Efficient Square-based Montgomery Multiplier for All Type C.1 Pentanomials

Yin Li[a,1], Xingpo Ma[a], Qin Chen[b], Chuanda Qi[a]

[a]*Department of Computer Science and Technology, Xinyang Normal University, Henan, China*
[b]*Department of Mathematics, Xinyang Normal University, Henan, China*

Abstract

In this paper, we present a low complexity bit-parallel Montgomery multiplier for $GF(2^m)$ generated with a special class of irreducible pentanomials $x^m + x^{m-1} + x^k + x + 1$. Based on a combination of generalized polynomial basis (GPB) squarer and a newly proposed square-based divide and conquer approach, we can partition field multiplications into a composition of sub-polynomial multiplications and Montgomery/GPB squarings, which have simpler architecture and thus can be implemented efficiently. Consequently, the proposed multiplier roughly saves 1/4 logic gates compared with the fastest multipliers, while the time complexity matches previous multipliers using divide and conquer algorithms.

Key words: Montgomery multiplication, Squaring, Bit-parallel, Type C.1 Pentanomial

1. Introduction

Finite field $GF(2^m)$ has several crucial applications in many areas such as combinatorial design, coding theory, computer algebra and cryptography [1, 2]. Much attention has been paid to efficient implementation of the $GF(2^m)$ multiplication, as it is an elementary arithmetic operation, and other complex arithmetic operations, e.g., exponentiation and inversion can be performed using multiplications. Nowadays, bit-parallel architectures have become very common because more and more circuit gates are assembled in a single chip. During recent years, a number of bit-parallel $GF(2^m)$ multipliers have been proposed to obtain lower space and time complexity. These schemes covered comprehensive cases, including different bases representations [4, 7] and generating polynomials [8, 9, 10, 12, 13]. Among them, polynomial basis (PB) and irreducible trinomial are more widely used. However, irreducible trinomial does not always exist for any field. As a substitution, irreducible pentanomials are more abundant. It is conjectured that there exist irreducible pentanomials for any degree $m \geq 4$ [14].

Note that the field multiplication using PB representation consists of a polynomial multiplication and a modular reduction. Generally, the PB multipliers based on pentanomials are less efficient than those based on trinomials, as pentanomials are more complicated in reduction process. Therefore, many space/time efficient solutions are proposed to exploit special form of pentanomial [24, 25, 4, 15], variant polynomial basis [23], etc. In [18], a new divide and conquer approach utilizing squaring operation, referred as PCHS approach, is adapted to design bit-parallel multiplier for type I and type II pentanomials. Their scheme requires high efficient squaring operation for pentanomials. Unfortunately, squarer for pentanomial is not very simple. Hariri and Reyhani-Masoleh [15] presented a Montgomery squarer for special pentanomials $x^m + x^{k+1} + x^k + x^{k-1} + 1$ where $(3 < k < (m-3)/2)$. Park [17] investigate the explicit formulae and complexities of squarers for general pentanomials. According to their results, the PB squarer for a general pentanomial costs at least $O(\frac{3m}{2})$ XOR gates with $3T_X$ delay. By contrast, squarer for type II pentanomial is more efficient, which costs about $\frac{3m}{2}$ XOR gates with $2T_X$ delay. In [7], Cilardo proposed a new PB variant, referred as *Generalized Polynomial Basis* (GPB), which optimized the multiplier architectures for irreducible pentanomials. Particularly, he suggested two types of pentanomials:
Type C.1: $x^m + x^{m-1} + x^k + x + 1$, $(m - 1 > k > 1)$,
Type C.2: $x^m + x^{m-k_1} + x^{k_2} + x^{k_1}$, $(m - k_1 > k_2 > k_1 > 1)$,
and gave corresponding optimal GPB parameters. He claimed that these types of GPB multipliers match or outperform the best special-type pentanomials. Based on Cilardo's work, Xiong and Fan [20] give an efficient GPB squarer for Type C.1 pentanomial $x^m + x^{m-1} + x^k + x + 1$, where $1 < k < \lfloor \frac{m}{2} \rfloor$.

In this paper, combining extensions of the previous GPB squarer and the PCHS approach, we can construct an efficient bit-parallel multiplier for type C.1 pentanomial $x^m + x^{m-1} + x^k + x + 1$, where $1 < k \leq \lfloor \frac{m}{2} \rfloor$. Please note that the GPB squarer is equivalent to Montgomery squarer [20]. The multiplier architecture we developed using GPB squarer actually performs Montgomery multiplication. Besides, applying an reciprocal property presented in [5, 7], we show that the same architecture can be employed to perform the Montgomery multiplication modulo $x^m + x^{m-1} + x^{m-k} + x + 1$, $\lceil \frac{m}{2} \rceil < m - k < m - 1$, only reversing input and output coefficients. As a result, the proposed multiplier has about 1/4 reduced space complexity compared with the fastest bit-parallel multipliers for all Type C.1 pentanomials. Furthermore, its space and time complexity nearly match Park et al. multiplier [18] for Type I and II pentanomials, where the same divide and conquer approach is applied.

Email addresses: yunfeiyangli@gmail.com (Yin Li), 1073397294@qq.com (Qin Chen)
[1]Corresponding author. Tel.:+86 18737627188

The rest of this paper is organized as follows: In Section 2, we briefly review the PCHS algorithm and the GPB squaring operation for Type C.1 pentanomials, then state the slight extensions for both of them. An important reciprocal property and some notations are also introduced. Based on these formulae, a new bit-parallel Montgomery multiplier is developed in Section 3 for $x^m + x^{m-1} + x^k + x + 1$, where $1 < k < \lfloor \frac{m}{2} \rfloor$. In Section 4, we will prove that previous architecture can be used for the field multiplication about $x^m + x^{m-1} + x^{m-k} + x + 1$ using the reciprocal property. In Section 5, we further analyze its complexity and present a comparison between our proposal and some others. Finally, some conclusions are drawn.

2. Preliminary

In this section, we briefly introduce some basic ingredients used in our scheme, including the PCHS algorithm, GPB squaring for Type C.1 pentanomials and some necessary lemmas.

2.1. The PCHS approach and its extension

The PCHS approach [18] is a divide and conquer algorithm for polynomial multiplication optimization, which works by breaking down a big polynomial into two sub-polynomials according to exponent parities of the indeterminate. The original one is only applicable for the polynomial multiplication of odd degree. Then it was extended to adapt to the polynomial multiplication of even degree [21]. We first assume that $A = \sum_{i=0}^{m-1} a_i x^i$ and $B = \sum_{i=0}^{m-1} b_i x^i$ are two polynomials in $\mathbb{F}_2[x]$ such that m is an odd integer. A, B can be partitioned into:

$$A = A_1^2 + xA_2^2 \text{ and } B = x^{-1}B_1^2 + B_2^2,$$

respectively, where

$$A_1 = \sum_{i=0}^{(m-1)/2} a_{2i}x^i,\ A_2 = \sum_{i=0}^{(m-3)/2} a_{2i+1}x^i,$$
$$B_1 = \sum_{i=1}^{(m-1)/2} b_{2i-1}x^i,\ B_2 = \sum_{i=0}^{(m-1)/2} b_{2i}x^i.$$

Then the polynomial multiplication AB can be rewritten as:

$$\begin{aligned} AB &= (A_1^2 + xA_2^2)(x^{-1}B_1^2 + B_2^2) \\ &= x^{-1}(A_1B_1)^2 + x(A_2B_2)^2 + (A_1B_2)^2 + (A_2B_1)^2 \\ &= (A_1B_1)^2(1 + x^{-1}) + (A_2B_2)^2(1 + x) + (CD)^2, \end{aligned} \tag{1}$$

where $C = A_1 + A_2, D = B_1 + B_2$. It is clear that (1) saves one partial multiplication at the cost of three extra partial additions. Thus, its key idea is analogous to Karatsuba algorithm. Equation (1) can be extended to the case of even m [21]. This case is a little different from the above case. A, B now are partitioned as:

$$A = A_1^2 + xA_2^2,\ \ B = B_1^2 + xB_2^2,$$

where

$$A_1 = \sum_{i=0}^{m/2-1} a_{2i}x^i,\ A_2 = \sum_{i=0}^{m/2-1} a_{2i+1}x^i,$$
$$B_1 = \sum_{i=0}^{m/2-1} b_{2i}x^i,\ B_2 = \sum_{i=0}^{m/2-1} b_{2i+1}x^i.$$

The polynomial multiplication AB here can be written as:

$$\begin{aligned} AB &= (A_1^2 + xA_2^2)(B_1^2 + xB_2^2) \\ &= (A_1^2 + xA_2^2)(x^{-1}B_1^2 + B_2^2) \cdot x \\ &= \left[x^{-1}(A_1B_1)^2 + x(A_2B_2)^2 + (A_1B_2)^2 + (A_2B_1)^2\right] \cdot x \\ &= \left[(A_1B_1)^2(1 + x^{-1}) + (A_2B_2)^2(1 + x) + (CD)^2\right] \cdot x \end{aligned} \tag{2}$$

where $C = A_1 + A_2, D = B_1 + B_2$. Obviously, besides polynomial multiplication and addition, Equation (1) and (2) contain squaring operation. To build efficient multiplier, these formulae should be combined with fast squaring operation. In [18], Park et al. utilized squaring formulae which is constructed using weakly dual basis (WDB) [17]. Montgomery squaring for trinomial is also utilized [21].

