Scalable Systolic Multiplier over Binary Extension Fields Based on Two-Level Karatsuba Decomposition

Chiou-Yng Lee, Wen-Yo Lee, Chieh-Tsai Wu, Cheng-Chen Yang

Abstract—Shifted polynomial basis (SPB) is a variation of polynomial basis representation. SPB has potential for efficient bit level and digit-level implementations of multiplication over binary extension fields with subquadratic space complexity. For efficient implementation of pairing computation with large finite fields, this paper presents a new SPB multiplication algorithm based on Karatsuba schemes, and used to derive a novel scalable multiplier architecture. Analytical results show that the proposed multiplier provides a trade-off between space and time complexities. Our proposed multiplier is modular, regular, and suitable for very large scale integration (VLSI) implementations. It involves less area complexity compared to the multipliers based on traditional decomposition methods. It is therefore, more suitable for efficient hardware implementation of pairing based cryptography and elliptic curve cryptography (ECC) in constraint driven applications. Several systolic architectures for multiplication over GF(2\(^m\)) are proposed, which could be categorized into bit-parallel and bit-serial architectures. Bit-parallel systolic multipliers perform fast computations, and they are suitable for high-throughput implementations [9], [10]. Nonetheless, such architectures require space-complexity of \(O(m^2)\) and typically involve latency of \(O(m)\). Bit-serial systolic array multipliers require only \(O(m)\) space-complexity [11], [12], but require longer computation time which is not preferable for high-speed applications. To achieve the trade-off between the time and space complexities, digit-serial systolic multipliers with digit-in-digit-out and digit-in-parallel-out structures have been proposed [13], [14]. Moreover, scalable multipliers have also been proposed to achieve a trade-off between time and space complexities. Scalable multipliers [15] are based on fixed \(d \times d\) Hankel matrix-vector product (HMVP) approach, which perform the multiplication through \(\frac{n^2}{2}\) partial products using classical decomposition method. Such kind of scalable feature is used by reconfigurable hardware to decide on the number of partial products to obtain the full multiplication results. Selection of appropriate HMVP structure can lead to less area-delay product compared to classical digit-serial systolic multipliers.

In this paper, we have used SPB for the representation of operands in the proposed algorithm for scalable multiplication over GF(2\(^m\)). The proposed multiplication algorithm utilizes two-level KA algorithm, where the outer-level KA performs multi-term decomposition of input polynomials; and the inner-level KA builds parallel systolic multiplier using the products of decomposed input words. The proposed parallel systolic multiplier is realized through \(\frac{n^2}{2}\) partial products of \(d\)-bit words, where \(n = \lceil \frac{m}{2} \rceil\). In this paper, we propose a reconfigurable approach to generate necessary operands of those partial products to be used in the proposed scalable systolic multiplier over GF(2\(^m\)). Through detail analytical results we have shown that the proposed approach results in a novel scalable systolic array multiplier for fields of large order, which provides a trade-off between space and time complexities.

II. MATHEMATICAL BACKGROUND

In this Section, we briefly review the classical SPB multiplication over GF(2\(^m\)) and the Karatsuba algorithm.

A. SPB Multiplication over GF(2\(^m\))

The ordered set \(N = \{1, x, x^2, \ldots, x^{m-1}\}\) is called the polynomial basis of binary extension field GF(2\(^m\)), where \(x\) is the root of the irreducible polynomial \(F(x)\) of degree \(m\). The field element \(A\) in GF(2\(^m\)) can be represented as \(A = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1}\) where \(a_i \in \{0, 1\}\) for all \(i\). Let \(A, B,\) and \(C\) be three elements in GF(2\(^m\)), where \(C = AB \mod F(x)\). Generally, the computation of the product \(C\) is a two-step operation: (1) the grade-school multiplication
\[ D = AB \] of at most degree \(2m - 2\), and (2) the polynomial reduction to compute \( C = D \mod F(x)\).

