JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 25 No. 1, pp. 37-43, January 2020
https://doi.org/10.9708/jksci.2020.25.01.037

Efficient Semi-systolic AB^2 Multiplier over Finite Fields

Keewon Kim*

*Professor, Dept. of Applied Computer Engineering, Dankook University, Yongin, Korea

[Abstract]

In this paper, we propose an efficient AB^2 multiplication algorithm using SPB(shifted polynomial basis) over finite fields. Using the feature of the SPB, we split the equation for AB^2 multiplication into two parts. The two partitioned equations are executable at the same time, and we derive an algorithm that processes them in parallel. Then we propose an efficient semi-systolic AB^2 multiplier based on the proposed algorithm. The proposed multiplier has less area-time (AT) complexity than related multipliers. In detail, the proposed AB^2 multiplier saves about 94%, 87%, 86% and 83% of the AT complexity of the multipliers of Wei, Wang-Guo, Kim-Lee, Choi-Lee, respectively. Therefore, the proposed multiplier is suitable for VLSI implementation and can be easily adopted as the basic building block for various applications.

▸ **Key words**: Finite fields, Multiplication, Shifted polynomial basis, Semi-systolic array, Cryptography

[요 약]

본 논문에서는 유한체상의 SPB(shifted polynomial basis)를 사용한 효율적인 AB^2 곱셈 알고리즘을 제안한다. SPB의 특징을 이용하여, AB^2 곱셈을 위한 수식을 두 부분으로 분할하였다. 분할된 두 수식은 동시에 실행가능하며, 이를 병렬로 처리하는 알고리즘을 도출하였다. 그리고 제안한 알고리즘을 기반으로 효율적인 세미-시스톨릭(semi-systolic) AB^2 곱셈기를 제안한다. 제안한 곱셈기는 기존의 곱셈기에 비해 낮은 공간-시간 복잡도(area-time complexity)를 가진다. 기존의 구조들과 비교하면, 제안한 AB^2 곱셈기는 공간-시간 복잡도면에서 Wei, Wang-Guo, Kim-Lee, 및 Choi-Lee의 곱셈기들의 약 94%, 87%, 86%, 및 83% 가량이 감소되었다. 따라서 제안한 곱셈기는 VLSI(very large scale integration) 구현에 적합하며 다양한 응용의 기초적인 구성 요소로 쉽게 적용할 수 있다.

▸ **주제어**: 유한체, 곱셈, 이동 다항식 기저, 세미-시스톨렉 어레이, 암호학

• First Author: Keewon Kim, Corresponding Author: Keewon Kim
*Keewon Kim (nirkim@dankook.ac.kr), Dept. of Applied Computer Engineering, Dankook University
• Received: 2019. 12. 24, Revised: 2020. 01. 14, Accepted: 2020. 01. 14.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

유한체는 암호 알고리즘(cryptographic algorithms)과 오류 정정 부호(error correction codes)와 같은 다양한 응용 분야에서 각광을 받아왔다 [1,2]. 유한체의 다양한 응용 분야에서는 곱셈, 나눗셈, 곱셈의 역원, 및 거듭제곱 등의 연산들이 사용된다. 이러한 연산들은 복잡하고 시간 소모가 많다. 그래서 적은 공간 및 시간 복잡도를 가지는 유한체 연산을 수행하는 효율적인 구조의 개발이 필요하다. 본 논문은 유한체 상의 모듈러(modular) AB^2 곱셈을 위한 효율적인 구조 개발에 초점을 맞춘다.

유한체상에서 거듭제곱 연산은 모듈러 AB 또는 모듈러 AB^2 곱셈기를 반복적으로 사용하여 수행할 수 있다. 지금까지의 연구된 결과를 보면, 유한체상의 모듈러 AB 곱셈을 계산하기 위한 다양한 구조들이 제안되었다 [3-13]. 최근 Kim [13]은 유한체상의 모듈러 AB 곱셈을 위해 낮은 지연 시간을 가지는 세미-시스톨릭 구조를 제안하였다. 또한 유한체상의 거듭제곱 연산을 고속으로 처리하기 위해서 모듈러 AB 곱셈과 제곱연산을 동시에 수행할 수 있으며, 이를 위한 다양한 구조들이 제안되었다 [14-16]. 최근 Ibrahim [16]은 Kim [14,15]이 제안한 AB 곱셈과 제곱연산을 동시에 수행하는 구조보다 효율적인 세미-시스톨릭 구조를 제안하였다. 모듈러 AB^2 곱셈을 계산하기 위해서, AB 곱셈기를 사용할 수도 있지만, 두 번의 AB 곱셈을 하는 것보다 효율적인 AB^2 곱셈기를 개발하는 것이 효율적이다.