2.2. GPB Squarer for Type C.1 pentanomials

In order to describe GPB squaring operation, we first introduce the GPB definition [7]:

Definition 1. *Let the ordered set $M = \{x^i | 0 \le i \le m-1\}$ be a polynomial basis of $GF(2^m)$ over $\mathbb{F}_2$ and $R(x) \in GF(2^m)^*$. The ordered set $\{R(x) \cdot x^i | 0 \le i \le m-1\}$ is called a Generalized Polynomial Basis with respect to M.*

Obviously, provide that $A, B, C \in GF(2^m)$ are in PB representation and $f(x)$ is an irreducible polynomial that generated $GF(2^m)$. The field multiplication using GPB is defined as $CR = AR \cdot BR \bmod f(x)$. Similarly, the GPB squaring operation is

$$CR = (AR)^2 \bmod f(x).$$

Particularly, notice that the GPB parameter R is a nonzero element. Divided both sides of above equation by R, we have $C = A^2 \cdot R \bmod f(x)$ which can be recognized as Montgomery multiplication, where R is now the Montgomery factor. In fact, the Montgomery multiplication and GPB product in $GF(2^m)$ are essentially the same operation [7]. Notice that the GPB squaring formulae given in [20] pertains to PB representation of C, not its GPB representation.

As presented in [7], the Type C.1 pentanomial is $x^m + x^{m-1} + x^k + x + 1$ and its GPB parameter is $R = x^{m-k} + x^{m-k-1} + 1$. Xiong [20] gave the explicit formulae of GPB squaring for the above pentanomial. Nevertheless, they only investigated the case of m odd with $1 < k < \frac{m-1}{2}$. In the appendix A, we generalize their results and give the Montgomery/GPB squaring formulae for all m with $1 < k \le \frac{m-1}{2}$ (or $\frac{m}{2}$).

2.3. Reciprocal Polynomial

In [5, 7], the authors introduced an important property about the similarities between the finite fields generated with an irreducible polynomial $f(x)$ and its reciprocal polynomial $\overline{f}(x)$. Related definitions and lemmas are presented as follows.

Definition 2. *[7] Let $f(x) = p_m x^m + p_{m-1}x^{m-1} + \cdots + p_1 x + p_0$ be an polynomial over $\mathbb{F}_2$ of degree m and its reciprocal polynomial $\overline{f}(x)$ is defined as:*

$$\overline{f}(x) = p_0 x^m + p_1 x^{m-1} + \cdots + p_{m-1}x + p_m.$$

First, notice that if $f(x)$ is irreducible, then its reciprocal $\overline{f}(x)$ is irreducible as well [3]. Define a map ψ as:

$$\psi : \mathbb{F}_2[x]/(f) \to \mathbb{F}_2[x]/(\overline{f}), A = \sum_{i=0}^{m-1} a_i x^i \to \overline{A} = (\sum_{i=0}^{m-1} a_i x^{-i})x^m,$$

where $A \in \mathbb{F}_2[x]/(f)$ and $\overline{A} \in \mathbb{F}_2[x]/(\overline{f})$. Then we have following lemma.

Lemma 1. *[5] ψ is bijective and has the following properties:*

1. *ψ preserves the addition, and maps the addition in $\mathbb{F}_2[x]/(f)$ to the addition in $\mathbb{F}_2[x]/(\overline{f})$: $\overline{a+b} = \overline{a} + \overline{b}$.*
2. *For any $A \in \mathbb{F}_2[x]/(f)$, we have: $\psi(A \cdot x) = \overline{A \cdot x} = \overline{A} \cdot x^{-1}$.*
3. *ψ preserves the multiplication, and maps the multiplication in $\mathbb{F}_2[x]/(f)$ to the Montgomery multiplication in $\mathbb{F}_2[x]/(\overline{f})$, i.e., $\psi(A \cdot B) = \overline{A \cdot B} = \overline{A} \cdot \overline{B} \cdot x^{-m}$.*

The proof of Lemma 1 can be found in [5]. Based on the above lemma, Cilardo halve the number of cases to be analyzed for the exhaustive proof of GPB multipliers [7]. His conclusion can be summarized in following lemma.

Lemma 2. *[7] The GPB multiplier for a given irreducible polynomial $f(x)$ with a parameter $R(x)$ can also perform the GPB multiplication for its reciprocal polynomial $\overline{f}(x)$ with parameter $R(x^{-1}) \cdot x^{-(m-1)}$, by simply driving the coefficients of the operands and reading the output coefficients in the reversed order.*

We will also utilize such a property to extend our result in section 4.

3. Montgomery multiplier for Type C.1 pentanomials

Based on extended PCHS approach combined with GPB squarer, a new bit-parallel Montgomery multiplier for Type C.1 pentanomials is proposed in this section.

Suppose that finite field $GF(2^m)$ is defined by an irreducible Type C.1 pentanomial $f(x) = x^m + x^{m-1} + x^k + x + 1$ $(1 < k < \lfloor \frac{m}{2} \rfloor)$ with a root x, and the field elements are represented using polynomial basis $\{1, x, \cdots, x^{m-1}\}$. Let $A, B \in GF(2^m)$ be two arbitrary elements in polynomial basis representation:

$$A(x) = a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1 x + a_0,$$
$$B(x) = b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + \cdots + b_1 x + b_0,$$

where $a_i,\ b_i \in \mathbb{F}_2$.

Denoted by $\gamma(x) \in GF(2^m)^*$ the Montgomery factor, the Montgomery multiplication over $GF(2^m)$ is given by

$$A(x) \cdot B(x) \cdot \gamma(x) \bmod f(x). \tag{3}$$

Applying Equation (1) and (2) to above expression, we can expand (3) as follows:
m is odd.

$$\begin{aligned} AB\gamma &= \left[(A_1^2 + xA_2^2)(x^{-1}B_1^2 + B_2^2)\right]\gamma \\ &= (A_1B_1)^2\gamma(1+x^{-1}) + (A_2B_2)^2\gamma(1+x) + (CD)^2\gamma, \end{aligned}$$

where $C = A_1 + A_2, D = B_1 + B_2$.
m is even.

$$\begin{aligned} AB\gamma &= \left[(A_1^2 + xA_2^2)(B_1^2 + xB_2^2)\right]\gamma \\ &= (A_1B_1)^2\gamma x(1+x^{-1}) + (A_2B_2)^2\gamma x(1+x) + (CD)^2\gamma x, \end{aligned}$$

where $C = A_1 + A_2, D = B_1 + B_2$.

The two expressions as above both transform Montgomery multiplication into the three squaring operations. In order to apply the GPB squaring formulae, we choose the factor $\gamma(x)$ as follows:

$$\gamma = \begin{cases} R, & m \text{ is odd}, \\ R \cdot x^{-1}, & m \text{ is even}, \end{cases} \tag{4}$$

where $R = x^{m-k} + x^{m-k-1} + 1$ if $f(x) = x^m + x^{m-1} + x^k + x + 1$. As a result, the Montgomery multiplication (3) in two cases have the same expansion.

$$AB\gamma = (A_1B_1)^2R(1+x^{-1}) + (A_2B_2)^2R(1+x) + (CD)^2R. \tag{5}$$

Such expansions can reduce the number of cases to be analyzed for the development of our Montgomery multiplier. Meanwhile, their Montgomery squarings keep the simplest form.

It is easy to check that the degrees of A_1B_1, A_2B_2 and CD are at most $m-1$. From now on, the following notations are used:

$$A_1B_1 = \sum_{i=0}^{m-1} c_i x^i, A_2B_2 = \sum_{i=0}^{m-1} d_i x^i, CD = \sum_{i=0}^{m-1} e_i x^i,$$

$$S_1 = (A_1B_1)^2R(1+x^{-1}) \bmod f(x) = \sum_{i=0}^{m-1} r_i x^i,$$

$$S_2 = (A_2B_2)^2R(1+x) \bmod f(x) = \sum_{i=0}^{m-1} s_i x^i,$$

$$S_3 = (CD)^2R \bmod f(x) = \sum_{i=0}^{m-1} t_i x^i.$$

In the next subsections, we analyze the detailed computation of S_1, S_2 and S_3, respectively.

