情報保護學會論文誌
第12券 第2號, 2002. 4

GF(2^m)상에서 AB^2 연산을 위한 세미시스톨릭 구조*

이 형 목**, 김 현 성***, 전 준 철**, 유 기 영**

AB^2 Semi-systolic Architecture over GF(2^m)

Hee-bong Choi**, Soo-hyun Oh***, Soon-jwa Hong**, Dong-ho Won**

요 약

본 논문에서는 유한체 GF(2^m)상의 AB^2연산을 위해 AOP(All One Polynomial)에 기반한 새로운 MSB(most significant bit) 알고리즘을 제안하고, 제안한 알고리즘에 기반하여 두 가지 병렬 세미시스톨릭 어레이를 설계한다. 제안된 구조들은 표준기저에 기반하고 기약다항식으로는 계수가 모두 1인 m차의 기약다항식 AOP를 사용한다. 먼저, 병렬 세미시스톨릭 어레이(PSM)는 각 셀 당 $D_{AND2}+D_{XOR2}$의 임계경로를 갖고 $m+1$의 지연시간을 가진다. 두 번째 구조인 변형된 병렬 세미시스톨릭 어레이(MPSM)는 각 셀 당 D_{XOR2}의 임계경로를 갖지만 지연시간은 PSM과 같다. 제안된 두 구조 PSM과 MPSM은 지연시간과 임계경로 면에서 기존의 구조보다 효율적이다. 제안된 구조는 GF(2^m) 상에서 효율적인 나눗셈기, 지수기 및 역원기를 설계하는데 기본 구조로 사용될 수 있다. 또한 구조 자체가 정규성, 모듈성, 병렬성을 가지기 때문에 VLSI구현에 효율적이다. 더욱이 제안된 구조는 유한체 상에서 지수 연산을 필요로 하는 Diffie-Hellman 키 교환 방식, 디지털 서명 알고리즘과 ElGamal 암호화 방식과 같은 알고리즘을 위한 기본 구조로 사용될 수 있다. 이러한 알고리즘을 응용해서 타원 곡선(Elliptic Curve)에 기초한 암호화시스템(Cryptosystem)의 구현에 사용될 수 있다.

ABSTRACT

In this contributions, we propose a new MSB(most significant bit) algorithm based on AOP(All One Polynomial) and two parallel semi-systolic architectures to computes AB^2 over finite field GF(2^m). The proposed architectures are based on standard basis and use the property of irreducible AOP(All One Polynomial) which is all coefficients of 1. The proposed parallel semi-systolic architecture(PSM) has the critical path of $D_{AND2}+D_{XOR2}$ per cell and the latency of $m+1$. The modified parallel semi-systolic architecture(MPSM) has the critical path of D_{XOR2} per cell and has the same latency with PSM. The proposed two architectures, PSM and MPSM, have a low latency and a small hardware complexity compared to the previous architectures. They can be used as a basic architecture for exponentiation, division, and inversion. Since the proposed architectures have regularity, modularity and concurrency, they are suitable for VLSI implementation. They can be used as a basic architecture for algorithms, such as the Diffie-Hellman key exchange scheme, the Digital Signature Algorithm(DSA), and the ElGamal encryption scheme which are needed exponentiation operation. The application of the algorithms can be used cryptosystem implementation based on elliptic curve.

keyword : *Galois field, AOP(All One Polynomial), Semi-systolic, Cryptosystem*

* 본 연구는 한국과학재단 목적기초 연구 2000-2-51200-081-2 지원으로 수행되었음.
** 경북대학교 컴퓨터공학과 정보보호 연구실(hmhl01@purple.knu.ac.kr)
*** 경일대학교 컴퓨터공학과(kim@kiu.ac.kr)

Ⅰ. 서 론

에러 교정 코드(error-correcting codes)[1], 디지털 신호 처리(digital signal processing)[2] 및 암호학(cryptography)[3~5]의 응용에서 갈로아 필드(Galois field, GF)[6,7] 연산은 아주 중요하다. 이러한 유한체 중에서 특별한 관심을 가지는 유한체는 GF(2^m)이다. 유한체 GF(2^m)은 2^m개의 원소를 가지고 각각의 원소들은 0과 1의 비트-스트링으로 이루어진다. 본 논문에서 다루고 있는 유한체 GF(2^m)은 0과 1로 이루어진 속성 때문에 컴퓨터 구조를 구현하기 위한 계산에 적당하다.