유한체상의 AB^2 곱셈을 수행하는 다양한 구조들이 제안되었다 [17-21]. Wei [17]는 유한체상의 다항식 기저를 사용한 모듈러 $C+AB^2$ 연산을 수행하는 시스톨릭(systolic) 구조를 제안하였다. Wei의 시스톨릭 어레이는 양방향 데이터 흐름(bidirectional data flow)을 가진다. 이러한 단점을 해결하기 위해서 Wang과 Guo [18]는 다항식 기저 기반에서 모듈러 $C+AB^2$ 연산을 실행하는 양방향 데이터 흐름이 없는 병렬-입력 병렬-출력(parallel-in parallel-out) 시스톨릭 어레이를 제안하였다. Kim과 Lee [19]는 Wang과 Guo [18]의 구조보다 낮은 공간-시간 복잡도를 갖는 병렬-입력 병렬-출력 시스톨릭 곱셈기와 직렬-입력 직렬-출력(serial-in serial-out) 시스톨릭 곱셈기를 제안하였다. Choi와 Lee [20]는 Kim과 Lee [19]의 곱셈기보다 효율적인 AB^2 곱셈기를 제안하였다. Kim과 Kim [21]은 여분 기저(redundant basis) 기반의 낮은 지연 시간의 몽고메리 AB^2 곱셈기를 제안하였다. 하지만, 여분 기저를 사용하기 위해서는 기저 변환의 오버헤드 때문에, 실질적 적용에 제약이 따른다. 기존의 AB^2 곱셈기들은 아직 높은 시간 및 공간 복잡도를 가지며, 기존의 곱셈기들보다 더 낮은 시간 및 공간 복잡도를 가지는 곱셈기의 개발이 필요하다.

유한체 연산의 효율적인 알고리즘을 위해서, 유한체 원소의 표현의 선택은 매우 중요하다. 유한체상의 효율적인 곱셈의 구조를 위해서, Fan과 Dai [22]는 다항식 기저(polynomial basis)를 변형한 새로운 기저, 즉 shifted polynomial basis (SPB)를 제안하였다. Fan과 Hasan [23]은 기약 type-II pentanomial과 trinomial 기반의 곱셈을 위한 비트-병렬 구조를 제안하였다.

본 논문에서는 SPB기반의 AB^2 곱셈 알고리즘을 제안하고 이를 이용하여 효율적인 세미-시스톨릭 곱셈기를 설계한다. 또한 제안한 곱셈기와 기존의 곱셈기들과 성능을 비교하고 분석한다.

본 논문의 구성은 다음과 같다. 2장에서는 SPB 기반의 AB^2 곱셈 알고리즘을 제안하고, 효율적인 세미-시스톨릭 AB^2 곱셈기를 설계한다. 3장은 제안한 곱셈기와 기존의 곱셈기들과의 공간 및 시간 복잡도를 비교하고 분석한다. 결론은 4장에서 제시한다.

II. The Proposed Semi-systolic AB^2 Multiplier

이장에서는 SPB기반의 AB^2 곱셈 알고리즘을 제안하고 이를 이용하여 세미-시스톨릭 곱셈기를 설계한다.

1. The proposed AB^2 multiplication algorithm

유한체 $GF(2^m)$에는 2^m개의 원소가 있고, 이를 생성하는 기약다항식 F는 다음과 같이 정의된다.

$$F(\alpha)=\sum_{i=0}^{m} f_i\alpha^i, \tag{1}$$

여기서 $f_i \in GF(2)$이다. 만약 x가 $F(\alpha)$의 근(root)이라면, 즉, $F(x)=0$, 집합 $\{1,x,x^2,\cdots,x^{m-1}\}$는 Polynomial Basis(PB) 이다. 그러면 정수 k $(0<k\le m)$가 있을 때, Shifted Polynomial Basis(SPB)인 집합 $\{x^{-k},x^{-k+1},\cdots,x^{m-k-1}\}$를 정의한다. $GF(2^m)$상의 두 원소 A와 B를 SPB기반으로 표현하면 아래와 같다.

$$A = \sum_{j=0}^{m-1} a_j x^{j-k} \tag{2}$$

$$B = \sum_{j=0}^{m-1} b_j x^{j-k} \tag{3}$$

여기서 $a_j,\ b_j \in GF(2)$이다.