To represent the elements over \(GF(2^m)\), Fan and Dai [6] have defined the SPB of \(GF(2^m)\) to derive efficient bit-parallel multiplier for all trinomials as follows:

**Definition 1.** Let \(v\) be an integer, and let the set \(N = \{1, x, x^2, \ldots, x^{m-1}\}\) be the polynomial basis of \(GF(2^m)\). Then the ordered set \(N_{x^{-v}} = \{x^{-v}, x^{-1-v}, x^{2-v}, \ldots, x^{m-1-v}\}\) is called the shifted polynomial basis of \(GF(2^m)\) with respect to \(N\).

Using the SPB, an element \(A = \sum_{i=0}^{m-1} a_i x^i \in GF(2^m)\) can be represented as \(\overline{A} = x^{-v}A = \sum_{i=0}^{m-1} a_i x^{-v-i}\). It is interesting that there is no hardware cost for the inter-conversion of elements \(A\) and \(\overline{A}\). For any two elements \(\overline{A} = x^{-v}A\) and \(\overline{B} = x^{-v}B\) in the SPB representation of \(GF(2^m)\), the SPB product \(C = x^vC\) of \(\overline{A}\) and \(\overline{B}\) can directly be obtained as

\[ C = x^vAB \mod F(x) \]  
(1)

The two-step computation of SPB multiplication of (1) is described as follows:

**Step-1:** Grade-school multiplication step

\[ T = AB = t_0 + t_1x + \cdots + t_{2m-2}x^{2m-2} \]  
(2)

where

\[ t_i = \begin{cases} \sum_{k=0}^{i} a_k b_{i-k}, & 0 \leq i \leq m - 1 \\ \sum_{i=0}^{m-1} a_k b_{m-1-k}, & m \leq i \leq 2m - 2 \end{cases} 
\]

**Step-2:** Polynomial reduction step

\[ C = Tx^{-v} \mod F(x) \]  
(3)

According to (3), the complexity of SPB multiplier depends on the chosen value of \(v\). The complexity of SPB multipliers for the field generated by certain types of irreducible polynomials, such as trinomials and pentanomials, is discussed in [6].

**B. Multi-term Karatsuba Algorithm**

Karatsuba algorithm [16] provides divide-and-conquer technique to multiply long polynomials. It uses three subproducts of half-length operands to replace the original grade-school multiplication. For example, let \(A = A_0 + x^{\frac{m}{2}} A_1\) and \(B = B_0 + x^{\frac{m}{2}} B_1\) be two polynomials of degree \(m\), where \(A_0, A_1, B_0,\) and \(B_1\) are four polynomials of degree \(\frac{m}{2}\). The product of \(A\) and \(B\) can be represented as

\[ AB = A_0 B_0 + [A_0 + A_1](B_0 + B_1) \]
\[ + A_0 B_0 + A_1 B_1 x^{m} + A_1 B_1 x^{m}. \]  
(4)

Based on Karatsuba algorithm, multiplication can be performed in three stages as follows.

1) **Evaluation Point (EP)** Generation Stage:

The polynomial \(A = (A_0, A_1)\) is split into the evaluation point vector \(EP(A) = (A_0, A_0 + A_1, A_1)\). Similarly, the polynomial \(B = (B_0, B_1)\) is also split into \(EP(B) = (B_0, B_0 + B_1, B_1)\).

2) **Point-Wise Multiplication (PWM)** Stage:

PWM stage performs point-wise multiplication of \(EP(A)\) and \(EP(B)\). The PWM is performed after EP generation to produce three products: \(D_0 = A_0B_0, D_1 = (A_0 + A_1)(B_0 + B_1),\) and \(D_2 = A_1B_1\). Thus, we can define that

\[ D = PWM(EP(A), EP(B)) = (D_0, D_1, D_2). \]  
(5)

3) **Reconstruction (R)** Stage:

In this step, the result of the PWM stage is used to construct the desired multiplication result, given by

\[ C = (C_0, C_1, C_2) \]

\[ = R(D) = (D_0, D_0 + D_1 + D_2, D_2). \]  
(6)

By applying this strategy recursively, each polynomial is transformed into three polynomials with their degrees reduced to about half of its previous polynomial. The decomposition algorithm could be terminated after the polynomials degenerate into single-bit coefficients. The multiplication based on recursive KA scheme is shown in the functional block architecture of Fig. 1. The complexity of KA multiplier is discussed in [17].

