공개키 암호 시스템을 위한 AB²곱셈기 설계
(Design of AB² Multiplier for Public-key Cryptosystem)

김 현 성 † 유 기 영 ††
(Hyun-Sung Kim) (Kee-Young Yoo)

요 약 본 논문에서는 GF(2^m)상에서 AB^2연산을 위한 두 가지 새로운 알고리즘과 구조를 제안한다. 먼저 Linear Feedback Shift Register 구조기반의 AB^2 곱셈 알고리즘을 제안하고, 이를 기반으로 비트순차 구조를 설계한다. 그리고, 기본 구조로부터 변형된 변형 AB^2 곱셈기를 설계한다. 제안된 구조는 기약다항식으로 모든 계수가 1인 속성의 All One Polynomial 을 이용한다. 시뮬레이션 결과 제안된 구조가 구조 복잡도면에서 기존의 구조들보다 훨씬 효율적이다. 제안된 곱셈기는 공개키 암호의 핵심이 되는 지수기의 구현을 위한 효율적인 기본구조로 사용될 수 있다.

키워드 : 공개키 암호 시스템, 유한체 연산, AOP 연산기, LFSR 구조

Abstract This paper presents two new algorithms and their architectures for AB^2 multiplication over GF(2^m). First, a new architecture with a new algorithm is designed based on LFSR (Linear Feedback Shift Register) architecture. Furthermore, modified AB^2 multiplier is derived from the multiplier. The multipliers and the structure use AOP (All One Polynomial) as a modulus, which has the properties of all coefficients with 1. Simulation results shows that proposed architecture has lower hardware complexity than previous architectures. They could be. Therefore it is useful for implementing the exponentiation architecture, which is the core operation in public-key cryptosystems.

Key word : Public-key Cryptosystem, Finite Fields Arithmetic, AOP Architecture, LFSR Architecture

1. 서 론

암호학(Cryptography), 디지털 신호 처리(Digital Signal Processing) 및 에러 교정 코드(Error-correcting Codes)의 응용에서 갈로아 필드(Galois field, GF) 연산은 아주 중요하다[1, 2, 3, 4, 5, 6, 7, 8, 9]. 특히, 유한체 GF(2^m)은 2^m개의 원소를 가지고 각각의 원소들은 0과 1의 비트-스트링으로 구성된다. 이러한 속성 때문에 갈로아 필드 연산의 하드웨어 구현에 유한체 GF(2^m)이 적당하다[9].

여러 가지 구조를 기반으로 다양한 연산기가 제안되었다. 특히, 많은 연구에서 모듈라로서 AOP (All One Polynomial)의 특성을 이용한 구조 복잡도 면에서 효율적인 구조들이 제안되었다[14, 15, 16, 17]. Itoh와 Tsujii는 효율적인 구조 복잡도를 가진 기약 다항식 AOP에 기초한 곱셈기와 기약 다항식 ESP (Equally Spaced Polyno mial)에 기초한 곱셈기를 설계하였다[14]. Fenn et al. 은 GF(2^m)상에서 LFSR (Linear Feedback Shift Register)구조를 이용하는 두 가지 형태의 AB곱셈기를 비트순차 (Bit-serial) 구조로 설계하였다[15]. Liu et al. 는 AB^2연산을 위한 내적 (Inner Product) 곱셈 알고리즘과 이를 위한 병렬 셀룰러 구조를 제시하였다[16]. 또한, 정형화된 기약 다항식을 이용한 여러 시스톨릭 구조들이 제안되었다[11, 12, 13]. Kim et al. 은 표준기저상에서 AB^2연산을 위한 비트순차 시스톨릭 구조를 제시하였다[13]. 지금까지의 연구에서 여러 구조들이 제안되었지만 시간과 공간 복잡도 면에서 보다 효율적인 구조 설계에 관한 꾸준한 연구가 필요하다.