식 (1)에서 $F(x)=0$를 이용하여, 다음과 같이 $G,\ G',\ \overline{G},\ \overline{G'}$를 정의한다.

$$\begin{aligned} x^m \bmod F &= \sum_{j=0}^{m-1} f_j x^j \\ &\equiv G = \sum_{j=0}^{m-1} g_j x^j \end{aligned} \tag{4}$$

$$\begin{aligned} x^{m+1} \bmod F &= \sum_{j=0}^{m-1} (f_{m-1} f_j + f_{j-1}) x^j \\ &\equiv G' = \sum_{j=0}^{m-1} g'_j x^j \end{aligned} \tag{5}$$

$$\begin{aligned} x^{-1} \bmod F &= \sum_{j=0}^{m-1} f_{j+1} x^j \\ &\equiv \overline{G} = \sum_{j=0}^{m-1} \overline{g}_j x^j \end{aligned} \tag{6}$$

$$\begin{aligned} x^{-2} \bmod F &= \sum_{j=0}^{m-1} (f_1 f_{j+1} + f_{j+2}) x^j \\ &\equiv \overline{G'} = \sum_{j=0}^{m-1} \overline{g}_j' x^j \end{aligned} \tag{7}$$

여기서 $f_{m+1} = f_{-1} = 0$ 이다.

식 (3)을 이용하여 B^2을 표현하면 아래와 같다.

$$B^2 = \sum_{j=0}^{m-1} b_j x^{2(j-k)} \tag{8}$$

식 (8)의 B^2을 사용하여 $GF(2^m)$상에서 SPB 기반의 $AB^2 \bmod F$는 다음과 같이 표현된다.

$$\begin{aligned} P &= AB^2 \bmod F \\ &= \sum_{j=0}^{m-1} b_j A x^{2(j-k)} \bmod F \end{aligned} \tag{9}$$

AB^2 곱셈을 위한 알고리즘의 도출의 편의성을 위해서, 우리는 m이 짝수라고 가정한다. 그리고 계산 구조의 병렬성을 효과적으로 이용하기 위해서 $k = m/2$로 정한다. 그러면 P는 다음과 같다.

$$\begin{aligned} P &= \sum_{j=0}^{m-1} b_j A x^{2(j-k)} \bmod F \\ &= \sum_{i=0}^{k-1} b_{k-i-1} A x^{-2(i+1)} \bmod F + \\ &\quad \sum_{i=0}^{k-1} b_{k+i} A x^{2i} \bmod F \\ &= \left(\sum_{i=0}^{k-1} b_{k-i-1} A x^{-2i} \right) x^{-2} \bmod F + \\ &\quad \sum_{i=0}^{k-1} b_{k+i} A x^{2i} \bmod F \\ &\equiv (S x^{-2} + T) \bmod F, \end{aligned} \tag{10}$$

여기서 S와 T는 다음과 같다.

$$S = \sum_{i=0}^{k-1} b_{k-i-1} A x^{-2i} \bmod F \tag{11}$$

$$T = \sum_{i=0}^{k-1} b_{k+i} A x^{2i} \bmod F \tag{12}$$

식 (11)과 (12)를 보면, S와 T를 계산하기 위해서 Ax^{-2i}와 Ax^{2i}의 계산이 필요하다. 이를 위해서 $\overline{A}^{(i)} = Ax^{-2i} \bmod F$와 $A^{(i)} = Ax^{2i} \bmod F$ $(0 \le i \le k-1)$를 정의한다. 여기서 $\overline{A}^{(0)} = A^{(0)} = A$이다. 식 (4)부터 (7)까지의 $G,\ G',\ \overline{G},\ \overline{G'}$를 이용하여 $A^{(i)}$와 $\overline{A}^{(i)}$를 다음과 같이 표현할 수 있다.