3.1. The Complexities of A_1B_1, A_2B_2, CD

In this subsection, we briefly analyze the complexities of the products A_1B_1, A_2B_2 and CD required in the computation of

S_1, S_2 and S_3. According to the previous description, the coefficients c_is of $A_1B_1 = \sum_{i=0}^{m-1} c_i x^i$ are given by:
m is odd.

$$c_i = \begin{cases} 0, & i = 0, \\ \sum_{j=0}^{i-1} a_{2j} b_{2(i-j)-1}, & 1 \le i \le \frac{m-1}{2}, \\ \sum_{j=i-\frac{m-1}{2}}^{\frac{m-1}{2}} a_{2j} b_{2(i-j)-1}, & \frac{m+1}{2} \le i \le m-1. \end{cases} \quad (6)$$

m is even.

$$c_i = \begin{cases} \sum_{j=0}^{i} a_{2j} b_{2(i-j)}, & 0 \le i \le \frac{m}{2} - 1, \\ \sum_{j=i-\frac{m}{2}+1}^{\frac{m}{2}-1} a_{2j} b_{2(i-j)}, & \frac{m}{2} \le i \le m-2. \end{cases} \quad (7)$$

Similarly, we can obtain the explicit formulae with respect to d_i. Notice that if m is odd, $c_0 = 0$ and $d_{m-1} = 0$, if m is even, we have $c_{m-1} = d_{m-1} = 0$. It is easy to check that the computation of c_is in (6) totally cost $\frac{m^2-1}{4}$ AND and $\frac{m^2-4m+3}{4}$ XOR gates with path delay $T_A + \lceil \log_2 \left(\frac{m-1}{2}\right) \rceil T_X$. When m is even, it requires $\frac{m^2}{4}$ AND and $\frac{m^2-4m+4}{4}$ XOR gates with path delay $T_A + \lceil \log_2 \left(\frac{m}{2}\right) \rceil T_X$. The space and time complexity related to A_2B_2 are the same as those of A_1B_1.

The computation of CD is a little different. Firstly note that the computation of $C = A_1 + A_2$ and $D = B_1 + B_2$ requires $m-1$ XOR gates (m gates if m is even) with one extra T_X gate delay. If m is odd, let $\sum_{i=0}^{\frac{m-1}{2}} u_i x^i = C$ and $\sum_{i=0}^{\frac{m-1}{2}} v_i x^i = D$, then we have

$$e_i = \begin{cases} \sum_{j=0}^{i} u_j v_{i-j}, & 0 \le i \le \frac{m-1}{2}, \\ \sum_{j=i-\frac{m-1}{2}}^{\frac{m-1}{2}} u_j v_{i-j}, & \frac{m+1}{2} \le i \le m-1. \end{cases} \quad (8)$$

If m is even, the degrees of C, D are at most $\frac{m}{2} - 1$, let $\sum_{i=0}^{\frac{m}{2}-1} u_i x^i = C$ and $\sum_{i=0}^{\frac{m}{2}-1} v_i x^i = D$, then the computation of e_is is

$$e_i = \begin{cases} \sum_{j=0}^{i} u_j v_{i-j}, & 0 \le i \le \frac{m}{2} - 1, \\ \sum_{j=i-\frac{m}{2}+1}^{\frac{m}{2}-1} u_j v_{i-j}, & \frac{m}{2} \le i \le m-2. \end{cases} \quad (9)$$

One can check that e_is in (8) cost $\frac{(m+1)^2}{4}$ AND and $\frac{(m-1)^2}{4}$ XOR gates with path delay $T_A + \lceil \log_2 \left(\frac{m+1}{2}\right) \rceil T_X$. Conversely, if m is even, e_is in (9) cost $\frac{m^2}{4}$ AND and $\frac{m^2-4m+4}{4}$ XOR gates with path delay $T_A + \lceil \log_2 \left(\frac{m}{2}\right) \rceil T_X$.

Moreover, the time complexity formulae immediately imply that the time delay of CD is equal to those of A_1B_1 and A_2B_2, except a few Type C.1 pentanomials. Only when m is odd and $\lceil \log_2 \left(\frac{m+1}{2}\right) \rceil > \lceil \log_2 \left(\frac{m-1}{2}\right) \rceil$, CD costs one more T_X compared with A_1B_1 and A_2B_2. This happens if and only if $m = 2^i + 1, i > 0$. In fact, we have checked the number of such irreducible Type C.1 pentanomials of degree between [7, 1025], and found that there are only 24 such pentanomials.

Example 3.1. Consider the field multiplication using PB representation over $GF(2^5)$ with the underlying irreducible pentanomial $x^5 + x^4 + x^2 + x + 1$. Since the degree is odd, the Montgomery factor is chosen as $\gamma = x^3 + x^2 + 1$. Assume that $A = \sum_{i=0}^{4} a_i x^{i-2}$ and $B = \sum_{i=0}^{4} b_i x^{i-2}$ are two elements in $GF(2^5)$. We partition A, B as $A = A_1^2 + xA_2^2, B = x^{-1}B_1^2 + B_2^2$, where

$$A_1 = a_4x^2 + a_2x + a_0,\ A_2 = a_3x + a_1,$$
$$B_1 = b_3x^2 + b_1x,\ B_2 = b_4x^2 + b_2x + b_0.$$

According to equation (1) and (3), then we have

$$\begin{aligned} ABR &= (A_1^2 + xA_2^2)(x^{-1}B_1^2 + B_2^2)R \\ &= [(A_1B_1)^2(1 + x^{-1}) + (A_2B_2)^2(1 + x) + (CD)^2]R \\ &= S_1 + S_2 + S_3, \end{aligned}$$

where $C = A_1 + A_2 = \sum_{i=0}^{2} u_i x^i = a_4x^2 + (a_2 + a_3)x + (a_0 + a_1)$, $D = B_1 + B_2 = \sum_{i=0}^{2} v_i x^i = (b_3 + b_4)x^2 + (b_1 + b_2)x + b_0$. Then,

$$\begin{aligned} A_1B_1 =& a_4b_3x^4 + (a_2b_3 + a_4b_1)x^3 + (a_0b_3 + a_2b_1)x^2 + a_0b_1x, \\ A_2B_2 =& a_3b_4x^3 + (a_1b_4 + a_3b_2)x^2 + (a_1b_2 + a_3b_0)x + a_1b_0, \\ CD =& u_2v_2x^4 + (u_1v_2 + u_2v_1)x^3 + (u_0v_2 + u_1v_1 + u_2v_0)x^2 \\ &+ (u_0v_1 + u_1v_0)x + u_0v_0. \end{aligned}$$

So the space and time complexities for A_1B_1, A_2B_2 and CD are straightforward. Also note that CD requires one more T_X than A_1B_1, A_2B_2, as $m = 5 = 2^2 + 1$ in this example.

3.2. The Computation of S_1, S_2, S_3

According to previous description, the key step in the computation of S_1, S_2, S_3 is Montgomery squaring (or GPB squaring) related to A_1B_1, A_2B_2 and CD. Consider the Montgomery/GPB squarer presented in the Appendix A, we classify Type C.1 pentanomials into eight categories. Then we analyze the computations of S_1, S_2, S_3 under different polynomial categories, respectively. The eight cases are as follows:

1. m is odd, k is even, $1 < k < \frac{m-1}{2}$;
2. m is odd, k is even, $k = \frac{m-1}{2}$;
3. m is odd, k is odd, $1 < k < \frac{m-1}{2}$;
4. m is odd, k is odd, $k = \frac{m-1}{2}$;
5. m is even, k is odd, $1 < k < \frac{m}{2}$;
6. m is even, k is odd, $k = \frac{m}{2}$;
7. m is even, k is even, $1 < k < \frac{m}{2}$;
8. m is even, k is even, $k = \frac{m}{2}$.

The above cases correspond to different Montgomery squaring formulae, resulting different expression of S_1, S_2 and S_3. Without loss of generality, we analyze two typical cases, i.e., case 1 and case 5.[2]

[2] We can follow a similar line of approaches used in case 1 and case 5.

