomials, namely, $f(u)=u^n+u^{v+1}+u^v+u^{v-1}+1$ $(3<v<(n-3)/2)$, we have presented exact formulae for the multiplier and show that the gate delay is $T_A+(1+\lceil \log_2(n+v-1) \rceil)T_X$ for the case $n+1<2v$. Combining the result of the reference [12] and this report, we know that it is possible to design SPB bit parallel multipliers with a gate delay of no more than $T_A+(1+\lceil \log_2 n \rceil)T_X$ for the five binary fields recommended by NIST for ECDSA applications.

## APPENDIX

Formulae for $c_{v+t}$: **Case 1** has been presented in Section IV, **Case 2** to **10** are given below.

**Case 2:** $1-v \le t \le -3$

$$
\begin{aligned}
c_{v+t} &= \sum_{i=0}^{2v+t} a_i b_{2v+t-i} + \sum_{i=t+2v+1}^{n-1} a_i b_{n+2v+t-i} + \sum_{i=0}^{t+v-1} a_i b_{v-1+t-i} + \sum_{i=0}^{t+v} a_i b_{v+t-i} + \sum_{i=0}^{t+v+1} a_i b_{v+1+t-i} \\
&= \sum_{i=0}^{v+t-1} a_i (b_{2v+t-i} + b_{v-1+t-i} + b_{v+t-i} + b_{v+1+t-i}) + a_{v+t}(b_0+b_1+b_v) \\
&\quad + \left\{ a_{v+t+1}(b_0+b_{v-1}) + \left[ \sum_{i=v+t+2}^{2v+t} a_i b_{2v+t-i} + \sum_{i=t+2v+1}^{n-1} a_i b_{n+2v+t-i} \right] \right\}
\end{aligned}
$$

The expressions of the corresponding rows of the Mastrovito matrix is

$$z_{v+t,i} = \begin{cases} b_{v-1+t-i} + b_{v+t-i} + b_{v+1+t-i} + b_{2v+t-i} & 0 \le i \le v-1+t \\ b_0 + b_1 + b_v & i = v+t \\ b_0 + b_{v-1} & i = v+t+1 \\ b_{2v+t-i} & v+t+2 \le i \le 2v+t \\ b_{n+2v+t-i} & 2v+t+1 \le i \le n-1 \end{cases}$$

Please note that summations $b_0 + b_1 + b_v$ and $b_0 + b_{v-1}$ also appear in Case 1, and they may be reused.

The XOR gate delay for computing $c_{v+t}$ $(1 - v \le t \le -3)$ is $2 + \lceil \log_2 (v + t + 1 + \lceil (1 + \lceil (n - v - t - 2)/2 \rceil)/2 \rceil) \rceil = 2 + \lceil \log_2 \lceil (n + 3v + 3t + 4)/4 \rceil \rceil$. The maximal delay is $2 + \lceil \log_2 \lceil (n + 3v - 5)/4 \rceil \rceil$ when $t = -3$.

From $0 \le i \le v - 1 + t$ and $1 - v \le t \le -3$, we know that $0 \le v - 1 + t - i \le v - 4$. Therefore, sum $b_{v-1+t-i} + b_{v+t-i} + b_{v+1+t-i} + b_{2v+t-i}$ are the same as sum $b_{j+v+1} + b_{j+2} + b_{j+1} + b_j$, where $0 \le j \le v - 4$.

**Case 3:** $t = -2$

$$\begin{aligned} c_{v-2} &= \sum_{i=0}^{2v-2} a_i b_{2v-2-i} + \sum_{i=2v-1}^{n-1} a_i b_{n+2v-2-i} + \sum_{i=0}^{v-3} a_i b_{v-3-i} + \sum_{i=0}^{v-2} a_i b_{v-2-i} + \sum_{i=0}^{v-1} a_i b_{v-1-i} + a_0 b_0 \\ &= \sum_{i=0}^{v-3} a_i (b_{v-3-i} + b_{v-2-i} + b_{v-1-i} + b_{2v-2-i}) + a_{v-2}(b_0 + b_1 + b_v) \\ &\quad + \left\{ a_{v-1}(b_0 + b_{v-1}) + \left[ \sum_{i=v}^{2v-2} a_i b_{2v-2-i} + \sum_{i=2v-1}^{n-1} a_i b_{n+2v-2-i} + a_0 b_0 \right] \right\} \end{aligned} \tag{10}$$