1984년에 Yeh[9]는 일반적인 GF(2^m)상에서 $AB+C$의 연산을 수행하는 병렬 시스톨릭(systolic) 어레이 구조를 구현하였다. 표준기저 상에서 세미시스톨릭(semi-systolic) 에레이 구조가 논문 [10]에 제시되었고 논문 [11]에서는 정규기저 상에서 곱셈과 곱셈 역원을 계산하기 위한 구조를 제안하였다. 논문 [12]에서는 AB^2+C를 계산하기 위한 시스톨릭 구조가 제안되었다. 그리고 그 후에도 많은 비트 단위의 병렬 세미시스톨릭 곱셈기들이 제안되었으나 시스템의 복잡도 때문에 이러한 곱셈기들은 암호화시스템의 구성에 효과적이지 못했다. 이러한 시스템의 복잡도를 줄이기 위해서 Itoh와 Tsujii[13]가 GF(2^m)상에서 m차의 기약 다항식 AOP(All One Polynomial)에 기초한 곱셈기와 m차의 기약 다항식 ESP(equally spaced polynomial)에 기초한 곱셈기를 설계하였다. 이렇게 설계된 두 개의 곱셈기는 효율적인 시스템 복잡도를 가졌다. 이 후에 Hasan[14]은 처리기로서 AOP에 기초한 병렬 곱셈기를 제안하고, 이를 이용하여 ESP에 기초한 병렬 곱셈기로 발전시켰다. 최근에는 GF(2^m)상에서 타원 곡선(elliptic curve) 기반의 공개키 암호화시스템들이 많이 제시되고있다.[15,16,17] 지금까지의 연구에서 효율적인 구조들이 제안되었지만 시간과 공간 복잡도 면에서 보다 효율적인 구조 설계에 관한 연구가 필요하다.

본 논문에서는 GF(2^m)상에서 기약 다항식 AOP의 속성에 기반하여 AB^2를 계산하는 MSB우선 알고리즘을 제시하고, 두 가지 병렬 세미시스톨릭 어레이 구조를 제안한다. 2-입력 AND와 XOR게이트의 딜레이(delay)를 D_{AND2}와 D_{XOR2}라 할 때, 제안된 병렬 세미시스톨릭 어레이 구조(PSM)의 전체 지연시간은 $m+1$이고, 각 셀 당 $D_{AND2}+D_{XOR2}$의 임계경로를 갖는다. 그리고 전체 게이트 수는 각각 $(m+1)^2$개의 AND 게이트와 XOR게이트를 갖는다. 재구성된 변형 병렬 세미시스톨릭 어레이 구조(MPSM)의 전체 지연시간은 $m+1$이다. 즉, PSM구조와 지연시간은 같지만 MPSM구조는 각 셀 당 D_{XOR2}의 보다 효율적인 임계경로를 갖는다. 본 논문에서 제안된 두 구조는 기존에 제안된 구조보다 구조가 더 간단하고 효율적인 시스템 복잡도를 가지므로 두 구조를 기반으로 보다 효율적이고 안전한 암호화시스템을 구현할 수 있다.

본 논문은 2장에서 AOP에 기반한 MSB 우선 알고리즘을 제시한다. 3장에서는 2장에서 제안한 알고리즘에 기초한 두 가지 곱셈기를 제시하고, 4장에서 기존의 구조와 본 논문에서 제안한 구조를 비교 및 분석을 한다. 그리고 마지막으로 5장에서 결론을 맺는다.

Ⅱ. AOP에 기반한 제안된 MSB우선 알고리즘

유한체 GF(2)의 유한 확대체를 GF(2^m)이라 하자.[6,7] 먼저 유한 확대체 GF(2^m)상의 원소는 표준, 정규, 이원기저의 세 가지 기저에 의해 표현된다. 첫 번째, 표준기저 $\{1,a,a^2,\cdots,a^{m-1}\}$에서 유한체 GF($2^m$)상의 임의의 원소 A를 나타내면 $A=a_{m-1}a^{m-1}+a_{m-2}a^{m-2}+\cdots+a_1a+a_0$로 나타낼 수 있다. 두 번째, 정규기저 $\{a,a^2,\cdots,a^{2^{m-2}}\}$에서 GF($2^m$)상의 임의의 원소 A를 나타내면 $A=a_{m-1}a^{2^{m-2}}+a_{m-2}a^{2^{m-4}}+\cdots+a_1a^2+a_0$로 나타낼 수 있다. 마지막으로 이원기저 $\{u_0,u_1,\cdots,u_{m-1}\}$에서 임의의 원소 A는 $A=a_{m-1}u_{m-1}+a_{m-2}u_{m-2}+\cdots+a_1u_1+a_0u_0$로 나타난다. 단, 각각의 $a_i(i=0,1,\cdots,m-1)$는 유한체 GF(2)상의 원소이다. 본 논문에서는 기저의 변환이 필요 없는 표준기저에 초점을 맞추었다.

요약에서 언급한 유한체 상에서 Diffie-Hellman 키 교환 방식, 디지털 서명 알고리즘과 ElGamal 암호화 방식과 같이 잘 알려진 알고리즘을 응용한 타원 곡선(elliptic curve) 기반의 공개키 암호화 시스템(cryptosystem)의 구현에 있어서 GF(p)나 GF(2^m) 상에서 효율적인 지수 연산이 필요하다. 이러한 지수 연산을 효율적으로 계산하는 알고리즘을 Knuth가 논문 [8]에서 제시하였다. 제시한 알고리즘은 LSB(least significant bit)와 MSB(most significant bit) 우선 방식이 있다. 제시한 알고리즘은 다음과 같다.