For reducing the number of sub-multiplications in the PWM stage, let us define the following identities

\[ D_i = A_iB_i, \]  
(7)

\[ D_{ij} = (A_i + A_j)(B_i + B_j). \]  
(8)

We can compute the product of a pair of three-term polynomials corresponding to 3-term KA scheme. Let \(A\) and \(B\) be represented by \(A = A_0 + A_1 x^{m/3} + A_2 x^{2m/3}\) and \(B = B_0 + B_1 x^{m/3} + B_2 x^{2m/3}\), respectively, where \(A_i\) and \(B_i\) are \(\left(\frac{m}{3}\right)\)-bit polynomials. The product of \(A\) and \(B\) can be rewritten

\[ C = AB = C_0 x^{m/3} + C_2 x^{2m/3} + C_3 x^{m} + C_4 x^{4m/3}, \]  
(9)

where

\[ D_0 = A_0B_0, D_1 = A_1B_1, D_2 = A_2B_2, \]
\[ D_{01} = (A_0 + A_1)(B_0 + B_1), \]
\[ D_{12} = (A_2 + A_1)(B_2 + B_1), \]
\[ D_{02} = (A_0 + A_2)(B_0 + B_2), \]
\[ C_0 = D_0, C_1 = D_{01} + D_0 + D_1, \]
\[ C_2 = D_{02} + D_0 + D_1 + D_2, \]
\[ C_3 = D_{12} + D_1 + D_2, C_4 = D_2. \]

In the above example, three-term KA requires 6 multiplications of decomposed operands to generate the partial products and 13 additions of decomposed operands and of partial products. Generalizing the above multi-term KA decomposition, we can obtain the following properties.

**Lemma 1.** Suppose \(A\) and \(B\) are two \(m\)-bit polynomials. Based on \(n\)-term KA scheme with one-step approach, both polynomials \(A\) and \(B\) are split into \((\frac{m}{n})\)-bit subword polynomials. In this case, to compute \(C = AB\), we require \(\frac{2^m + m}{2}\) partial products.
Fig. 1. The functional block of the KA architecture.

In the structure of Fig. 1, it is shown that three stages are performed sequentially and based on that we can have Lemma 2 in the following.

**Lemma 2.** Assume that \( C = C_1 + C_2 \), where \( C_1 = A_1B_1 \) and \( C_2 = A_2B_2 \). In the three stage computation of Fig.1, \( C_1 \) and \( C_2 \) can be represented by \( C_1 = R(\text{PWM}(\text{EP}(A_1), \text{EP}(B_1))) \) and \( C_2 = R(\text{PWM}(\text{EP}(A_2), \text{EP}(B_2))) \), respectively. \( C = C_1 + C_2 \) is then directly obtained by the following recombination structure:

\[
C = R(\text{PWM}(\text{EP}(A_1), \text{EP}(B_1))) + \text{PWM}(\text{EP}(A_2), \text{EP}(B_2)).
\]

(10)

### III. PROPOSED SCALABLE SYSTOLIC SPB MULTIPLIER

In this Section, we utilize the multi-way KA scheme to derive a novel scalable multiplier over \( GF(2^m) \), where the field element is represented by the SPB.