$$\begin{aligned} A^{(i)} &= A^{(i-1)} x^2 \bmod F \\ &= \sum_{j=0}^{m-1} (a_{j-2}^{(i-1)} + a_{m-2}^{(i-1)} g_j + a_{m-1}^{(i-1)} g'_j) x^{j-k} \end{aligned} \tag{13}$$

$$\begin{aligned} \overline{A}^{(i)} &= \overline{A}^{(i-1)} x^{-2} \bmod F \\ &= \sum_{j=0}^{m-1} (\overline{a}_{j+2}^{(i-1)} + \overline{a}_1^{(i-1)} \overline{g}_j + \overline{a}_0^{(i-1)} \overline{g}'_j) x^{j-k}, \end{aligned} \tag{14}$$

여기서 $\overline{A}^{(0)} = A^{(0)} = A$이고 $a_{-2}^{(i-1)} = a_{-1}^{(i-1)} = \overline{a}_{m+1}^{(i-1)} = \overline{a}_m^{(i-1)} = 0$ $(0 \le i \le k-1)$이다.

$A^{(i)}$와 $\overline{A}^{(i)}$를 이용하여 S와 T를 다음과 같이 표현할 수 있다.

$$\begin{aligned} S &= \sum_{i=0}^{k-1} b_{k-i-1} A x^{-2i} \bmod F \\ &= \sum_{i=0}^{k-1} b_{k-i-1} \overline{A}^{(i)} \end{aligned} \tag{15}$$

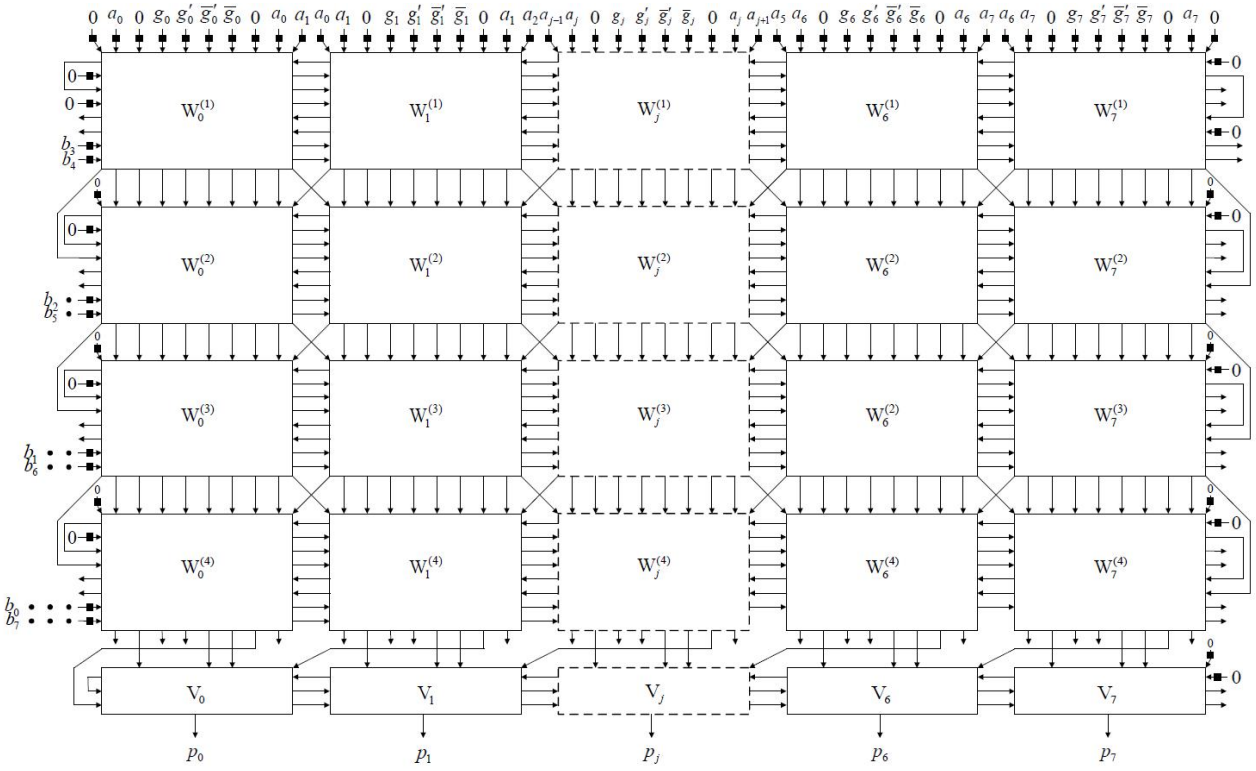

Fig. 1. The proposed semi-systolic AB^2 multiplier

$$T = \sum_{i=0}^{k-1} b_{k+i} A x^{2i} \bmod F = \sum_{i=0}^{k-1} b_{k+i} A^{(i)} \quad (16)$$