C와 M을 GF(2^m)의 원소라 하자. 그러면 지수 연산은 다음과 같이 표현될 수 있다.

$$C=M^E, 0\le E\le n, n=2^m-1 \quad (1)$$

여기서, 지수 E를 처리하는 방법에 따라서 알고리즘은 크게 두 가지로 나눌 수 있다. 지수의 LSB와 MSB부터 시작해서 각각 M^E을 계산 할 수 있다. 먼저, 지수의 LSB부터 시작해서 M^E를 계산하면 다음과 같다.

$$M^E=M^{e_0}(M^{2^1})^{e_1}(M^{2^2})^{e_2}\cdots(M^{2^{m-1}})^{e_{m-1}} \quad (2)$$

다음으로, 지수의 MSB부터 시작해서 M^E를 계산하면 다음과 같다.

$$M^E=M^{e_0}(M^{e_1}\cdots(M^{e_{m-2}}(M^{e_{m-1}})^2)^2)\cdots)^2 \quad (3)$$

이들 연산을 위해서 Knuth가 이진 방식(Binary Method)을 제안했다.[8] 식 (3)에 기초한 MSB우선 지수 연산 알고리즘은 다음과 같다.

[알고리즘1] Knuth[8]의 MSB 우선 지수 알고리즘

입력 : A, E, $f(x)$
출력 : $C=AE \bmod f(x)$

단계1 : if($e_{m-1}==1$) $C=A$ else $C=a^0$
단계2 : for $i=m-2$ to 0
단계3 : if($e_i==1$) $C=AC^2 \bmod f(x)$
else $C=a^0C^2 \bmod f(x)$

MSB 우선 알고리즘의 단계3에서 $C=AC^2 \bmod f(x)$ 연산이 필요하다. 즉, 효율적인 $AC^2 \bmod f(x)$ 연산을 통하여 효율적인 지수 연산을 수행할 수 있다. 본 논문에서는 MSB 우선 지수 연산 알고리즘을 위한 기본 구조로서 AB^2 연산을 위한 새로운 알고리즘과 두 가지 세미시스톨릭 구조를 제안한다.

다항식 $f(x)$의 근을 a라 하자. GF(2^m) 상에서 $f(x)$를 $f(x)=f_mx^m+f_{m-1}x^{m-1}+\cdots+f_1x+f_0$라 할 때, 만약 $f_i=1(i=0,1,\cdots,m)$이면 이 $f(x)$를 m차의 AOP(All One Polynomial)이라고 한다. 다항식 AOP에서 $m+1$이 소수이고 2가 모듈라 $m+1$에 대해 원시 근이 되면 기약다항식이 된다. 그리고 위의 AOP $f(x)$의 근 a에 의해 생성된 집합 $\{1,a,a^2,\cdots,a^{m-1}\}$은 유한체 GF($2^m$)의 표준기저가 되고 유한체 GF($2^m$)상의 원소 A는 표준기저에서 $A=a_{m-1}a^{m-1}+a_{m-2}a^{m-2}+\cdots+a_1a+a_0$로 표현된다.

기약다항식 AOP의 속성을 모듈라(modular)로 사용하기 위해서 기저의 확장이 필요하다. 표준기저에서 확장된 기저를 $\{1,a,a^2,\cdots,a^{m-1},a^m\}$이라 하면, 확장된 기저 상에서 유한체 GF(2^m)상의 원소 A는 $A=A_ma^m+A_{m-1}a^{m-1}+\cdots+A_1a+A_0(A_m=0,\ A_i=a_i,\ 0\le i\le m-1)$로 표현되고 확장된 기저상의 원소가 된다. 그러므로 GF(2^m)상의 원소 A는 두 가지 다른 표현을 가진다. 여기서, $F(x)=x^m+x^{m-1}+\cdots+x+1$를 m차의 기약 AOP라하고 a를 $F(x)$의 근이라 하자. 즉, $F(a)=a^m+a^{m-1}+\cdots+a+1=0$ 이다. 그리고 $F(a)=0$을 $a^m=a^{m-1}+\cdots+a+1$로 나타낼 수 있고 양변에 a를 곱하고 정리하면 다음 방정식을 만족한다.

$$a^{m+1}=1 \quad (4)$$

이제 AOP의 속성이 적용된 $P=a^{m+1}+1$를 모듈라로 사용해서 GF(2^m)의 확대체 상에서의 원소 A와 B^2의 곱 즉, $AB^2 \bmod P$연산을 수행한다. 이렇게 곱셈한 연산의 결과 역시 확대체 상의 원소가 된다. 곱셈 $AB^2 \bmod P$ 연산의 결과를 $R=r_ma^m+r_{m-1}a^{m-1}+\cdots+r_1a+r_0$라 할 때, 기약다항식 AOP의 성질을 이용해서 본 논문에서 제안한 $AB^2 \bmod P$를 계산하는 식은 다음과 같다.