**A. Parallel Systolic Array for Computing Partial Product Multiplication**

Assume that \( \mathcal{A} = \sum_{i=0}^{n-1} a_i x^i \) and \( \mathcal{B} = \sum_{i=0}^{n-1} b_i x^i \) are two subword polynomials, and \( \overline{C} \) be their product prior to the reduction operation, such that

\[
\overline{C} = \mathcal{A}\mathcal{B} = b_0\mathcal{A} + b_1x\mathcal{A} + \ldots + b_{n-1}x^{n-1}\mathcal{A}.
\]

(11)

For digit-size \( d \), operand and \( \mathcal{B} \) could be decomposed into \( p \) number of \( d \)-bit sub-words with \( p = \left\lceil \frac{n}{d} \right\rceil \), such that

\[
\mathcal{B} = \sum_{i=0}^{p-1} \mathcal{B}_i x^{id}.
\]

(12)

where

\[
\mathcal{B}_i = \sum_{j=0}^{d-1} b_{id+j} x^j.
\]

Thus, the product \( \overline{C} \) can be represented as

\[
\overline{C} = \sum_{i=0}^{p-1} \mathcal{A}\mathcal{B}_i x^{id}.
\]

(13)

Next, according to multi-term KA algorithm (Sec. II-B), we can use \( d \)-term KA to derive the partial product \( \overline{C}_i \) in (9). According to the structure of Fig. 1, the product of two \( d \)-bit polynomials can be constructed in three stages, such as evaluation stage, point-wise multiplication stage, and reconstruction stage. We have the following complexities for each of these stages.

**Lemma 3.** Assume that \( A \) and \( B \) are two \( d \)-bit polynomials, and the product of \( A \) and \( B \) is based on 1-step \( d \)-term KA scheme. The components in Fig. 1 then have the following time and space complexities:

- Each EP circuit requires \( \frac{d^2-d}{2} \) XOR gates and involves one XOR gate delay.
- The PWM circuit requires \( \frac{d^2+id}{2} \) XOR gates and involves one AND gate delay.
- The R circuit requires \( (d^2 - d) \) XOR gates and involves \( \lceil \log_2(1.5d) \rceil \) XOR gate delays.

For the selected digit-size \( d \), the element \( \mathcal{A} \) is represented by \( \mathcal{A} = \bar{A}_0 + \bar{A}_1 x^d + \ldots + \bar{A}_{d-1} x^{(d-1)} \), where \( \bar{A}_i = \sum_{j=0}^{d-1} a_{id+j} x^j \) are the sub-words. Let us denote the evaluation point of \( \mathcal{A} \) given by \( P_{\mathcal{A}} = \text{EP}(\mathcal{A}) \), which could be rewritten as

\[
P_{\mathcal{A}} = P_{\mathcal{A}_0} + P_{\mathcal{A}_1} x^d + \ldots + P_{\mathcal{A}_{d-1}} x^{(d-1)}
\]

(14)

Utilizing the recombination property (stated in Lemma 2), the partial product \( C_i \) in (9) can be obtained as

\[
\overline{C} = R\left(\sum_{i=0}^{p-1} \text{PWM}(P_{\mathcal{A}_i}, P_{\mathcal{B}_i})x^{id}\right),
\]

(15)

where

\[
\text{PWM}(P_{\mathcal{A}}, P_{\mathcal{B}}) = \sum_{j=0}^{p-1} \text{PWM}(P_{\mathcal{A}_j}, P_{\mathcal{B}_j})x^{jd}
\]

(16)

Fig. 2 shows the signal-flow graph (SFG) for the computation of (15) based on one-step KA decomposition. In Fig. 2, the EP-A module is comprised of \( p \) number of EP circuits, the PWM-A module is comprised of \( p \) PWM circuits to perform \( \text{PWM}(P_{\mathcal{A}_i}, P_{\mathcal{B}_i}) \), and the final reconstruction (FR) requires \( (2p - 1) \) R circuits. We can use Lemma 3 to evaluate the time complexities of EP, PWM and R circuits as \( T_X \), \( T_A \) and \( \log_2(1.5d)T_X \) gate delays, respectively. To achieve the minimum critical path, we assume that \( k = \left\lceil \frac{l}{2} \right\rceil \), where \( l = 2^{\lceil \log_2(1.5d) \rceil - 2} \). For example, if the multiplier selects 5-bit digit-size to implement the partial product, then we have \( l = 2 \). We can use cut-set retiming with \( l = 2 \) (as shown in Fig.2) to reduce the delay between PWM-EP-adder and FR. Thus, the product \( \overline{C} \) is selected by \( l \) PWM-A modules given by the following formula