위의 식에서 S와 T의 재귀식(recurrence equation)을 다음과 같이 도출할 수 있다.

$$S^{(i)} = S^{(i-1)} + b_{k-i}\overline{A}^{(i-1)} \quad (17)$$

$$T^{(i)} = T^{(i-1)} + b_{k+i-1}A^{(i-1)} \quad (18)$$

여기서 $S^{(0)} = T^{(0)} = 0 \ (0 \le i \le k)$이다.

S와 T를 계산한 후에, 최종적인 $P = AB^2 \bmod F$ 결과를 얻기 위해서, $P = (S^{(k)}x^{-2} + T^{(k)}) \bmod F$ 계산이 필요하다.

$$P = (S^{(k)}x^{-2} + T^{(k)}) \bmod F = \sum_{j=0}^{m-1} (s_{j+2}^{(k)} + s_1^{(k)}\overline{g}_j + s_0^{(k)}\overline{g_j}' + t_j^{(k)})x^{j-k} \quad (19)$$

2. The proposed semi-systolic AB^2 multiplier

앞 절에서 제안한 SPB기반의 AB^2 곱셈 알고리즘을 이용하여 세미-시스톨릭 구조의 곱셈기를 제안한다. Fig. 1은 $GF(2^8)$상에서 제안하는 세미-시스톨릭 곱셈기를 나타낸다. 여기서 "■"는 1-비트 래치(1-bit latch)이다. $GF(2^m)$상의 제안한 곱셈기는 $k \times m$개 $\mathrm{W}_j^{(i)}$ 셀, m개 V_j 셀로 구성된다. 여기서 $\mathrm{W}_j^{(i)}$ 셀과 V_j 셀의 자세한 구조는 Fig. 2에서 제시한다.

제안한 어레이의 상단에서 A, G, G', $\overline{G}$, $\overline{G'}$가 입력되고, 왼쪽에서 B가 입력된다. 각 $\mathrm{W}_j^{(i)}$셀은 식 (13), (14), (17), (18)을 이용하여 각각 하나의 항을 계산하고, 각 V_j셀은 식 (19)를 이용하여 각각 하나의 항을 계산한다. $\mathrm{W}_j^{(i)}$셀은 6개의 2-입력 AND 게이트, 6개의 2-입력 XOR 게이트, 8개의 1-비트 래치로 구성된다. V_j셀은 2개의 2-입력 AND 게이트, 3개의 2-입력 XOR 게이트, 1개의 1-비트 래치로 구성된다. 제안한 곱셈기는 $k+1$ 클럭 사이클(clock cycle)이후에 어레이의 아래에서 AB^2 곱셈 결과를 출력한다.

제안한 곱셈기의 지연시간은 $k+1$ 클럭 사이클이며, 임계 경로 지연(critical path delay)은 $T_{AND2} + 2T_{XOR2} + T_{LATCH1}$, 여기서 T_{AND2}, T_{XOR2}, T_{LATCH1}는 각각 2-입력 AND 게이트, 2-입력 XOR 게이트, 1-비트 래치의 지연시간을 의미한다.