본 논문에서는 GF(2^m)상에서 AB^2연산을 위한 두 가지 새로운 알고리즘과 구조를 제안한다. 먼저 LFSR 구조기반의 새로운 AB^2연산 알고리즘과 비트 순차 AB^2

† 정 회 원 : 경일대학교 컴퓨터학과
kim@kiu.ac.kr
†† 종신회원 : 경북대학교 컴퓨터학과 교수
yook@knu.ac.kr
논문접수 : 2002년 5월 16일
심사완료 : 2002년 11월 18일

곱셈기 (Power Multiplier, PM)를 설계한다. 그리고, PM 구조로부터 변형된 변형 AB^2 곱셈기 (Modified Power Multiplier, MPM)를 설계한다. 제안된 구조들은 기약다항식으로 모든 계수가 1인 속성의 AOP를 이용한다. 시뮬레이션 결과 제안된 구조가 구조복잡도면에서 기존의 구조들보다 훨씬 효율적임을 알 수 있었다. 제안된 곱셈기는 공개키 암호의 핵심이 되는 지수기의 구현을 위한 효율적인 기본구조로 사용될 수 있다.

본 논문의 구성은 다음과 같다. 2장에서 유한 체에 대한 기본적인 정의와 기약 다항식으로서의 AOP 속성에 대하여 설명한다. 또한, 공개키 암호 시스템에 대해서 논하고 기본적인 연산에 대해서 살펴 본다. 3장에서는 AB^2연산을 위한 새로운 알고리즘으로부터 새로운 구조 (PM)를 설계하고, PM으로부터 변형된 새로운 구조 (MPM)를 설계한다. 그리고, 4장에서 기존의 구조들과 비교 및 분석을 제시하고, 5장에서 결론을 맺는다.

2. 유한 체와 공개키 암호 시스템

유한 체 (Finite Field)는 갈로아 체(Galois Field, GF)라고도 불리며, 암호이론이나 부호이론에서 주로 사용되는 원소의 개수가 유한인 체를 말한다[9]. 유한 체는 0에 의한 나눗셈을 제외한 사칙연산에 대해서 닫혀 있다. 유한체 GF(2)의 유한 확대체를 GF(2^m)이라 하자. 먼저 유한 확대체 GF(2^m)상의 원소는 표준, 정규, 이원 기저의 세 기저에 의해서 표현될 수 있다. 표준 기저를 제외한 다른 두 기저, 즉, 정규기저와 이원기저에서는 연산 전후에 기저의 변환이 필요하다. 본 논문에서는 원소표현에 있어서 연산 전후에 기저의 변환이 필요 없는 표준기저를 이용한다.

다항식 $f(x)$의 근을 α라 하자. GF(2^m)상에서 $f(x)$를 $f(x)=f_m x^m+f_{m-1}x^{m-1}+\cdots+f_1x+f_0$라 할 때, $f_i=1(i=0,1,\cdots,m)$인, 즉, 다항식의 항이 모두 1인 $f(x)$를 AOP (All One Polynomial)라고 한다. 다항식 AOP에서 $m+1$이 소수이고 2가 모듈라 $m+1$에 대해 원시 근이 되는 다항식을 기약 다항식이라 한다. 100보다 작은 m에 대해서 m이 2, 4, 10, 12, 18, 28, 36, 52, 58, 60, 66, 82 일 때 기약 다항식으로서의 AOP를 만족한다[14]. 위의 AOP $f(x)$의 근 α에 의해 생성된 집합 { 1, α, … , α^{m-2}, α^{m-1} }은 유한체 GF(2^m)의 표준기저가 되고 유한체 GF(2^m)상의 한 원소 a는 $a=a_{m-1}\alpha^{m-1}+a_{m-2}\alpha^{m-2}+\cdots+a_1\alpha+a_0$로 표현된다.

기약다항식 AOP는 기저를 한차원 확장했을 때 모듈라 (Modular)로서 아주 효율적인 속성을 가진다. 표준 기저에서 확장된 기저를 { 1, α, … , α^{m-2}, α^{m-1}, α^m }이라 하면, 확장된 기저 상에서 유한체 GF(2^m)의 원소 A는 $A=A_m\alpha^m+A_{m-1}\alpha^{m-1}+A_{m-2}\alpha^{m-2}+\cdots+A_1\alpha+A_0$ (여기서, $A_m=0$, $A_i=a_i$, $0\le i\le m-1$)로 표현된다. 여기서, $F(x)=x^m+x^{m-1}1+\cdots+x+1$를 m차의 기약 다항식 AOP라하고 α를 $F(x)$의 근이라 하자. 즉, $F(\alpha)=\alpha^m+\alpha^{m-1}+\cdots+\alpha+1=0$ 이다. 그러면 $F(\alpha)=0$을 $\alpha^m=\alpha^{m-1}-\cdots+\alpha+1$로 나타낼 수 있고 양변에 α를 곱하고 정리하면 다음 방정식을 만족한다.