\[
\overline{C} = R\left(\sum_{i=0}^{k-1} \overline{C}_i x^{id}\right)
\]

(16)
\[
\mathcal{I} \rightarrow \text{EP-A} \rightarrow \mathcal{T}
\]

Fig. 2. Signal-flow graph (SFG) for computing partial products

\[
\tilde{B}_t = \tilde{B}_{0t} + \tilde{B}_{i+1} x^d + \cdots + \tilde{B}_{t-l+1} x^d (l-1). \tag{18}
\]

In order to reduce the latency, let us consider a pair of integers \( t \) and \( w \) which satisfy \( w = \left\lceil \frac{k}{t} \right\rceil \). The product \( \tilde{C} \) in (16) can then be expressed as

\[
\tilde{C} = R\left( \sum_{i=0}^{t-1} \overline{C}_i x^{il_d} \right) \tag{19}
\]

where

\[
\overline{C}_i = \sum_{j=0}^{w-1} \overline{C}_j x^{il_d}. \tag{20}
\]

Fig. 3 shows the proposed 2-D parallel systolic array for computing the partial products based on (19). It consists of one EP-A, \( w \) parallel systolic arrays (PSA), one pipelined adder-tree (PAT), and one FR. Each PSA is composed of \( t \) PEs to implement (20). Fig.4 shows the design of PE, which is composed of one PWM multiplier core, one adder, and one EP-B. Each PWM multiplier core performs the computation of (17). It consists of \( p \) PWMs. The EP-B is based on (18) to compute the evaluation point \( \tilde{P}_{B_i} \). It consists of \( l \) EPs. Let us define \( S_{\theta} = \frac{d(d+1)}{2} \). The EP-B module in Fig.4 produces \( lS_{\theta} \) output bits, and the PWM multiplier core produces \( (p + l - 1)S_{\theta} \)-bits of results.

**B. Final Polynomial Reduction circuit**

After the degree alignment operation, we get the result \( D \) which is a \((2m-1)\)-bit polynomial. The most significant \( m-1 \) terms of \( D \) are recursively reduced through polynomials of degree less than \( m \) using the irreducible polynomial \( F(x) \) to obtain \( C = x^{-v} D \mod F(x) \). In [18], it is shown that \( C = x^{-v} D \mod F(x) \) can be represented by

\[
C = \left[ \begin{array}{c} 1_{m \times m} \quad Q \end{array} \right] \left[ \begin{array}{c} d_0 \ d_1 \ \cdots \ d_{2m-2} \end{array} \right] \tag{21}
\]

where \( Q \) is the reduction matrix associated with the irreducible polynomial \( F(x) \). For any general reduction polynomial \( F(x) \), the final polynomial reduction (FPR) module requires \( H(Q) \) XOR gates and \( \log_2(\theta + 1)T_X \) critical path, where \( H(Q) \) is the Hamming weight of the reduction matrix \( Q \), and \( \theta \) is the maximum Hamming weight of the column vectors in matrix \( Q \). For the NIST recommended irreducible polynomials for elliptic curve cryptosystems [2], Table I lists the complexity of FPR module.