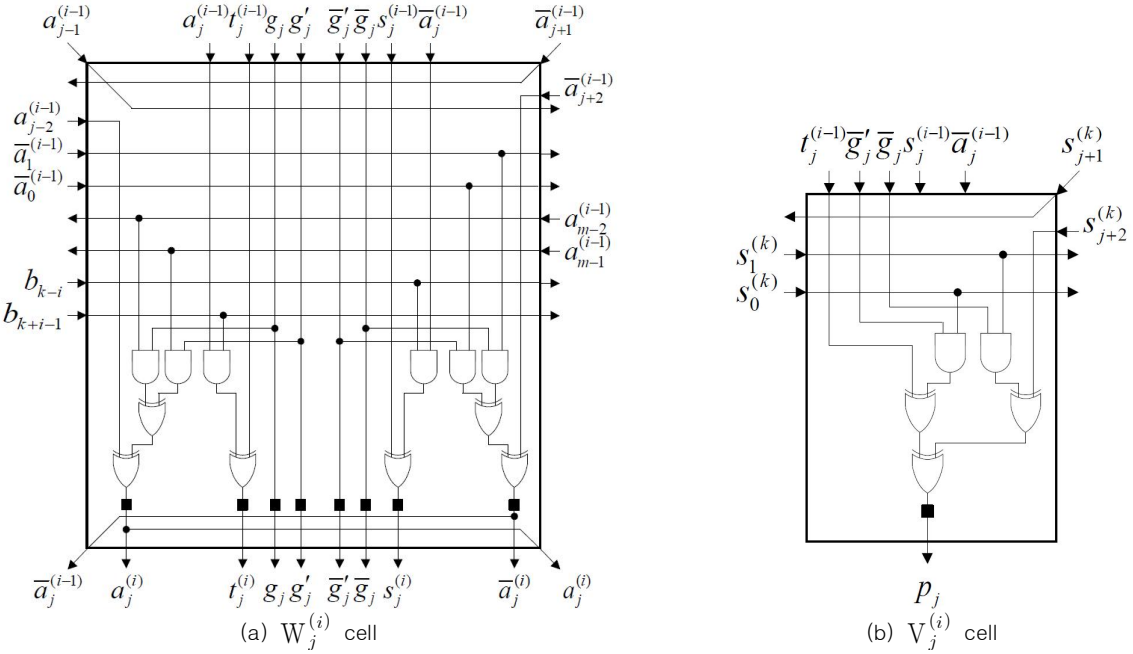

Fig. 2. The detailed cells

III. Complexity Analysis

본 장에서는 기존의 AB^2 곱셈기들과 제안한 AB^2 곱셈기의 성능을 비교하고 분석한다. 제안한 곱셈기와 기존의 곱셈기의 실질적인 시간 및 공간 복잡도를 계산하기 위하여 "SAMSUNG STD 150 0.13μm 1.2V CMOS Standard Cell Library"를 사용한다. A_{GATEn}이 n-입력 게이트의 트랜지스터 카운트(transistor count)를 나타낸다고 정의하면, $A_{AND2}=6.68$, $A_{XOR2}=12.00$, $A_{LATCH}=16.00$이다. 또한 T_{GATEn} 이 n-입력 게이트의 전파 지연(propagation delay) 시간을 나타낸다고 정의하면, $T_{AND2}=0.094ns$, $T_{XOR2}=0.167ns$, $T_{LATCH}=0.157ns$이다.

Table 1은 기존의 AB^2 곱셈기들과 제안한 곱셈기를 비교한 것이다. Wei [17], Wang과 Guo [18], Kim과 Lee [19], Choi와 Lee [20]의 AB^2 곱셈기들의 트랜지스터 카운트는 각각 $264.04m^2$, $192.04m^2$, $208.04m^2+36m$, $208.04m^2$이다. 제안한 AB^2 곱셈기의 트랜지스터 카운트는 $120.04m^2+273.36m+32$이며, 기존의 Wei [17], Wang과 Guo [18], Kim과 Lee [19], Choi와 Lee [20]의 곱셈기들과 비교하면, 약 54%, 37%, 42%, 42% 감소되었다.

Wei [17], Wang과 Guo [18], Kim과 Lee [19], Choi와 Lee [20]의 AB^2 곱셈기들의 셀 처리 시간은 각각 $T_{AND2}+2T_{XOR2}+T_{LATCH1}$, $T_{AND2}+2T_{XOR2}+T_{LATCH1}$, $2T_{XOR2}+T_{LATCH1}$, $T_{AND2}+T_{XOR2}+T_{LATCH1}$이다. Wei [17]의 곱셈기의 지연 시간은 $4m$, Wang과 Guo [18]는 $2.5m$, Kim과 Lee [19]는 $2.5m+1$, Choi와 Lee [20]는 $2.5m$ 클록 사이클이다. 제안한 곱셈기의 지연 시간은 $0.5m+1$ 클록 사이클이다. 곱셈기의 전체 처리 시간을 비교하기 위해서, 곱셈기의 셀 처리 시간과 지연 시간을 같이 고려하면, 제안한 곱셈기는 Wei [17], Wang과 Guo [18], Kim과 Lee [19], Choi와 Lee [20]의 곱셈기에 비해 각각 약 87.5%, 80%, 76%, 72% 감소되었다.

제안한 곱셈기와 Wei[17], Wang과 Guo[18], Kim과 Lee[19], Choi와 Lee[20]의 곱셈기의 공간-시간 복잡도(AT complexity)를 비교하면, 각각 약 94%, 87%, 86%, 83% 감소되었다.