Case 1: Denote $\sum_{i=0}^{m-1} z_i x^i$ as the Montgomery squaring $(A_1B_1)^2R \bmod f(x)$, we have following squaring formula:

$$z_i = \begin{cases} c_{k/2} + c_{(m+k-1)/2} + c_0, & i = 0, \\ c_{k/2} + c_{(m+k-1)/2}, & i = 1, \\ c_{(i+k)/2} + c_{(i+m+k-1)/2} + c_{i/2}, & i = 2, 4, \cdots, k-2, \\ c_{(i+k-1)/2} + c_{(i+m+k-2)/2}, & i = 3, 5, \cdots, k-1, \\ c_{(i+k)/2} + c_{(i+m+k-1)/2} + c_{(i+m-1)/2}, & i = k, k+2, \cdots, m-k-3, \\ c_{(i+k-1)/2} + c_{(i+m+k-2)/2}, & i = k+1, k+3, \\ & \cdots, m-k-2, \\ c_0 + c_{(m-1)/2} + c_{m-1} + c_{m-k/2-1}, & i = m-k-1, \\ c_0 + c_{(m-1)/2} + c_{m-1}, & i = m-k, \\ c_{(i+k)/2} + c_{(i-m+k-1)/2} + c_{(i+m-1)/2}, & i = m-k+1, m-k+3, \\ & \cdots, m-3, \\ c_{(i+k-1)/2} + c_{(i-m+k)/2}, & i = m-k+2, m-k+4, \\ & \cdots, m-2 \\ c_{m-1}, & i = m-1. \end{cases} \tag{10}$$

Since $x^m + x^{m-1} + x^k + x = 1$, we have $x^{-1} = x^{m-1} + x^{m-2} + x^{k-1} + 1$. It follows that:

$$\begin{aligned} S_1 &= \sum_{i=0}^{m-1} z_i x^i (1 + x^{-1}) \bmod x^m + x^{m-1} + x^k + x + 1 \\ &= \sum_{i=1, i\notin\Theta}^{m-3} (z_i + z_{i+1}) x^i + z_1 + (z_{k-1} + z_k + z_0) x^{k-1} + \\ &\quad (z_{m-1} + z_{m-2} + z_0) x^{m-2} + (z_{m-1} + z_0) x^{m-1}, \end{aligned} \tag{11}$$

where Θ represents a group $\{0, k-1, m-2, m-1\}$. Then we substitute z_i with the expressions in (10).The coefficients of S_1 are given by equation (13).

The computation of S_2 follows the same line of S_1. Let $\sum_{i=0}^{m-1} z'_i x^i$ denote the Montgomery squaring respect to A_2B_2, then we have:

$$\begin{aligned} S_2 &= \sum_{i=0}^{m-1} z'_i x^i (1 + x) \bmod x^m + x^{m-1} + x^k + x + 1 \\ &= \sum_{i=3, i\notin\Theta}^{m-2} (z'_i + z'_{i-1}) x^i + z'_{m-2} x^{m-1} + (z'_k + z'_{k-1} + z'_{m-1}) x^k + \\ &\quad + (z'_0 + z'_1 + z'_{m-1}) x + (z'_{m-1} + z'_0), \end{aligned} \tag{12}$$

where Θ represents a group of $\{0, 1, k, m-1\}$. The explicit formulae for the coefficients of S_2 are given in (14).

$$r_i = \begin{cases} c_{k/2} + c_{(m+k-1)/2}, & i = 0, \\ c_{(i+k+1)/2} + c_{(i+m+k)/2} + c_{(i+1)/2} & \\ \quad + c_{(i+k-1)/2} + c_{(i+m+k-2)/2}, & i = 1, 3, \cdots, k-3, \\ c_{i/2}, & i = 2, 4, \cdots, k-2, \\ c_{k/2} + c_0 + c_{k-1} + c_k & \\ \quad + c_{(m-1)/2+k} + c_{(m-3)/2+k}, & i = k-1, \\ c_{(i+m-1)/2}, & i = k, k+2, k+4, \\ & \cdots, m-k-3, \\ c_{(i+k+1)/2} + c_{(i+m+k)/2} + c_{(i+m)/2} & \\ \quad + c_{(i+k-1)/2} + c_{(i+m+k-2)/2}, & i = k+1, k+3, \\ & \cdots, m-k-4, \\ c_0 + c_{(m-1)/2} + c_{(m-3)/2} + & \\ \quad c_{m-k/2-1} + c_{m-2} + c_{m-1}, & i = m-k-2, \\ c_{m-k/2-1}, & i = m-k-1, \\ c_0 + c_1 + c_{(m-1)/2} + & \\ \quad c_{(m+1)/2} + c_{m-k/2} + c_{m-1} & i = m-k, \\ c_{(i+m-1)/2}, & i = m-k+1, m-k+3, \\ & \cdots, m-3, \\ c_{(i+k+1)/2} + c_{(i+m)/2} + c_{(i+k-1)/2} & \\ \quad + c_{(i-m+k)/2} + c_{(i-m+k+2)/2}, & i = m-k+2, m-k+4, \\ & \cdots, m-4, \\ c_{k/2} + c_{(m+k-1)/2} + c_0 + c_{m-1} + & \\ \quad c_{(m+k-3)/2} + c_{k/2-1}, & i = m-2, \\ c_{k/2} + c_{(m+k-1)/2} + c_0 + c_{m-1}, & i = m-1. \end{cases} \tag{13}$$

$$s_i = \begin{cases} d_{k/2} + d_{(m+k-1)/2} + d_0 + d_{m-1}, & i = 0, \\ d_0 + d_{m-1}, & i = 1, \\ d_{(i+k)/2} + d_{(i+m+k-1)/2} + d_{i/2} & \\ \quad + d_{(i+k-2)/2} + d_{(i+m+k-3)/2}, & i = 2, 4, \cdots, k-2, \\ d_{(i-1)/2}, & i = 3, 5, \cdots, k-1, \\ d_{k-1} + d_k + d_{(m-1)/2+k} & \\ \quad + d_{(m-3)/2+k} + d_{(k+m-1)/2} + d_{m-1}, & i = k, \\ d_{(i+k)/2} + d_{(i+m+k-1)/2} + d_{(i+m-1)/2} & \\ \quad + d_{(i+k-2)/2} + d_{(i+m+k-3)/2}, & i = k+2, k+4, \cdots, m-k-3, \\ & \cdots, m-k-3, \\ d_{(i+m-2)/2}, & i = k+1, k+3, \cdots, m-k-2, \\ d_0 + d_{(m-1)/2} + d_{(m-3)/2} + & \\ \quad d_{m-k/2-1} + d_{m-2} + d_{m-1}, & i = m-k-1, \\ d_{m-k/2-1}, & i = m-k, \\ d_0 + d_1 + d_{(m-1)/2} + & \\ \quad d_{(m+1)/2} + d_{m-k/2} + d_{m-1} & i = m-k+1, \\ d_{(i+k)/2} + d_{(i+m-1)/2} + d_{(i+k-2)/2} & \\ \quad + d_{(i-m+k+1)/2} + d_{(i-m+k-1)/2}, & i = m-k+3, m-k+5, \\ & \cdots, m-3, \\ d_{(i+m-2)/2}, & i = m-k+2, m-k+4, \\ & \cdots, m-2 \\ d_{(m+k-3)/2} + d_{k/2-1}, & i = m-1. \end{cases} \tag{14}$$

When we add S_1 and S_2 together using binary XOR tree, it is each to check that each coefficient $r_i + s_i$ consists of at most 7 items, which indicate that the parallel implementation of S_1+S_2 costs at most $\lceil \log_2 7 \rceil = 3$ XOR gates delay. Table 1 summarize the explicit number of items for each coefficient computation related to $S_1 + S_2$. We found that except several coefficients, most of them consist of 6 items. Note that $c_0 = d_{m-1} = 0$ in this case, it totally requires $5m-2$ XOR to obtain the coefficients of $S_1 + S_2$.

Table 1: Number items contained in $r_i + s_i$ of Case 1

$r_i + s_i$	#Items	Time delay
$i = 0$	6	$3T_X$
$i = 1$	7	$3T_X$
$i = 2, 3, \cdots, k-2$	6	$3T_X$
$i = k-1, k$	7	$3T_X$
$i = k+1, k+2, \cdots, m-k-3$	6	$3T_X$
$i = m-k-2, \cdots, m-k+1$	7	$3T_X$
$i = m-k+2, m-k+3, \cdots, m-3$	6	$3T_X$
$i = m-2$	7	$3T_X$
$i = m-1$	6	$3T_X$

Case 5: In this case, it is easy to check that S_1 and S_2 have the same transformation as case 1 presented in (11) and (12), but the Montgomery squaring formula is different. We have the coefficients formulae presented in (15) and (16).

Table 2 indicated that the parallel implementation of $S_1 + S_2$ in this case also requires at most $\lceil \log_2 7 \rceil = 3$ XOR gates delay. The explicit formulae about S_1, S_2 of other cases can be found in the appendix B. In this case, we have $c_{m-1} = d_{m-1} = 0$, therefore, it requires $5m - 1$ XOR to obtain $S_1 + S_2$ after we calculate A_1B_1, A_2B_2. Similarly we can easily obtain the time delay of $S_1 + S_2$ of other cases, one can check that all these computations can be finished in 3 T_X gates delay.