$$\begin{aligned}R&=AB^2 \bmod P\\&=\{\cdots[[Ab_m]a^2 \bmod P+Ab_{m-1}]a^2 \bmod P+\cdots\\&\quad +Ab_1\}a^2 \bmod P+Ab_0\\&=r_ma^m+r_{m-1}a^{m-1}+\cdots+r_1a+r_0\end{aligned} \quad (5)$$

위의 방정식 (5)에서 $AB^2 \bmod P$ 연산은 크게 두 부분으로 나뉘어진다. 하나는 곱셈 연산을 위한 부분이고 다른 하나는 모듈라 감소 연산을 위한 부분이다. 전자는 정수 연산에서의 곱셈 연산과 같고, 후자는 2-비트 순환 시프트(2-bit circular shift)에 의해서 수행될 수 있다. 이 두 연산을 한 후에 결과 값 R을 쉽게 얻을 수 있다. 방정식 (5)로부터, AOP의 속성에 기반하여 $AB^2 \bmod P$ 연산을 더 효율적으로 계산하는 MSB 우선 알고리즘을 다음과 같이 제안한다.

[알고리즘2] AOP에 기반한 제안된 MSB 우선 곱셈 알고리즘

입력 : $A=(a_m,a_{m-1},\cdots,a_1,a_0)$,
$B=(b_m,b_{m-1},\cdots,b_1,b_0)$

출력 : $R=AB^2 \bmod P$
초기값 : $R_{m+1}=(0,r_{m-1}, \cdots, r_1, r_0)$
$=(0,0, \cdots, 0,0)$

단계1 : for $i=m$ to 0
단계2 : for $j=m$ to 0
단계3 : $r^i_j=r^i_{\langle j-2\rangle}+a_jb_i$

단계3에서 $\langle x\rangle$는 $x \bmod m+1$을 의미한다. 알고리즘2는 A와 B를 입력으로 하여 AB^2의 결과인 R을 출력한다. 이 알고리즘의 주된 처리는 단계3에서 이루어진다. 단계3은 크게 계수의 곱셈 연산과 모듈라 감소 연산의 두 가지 연산으로 나뉘어진다. 먼저, 계수의 곱은 a_jb_i연산에 의해서 수행된다. 모듈라 감소 연산은 r^i_j를 왼쪽으로 2비트 순환 시프트 시킴으로 해서 수행할 수 있다. 이러한 특성은 기약다항식으로서 AOP의 특성을 이용하였기 때문에 가능하다. 그러나 일반적인 기약 다항식을 사용한 모듈라 감소 연산에 있어서는 이전 곱셈의 임시 결과값의 최상위 두 비트에 의해서 모듈라 감소 연산의 필요성이 결정되고, 본 논문에서 제안한 알고리즘보다 상당히 큰 복잡도를 갖는 연산이 필요하게 된다. 즉, 단계 3에서의 $r^i_j=r^i_{\langle j-2\rangle}$을 수행함으로써 모듈라 감소 연산이 수행된다. 단계2의 루프내의 연산은 병렬로 수행된다.

다음 장에서는 병렬 입출력 형태의 $AB^2 \bmod P$ 연산을 위한 병렬 세미시스톨릭 어레이 구조와 변형된 병렬 세미시스톨릭 어레이 구조를 알고리즘2에 기초하여 제시한다.

Ⅲ. 제안된 곱셈기 구조

본 장에서는 두 가지 병렬 세미시스톨릭 어레이 구조를 제안한다.[10,18] 먼저 알고리즘2에 기초한 병렬 세미시스톨릭 어레이 구조(PSM)를 구현한다. 그리고 PSM구조에서 중간 결과값의 누적 연산을 한 단계 늦춤으로 해서 임계경로 면에서 보다 효율적인 구조 즉, 변형된 세미시스톨릭 어레이 구조(MPSM)를 새롭게 구현한다.

3.1 병렬 세미시스톨릭 어레이 구조(PSM)

유한체 GF(2^4) 상에서의 원소 A, B 및 B^2은 확장된 기저 상에서 각각

$$A=a_4\alpha^4+a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0$$
$$B=b_4\alpha^4+b_3\alpha^3+b_2\alpha^2+b_1\alpha+b_0$$
$$B^2=b_4\alpha^8+b_3\alpha^6+b_2\alpha^4+b_1\alpha^2+b_0$$

로 표현된다. $P^*=\alpha^5+1$라 하면, 유한 체GF(2^4)상의 원소 A와 B^2의 확장된 기저 상에서의 곱, $AB^2 \bmod P^*$연산은 알고리즘2에 의해 다음과 같이 계산된다.