IV. Conclusions

본 논문은 유한체상에서 SPB기반의 효율적인 모듈러 AB^2 세미-시스톨릭 곱셈기를 제안하였다. 기존의 AB^2 곱셈기들과 성능을 비교한 결과, 제안한 곱셈기가 시간 및 공간 복잡도면에서 더욱 효율적인 성능을 보였다. 더욱이, 제안한 구조는 정규성, 간결성, 모듈성으로 인해서 VLSI로

Table 1. Comparison of AB^2 multipliers over GF(2^m)

	Wei [17]	Wang-Guo[18]	Kim-Lee [19]	Choi-Lee [20]	Fig. 1
Area complexity					
AND_2	$3m^2$	$3m^2$	$3m^2$	$3m^2$	$3m^2+2m$
XOR_2	$3m^2$	$3m^2$	$3m^2+3m$	$3m^2+3m$	$3m^2+3m$
Latch	$13m^2$	$8.5m^2$	$9.5m^2$	$9.5m^2$	$4m^2+14m+2$
Total transistors	$264.04m^2$	$192.04m^2$	$208.04m^2+36m$	$208.04m^2$	$120.04m^2+273.36m+32$
Time complexity					
Cell delay	0.585	0.585	0.491	0.418	0.585
Latency	$4m$	$2.5m$	$2.5m+1$	$2.5m$	$0.5m+1$
Total delay	$2.34m$	$1.46m$	$1.23m+0.49$	$1.05m$	$0.29m+0.59$
AT complexity	$617.85m^3$	$280.86m^3$	$255.37m^3+146.34m^2+17.68m$	$217.40m^3$	$35.11m^3+150.19m^2+169.28m+18.72$

구현하기 적합하다. 따라서 제안한 구조는 암호 보조프로세서(coprocessor)의 설계에 기본 구성요소로 효율적으로 적용 가능할 것으로 기대한다.

ACKNOWLEDGEMENT

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2019R1F1A1058931).

REFERENCES

[1] A. J. Menezes, P.C. van Oorschot, S.A. Vanstone, “Handbook of Applied Cryptography” Boca Raton, FL, CRC Press, 1996.

[2] R. Lidl, H. Niederreiter, “Introduction to Finite Fields and Their Applications” New York, Cambridge University Press, 1994.

[3] C. L. Wang, J. L. Lin, “Systolic Array Implementation of Multipliers for Finite Fields,” IEEE Trans. Circuits Syst., Vol. 38, No. 7, pp.796-800, Jul. 1991. DOI: 10.1109/31.135751

[4] C. S. Yeh, I. S. Reed, T. K. Troung, “Systolic Multipliers for Finite Fields,” IEEE Trans. Comput., Vol. C-33, No. 4, pp. 357-360, Apr. 1984. DOI: 10.1109/TC.1984.1676441

[5] C. Y. Lee, J. S. Horng, I. C. Jou, “Low-complexity Bit-parallel Systolic Montgomery Multipliers for Special Classes of GF(2^m),” IEEE Transactions on Computers, Vol. 54, No. 9, pp. 1061-1070, July 2005. DOI: 10.1109/TC.2005.147

[6] C. W. Chiou, C. Y. Lee, A. W. Deng, J. M. Lin, “Concurrent Error Detection in Montgomery Multiplication over GF(2^m),” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E89-A, No. 2, pp. 566-574, Feb. 2006. DOI: 10.1093/ietfec/e89-a.2.566

[7] W. T. Huang, C. H. Chang, C. W. Chiou, F. H. Chou, “Concurrent Error Detection and Correction in a Polynomial Basis Multiplier over GF(2^m),” IET Inf. Secur., Vol. 4, No. 3, pp. 111-124, Sep. 2010. DOI: 10.1049/iet-ifs.2009.0160

[8] K. W. Kim, S. H. Kim, “A Low Latency Semi-systolic Multiplier over GF(2^m),” IEICE Electron. Express, Vol. 10, No. 13, pp. 20130354, Jul. 2013. DOI: 10.1587/elex.10.20130354

[9] S. H. Choi, K. J. Lee, “Low Complexity Semi-systolic Multiplication Architecture over GF(2^m),” IEICE Electron. Express, Vol. 11, No. 20, pp. 20140713, Oct. 2014. DOI: 10.1587/elex.11.20140713