Table 2: Number items contained in $r_i + s_i$ in Case 5

$r_i + s_i$	#Items	Time delay
$i = 0$	6	$3T_X$
$i = 1$	7	$3T_X$
$i = 2, 3, \cdots, k-2$	6	$3T_X$
$i = k-1, k$	7	$3T_X$
$i = k+1, k+2, \cdots, m-k-3$	6	$3T_X$
$i = m-k-2, \cdots, i = m-k+1$	7	$3T_X$
$i = m-k+3, m-k+4, \cdots, m-3$	6	$3T_X$
$i = m-2$	7	$3T_X$
$i = m-1$	6	$3T_X$

$$
r_i = \begin{cases}
c_{(k+1)/2} + c_{(m+k-1)/2}, & i = 0, \\
c_{(i+1)/2} + c_{(i+m+k-2)/2} + c_{(i+m+k)/2}, & i = 1, 3, 5, \cdots, k-2, \\
c_{i/2} + c_{(i+k-1)/2} + c_{(i+k+1)/2}, & i = 2, 4, \cdots, k-3, \\
c_0 + c_{(k-1)/2} + c_k + c_{k-1}, & i = k-1, \\
c_{(m+k-1)/2} + c_{m/2+k} + c_{m/2+k-1}, & i = k, \\
c_{(i+k+1)/2} + c_{(i+m)/2} + c_{(k+i-1)/2}, & i = k+1, k+3, \cdots, m-k-3, \\
c_{(i+m+k)/2} + c_{(i+m+k-2)/2} + c_{(i+m-1)/2}, & i = k+2, k+4, \cdots, m-k-4, \\
c_0 + c_{m-(k+3)/2} + c_{m-2} + c_{m-1}, & i = m-k-2, \\
c_{m/2-1} + c_{m/2} + c_{m-(k+1)/2}, & i = m-k-1, \\
c_0 + c_1 + c_{m-1} + c_{m-(k+1)/2} & i = m-k, \\
c_{(i+k+1)/2} + c_{(i+m)/2} + c_{(i+k-1)/2} & i = m-k+1, m-k+3, \\
 & \quad \cdots, m-4, \\
c_{(i-m+k)/2} + c_{(i-m+k+2)/2} + c_{(i+m-1)/2}, & i = m-k+2, m-k+4, \\
 & \quad \cdots, m-3, \\
c_0 + c_{(m+k-1)/2} + c_{m-1} + c_{(m+k-3)/2}, & i = m-2, \\
c_0 + c_{(k-1)/2} + c_{(m+k-1)/2} + c_{m-1}, & i = m-1.
\end{cases} \tag{15}
$$

and

$$
s_i = \begin{cases}
d_0 + d_{(k-1)/2} + d_{(m+k-1)/2} + d_{m-1}, & i = 0, \\
d_0 + d_{(k-1)/2} + d_{(k+1)/2} + d_{m-1}, & i = 1, \\
d_{i/2} + d_{(i+m+k-3)/2} + d_{(i+m+k-1)/2}, & i = 2, 4, \cdots, k-1, \\
d_{(i-1)/2} + d_{(i+k-2)/2} + d_{(i+k)/2}, & i = 3, 5, \cdots, k-2, \\
d_k + d_{(m+k-1)/2} + d_{k-1} + d_{m-1}, & i = k, \\
d_{(m+k-1)/2} + d_{m/2+k} + d_{m/2+k-1}, & i = k+1, \\
d_{(i+k)/2} + d_{(i+m-1)/2} + d_{(k+i-2)/2}, & i = k+2, k+4, \cdots, m-k-2, \\
d_{(i+m+k-1)/2} + d_{(i+m+k-3)/2} + d_{(i+m-2)/2}, & i = k+3, k+5, \cdots, m-k-3, \\
d_0 + d_{m-(k+3)/2} + d_{m-2} + d_{m-1}, & i = m-k-1, \\
d_{m/2-1} + d_{m/2} + d_{m-(k+1)/2}, & i = m-k, \\
d_0 + d_1 + d_{m-1} + d_{m-(k+1)/2} & i = m-k+1, \\
d_{(i-m+k-1)/2} + d_{(i-m+k+1)/2} + d_{(i+m-2)/2}, & i = m-k+3, m-k+5, \\
 & \quad \cdots, m-2, \\
d_{(i+k)/2} + d_{(i+m-1)/2} + d_{(i+k-2)/2}, & i = m-k+2, m-k+4, \\
 & \quad \cdots, m-3, \\
d_{(k-1)/2} + d_{(m+k-3)/2}, & i = m-1.
\end{cases} \tag{16}
$$

We then consider the computation of S_3. After calculating CD, we just perform a Montgomery squaring to obtain S_3. According to the Montgomery squaring formulae presented in (10) and the appendix A, such operations can be implemented in $2T_X$ with no more than $\frac{3m}{2}$ XOR gates. Furthermore, as stated previously, the parallel pre-computation of $C = A_1 + A_2$ and $D = B_1 + B_2$ requires one extra T_X gate delay. Note that the circuit delay of CD is equal to A_1B_1 and A_2B_2 (except a few polynomials). Adding all these circuit delay together, we found that S_3 actually has same time delay as $S_1 + S_2$. Therefore, these two expressions can be calculated in parallel. In the end, we only need to add S_1+S_2 and S_3 together to obtain the result, which requires m XOR gates with one T_X delay.

The computation sequence can be arranged as follows:

$$\left\{\begin{array}{c|c|c} \underbrace{C,\ D}_{1T_X} & \underbrace{S_3=(CD)^2R}_{T_A+(2+\lceil\log_2\frac{m+1}{2}\rceil)T_X} & \\ \hline \underbrace{A_1B_1, A_2B_2}_{T_A+\lceil\log_2\frac{m-1}{2}\rceil T_X} & \underbrace{S_1+S_2}_{3T_X} & \underbrace{\begin{array}{c} AB\gamma= \\ (S_1+S_2)+S_3 \end{array}}_{1T_X} \end{array}\right. \tag{17}$$

where (S_1+S_2) denotes the result of S_1+S_2. We summarize the space complexity for each computation part presented as above in Table 3. Consequently, the total theoretic complexities of the

Table 3: The space complexity for each part of (17)

Case 1: m odd, k even, $1<k<(m-1)/2$		
Parts	# AND	#XOR
A_1B_1	$\frac{m^2-1}{4}$	$\frac{m^2-4m+3}{4}$
A_2B_2	$\frac{m^2-1}{4}$	$\frac{m^2-4m+3}{4}$
C, D	-	$m-1$
CD	$\frac{(m+1)^2}{4}$	$\frac{(m-1)^2}{4}$
S_1+S_2	-	$5m-2$
S_3	-	$m+1$
$AB\gamma$	-	m
Case 5: m even, k odd, $1<k<m/2$		
A_1B_1	$\frac{m^2}{4}$	$\frac{m^2-4m+4}{4}$
A_2B_2	$\frac{m^2}{4}$	$\frac{m^2-4m+4}{4}$
C, D	-	m
CD	$\frac{m^2}{4}$	$\frac{m^2-4m+4}{4}$
S_1+S_2	-	$5m-1$
S_3	-	$\frac{3m}{2}$
$AB\gamma$	-	m

proposed multiplier in case 1 are

$$\begin{aligned} &\#\text{AND}: \tfrac{3m^2}{4}+\tfrac{m}{2}-\tfrac{1}{4},\\ &\#\text{XOR}: \tfrac{3m^2}{4}+\tfrac{11m}{2}-\tfrac{1}{4},\\ &\text{Delay}: T_A+(3+\lceil\log_2(m+1)\rceil)\,T_X. \end{aligned}$$

Similarly, in case 5 the complexities are

$$\begin{aligned} &\#\text{AND}: \tfrac{3m^2}{4}\\ &\#\text{XOR}: \tfrac{3m^2}{4}+\tfrac{11m}{2}+2,\\ &\text{Delay}: T_A+(3+\lceil\log_2 m\rceil)\,T_X. \end{aligned}$$

The computation strategy of other cases are the same as those we presented in Case 1 and 5. Finally, we summarize the theoretic space and time complexity of these corresponding multipliers in the Table 4. Specially, the multiplier complexities of other cases are almost equal to those of case 1 and 5.

Example 3.2. Consider the computation of S_1, S_2, S_3 presented in Example 3.1. Based on the formulae in Appendix A and B, it is easy to obtain the coefficients of S_1, S_2, S_3 as follows:

$$S_1:\ \begin{cases} r_0+s_0=c_1+c_3,\\ r_1+s_1=c_2+c_3+c_4,\\ r_2+s_2=c_3,\\ r_3+s_3=c_2+c_1+c_3,\\ r_4+s_4=c_0+c_1+c_3+c_4. \end{cases}$$

$$S_2:\ \begin{cases} r_0+s_0=d_0+d_1+d_3+d_4,\\ r_1+s_1=d_0+d_4,\\ r_2+s_2=d_1+d_0+d_2,\\ r_3+s_3=d_3,\\ r_4+s_4=d_0+d_2+d_4. \end{cases}$$

$$S_3:\ \begin{cases} t_0=e_0+e_1+e_3,\\ t_1=e_1+e_3,\\ t_2=e_0+e_2+e_3+e_4,\\ t_3=e_0+e_2+e_4,\\ t_4=e_4. \end{cases}$$

It is obvious that each coefficient of S_1+S_2 consists of at most 7 terms, and thus can be calculated in $3T_X$. Meanwhile, each coefficient of S_3 contain at most 4 terms, which can be computed in $2T_X$. Thus, the computation of S_3 and S_1, S_2 can be arranged as (17).