<table>
<thead>
<tr>
<th>#XOR(H(Q))</th>
<th>time delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 2m - 2 )</td>
<td>( 2T_X )</td>
</tr>
<tr>
<td>( 3m + k_1 - 3 )</td>
<td>( 4T_X )</td>
</tr>
</tbody>
</table>

**C. Proposed Scalable Architecture**

Let the field element \( A = \overline{\pi}_0 + \overline{\pi}_1 x + \cdots + \overline{\pi}_{m-1} x^{m-1} \) in \( GF(2^m) \) be represented by \( A = A_0 + A_1 x + A_2 x^2 \), where \( n = \left\lceil \frac{m}{2} \right\rceil \) and \( A_1 = a_{i,0} + a_{i,1} x + \cdots + a_{i,n-1} x^{n-1} \) for \( 0 < i < 2 \) and \( a_{i,j} = \overline{\pi}_{n+i-j} \). Let the field \( GF(2^m) \) be constructed from an irreducible polynomial \( F(x) \) of degree \( m \). For \( A, B \in GF(2^m) \), the SPB product \( C = RAB \mod F(x) \) can be represented as

\[
C = R[A_0B_0 + (A_0B_1 + A_1B_0 + A_0B_0) x^n + (A_0B_2 + A_1B_1 + A_2B_0)x^{2n} + A_2B_0x^{3n}] \mod F(x)
\]

\[
= R[A_0B_0(1 + x^n + x^{2n}) + A_1B_1(x^{n} + x^{2n} + x^{3n})
\]

Fig. 3. The proposed parallel systolic array architecture for computing partial products
where
\[ \text{operands are generated in different configurations realized by} \]

\[ \text{the proposed SPB/GPB multiplier with scalable hardware} \]

\[ \text{Step 9 does the final polynomial reduction. Fig. 5 shows} \]

\[ \text{is based on Sec.III-A to carry out subword multiplication.} \]

\[ \text{are computed sequentially in the order} \]

\[ \text{from (21), we can find that the product} \]

\[ \text{includes six partial products} \]

\[ \text{involves 6 partial products} \]

\[ \text{and one FPR.} \]

\[ \text{According to (21), the KA for three-way decomposition} \]

\[ \text{involves} \]

\[ \text{products involve the multiplication of different combinations} \]

\[ \text{of input subwords. Three control vectors} \]

\[ \text{are stored in the circular shift-register in the control unit. During} \]

\[ \text{each iteration of partial product computations, the decomposed} \]

\[ \text{operand generation circuit (using a pair of control vectors} \]

\[ \text{and} \]

\[ \text{the proposed architecture} \]

\[ \text{selects one of the six different terms for product reconstruction using the control} \]

\[ \text{vector} \]

\[ \text{for example, in Table II, we select the three control vectors} \]

\[ \text{to perform the computation of} \]

\[ \text{in (21), as shown in the path diagram by the red lines in Fig.} \]

\[ \text{Based on this approach, we use three control vectors} \]

\[ \text{to calculate} \]

\[ \text{and so on.} \]

\[ \text{IV. TIME AND SPACE COMPLEXITIES} \]

\[ \text{In Fig.5 we have used two-level KA decomposition to implement the proposed scalable SPB multiplier. The proposed architecture is composed of two decomposed operand generation circuits, one parallel systolic multiplier, one degree-} \]

\[ \text{alignment circuit, one final reduction circuit, and three registers. The decomposed operand generation circuit} \]

\[ \text{is based on the outer-level KA scheme to produce the low-order polynomials. The parallel systolic multiplier is used} \]

\[ \text{to compute product of low-order decomposed polynomials} \]

\[ \text{obtained from the inner-level KA scheme. The degree-} \]

\[ \text{alignment circuit is used to perform the reconstruction function} \]

\[ \text{to obtain product word according to the outer-level KA} \]

\[ \text{uniquely to perform subword multiplication.} \]

\[ \text{are decomposed operands} A_i \]

\[ \text{and} \]

\[ \text{for} \]

\[ \text{where} \]

\[ \text{is an} \]

\[ \text{are computed sequentially} \]

\[ \text{for} \]

\[ \text{to perform} \]

\[ \text{products involve multiplication of different terms for product reconstruction using the control vector} \]