The expressions of the corresponding row of the Mastrovito matrix is

$$z_{v-2,i} = \begin{cases} b_{v-3} + b_{v-2} + b_{v-1} + b_{2v-2} + b_0 & i = 0 \\ b_{v-3-i} + b_{v-2-i} + b_{v-1-i} + b_{2v-2-i} & 1 \le i \le v-3 \\ b_0 + b_1 + b_v & i = v-2 \\ b_0 + b_{v-1} & i = v-1 \\ b_{2v-2-i} & v \le i \le 2v-2 \\ b_{n+2v-2-i} & 2v-1 \le i \le n-1 \end{cases}$$

Please note that $z_{v-2,0} = b_{v-3} + b_{v-2} + b_{v-1} + b_{2v-2} + b_0$ is a summation of five terms. Thus the gate delay of the type-II SPB multiplier is $T_A + (3 + \lceil \log_2 n \rceil) T_X$. But we may use formula (10) to compute $c_{v-2}$, where $a_0 b_0$ is added in the square bracket. The total XOR gate delay for computing $c_{v+t}$ is $2 + \lceil \log_2 (1 + v - 3 + 1 + \lceil (1 + \lceil (n - v + 1)/2 \rceil)/2 \rceil) \rceil = 2 + \lceil \log_2 \lceil (n + 3v - 1)/4 \rceil \rceil$ and $n + 1$ AND gates are required in (10). We note that only $n$ AND gates are required in other $n - 2$ cases except this case and the case $t = n - 2v$. Please refer to **Case 8** for more details.

From $1 \le i \le v - 3$ and $t = -2$, we know that $0 \le v - 3 - i \le v - 4$. Therefore, sum $b_{v-3-i} + b_{v-2-i} + b_{v-1-i} + b_{2v-2-i}$ are the same as sum $b_{j+v+1} + b_{j+2} + b_{j+1} + b_j$, where $0 \le j \le v - 4$.

**Case 4:** $t=-1$

$$\begin{aligned} c_{v-1} &= \sum_{i=0}^{2v-1} a_i b_{2v-1-i} + \sum_{i=v+1}^{n-1} a_i b_{n+v-i} + \sum_{i=2v}^{n-1} a_i b_{n+2v-1-i} + \sum_{i=0}^{v-2} a_i b_{v-2-i} + \sum_{i=0}^{v-1} a_i b_{v-1-i} + a_0 b_0 \\ &= a_0(b_{v-2}+b_{v-1}+b_{2v-1}+b_0) + \sum_{i=1}^{v-2} a_i (b_{v-2-i}+b_{v-1-i}+b_{2v-1-i}) \\ &\quad + \left\{ a_{v-1}(b_0+b_v) + a_v b_{v-1} + \sum_{i=v+1}^{2v-1} a_i (b_{2v-1-i}+b_{n+v-i}) + \sum_{i=2v}^{n-1} a_i (b_{n+2v-1-i}+b_{n+v-i}) \right\} \end{aligned}$$

The expressions of the corresponding row of the Mastrovito matrix is

$$z_{v-1,i} = \begin{cases} b_{v-2}+b_{v-1}+b_{2v-1}+b_0 & i=0 \\ b_{v-2-i}+b_{v-1-i}+b_{2v-1-i} & 1 \le i \le v-2 \\ b_0+b_v & i=v-1 \\ b_{v-1} & i=v \\ b_{2v-1-i}+b_{n+v-i} & v+1 \le i \le 2v-1 \\ b_{n+v-i}+b_{n+2v-1-i} & 2v \le i \le n-1 \end{cases}$$

The XOR gate delay for computing $c_{v-1}$ is $2+\lceil \log_2 (v-1+\lceil (n-v+1)/2 \rceil) \rceil = 2+\lceil \log_2 \lceil (n+v-1)/2 \rceil \rceil$.

From $1 \le i \le v-2$, we know that $0 \le v-2-i \le v-3$. Therefore, sum $b_{v-2-i}+b_{v-1-i}+b_{2v-1-i}$ are the same as sum $b_{j+v+1}+b_{j+1}+b_j$ , where $0 \le j \le v-3$.

From $v+1 \le i \le 2v-1$, we know that $n-v+1 \le n+v-i \le n-1$. Therefore, sum $b_{2v-1-i}+b_{n+v-i}$ are the same as sum $b_{j+v-1-n}+b_j$ , where $n-v+1 \le j \le n-1$.