[10] K. W. Kim, J. C. Jeon, “A Semi-systolic Montgomery Multiplier over GF(2^m),” IEICE Electonics Express, Vol. 12, No. 21, pp. 20150769, Nov. 2015. DOI: 10.1587/elex.12.20150769

[11] K. W. Kim, S. C. Han, “Low Latency Systolic Multiplier over GF(2^m) Using Irreducible AOP,” IEMEK J. Embed. Sys. Appl., Vol. 11, No. 4, pp. 227-233, Aug. 2016. DOI: 10.14372/IEMEK.2016.11.4.227

[12] S. H. Choi, K. J. Lee, “Reduced Complexity Polynomial Multiplier Architecture for Finite Fields GF(2^m),” IEICE Electron. Express, Vol. 14, No. 17, pp. 20160797, 2017. DOI: 10.1587/elex.14.20160797

[13] K. W. Kim, “Low-latency Semi-systolic Architecture for Multiplication over Finite Fields,” IEICE Electron. Express, Vol. 16, No. 10, pp. 20190080, 2019. DOI: 10.1587/elex.16.20190080

[14] K. W. Kim, J. D. Lee, “Efficient Unified Semi-systolic Arrays for Multiplication and Squaring over GF(2^m),” IEICE Electron. Express, Vol. 14, No. 12, pp. 20170458, 2017. DOI: 10.1587/elex.14.20170458

[15] K. W. Kim, S. H. Kim, “Efficient Bit-parallel Systolic Architecture for Multiplication and Squaring over GF(2^m),” IEICE Electron. Express, Vol. 15, No. 2, pp. 20171195, 2018. DOI: 10.1587/elex.14.20171195

[16] A. Ibrahim, U. Tariq, T. Ahmad, A. Elmogy, Y. Bouteraa, F. Gebali, “Efficient Parallel Semi-systolic Array Structure for Multiplication and Squaring in GF(2^m),” IEICE Electron. Express, Vol. 16, No. 12, pp. 20190268, 2019. DOI:

10.1587/elex.16.20190268

[17] S. W. Wei, "A Systolic Power-sum Circuit for GF(2^m)," IEEE Transactions on Computers, Vol. 43, No. 2, pp. 226-229, Feb. 1994. DOI: 10.1109/12.262128

[18] C. L. Wang, J. H. Guo, "New Systolic Arrays for C+AB^2, Inversion, and Division in GF(2^m)," IEEE Transactions on Computers, Vol. 49, No. 10, pp. 1120-1125, Oct. 2000. DOI: 10.1109/12.888047

[19] K. W. Kim, W. J. Lee, "Low-complexity Parallel and Serial Systolic Architectures for AB^2 Multiplication in GF(2^m)," IETE Technical Review, Vol. 30, No. 2, pp. 134-141, 2013. DOI: 10.4103/0256-4602.110552

[20] S. H. Choi, K. J. Lee, "Parallel in/out Systolic AB^2 Architecture with Low Complexity in GF(2^m)," Electron. Lett., Vol. 52, No. 13, pp. 1138-1140, 2016. DOI: 10.1049/el.2015.3681

[21] T. W. Kim, K. W. Kim, "Low-latency Montgomery AB^2 Multiplier Using Redundant Representation over GF(2^m)," IEMEK Journal of Embedded Systems and Applications, Vol. 12, No. 1, pp. 11-18, Feb. 2017. DOI: 10.14372/IEMEK.2017.12.1.11

[22] H. Fan, Y. Dai, "Fast Bit-parallel GF(2^m) Multiplier for All Trinomials," IEEE Trans. Comput., Vol. 54, No. 4, pp. 485-490, 2005. DOI: 10.1109/TC.2005.64

[23] H. Fan, M. Hasan, "Fast Bit Parallel Shifted Polynomial Basis Multipliers in GF(2^n)," IEEE Trans. Circuits Syst. I: Fundam. Theory Appl., Vol. 53, No. 12, pp. 2606-2615, 2006. DOI: 10.1109/TCSI.2006.883855

Authors

Keewon Kim received the M.S. and Ph.D. degrees in Computer Engineering from Kyungpook National University, Korea, in 2001 and 2006, respectively. He is currently an assistant professor in the department of Applied Computer Engineering, Dankook University. He is interested in information security, security protocol, VLSI, and big data analysis.