4. Reciprocal property

Until now, we only analyze the Montgomery multiplier for the Type C.1 pentanomial $f(x)=x^m+x^{m-1}+x^k+x+1$ with k satisfying $1<k\le\frac{m-1}{2}$ (or $\frac{m}{2}$). According to the description in section 2.3, $\overline{f}(x)=x^m+x^{m-1}+x^{m-k}+x+1$ is the reciprocal polynomial of $f(x)$ and also irreducible over $\mathbb{F}_2$. Apparently, $\frac{m-1}{2}<m-k<m-1$ (or $\frac{m}{2}<m-k<m-1$), and such a type of pentanomial belongs to Type C.1 pentanomial as well. From Lemma 2, we know that the GPB multiplier circuits for $f(x)$ and $\overline{f}(x)$ can be identical by choosing proper GPB parameter. Notice that GPB multiplication is equivalent to Montgomery multiplication with the same parameter. However, as we use different architecture and a slightly different parameter γ (see equation (4)) to implement the Montgomery multiplication, the conclusion is not direct.

In this section, we will show that the square-based Montgomery multiplier with respect to $f(x)$ and its reciprocal polynomial $\overline{f}(x)$ can also be built using an identical circuit.

Theorem 1. *The circuit of square-based Montgomery multiplier for $\overline{f}(x)$ with the Montgomery factor $\gamma(x^{-1})\cdot x^{-(m-1)}$, is identical to that of $f(x)$ with Montgomery factor $\gamma(x)$.*

Before proving the above theorem, we first introduce a notation pertaining to the proof. Let $h(x)=\sum_{i=0}^{q}h_ix^i$ be an element in PB representation in $GF(2^m)$ with degree $q<m-1$, where q is the largest index that $h_q\neq 0$. $\tilde{h}(x)$ is denoted as $\sum_{i=0}^{q}h_ix^{q-i}$. That is to say the symbol $\tilde{(*)}$ denotes the reversion of the coefficients of $h(x)$ from index 0 to q. Please note that such a symbol is different from $\overline{(*)}$. For example, $h(x)=h_1x+h_0$ is an element of $GF(2^5)$, $\tilde{h}=h_0x+h_1$, while $\overline{h}=h_0x^5+h_1x^4$.

Table 4: Complexities of Montgomery multiplier for Type C.1 pentanomials

Case	#AND	#XOR	Delay
m odd, k even $1 < k \leq \frac{m-1}{2}$	$\frac{3m^2}{4} + \frac{m}{2} - \frac{1}{4}$	$\frac{3m^2}{4} + \frac{11m}{2} - \frac{1}{4}$	$T_A + (3 + \lceil \log_2(m+1) \rceil) T_X$
m odd, k odd $1 < k \leq \frac{m-1}{2}$			
m even, k odd $1 < k \leq \frac{m}{2}$	$\frac{3m^2}{4}$	$\frac{3m^2}{4} + \frac{11m}{2} + 2$	$T_A + (3 + \lceil \log_2 m \rceil) T_X$
m even, k even $1 < k \leq \frac{m}{2}$		$\frac{3m^2}{4} + \frac{11m}{2} + 1$	

Proof. Firstly, based on Lemma 1, we note that these two quotient ring $\mathbb{F}_2[x]/(f)$ and $\mathbb{F}_2[x]/(\overline{f})$ are isomorphic and the map ψ stated in section 2.3 is bijective. Any multiplication in $\mathbb{F}_2[x]/(f)$ is mapped to that of $\mathbb{F}_2[x]/(\overline{f})$. As presented in (5), our scheme split the Montgomery multiplication of $\mathbb{F}_2[x]/(f)$ into three parts, i.e., $AB\gamma = S_1 + S_2 + S_3$. Thus we have:

$$\begin{aligned}\psi(AB\gamma) &= \textstyle\sum_{i=0}^{m-1} h_i x^{m-i} = \psi(S_1) + \psi(S_2) + \psi(S_3) \\ &= \psi\left((A_1B_1)^2 R(1+x^{-1})\right) + \psi\left((A_2B_2)^2 R(1+x)\right) \\ &\qquad + \psi((CD)^2 R).\end{aligned} \tag{18}$$

Then we analyze the map of each part in above expression. Based on property 1 and 2 of Lemma 1, we have

$$\begin{aligned}\psi\left((A_1B_1)^2 R(1+x^{-1})\right) &= \psi\left((A_1B_1)^2 R\right) \cdot (1+x), \\ \psi\left((A_2B_2)^2 R(1+x)\right) &= \psi\left((A_2B_2)^2 R\right) \cdot (1+x^{-1}).\end{aligned} \tag{19}$$

According to Lemma 1, property 3, it is clear that

$$\begin{aligned}\psi\left((A_iB_i)^2 R\right) &= \psi\left((A_iB_i)^2\right) \cdot \psi(R) \cdot x^{-m} \\ &= \psi^2(A_iB_i) \cdot \psi(R) \cdot x^{-2m}, \ i = 1, 2, \\ \psi\left((CD)^2 R\right) &= \psi\left((CD)^2\right) \cdot \psi(R) \cdot x^{-m} \\ &= \psi^2(CD) \cdot \psi(R) \cdot x^{-2m}.\end{aligned} \tag{20}$$

One can also check that $\psi(A_iB_i) = \psi(A_i)\psi(B_i)x^{-m}$ (for $i = 1, 2$) and $\psi(CD) = \psi(C)\psi(D)x^{-m}$. Notice that the degrees of A_i, B_i, C, D are at most $\frac{m-1}{2}$ ($\frac{m}{2} - 1$ if m is even). It means that these expressions consist of at most $\frac{m+1}{2}$ (or $\frac{m}{2}$) nonzero elements. Thus, $\psi(A_i), \psi(B_i), \psi(C)$ and $\psi(D)$ can be recognized as left-shifting $\tilde{A}_i, \tilde{B}_i, \tilde{C}, \tilde{D}$ by certain bits. For example, if m is odd, $\psi(A_1) = \sum_{i=0}^{\frac{m-1}{2}} a_{2i} x^{m-i} = (\sum_{i=0}^{\frac{m-1}{2}} a_{2i} x^{\frac{m-1}{2}-i}) \cdot x^{\frac{m+1}{2}} = \tilde{A}_1 \cdot x^{\frac{m+1}{2}}$. If m is even, $\psi(A_1) = \sum_{i=0}^{\frac{m}{2}-1} a_{2i} x^{m-i} = (\sum_{i=0}^{\frac{m}{2}-1} a_{2i} x^{\frac{m}{2}-1-i}) \cdot x^{\frac{m}{2}+1} = \tilde{A}_1 \cdot x^{\frac{m}{2}+1}$. As a result, we immediately know that

$$\begin{cases} \psi(A_1B_1) = \psi(A_1)\psi(B_1)x^{-m} = \tilde{A}_1\tilde{B}_1 x^{m+1} x^{-m} = \tilde{A}_1\tilde{B}_1 x, \\ \psi(A_2B_2) = \psi(A_2)\psi(B_2)x^{-m} = \tilde{A}_2\tilde{B}_2 x^{m+2} x^{-m} = \tilde{A}_2\tilde{B}_2 x^2, \\ \psi(CD) = \psi(C)\psi(D)x^{-m} = \tilde{C}\tilde{D} x^{m+1} x^{-m} = \tilde{C}\tilde{D}x, \ (m \text{ odd}), \end{cases}$$

or

$$\begin{cases} \psi(A_iB_i) = \psi(A_i)\psi(B_i)x^{-m} = \tilde{A}_i\tilde{B}_i x^{m+2} x^{-m} = \tilde{A}_i\tilde{B}_i x^2, i = 1, 2, \\ \psi(CD) = \psi(C)\psi(D)x^{-m} = \tilde{C}\tilde{D} x^{m+2} x^{-m} = \tilde{C}\tilde{D}x^2, \ (m \text{ even}). \end{cases}$$

If m is odd, plug above expressions into (19) and (20), the equation (18) can be rewritten as:

$$\psi(AB\gamma) = \left((\tilde{A}_1\tilde{B}_1)^2(1+x) + (\tilde{A}_2\tilde{B}_2 x)^2(1+x^{-1}) + (\tilde{C}\tilde{D})^2\right) \cdot \psi(R) x^{-2m+2}.$$

Specially, notice that $\deg(\tilde{A}_2) = \frac{m-3}{2}$ and $\deg(\tilde{B}_2) = \frac{m-1}{2}$, then $\deg(A_2B_2x) = m-1$. It is easy to check that the degrees of $\tilde{A}_1\tilde{B}_1$ and $\tilde{C}\tilde{D}$ are both $m-1$. Since $R = x^{m-k} + x^{m-k-1} + 1$, we have $\psi(R) = x^k + x^{k+1} + x^m$. Multiplying both sides by x^{-1}, we get

$$\begin{aligned}\sum_{i=0}^{m-1} h_i x^{m-i-1} = &\left((\tilde{A}_1\tilde{B}_1)^2(1+x) + (\tilde{A}_2\tilde{B}_2)^2(1+x^{-1})\right. \\ &\left. + (\tilde{C}\tilde{D})^2\right) \cdot (x^{k-1} + x^k + x^{m-1}) x^{-2m+2},\end{aligned}$$

where $\sum_{i=0}^{m-1} h_i x^{m-i-1}$ is the reciprocal of $AB\gamma = \sum_{i=0}^{m-1} h_i x^i$.