From $2v \le i \le n-1$, we know that $v+1 \le n+v-i \le n-v$. Therefore, sum $b_{n+v-i}+b_{n+2v-1-i}$ are the same as sum $b_{j+v-1}+b_j$, where $v+1 \le j \le n-v$.

**Case 5:** $t=0$

$$\begin{aligned} c_v &= \sum_{i=0}^{2v} a_i b_{2v-i} + \sum_{i=v+1}^{n-1} a_i b_{n+v-i} + \sum_{i=v+2}^{n-1} a_i b_{n+v+1-i} + \sum_{i=2v+1}^{n-1} a_i b_{n+2v-i} + \sum_{i=0}^{v-1} a_i b_{v-1-i} + a_0 b_0 \\ &= a_0(b_0+b_{v-1}+b_{2v}) + \left\{ \sum_{i=1}^{v-1} a_i (b_{v-1-i}+b_{2v-i}) + a_v b_v + a_{v+1}(b_{v-1}+b_{n-1}) \right\} \\ &\quad + \sum_{i=v+2}^{2v} a_i (b_{2v-i}+b_{n+v-i}+b_{n+v+1-i}) + \sum_{i=2v+1}^{n-1} a_i (b_{n+v-i}+b_{n+v+1-i}+b_{n+2v-i}) \end{aligned}$$

The expressions of the corresponding row of the Mastrovito matrix is

$$z_{v,i} = \begin{cases} b_0+b_{v-1}+b_{2v} & i=0 \\ b_{v-1-i}+b_{2v-i} & 1 \le i \le v-1 \\ b_v & i=v \\ b_{v-1}+b_{n-1} & i=v+1 \\ b_{2v-i}+b_{n+v-i}+b_{n+v+1-i} & v+2 \le i \le 2v \\ b_{n+v-i}+b_{n+v+1-i}+b_{n+2v-i} & 2v+1 \le i \le n-1 \end{cases}$$

The XOR gate delay for computing $c_v$ is $2+\lceil \log_2 (1+n-v-2+\lceil (v+1)/2 \rceil) \rceil = 2+\lceil \log_2 \lceil (2n-v-1)/2 \rceil \rceil$, which is the maximal XOR gate delay of the new multiplier.

From $1 \leq i \leq v-1$, we know that $0 \leq v-1-i \leq v-2$. Therefore, sum $b_{v-1-i}+b_{2v-i}$ are the same as sum $b_{j+v+1}+b_j$, where $0 \leq j \leq v-2$.

From $v+2 \leq i \leq 2v$, we know that $n-v \leq n+v-i \leq n-2$. Therefore, sum $b_{2v-i}+b_{n+v-i}+b_{n+v+1-i}$ are the same as sum $b_{j+v-n}+b_{j+1}+b_j$, where $n-v \leq j \leq n-2$.

From $2v+1 \leq i \leq n-1$, we know that $v+1 \leq n+v-i \leq n-v-1$. Therefore, sum $b_{n+v-i}+b_{n+v+1-i}+b_{n+2v-i}$ are the same as sum $b_{j+v}+b_{j+1}+b_j$, where $v+1 \leq j \leq n-v-1$.

**Case 6:** $1 \leq t \leq n-2v-2$

$$\begin{aligned}
c_{v+t} &= \sum_{i=0}^{2v+t} a_i b_{2v+t-i} + \sum_{i=t+v}^{n-1} a_i b_{n+v-1+t-i} + \sum_{i=t+v+1}^{n-1} a_i b_{n+v+t-i} \\
&\quad + \sum_{i=t+v+2}^{n-1} a_i b_{n+v+1+t-i} + \sum_{i=t+2v+1}^{n-1} a_i b_{n+2v+t-i} \\
&= \left\{ \left[ \sum_{i=0}^{v+t-1} a_i b_{2v+t-i} \right] + a_{t+v}(b_v + b_{n-1}) \right\} + a_{t+v+1}(b_{v-1} + b_{n-2} + b_{n-1}) \\
&\quad + \sum_{i=t+v+2}^{2v+t} a_i (b_{2v+t-i} + b_{n+v-1+t-i} + b_{n+v+t-i} + b_{n+v+1+t-i}) \\
&\quad + \sum_{i=t+2v+1}^{n-1} a_i (b_{n+v-1+t-i} + b_{n+v+t-i} + b_{n+v+1+t-i} + b_{n+2v+t-i})
\end{aligned}$$