\[ \text{for example, in Table II, we select the three control vectors} \]

\[ \text{to perform the computation of} \]

\[ \text{in (21), as shown in the path diagram by the red lines in Fig.} \]

\[ \text{Based on this approach, we use three control vectors} \]

\[ \text{to calculate} \]

\[ \text{and so on.} \]

\[ \text{IV. TIME AND SPACE COMPLEXITIES} \]

\[ \text{In Fig.5 we have used two-level KA decomposition to implement the proposed scalable SPB multiplier. The proposed architecture is composed of two decomposed operand generation circuits, one parallel systolic multiplier, one degree-} \]

\[ \text{alignment circuit, one final reduction circuit, and three registers. The decomposed operand generation circuit} \]

\[ \text{is based on the outer-level KA scheme to produce the low-order polynomials. The parallel systolic multiplier is used} \]

\[ \text{to compute product of low-order decomposed polynomials} \]

\[ \text{obtained from the inner-level KA scheme. The degree-} \]

\[ \text{alignment circuit is used to perform the reconstruction function} \]

\[ \text{to obtain product word according to the outer-level KA} \]
scheme. Two-level KA is used in one-step $d$-term KA to develop our proposed scalable multiplier. Tables III and IV show space and time complexities, respectively. In Table IV, it is shown that, if we choose the $d$-term KA scheme, the proposed architecture needs $d^2+2d$ partial products, while the corresponding scalar multipliers [19], [20] require $d^2$ partial products. As the number of terms in KAs increases, the partial products used in Fig. 3 could be reduced and hence the hardware complexity of implementation could be reduced. Therefore, the proposed multiplier can efficiently make a trade-off between space and time complexities.

For pairing computation with the 128-bit security level, the field $GF(2^{1223})$ constructed by the trinomial $x^{1223}+x^{255}+1$ is used. We, therefore, choose this field to estimate critical-path, area complexity, and area-delay product of digit-serial/scalable systolic multipliers. To make a fair comparison, we have used the NanGate’s Library Creator and the 45-nm FreePDK Base Kit from North Carolina State University (NCSU) [21] to synthesize the proposed and the corresponding existing digit-serial multipliers and obtained time and area complexities. As shown in Table V, for digit-size $d = 10$, the area×delay product (ADP) of our proposed architecture is significantly lower than those of the existing multipliers. Amongst all the existing digit-serial/scalable systolic multipliers, Lee’s multiplier [22] has the minimum time-complexity. But as shown in Table V, the proposed multiplier involves less area-complexity and area-delay product (ADP) compared with those of [22]. When the number of terms in outer-level decomposition is increased, our proposed scalable multiplier involves the lowest area-complexity amongst the digit-wise systolic multipliers [20], [13], [22]. Therefore, our proposed architecture can achieve a tradeoff between space and time complexities.

<table>
<thead>
<tr>
<th>TABLE II. THREE CONTROL TABLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) $S_0$ CONTROL TABLE</td>
</tr>
<tr>
<td>$S_0$</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TABLE III. COMPARISON OF TIME COMPLEXITIES OF MULTIPLIERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiplication</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>[22]</td>
</tr>
<tr>
<td>[20], [19]</td>
</tr>
<tr>
<td>[23]</td>
</tr>
</tbody>
</table>

Note: (1) $T_A = \frac{A}{d^2}$, and $d$ is the selected digit-size. (2) $T_A$, $T_X$, and $T_M$ denote the propagation delays of a 2-input AND gate, a 2-input XOR gate, and a $2 \times 1$ MUX gate, respectively.
### TABLE III. COMPARISON OF SPACE COMPLEXITIES OF MULTIPLIERS