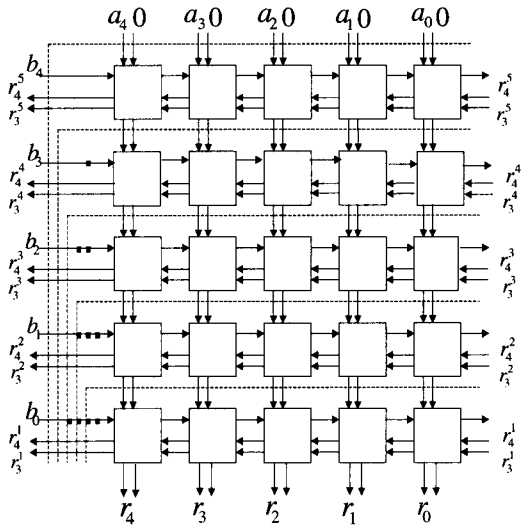
$$\begin{aligned}R&=AB^2 \bmod P^*\\&=A(b_4\alpha^4+b_3\alpha^3+b_2\alpha^2+b_1\alpha+b_0)^2 \bmod P^*\\&=\{\cdots[[Ab^4]\alpha^2 \bmod P^*+Ab_3]\alpha^2 \bmod P^*\\&\quad+\cdots+Ab_1\}\alpha^2 \bmod P^*+Ab_0\\&=r_4\alpha^4+r_3\alpha^3+r_2\alpha^2+r_1\alpha+r_0\end{aligned} \quad (6)$$

각각의 중간 결과값 계수 T^i는 다음과 같이 계산된다.

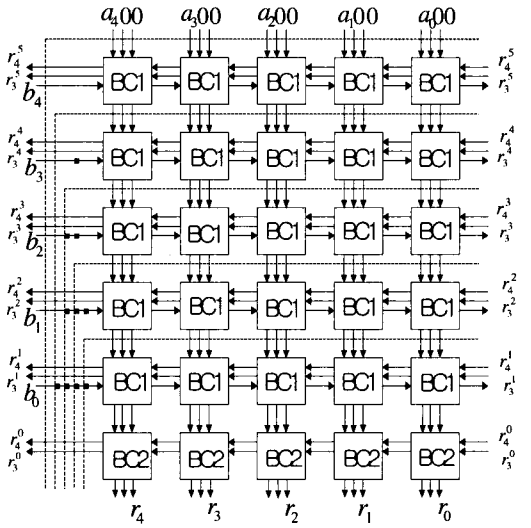
$$\begin{aligned}T^4&=a_1b_4\alpha^4+a_0b_4\alpha^3+a_4b_4\alpha^2+a_3b_4\alpha+a_2b_4\\T^3&=a_3b_3\alpha^4+a_2b_3\alpha^3+a_1b_3\alpha^2+a_0b_3\alpha+a_4b_3\\T^2&=a_0b_2\alpha^4+a_4b_2\alpha^3+a_3b_2\alpha^2+a_2b_2\alpha+a_1b_2\\T^1&=a_2b_1\alpha^4+a_1b_1\alpha^3+a_0b_1\alpha^2+a_4b_1\alpha+a_3b_1\\T^0&=a_4b_0\alpha^4+a_3b_0\alpha^3+a_2b_0\alpha^2+a_1b_0\alpha+a_0b_0\end{aligned} \quad (7)$$

위의 식 (7)에서 T^i는 각각의 중간 계산 결과값이다. 방정식 (6)에 의해서, [그림 1]은 유한체GF(2^4)상의 병렬 세미시스톨릭 어레이 구조(PSM)를 보여준다. PSM은 $(m+1)^2$의 기본 셀을 갖는다. [그림 1]의 연산은 알고리즘2를 기반으로 한다.

PSM구조는 a_j값과 $b_i(0\le i,\ j\le m)$값이 동시에 입력되는 병렬 구조이다. a_j값들은 같은 열(column)에 있는 인접 셀에 전송되지만 b_i값들은 한번에 같은 행(row)에 있는 모든 셀에 브로드캐스트(broadcasting)되는 세미시스톨릭 어레이 속성을 갖는다.[14] 다시 말해서 $(m+1)$비트의 데이터 a_j가 최상위 열에서 입력되고, 셀의 연산 후에 다음 열에 전송된다. 즉, 각각의 인접한 열들의 셀에 전송된다. 그러나 각 열에 있는 b_i들은 같은 행에서 브로드캐스트 된다. PSM에서 각 셀들은 알고리즘2의 단계3에 해당하는 연산을 수행한다. 단계 3의 $r^i_j=r^i_{\langle j-2\rangle}+a_jb_i$ 연산은 수식 (7)의 결과에서 같은 차수의α의 계수의 합을 구함으로서 수행된다. 즉, 각 인덱스 i에 대해, j 인덱스에 해당하는 연산을 병렬로 수행함으로써 원하는 $AB^2 \bmod P$ 연산의 결과를 얻을 수 있다. 여기서, 한 행에 있는 모든 열들 간에는 의존성(dependency)이