The expressions of the corresponding rows of the Mastrovito matrix is

$$z_{v+t,i} = \begin{cases}
b_{2v+t-i} & 0 \leq i \leq t+v-1 \\
b_v + b_{n-1} & i = t+v \\
b_{v-1} + b_{n-2} + b_{n-1} & i = t+v+1 \\
b_{2v+t-i} + b_{n+v-1+t-i} + b_{n+v+t-i} + b_{n+v+1+t-i} & t+v+2 \leq i \leq 2v+t \\
b_{n+v-1+t-i} + b_{n+v+t-i} + b_{n+v+1+t-i} + b_{n+2v+t-i} & t+2v+1 \leq i \leq n-1
\end{cases}$$

The XOR gate delay for computing $c_{v+t}$ is $2+\lceil \log_2 (n-t-v-1+\lceil (v+t+1)/2 \rceil) \rceil = 2+\lceil \log_2 \lceil (2n-v-t-1)/2 \rceil \rceil$. The maximal delay is $2+\lceil \log_2 \lceil (2n-v-2)/2 \rceil \rceil$ when $t=1$.

From $t+v+2 \leq i \leq 2v+t$ and $1 \leq t \leq n-2v-2$, we know that $n-v-1 \leq n+v-1+t-i \leq n-3$. Therefore, sum $b_{2v+t-i}+b_{n+v-1+t-i}+b_{n+v+t-i}+b_{n+v+1+t-i}$ are the same as sum $b_{j+1+v-n}+b_{j+2}+b_{j+1}+b_j$, where $n-v-1 \leq j \leq n-3$.

From $t+2v+1 \leq i \leq n-1$ and $1 \leq t \leq n-2v-2$, we know that $v+1 \leq n+v-1+t-i \leq n-v-2$. Therefore, sum $b_{n+v-1+t-i}+b_{n+v+t-i}+b_{n+v+1+t-i}+b_{n+2v+t-i}$ are the same as sum $b_{j+1+v}+b_{j+2}+b_{j+1}+b_j$, where $v+1 \leq j \leq n-v-2$.

**Case 7:** $t = n - 2v - 1$

$$\begin{aligned} c_{n-v-1} &= \sum_{i=0}^{n-1} a_i b_{n-1-i} + \sum_{i=n-v-1}^{n-1} a_i b_{2n-v-2-i} + \sum_{i=n-v}^{n-1} a_i b_{2n-v-1-i} + \sum_{i=n-v+1}^{n-1} a_i b_{2n-v-i} \\ &= \left\{ \left[ \sum_{i=0}^{n-v-2} a_i b_{n-1-i} \right] + a_{n-v-1}(b_v + b_{n-1}) \right\} + a_{n-v}(b_{v-1} + b_{n-2} + b_{n-1}) \\ &\quad + \sum_{i=n-v+1}^{n-1} a_i (b_{n-1-i} + b_{2n-v-2-i} + b_{2n-v-1-i} + b_{2n-v-i}) \end{aligned}$$

The expressions of the corresponding row of the Mastrovito matrix is

$$z_{n-v-1,i} = \begin{cases} b_{n-1-i} & 0 \le i \le n-v-2 \\ b_v + b_{n-1} & i = n-v-1 \\ b_{v-1} + b_{n-2} + b_{n-1} & i = n-v \\ b_{n-1-i} + b_{2n-v-2-i} + b_{2n-v-1-i} + b_{2n-v-i} & n-v+1 \le i \le n-1 \end{cases}$$

The XOR gate delay for computing $c_{n-v-1}$ is $2 + \lceil \log_2 (v + \lceil (1 + \lceil (n-v-1)/2 \rceil)/2 \rceil) \rceil = 2 + \lceil \log_2 \lceil (n+3v+1)/4 \rceil \rceil$.

From $n - v + 1 \le i \le n - 1$, we know that $n - v - 1 \le 2n - v - 2 - i \le n - 3$. Therefore, sum $b_{n-1-i} + b_{2n-v-2-i} + b_{2n-v-1-i} + b_{2n-v-i}$ are the same as sum $b_{j+1+v-n} + b_{j+2} + b_{j+1} + b_j$, where $n - v - 1 \le j \le n - 3$.