If m is even, the transformation of $\psi(AB\gamma)$ is a little different,

$$\begin{aligned}\psi(AB\gamma) = &\left((\tilde{A}_1\tilde{B}_1 x)^2(1+x) + (\tilde{A}_2\tilde{B}_2 x)^2(1+x^{-1})\right. \\ &\left. + (\tilde{C}\tilde{D}x)^2\right) \cdot \psi(R) x^{-2m+2}.\end{aligned}$$

Notice that the degrees of A_i, B_i and C, D in this case are all $\frac{m}{2} - 1$, so $\deg(A_iB_ix) = \deg(CDx) = m-1$. Then we also have,

$$\begin{aligned}\sum_{i=0}^{m-1} h_i x^{m-i-1} = &\left((\tilde{A}_1\tilde{B}_1 x)^2(1+x) + (\tilde{A}_2\tilde{B}_2 x)^2(1+x^{-1})\right. \\ &\left. + (\tilde{C}\tilde{D}x)^2\right) \cdot (x^{k-1} + x^k + x^{m-1}) x^{-2m+2}.\end{aligned}$$

We note that $(x^{k-1} + x^k + x^{m-1})x^{-2m+2} = (x^{k-m} + x^{k-m+1} + 1)x^{-m+1} = R(x^{-1}) \cdot x^{-(m-1)} = R'(x)$, which is identical to the optimal GPB parameter for $\overline{f}(x)$ proposed in [7]. Let

$$\begin{aligned}S'_1 &= (\tilde{A}_2\tilde{B}_2 x)^2 R'(1+x^{-1}) \bmod \overline{f}(x), \\ S'_2 &= (\tilde{A}_1\tilde{B}_1)^2 R'(1+x) \bmod \overline{f}(x), \\ S'_3 &= (\tilde{C}\tilde{D})^2 R' \bmod \overline{f}(x), \text{ if } m \text{ is odd},\end{aligned}$$

or

$$\begin{aligned}S'_1 &= (\tilde{A}_2\tilde{B}_2 x)^2 R'(1+x^{-1}) \bmod \overline{f}(x), \\ S'_2 &= (\tilde{A}_1\tilde{B}_1 x)^2 R'(1+x) \bmod \overline{f}(x), \\ S'_3 &= (\tilde{C}\tilde{D}x)^2 R' \bmod \overline{f}(x), \text{ if } m \text{ is even}.\end{aligned}$$

Therefore, the computation of $\sum_{i=0}^{m-1} h_i x^{m-i-1}$ can be partitioned into three parts that are identical to that of $\sum_{i=0}^{m-1} h_i x^i$, and the

corresponding Montgomery squaring operations are related to $\overline{f}(x)$ with R'. From Lemma 2, we know that the GPB (Montgomery) squarers for both $f(x)$ with R and $\overline{f}(x)$ with R' are identical. Thus, the circuits for computation S'_1, S'_2, S'_3 are the same as that of S_1, S_2, S_3. Furthermore, according to the definition of $(\tilde{*})$, $\tilde{A}_i, \tilde{B}_i, i = 1, 2$ can constitute to $\tilde{A}$, $\tilde{B}$, which are the reverses of A, B.

Besides, if we do not split the Montgomery multiplication $AB\gamma$ and follow the same line of Lemma 2 proof presented in [6], it is easy to obtain the Montgomery factor for $\overline{f}(x)$ is $\gamma' = \gamma(x^{-1}) \cdot x^{-(m-1)}$. In conclusion, the circuit of square-based Montgomery multiplier for $\overline{f}(x)$ is identical to that of $f(x)$, by by simply driving the coefficients of the operands and reading the output coefficients in the reversed order. □

5. Comparison and Discussion

Since irreducible trinomials can offer the best performance [4, 15], irreducible pentanomials are most often exploited as alternative polynomials for those fields where irreducible trinomials do not exist. Moreover, special form of pentanomials are often considered. Such pentanomials include Type I, Type II, [24, 25, 4, 15], Type C.1 and Type C.2 pentanomials [7].

In Table 5, we give a comparison of several different bit-parallel multipliers for irreducible pentanomials according to space and time complexity. We especially focus on special types of pentanomials as above. All these multipliers are using PB representations except particular description. It is easy to check that our proposal is as fast as those multipliers for Type I and Type II pentanomials expect a few schemes, but obtains roughly 1/4 logic gates gain. Compared with original GPB multipliers for Type C.1 and C.2 pentanomials, our proposal is at most $2T_X$ slower than the fastest result (for good field, it requires only $1T_X$ more gates delay). In addition, Our scheme matches the original PCHS multiplier [18] with respect to the space and time complexities.

6. Conclusion

In this paper, we proposed a new square-based bit-parallel Montgomery multiplier architecture for a class of pentanomials. We have extended the square-based divide and conquer approach (PCSH scheme) to the modular multiplication for irreducible Type C.1 pentanomials, which are abundant and efficient to implement. The developed computation approach effectively exploits subexpression sharing and the complexity analyses are given in detail. Meanwhile, a reciprocal property is utilized to prove that two reciprocal Type C.1 pentanomials shares the same circuit. It is argued that the space complexity of our proposal is about the same as those of the original PCHS multipliers, while the time complexity can match some previous multipliers and Montgomery multipliers, which are developed without any divide and conquer algorithms.

Since the our proposal relies on efficient squaring operations, the possible future work in this line should include Montgomery multiplier for Type C.2 pentanomials based on efficient GPB squaring operations.

Acknowledgements

The first author is supported by the National Natural Science Foundation of China (Grant No. 61402393, 61601396) and Shanghai Key Laboratory of Integrated Administration Technologies for Information Security (No. AGK201607).

References

[1] A.J. Menezes, I.F. Blake, X. Gao, R.C. Mullin, S.A. Vanstone, T. Yaghoobian, Applications of Finite Fields, Kluwer Academic, Norwell, Massachusetts, USA, 1993.

[2] I. Blake, G. Seroussi, N. Smart, Elliptic Curves in Cryptography, Lond. Math. Soc. Lect. Note Ser., vol. 265, Cambridge University Press, 1999.

[3] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, New York, NY, USA, 1996.

[4] H. Fan, M.A. Hasan, Fast Bit Parallel-Shifted Polynomial Basis Multipliers in $GF(2^n)$, IEEE Trans. Circuits and Systems I: Fundamental Theory and Applications, 53(12) (Dec. 2006) 2606–2615.

[5] A. Cilardo, A. Mazzeo,N. Mazzocca, Representation of elements in F_{2^m} enabling unified field arithmetic for elliptic curve cryptography, Electronics Letters, 2005, 41, 798-800

[6] A. Cilardo. Efficient bit-parallel $GF(2^m)$ multiplier for a large class of irreducible pentanomials. *IEEE Transactions on Computers*, 58(7):1001–1008, July 2009.

[7] A. Cilardo, Fast Parallel $GF(2^m)$ Polynomial Multiplication for All Degrees, IEEE Transactions on Computers, 62(5) (May 2013) 929–943.

[8] B. Sunar and Ç.K. Koç, Mastrovito multiplier for all trinomials, IEEE Transactions on Computers, 48(5) (1999) 522–527.

[9] A. Halbutogullari and Ç.K. Koç, Mastrovito multiplier for general irreducible polynomials, IEEE Transactions on Computers, 49(5) (May 2000) 503–518.

[10] T. Zhang and K.K. Parhi, Systematic design of original and modified mastrovito multipliers for general irreducible polynomials, IEEE Transactions on Computers, 50(7) (July 2001) 734–749.

[11] H. Fan and M.A. Hasan, Relationship between $GF(2^m)$ Montgomery and Shifted Polynomial Basis Multiplication Algorithms Computers, IEEE Transactions on, 2006, 55, 1202–1206.

[12] H. Fan, A Chinese Remainder Theorem Approach to Bit-Parallel $GF(2^n)$ Polynomial Basis Multipliers for Irreducible Trinomials, IEEE Transactions on Computers, 2016, 65(2), 343–352.