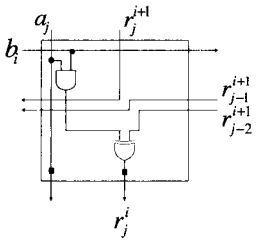


〔그림 1〕 GF(2^4)상에서 PSM을 위한 병렬 세미시스톨릭 어레이 곱셈기



〔그림 3〕 GF(2^4)상에서 MPSM을 위한 병렬 세미시스톨릭 어레이 곱셈기

없다. 그러므로 같은 행에 있는 각각의 셀들은 병렬로 수행될 수 있다. 제시한 PSM구조의 분석을 위해서 D_{AND2}와 D_{XOR2}를 각각 2-입력 AND와 XOR 게이트의 딜레이(delay)라고 하면, PSM 구조는 각 셀 당 $D_{AND2}+D_{XOR2}$의 임계경로를 갖는다. 그리고 전체 지연시간(latency)은 $m+1$이다. 〔그림 1〕로부터 GF(2^m) 상에서 PSM구조가 $m=4$에서 뿐만 아니라, 모든 m에 대해서도 확장시킬 수 있다. 〔그림 2〕는 그림 1의 각 셀에 해당하는 구조를 보여준다. 이 기본 셀은 하나의 AND와 XOR게이트로 이루어진다.



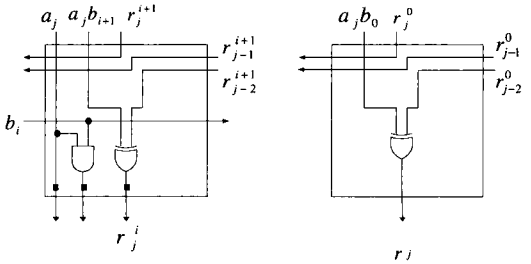
〔그림 2〕 PSM의 기본 구조

3.2 변형된 병렬 세미시스톨릭 어레이 구조(MPSM)

제안된 PSM구조는 하나의 AND와 XOR게이트로 이루어지고 한 셀의 임계경로는 $D_{AND2}+D_{XOR2}$이다. 그러나 중간 결과값의 누적 연산을 한 단계 늦춤으로 해서 PSM보다 한 셀의 임계경로가 좀 더 효율적인 구조를 제시할 수 있다. 〔그림 3〕은 〔그림 1〕에서 보여준 세미시스톨릭 어레이 구조의 변형된 병렬 세미시스톨릭 어레이 구조(MPSM)를 보여준다.

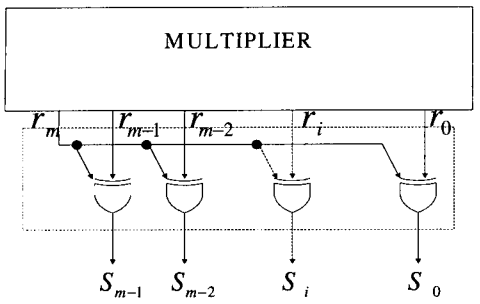
〔그림 3〕에서 제안된 구조는 〔그림 1〕에서 제안된 구조의 임계경로를 줄이기 위해 새롭게 변형된 구조이다. MPSM구조는 마지막 행을 제외한 m개의 행은 〔그림 4〕의 (a)구조를 갖는다. 마지막 행은 XOR 연산만을 필요로 하는 〔그림 4〕의 (b)와 같은 구조를 갖는다. 제안된 MPSM구조의 전체 지연시간은 앞에서 제시된 PSM과 같다. 하지만 〔그림 4〕에서 제시된 바와 같이 각 셀 당 D_{XOR2}의 임계경로만을 갖는다. 결과적으로 말하면 MPSM의 지연시간은 PSM과 같다. 그렇지만 전체 임계경로는 PSM보다 훨씬 더 효율적이다. 〔그림 3〕으로부터 GF(2^m)상에서 MPSM 구조를 $m=4$에서 뿐만아니라, 모든 m에 대해서도 확장시킬 수 있다.

본 논문에서 제시한 두 구조에서 한 가지 고려되



(a)MPSM의 기본구조1 (b)MPSM의 기본구조2

〔그림 4〕 MPSM의 기본 구조들



〔그림 5〕 모듈라 감소연산을 위한 세미시스톨릭 어레이 곱셈기

어야 할 사항은 효율적인 모듈라 감소 연산을 위하여 표준기저 보다 확장된 기저 상에서 연산이 이루어진다는 것이다. 따라서 결과값도 확장된 기저 상에서의 값이다. 이 문제를 해결하기 위해서는 PSM과 MPSM의 연산 후 그 결과를 다시 모듈라 감소 연산(modular reduction)을 해줌으로써 표준기저 상에서의 결과값을 얻을 수 있다. 추가적인 모듈라 감소 연산을 위한 구조를 〔그림 5〕에서 보여준다.

Ⅳ. 비교 및 분석

본 논문에서는 AB^2 연산을 위한 두 가지 병렬 세미시스톨릭 어레이 구조, 즉, PSM과 MPSM을 유한체 GF(2^m) 상에서 제안하였다. 역원/나눗셈을 계산하기 위해서 각각 병렬 입출력 세미시스톨릭 구조, 시스톨릭 파워 썸(power-sum)구조 및 AOP를 기반으로 한 병렬 입출력 구조가 논문 〔10〕, 〔12〕와 〔13〕에 제안되었다. 〔표 1〕은 본 논문에서 제시한 구조와 이와 관계된 구조들의 성능 비교를 보여준다.