**Case 8:** $n - 2v \le t \le n - v - 3$

$$\begin{aligned} c_{v+t} &= \sum_{i=2v-n+t+1}^{n-1} a_i b_{2v+t-i} + \sum_{i=t+v}^{n-1} a_i b_{n+v-1+t-i} + \sum_{i=t+v+1}^{n-1} a_i b_{n+v+t-i} \\ &\quad + \sum_{i=t+v+2}^{n-1} a_i b_{n+v+1+t-i} + \sum_{i=0}^{2v-n+t} a_i b_{2v-n+t-i} \\ &= \left\{ \left[ \sum_{i=0}^{2v-n+t} a_i b_{2v-n+t-i} + \sum_{i=2v-n+t+1}^{v+t-1} a_i b_{2v+t-i} \right] + a_{v+t}(b_v + b_{n-1}) \right\} \\ &\quad + a_{v+t+1}(b_{v-1} + b_{n-2} + b_{n-1}) \\ &\quad + \sum_{i=v+t+2}^{n-1} a_i (b_{2v+t-i} + b_{n+v-1+t-i} + b_{n+v+t-i} + b_{n+v+1+t-i}) \end{aligned} \tag{11}$$

The expressions of the corresponding rows of the Mastrovito matrix is

$$z_{v+t,i} = \begin{cases} b_{2v-n+t-i} & 0 \le i \le 2v-n+t \\ b_{2v+t-i} & 2v-n+t+1 \le i \le v+t-1 \\ b_v + b_{n-1} & i = v+t \\ b_{v-1} + b_{n-2} + b_{n-1} & i = v+t+1 \\ b_{2v+t-i} + b_{n+v-1+t-i} + b_{n+v+t-i} + b_{n+v+1+t-i} & v+t+2 \le i \le n-1 \end{cases}$$

Please note that we have obtained the term $a_0 b_0$ in **Case 3** at the cost of 1 AND gate. Since this term also appears in the case $t = n - 2v$ (the first term in the square brackets of (11), $t = n - 2v$ and $i = 0$), only $n - 1$ AND gates are required for the case $t = n - 2v$.

The XOR gate delay for computing $c_{v+t}$ is $2+\lceil \log_2 (n-v-t-1+\lceil (1+\lceil (v+t)/2 \rceil)/2 \rceil) \rceil = 2+\lceil \log_2 \lceil (4n-3v-3t-2)/4 \rceil \rceil$. The maximal delay for $n-2v \leq t \leq n-v-3$ is $2+\lceil \log_2 \lceil (n+3v-2)/4 \rceil \rceil$, which occurs in the case of $t=n-2v$.

From $v+t+2 \leq i \leq n-1$ and $n-2v \leq t \leq n-v-3$, we know that $n-v \leq n+v-1+t-i \leq n-3$. Therefore, sum $b_{2v+t-i}+b_{n+v-1+t-i}+b_{n+v+t-i}+b_{n+v+1+t-i}$ are the same as sum $b_{j+1+v-n}+b_{j+2}+b_{j+1}+b_j$, where $n-v \leq j \leq n-3$.

**Case 9:** $t=n-v-2$

$$\begin{aligned} c_{n-2} &= \sum_{i=v-1}^{n-1} a_i b_{n+v-2-i} + a_{n-2}b_{n-1} + a_{n-1}b_{n-2} + a_{n-1}b_{n-1} + \sum_{i=0}^{v-2} a_i b_{v-2-i} \\ &= \left\{ \left[ \sum_{i=0}^{v-2} a_i b_{v-2-i} + \sum_{i=v-1}^{n-3} a_i b_{n+v-2-i} \right] + a_{n-2}(b_v + b_{n-1}) \right\} + a_{n-1}(b_{v-1}+b_{n-2}+b_{n-1}) \end{aligned}$$

The expressions of the corresponding row of the Mastrovito matrix is

$$z_{n-2,i} = \begin{cases} b_{v-2-i} & 0 \leq i \leq v-2 \\ b_{n+v-2-i} & v-1 \leq i \leq n-3 \\ b_v + b_{n-1} & i = n-2 \\ b_{v-1}+b_{n-2}+b_{n-1} & i = n-1 \end{cases}$$

The XOR gate delay for computing $c_{n-2}$ is $2+\lceil \log_2 (1+\lceil (1+\lceil (n-2)/2 \rceil)/2 \rceil) \rceil = 2+\lceil \log_2 \lceil (n+4)/4 \rceil \rceil$.