$$\alpha^{m-1}=1 \qquad (1)$$

본 논문에서 제안된 구조는 AOP를 모듈라로 사용하여 AB^2 mod $F(x)$연산을 수행한다. 연산에 사용된 원소들은 모두 확대체 상의 원소가 되고, 곱셈의 결과 또한 확대체 상의 원소이다.

유한체 상에서 Diffie-Hellman 키 교환 방식, 디지털 서명 알고리즘과 ElGamal 암호화 방식과 같이 잘 알려진 알고리즘을 응용한 타원 곡선 (Elliptic Curve) 기반의 공개키 암호 시스템의 구현에 있어서 GF(p)나 GF(2^m) 상에서 지수 연산이 필요하다[8]. Knuth는 효율적인 지수 연산을 위해서 지수의 처리 방식에 따라서 LSB (Least Significant Bit)와 MSB (Most Significant Bit) 우선 방식의 알고리즘을 제시했다[10]. 본 논문에서는 MSB 방식의 알고리즘을 위한 기본 구조 제안에 그 목적이 있다. Knuth의 MSB 알고리즘은 다음과 같다.

[알고리즘 1] Knuth의 MSB 우선 지수 알고리즘
입력 : A, E, $f(x)$
출력 : $B=A^E$ mod $f(x)$
단계1 : if (e_{m-1}==1) $B=A$ else $B=\alpha^0$
단계2 : for $i=m-2$ to 0
단계3 : if (e_i==1) $B=AB^2$ mod $f(x)$
else $B=\alpha^0B^2$ mod $f(x)$

알고리즘1의 단계3에서 AB^2 mod $f(x)$ 연산이 필요하다. 즉, 효율적인 AB^2 mod $f(x)$ 연산을 통하여 효율적인 지수 연산을 수행할 수 있다. 본 논문에서는 MSB 우선 지수 연산 알고리즘을 위한 기본 구조로서 AB^2 mod $f(x)$ 연산을 위한 새로운 두 가지 구조를 제안한다.

3. 비트 순차 AB^2 곱셈기

본 장에서는 LFSR 구조에 기반 한 두 가지 새로운 알고리즘과 AB^2곱셈기를 설계한다. 먼저 AB^2연산을 위한 새로운 알고리즘을 유도하고, 이 알고리즘에 기반 한 새로운 구조의 AB^2곱셈기(PM)를 설계한다. 그리고, PM으로부터 유도된 변형된 AB^2곱셈기(MPM)를 설계한다.

3.1 AB^2 곱셈기(PM)

AB^2곱셈기 설계를 위해서 먼저 B^2 연산에 대하여 살펴보자. B^2은 모듈라 AOP의 속성에 의해서 계수의 재배치에 의해 다음과 같이 계산된다.

$$B^2 = (B_m a^m + B_{m-1}a^{m-1} + \cdots + B_1 a + B_0)^2 \bmod (a^{m-1}+1) \quad (2)$$
$$= (B_m a^{2m} + B_{m-1}a^{2(m-1)} + \cdots + B_2 a^2 + B_1 a + B_0) \bmod (a^{m-1}+1)$$
$$= B_{m-2}a^m + B_m a^{m-1} + \cdots + B_1 a^2 + B_{m-2} + B_0$$

예를들어 $GF(2^4)$상의 한 원소 $B = B_3a^3 + B_2a^2 + B_1a + B_0$의 B^2 연산은 다음과 같다(여기서, $a^{m-1}+1$의 AOP 속성이 모듈라로 이용된다).

$a^5 = 1$, $a^6 = a$, $a^7 = a^2$, $a^8 = a^3$

$B^2 = (B^4a^4 + B^3a^3 + B^2a^2 + B^1a + B_0)^2 \bmod (a^5+1) = B_2a^4 + B_1a^3 + B_3a^2 + B_0a + B_0$.

AB^2곱셈은 B^2의 결과를 이용한 $GF(2^4)$상에서의 곱셈 알고리즘은 다음과 같다.