표에서 2-입력 AND와 XOR게이트의 딜레이(delay)는 각각 D_{AND2}와 D_{XOR2}이고, latch는 1bit이다.

〔표 1〕 구조의 성능 비교 및 분석

구조 / 항목	Jain[10]	Wang[12]	PSM	MPSM
기능	AB^2	AB^2+C	AB^2	AB^2
셀수	m^2	$m^2/2$	$(m+1)\times(m+1)$	$(m+1)\times(m+2)$
셀 복잡도	2 AND 2 XOR 3 latches	6 AND 2 XOR 17 latches	1 AND 1 XOR 2 latches	1 AND 1 XOR 3 latches
지연 시간	$m+1$	$2m+m/2$	$m+1$	$m+1$
임계 경로	$D_{AND2}+D_{XOR2}$	$D_{AND2}+D_{XOR4}$	$D_{AND2}+D_{XOR2}$	D_{XOR2}

먼저 논문 〔10〕에서 AND와 XOR게이트는 각각 2-입력이고 지연시간이 $m+1$이고 임계경로는 $D_{AND2}+D_{XOR2}$이다. 그리고 논문 〔12〕에서는 AND게이트는 2-입력이고 XOR게이트는 4-입력이다. 그리고 지연시간은 $2m+m/2$이고 임계경로는 $D_{AND2}+D_{XOR4}$이다. 또한, 논문 〔13〕에서 Itoh가 제안한 구조의 AND와 XOR의 전체 게이트 수는 각각 m^2+2m+1과 m^2+2m이다. 그리고 지연시간은 $D_{AND2}+\lceil \log_2 m+\log_2(m+2)\rceil D_{XOR2}$이다. 본 논문에서 제안된 구조 PSM의 AND와 XOR게이트는 각각 2-입력이다. PSM은 $m+1$의 지연시간을 가졌고 $D_{AND2}+D_{XOR2}$의 임계경로를 가졌다. 이에 비해 변형된 구조인 MPSM은 지연시간은 $m+1$을 임계경로로는 D_{XOR2}를 가졌다. 결국 본 논문에서 제안된 두 구조가 논문〔10〕과 비교할 때, 지연시간과 임계경로 면에서는 같지만 셀 복잡도 면에서 많이 향상됨을 확인 할 수 있다. 그리고 논문 〔12〕와 비교하면, 셀 복잡도 및 지연시간과 임계경로 면에서 아주 효율적이었다. 또한 본 논문에서 제시한 구조와 논문 〔13〕의 구조와 구조 복잡도를 비교해보면 AND 및 XOR게이트 수는 비슷하지만 Itoh의 구조는 병렬 입력을 위한 추가적인 연산이 필요하기 때문에 제안한 구조가 Itoh의 구조에 비해서 더 효율적이고 세미시스톨릭 속성을 사용하기 때문에 구조의 정규성을 더 가진다. 제안된 구조는 Altera MAX Plus II 시뮬레이션 툴을 이용하여 시뮬레이션 되었다.

본 논문에서 제안된 AB^2를 계산하는 PSM과 MPSM 구조는 셀 복잡도, 지연시간과 임계경로 면에서 기존의 구조보다 더 효율적이다. 따라서 PSM과 MPSM을 기반으로 공개키 암호화시스템의 기본 연산인 지수 연산을 한다면, 기존의 구조로 지수 연산을 하는 것 보다 더 낳은 결과를 얻을 수 있다. 뿐만 아니라, PSM과 MPSM을 기반으로 한다면 나눗셈과 역원 연산에 있어서도 사용될 수 있고, 공개키 암호화시스템의 성능 향상에 있어서도 기여할 수 있다.

Ⅴ. 결 론

본 논문에서는 GF(2^m)상의 AB^2를 계산하는 새로운 MSB알고리즘과 두 가지 병렬 세미시스톨릭 어레이 구조를 제안하였다. 일반 기약다항식을 사용하는 것 보다 기약다항식으로 AOP의 속성을 사용함으로써 제안된 PSM구조는 전체 $m+1$의 지연시간을 가졌고 각 셀 당 $D_{AND2}+D_{XOR2}$의 임계경로를

가졌다. 또한 변형된 MPSM구조는 전체 지연시간은 $m+1$로 PSM과 같지만 각 셀 당 D_{XOR2}의 임계경로만을 가졌다. 본 논문에서 제안된 두 구조는 기존의 구조보다 지연시간과 임계경로 면에서 보다 효율적이다. 이 두 구조는 일반 기약다항식을 사용할 때보다 시간 및 공간 복잡도를 줄일 수 있는 장점을 제공한다. 제안된 PSM및 MPSM구조를 기반으로 하여 보다 효율적이고 안전한 공개키 암호화시스템을 구현할 수 있다. 또한 제안된 구조는$GF(2^m)$상에서의 효율적인 나눗셈기, 지수기 및 역원기를 설계하는데 기본 구조로 사용 될 수 있다. 더욱이 제안된 구조 자체가 정규성(regu-l arity), 모듈성(modularity), 병렬성(concurrency)을 가지기 때문에 VLSI구현에 효율적이다.