[13] H. Fan and M.A. Hasan, A survey of some recent bit-parallel multipliers, Finite Fields and Their Applications, 32 (2015) 5–43.

[14] G. Seroussi, Table of Low-Weight Binary Irreducible Polynomials, Technical Report HPL-98- 135, Hewlett-Packard Laboratones, Aug. 1998.

[15] A. Hariri and A. Reyhani-Masoleh, Bit-serial and bit-parallel Montgomery multiplication and squaring over $GF(2^m)$, IEEE Transactions on Computers, 58(10) (October 2009) 1332–1345.

[16] S. Park, K. Chang, D. Hong, Efficient Bit-Parallel Multiplier for Irreducible Pentanomials Using a Shifted Polynomial Basis, IEEE Transactions on Computers, IEEE Computer Society, 55, (2006) 1211–1215

[17] S. Park, Explicit formulae of polynomial basis squarer for pentanomials using weakly dual basis Integration, Integration, the VLSI Journal, 45 (2012) 205–210.

[18] S. Park, K, Chang, D. Hong, and C. Seo, New efficient bit-parallel polynomial basis multiplier for special pentanomials, Integration, the VLSI Journal, 47(1) (2014) 130–139.

[19] Y. Cho, N. Chang, C. Kim, Y. Park, and S. Hong, New bit parallel multiplier with low space complexity for all irreducible trinomials over $GF(2^n)$, IEEE Transaction on Very Large Scale Integration (VLSI) Systems, 20(10) (October 2012) 1903–1908.

[20] X. Xiong, H. Fan, $GF(2^n)$ bit-parallel squarer using generalised polynomial basis for new class of irreducible pentanomials, Electronics Letters , 50(9) (April 2014) 655–657.

[21] Y. Li, Y. Chen, New bit-parallel Montgomery multiplier for trinomials using squaring operation, Integration, the VLSI Journal, 52, (2016) 142–155

[22] J. L. Imaña, R. Hermida, and F. Tirado. Low complexity bit-parallel multipliers based on a class of irreducible pentanomials. IEEE Transactions

Table 5: Comparison of Some Bit-Parallel Multipliers for Irreducible Pentanomials

Pentanomial	Bases	# AND	# XOR	Time delay
$x^m + x^{k_3} + x^{k_2} + x^{k_1} + 1$	SPB [16] ($k_3 \le \frac{m}{2}$)	m^2	$m^2 + 2m - 3$	$T_A + (3 + \lceil \log_2(m-1) \rceil) T_X$
	SPB [6] ($k_3 - k_1 \le \frac{m}{2}$)	m^2	$m^2 + 2m - 3$	$T_A + (3 + \lceil \log_2(m-1) \rceil) T_X$
$x^m + x^{k_3} + x^{k_2} + x + 1$	PB [24] ($k_3 \le \frac{m}{2}$)	m^2	$m^2 + 2m - 3$	$T_A + (3 + \lceil \log_2(m-1) \rceil) T_X$
$x^{m+1} + x^{k_2} + x^{k_1} + 1$	Redundant [23]	m^2	$m^2 + 2m + k_2 - k_1$	$T_A + (2 + \lceil \log_2(m+1) \rceil) T_X$
Type I:	PB [25]	m^2	$m^2 + m + 2k$	$T_A + (3 + \lceil \log_2 m \rceil) T_X$
$x^m + x^{k+1} + x^k + x + 1$	PB [24]	m^2	$m^2 + m$	$T_A + (3 + \lceil \log_2(m-1) \rceil) T_X$
$(2 < k < \frac{m}{2})$	PB [22]	m^2	$m^2 + m - 1$	$T_A + (3 + \lceil \log_2(m-1) \rceil) T_X$
	PCHS [18] (k even)	$\frac{3m^2}{4} + \frac{m}{2} - \frac{1}{4}$	$\frac{3m^2}{4} + 6m + 2k + \frac{17}{4}$	$T_A + (3 + \lceil \log_2(m+1) \rceil) T_X$
	(k odd)	$\frac{3m^2}{4} + \frac{m}{2} - \frac{1}{4}$	$\frac{3m^2}{4} + 6m + 2k + \frac{21}{4}$	$T_A + (3 + \lceil \log_2(m+1) \rceil) T_X$
Type II:	DB[25] ($2 \le k < \frac{m}{2}$)	m^2	$m^2 + \lceil \frac{3m}{2} \rceil + 3k - 6$	$T_A + (3 + \lceil \log_2 m \rceil) T_X$
$x^m + x^{k+2} + x^{k+1} + x^k + 1$	SPB[4] ($2k > m + 1$)	m^2	$m^2 + 3m - 7$	$T_A + \lceil \log_2(2m + 2k - 2) \rceil T_X$
	($2k \le m + 1$)			$T_A + \lceil \log_2(4m - 2k - 2) \rceil T_X$
	Montgomery [15] ($2k \ge m + 1$)	m^2	$m^2 + 3m - 9$	$T_A + \lceil \log_2(2m + 2k - 2) \rceil T_X$
	($2k < m + 1$)			$T_A + \lceil \log_2(4m - 2k - 2) \rceil T_X$
	PCHS [18] (k even)	$\frac{3m^2}{4} + \frac{m}{2} - \frac{1}{4}$	$\frac{3m^2}{4} + 6m + \frac{7k}{2} + \frac{45}{4}$	$T_A + (3 + \lceil \log_2(m+1) \rceil) T_X$
	(k odd, $k \le \frac{3(m-7)}{8}$	$\frac{3m^2}{4} + \frac{m}{2} - \frac{1}{4}$	$\frac{3m^2}{4} + 6m + \frac{7k}{2} + \frac{35}{4}$	$T_A + (3 + \lceil \log_2(m+1) \rceil) T_X$
	PB[26]	m^2	$m^2 + 2m + 3k + \alpha - \beta$	$T_A + (\lfloor \log_2 m \rfloor + \lceil \log_2 \lceil \frac{4m+3k-9}{2^{\lfloor \log_2 m \rfloor}} \rceil \rceil) T_X$
Type C.1:	GPB [7] ($2k < m - 1$)	m^2	$m^2 + m + 3$	$T_A + (\lceil \log_2(4m - 2k) \rceil) T_X$
$x^m + x^{m-1} + x^k + x + 1$	$2k = m - 1$			$T_A + (\lceil \log_2(3m + 3) \rceil) T_X$
	$2k = m$			$T_A + (\lceil \log_2(3m + 4) \rceil) T_X$
	Proposed (m even)	$\frac{3m^2}{4}$	$\frac{3m^2}{4} + \frac{11m}{2}$	$T_A + (3 + \lceil \log_2 m \rceil) T_X$
	Proposed (m odd)	$\frac{3m^2}{4} + \frac{m}{2} - \frac{1}{4}$		$T_A + (3 + \lceil \log_2(m+1) \rceil) T_X$
Type C.2:	GPB [7] ($2k_2 < m - k_1$)	m^2	$m^2 + m + O(k_1)$	$T_A + \lceil \log_2(4m - 2k_2 + 2k_1 - 2) \rceil T_X$
$x^m + x^{m-k_1} + x^{k_2} + x^{k_1} + 1$	($2k_2 = m - k_1$)			$T_A + \lceil \log_2(3m + 3k_1) \rceil T_X$
$k_2 \le m - k_1$	($2k_2 = m, m$ even)			$T_A + \lceil \log_2(3m + 4) \rceil T_X$
Description: $\alpha = 3(\Upsilon_{m-1} + \Upsilon_{k+1})$, $\beta = H_k + \Sigma_m + H_\theta$ ($\theta = k$ for even k and $\theta = k - 1$ for odd k).				
H_i represents the hamming weight of integer i, function $\Upsilon_h = \sum_{i=1}^{h} (H_i - 1)$, $\Sigma_m = \sum_{i=2,4,\cdots} H_i$.				

on Very Large Scale Integration (VLSI) Systems, 14(12):1388–1393, Dec 2006.

[23] C. Negre. Quadrinomial modular arithmetic using modified polynomial basis. In International Conference on Information Technology: Coding and Computing (ITCC'05) - Volume II, volume 1, pages 550–555 Vol. 1, April 2005.

[24] Arash Reyhani-Masoleh and M. Anwar Hasan. Low complexity bit parallel architectures for polynomial basis multiplication over $GF(2^m)$. IEEE Transactions on Computers, 53(8):945–959, 2004.

[25] Francisco Rodríguez-Henríquez and Çetin Kaya Koç. Parallel multipliers based on special irreducible pentanomials. IEEE Transactions on Computers, 52(12):1535–1542, 2003.

[26] J. L. Imaña. High-speed polynomial basis multipliers over $GF(2^m)$ for special pentanomials. IEEE Transactions on Circuits and Systems I: Regular Papers, 63(1):58–69, Jan 2016.