**Case 10:** $t=n-v-1$

$$\begin{aligned} c_{n-1} &= \sum_{i=v}^{n-1} a_i b_{n+v-1-i} + \sum_{i=0}^{v-1} a_i b_{v-1-i} + a_0 b_0 + a_{n-1}b_{n-1} \\ &= a_0(b_0+b_{v-1}) + \left\{ \left[ \sum_{i=1}^{v-1} a_i b_{v-1-i} + \sum_{i=v}^{n-2} a_i b_{n+v-1-i} \right] + a_{n-1}(b_v + b_{n-1}) \right\} \end{aligned}$$

The expressions of the corresponding row of the Mastrovito matrix is

$$z_{n-1,i} = \begin{cases} b_0 + b_{v-1} & i = 0 \\ b_{v-1-i} & 1 \leq i \leq v-1 \\ b_{n+v-1-i} & v \leq i \leq n-2 \\ b_v + b_{n-1} & i = n-1 \end{cases}$$

The XOR gate delay for computing $c_{n-1}$ is $1+\lceil \log_2 (n-1) \rceil$.

## REFERENCES


[1] G. Seroussi, "Table of Low-Weight Binary Irreducible Polynomials," *Technical Report HPL*-98-135, *Hewlett-Packard Laboratories*, Palo Alto, Calif., Aug. 1998, Available at http://www.hpl.hp.com/techreports/98/HPL-98-135.html.

[2] B. Sunar and C. K. Koc, "Mastrovito Multiplier for All Trinomials," *IEEE Transactions on Computers*, vol. 48, no. 5, pp. 522-527, May 1999.

[3] T. Zhang and K. K. Parhi, "Systematic Design of Original and Modified Mastrovito Multipliers for General Irreducible Polynomials," *IEEE Transactions on Computers*, vol. 50, no. 7, pp. 734-749, July 2001.

[4] A. Halbutogullari and C. K. Koc, "Mastrovito Multiplier for General Irreducible Polynomials," *IEEE Transactions on Computers*, vol. 49, no. 5, pp. 503-518, May 2000.

[5] A. Reyhani-Masoleh and M.A. Hasan, "Low Complexity Bit Parallel Architectures for Polynomial Basis Multiplication over $GF(2^m)$," *IEEE Transactions on Computers*, vol. 53, no. 8, pp. 945-959, Aug. 2004.

[6] H. Wu, "Bit parallel Finite Field Multiplier and Squarer Using Polynomial Basis," *IEEE Transactions on Computers*, vol. 51, no. 7, pp. 750-758, July 2002.

[7] H. Wu, "Montgomery Multiplier and Squarer for a Class of Finite Fields," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 521-529, May 2002.

[8] 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, July 1996.

[9] E. D. Mastrovito, "VLSI Architectures for Multiplication over Finite Field $GF(2^m)$," *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, T. Mora, ed., pp. 297-309, Springer-Verlag, 1988.

[10] C. K. Koc and T. Acar, "Montgomery Multiplication in $GF(2^k)$," *Designs, Codes, and Cryptography*, vol. 14, pp. 57-69, 1998.

[11] S. O. Lee, S. W. Jung, Ch. H. Kim, J. Yoon, J. Koh, and D. Kim, "Design of Bit Parallel Multiplier with Lower time complexity," *In Proc. ICICS'*2003, LNCS 2971, pp. 127-139, Springer-Verlag, 2004.

[12] 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.

[13] F. Rodriguez-Henriquez, and C. K. Koc, "Parallel Multipliers Based on Special Irreducible Pentanomials," *IEEE Transactions on Computers*, vol. 52, no. 12, pp. 1535-1542, Dec. 2003.

[14] Christophe Negre, "Quadrinomial Modular Arithmetic Using Modified Polynomial Basis," In *Proceedings of the International Conference on Information Technology: Coding and Computing* ( *ITCC*'2005), volume-I, pp. 550-555, 2005.

[15] H. Fan and M.A. Hasan, "Relationship between $GF(2^m)$ Montgomery and Shifted Polynomial Basis Multiplication Algorithms," *Technical Report, CACR 2005-30, University of Waterloo*, Waterloo, Canada., Aug. 2005.