<table>
<thead>
<tr>
<th>Multipliers</th>
<th>Basis</th>
<th>structure</th>
<th>#AND</th>
<th>#XOR</th>
<th>#MUX</th>
<th>#Latch</th>
</tr>
</thead>
<tbody>
<tr>
<td>[22]</td>
<td>PB</td>
<td>digit-serial</td>
<td>(m\sqrt{m})</td>
<td>(\sqrt{m}(2m + d) + d)</td>
<td>(\sqrt{m}(2m + d - 1) + 2m)</td>
<td></td>
</tr>
<tr>
<td>[20]</td>
<td>Montgomery</td>
<td>scalable</td>
<td>(n^*)</td>
<td>(n^* + 3n - 1)</td>
<td>(n + 2)</td>
<td>(2m^* + 5dn - 2d + n)</td>
</tr>
<tr>
<td>[19]</td>
<td>DB</td>
<td>scalable</td>
<td>(n^*)</td>
<td>(n^* + 2)</td>
<td>(4n + n)</td>
<td>(2m^* + 2dn + 2d)</td>
</tr>
<tr>
<td>[23]</td>
<td>PB</td>
<td>digit-serial</td>
<td>(md)</td>
<td>(md + d)</td>
<td>(2m)</td>
<td>(4m + 3d + d + 1)</td>
</tr>
</tbody>
</table>

Note: (1) \(d\) is the selected digit-size, and is also the number of splitting terms. (2) \(n = \lfloor \frac{d}{m} \rfloor\), \(S_{\phi} = \frac{d^* - d}{2}\), and \(S_{\phi} = \frac{d^* + d}{2}\). (3) \(H(Q)\) is the Hamming weight of the reduction matrix \(Q\) for an irreducible polynomial.

### TABLE V. COMPARISON OF VARIOUS DIGIT-SERIAL/SCALABLE MULTIPLIERS OVER \(GF(2^{1223})\) IN TERMS OF LATENCY, TOTAL CRITICAL DELAY \(T_{RCD}(\text{ns})\), AREA (\(\mu\text{m}^2\)), AREA×DELAY PRODUCT (ADP) (\(\mu\text{m}^2\text{ns}\)) FOR DIGIT-SIZE \(d = 10\)

<table>
<thead>
<tr>
<th>Multipliers</th>
<th>Latency</th>
<th>(T_{RCD}) (ns)</th>
<th>Area ((\mu\text{m}^2))</th>
<th>ADP ((\mu\text{m}^2\text{ns}))</th>
</tr>
</thead>
<tbody>
<tr>
<td>[22]</td>
<td>24</td>
<td>6.24</td>
<td>406,855</td>
<td>2,538,778</td>
</tr>
<tr>
<td>[20]</td>
<td>344</td>
<td>48.16</td>
<td>206,166</td>
<td>9,928,952</td>
</tr>
<tr>
<td>[19]</td>
<td>344</td>
<td>48.16</td>
<td>191,196</td>
<td>9,208,072</td>
</tr>
<tr>
<td>[23]</td>
<td>346</td>
<td>79.41</td>
<td>59,379</td>
<td>344,322</td>
</tr>
<tr>
<td>Fig.5</td>
<td>62</td>
<td>16.12</td>
<td>100,713</td>
<td>1,623,496</td>
</tr>
</tbody>
</table>

### V. CONCLUSIONS

In this paper, we propose a new scalable systolic SPB multiplier over \(GF(2^{1223})\). We have derived a SPB multiplication algorithm and its architecture to realize the proposed scalable systolic multiplier. To explore the area-time trade-off for large field arithmetic architectures, we have used two-level Karatsuba schemes to implement the scalable systolic multiplier over \(GF(2^{1223})\). As the number of terms in the Karatsuba method increases, it involves significantly less area and ADP. The analytical results provide a valuable reference for implementing pairing algorithm and elliptic curve digital signature algorithm (ECDSA) in resource-constrained embedded systems and smart phones. Moreover, our proposed multiplier has regularity and modularity which make it suitable of VLSI realization.

### ACKNOWLEDGEMENT

The work is supported by the Taiwan National Science Council (NSC) under Grant NSC 1022221-E-262-018.

### REFERENCES