참 고 문 헌

[1] W. W. Peterson and E. J. Weldon, *Error-Correcting Codes*, Cambridge, MA: MIT Press, 1972.

[2] I. S. Reed and T. K. Truong, "The use of finite fields to compute convolutions," *IEEE Trans. Inform. Theory*, Vol. IT-21, pp. 208~213, Mar. 1975.

[3] D. E. R. Denning, *Cryptography and data security*, Reading, MA: Addison-Wesley, 1983.

[4] A. M. Odlyzko, "Discrete logarithms in finite fields and their cryptographic significance," in *Adv. Cryptol., Proc. Eurocrypt* 84, Paris, France, pp. 224~314, Apr. 1984.

[5] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Trans. on Info. Theory*, Vol. 22, pp. 644~654, 1976.

[6] E. R. Berlekamp, *Algebraic Coding Theory*, New York: McGraw-Hill, 1968.

[7] B. Benjauthrit and I. S. Reed, "Galois switching function and their applications," *IEEE Trans. on Computers*, Vol. C-25, pp. 78~86, Jan. 1976.

[8] D. E. Knuth, *The art of Computer Programing. Volume 1: Fundamental Algorithm*, Addison-Wesley, Reading, Massachusetts, 2nd edition, 1997.

[9] C. S. Yeh, S. Reed, and T.K. Truong, "Systolic multipliers for finite fields $GF(2^m)$," *IEEE Trans. on Computers*, Vol. C-33, pp. 357~360, Apr. 1984.

[10] S. K. Jain and L. Song, "Effcient Semi-systolic Architectures for finite fields Arithmetic," *IEEE Trans. on VLSI System*, Vol. 6, No. 1, Mar. 1998.

[11] J. L. Massey and J. K. Omura, "Computational method and apparatus for finite field arithmetic," U. S. Patent application, submitted 1981.

[12] C. L. Wang and Y. H. Guo, "New Systolic for AB^2+C, Inversoin and Division in $GF(2^m)$," *IEEE Trans. on Computres*. Vol. 49, No. 10, pp. 1120~1125, Otc. 2000.

[13] T. Itoh and S. Tsujii, "Structure of parallel multipliers for a class of finite fields $GF(2m)$," *IEEE Info. Comp.*, Vol. 83, pp. 21~40. 1989.

[14] M. A. Hasan, M. Z. Wang and V. K. Bhargava, "Modular Construction of low complexity parallel multipliers for a class of finite fields $GF(2m)$," *IEEE Trans. on Computers*. Vol. 41, No. 8, pp. 962~971, Aug. 1992.

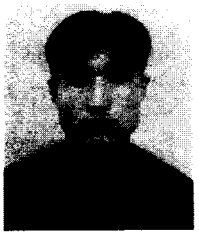
[15] M. Aydos, T. Yanik and C. K. Koc, "High-speed implementation of an ECC-based wireless authentication protocol on an ARM microprocessor," *IEE Proc. Comm.*, Vol. 148, pp. 273~279, Oct. 2001.

[16] V. Pandiarajan, T. L. Martin and L. L. Joiner, "Recommendations on a new cellular encryption standard using elliptic curve cryptography," *IEEE Proceedings*. pp. 136~142, 2001.

[17] H. S. Kim, *Bit-Serial AOP Arithmetic Architecture for Modular Exponentiation*, Ph.D. Thesis, Kyungpook National University, 2002.

[18] S. Y. Kung, *VLSI Array Processors*, Prentice Hall, 1998.

〈著者紹介〉



이 형 목 (Hyung-Mok Lee)
2001년 2월 : 계명대학교 수학과 이학사
2001년 8월~현재 : 경북대학교 컴퓨터공학과 석사과정
〈관심분야〉 암호학, 정보보호, PKI

김 현 성 (Hyun-Sung Kim)
1996년 2월 : 경일대학교 컴퓨터공학과 공학사
1998년 2월 : 경북대학교 컴퓨터공학과 공학석사
2002년 2월 : 경북대학교 컴퓨터공학과 공학박사
2002년 3월~현재 : 경일대학교 컴퓨터공학과 교수
〈관심분야〉 암호화 프로세서 설계, 정보보호, PKI

전 준 철 (Jun-Cheol Jeon)
2000년 2월 : 국립 금오공과대학 컴퓨터공학과 공학사
2002년 8월~현재 : 경북대학교 컴퓨터공학과 석사과정
〈관심분야〉 암호화 프로세서 설계, 정보보호, IDS

유 기 영 (Kee-Young Yoo)
1978년 2월 : 경북대학교 수학교육과 학사졸업
1980년 2월 : 한국과학기술원 컴퓨터공학과 석사졸업
1993년 2월 : Rensselaer Polytechnic Institute, New York, 컴퓨터 공학과 박사졸업
1980년 2월~현재 : 경북대학교 컴퓨터공학과 교수
〈관심분야〉 정보보호, 암호학, 암호칩 설계, 스마트 카드, 병렬처리