	$A=$			A_4	A_3	A_2	A_1	A_0
×	$B^2=$			B_2	B_1	B_3	B_3	B_0
				A_4B_0	A_3B_0	A_2B_0	A_1B_0	A_0B_0
			A_4B_3	A_3B_3	A_2B_3	A_1B_3	A_0B_3	
		A_4B_1	A_3B_1	A_2B_1	A_1B_1	A_0B_1		
	A_4B_1	A_3B_1	A_2B_1	A_1B_1	A_0B_1			
A_4B_2	A_3B_2	A_2B_2	A_1B_2	A_0B_2				
P_8	P_7	P_6	P_5	P_4	P_3	P_2	P_1	P_0

(a) AB^2 곱셈.

a^4	a^3	a^2	a^1	a^0
A_4B_0	A_3B_0	A_2B_0	A_1B_0	A_0B_0
A_4B_3	A_3B_3	A_2B_3	A_1B_3	A_0B_3
A_3B_1	A_2B_1	A_1B_1	A_0B_1	A_4B_1
A_2B_1	A_1B_1	A_0B_1	A_4B_1	A_3B_1
A_1B_2	A_0B_2	A_4B_2	A_3B_2	A_2B_2
P_4	P_3	P_2	P_1	P_0

(b) 모듈라 감소 연산이 적용된 AB^2 곱셈

그림 1 AB^2곱셈 알고리즘

그림1(a)는 AB^2곱셈 과정을 보여준다. 곱셈 후 연산의 결과에 모듈라 연산을 적용하면 그림1(b)와 같다. 즉, 곱셈 후 그림1(a)의 왼쪽에 강조된 부분의 값에 따라서 모듈라 감소 연산이 적용되어야 하고, $a^{m-1}+1$이 모듈라로서 사용되면 모듈라 감소는 그림1(b)에서 보여주는 바와 같이 계산된다. 여기서, 모듈라 감소 연산은 그림1(a)에서 왼쪽 강조된 부분이 그림1(b)에서 보여준 것처럼 오른쪽으로 치환 됨으로 계산된다.

그림2는 그림1에서 제시한 알고리즘에 기반 한 $GF(2^4)$상의 비트순차 AB^2곱셈기(Power Multiplier, PM)를 보여준다.

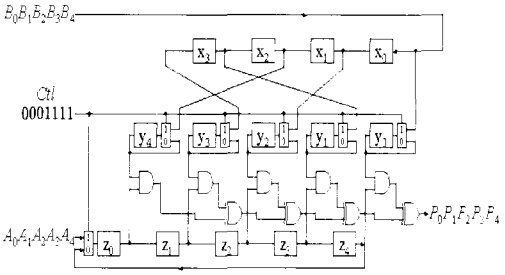


그림 2 비트순차 AB^2 곱셈기

그림2의 PM구조는 m차의 구조로 쉽게 일반화 시킬 수 있다. PM구조는 레지스터 Y를 기준으로 제곱부분과 곱셈부분의 두 부분으로 나눌 수 있다. 레지스터 Y를 포함한 윗 부분이 B^2연산을 위한 제곱 부분이고, 레지스터 Y를 포함한 아랫 부분이 계산된 B^2연산을 이용한 곱셈 부분이다. PM은 다음 연산을 수행한다.

[알고리즘 2] PM의 동작 알고리즘

입력 : A, B

출력 : $P=AB^2 \bmod a^{m-1}+1$

단계1 : for $i=m$ to 0

단계2 : Left_Shift(x, B_i), Right_Shift(z, A_i), $P_i = 0$

단계3 : if ($i=0$) $y_0=x_0$, $y_1=x_{m-1}$, $y_2=x_{m-2}$, $y_{m-1}=x_m$, $y_m=x_{m-2}$

단계4 : for $i=m$ to 0

단계5 : for $j=0$ to m

단계6 : $P_j = P_j + y_{m-j} \times z_j$

단계7 : Circular_Right_Shift(z)

단계 2에서 Left_Shift(x, y)는 y를 입력으로 레지스터 x의 왼쪽 한 비트 쉬프트 연산을 의미한다. Right_Shift(x, y)는 오른쪽으로 한 비트 쉬프트 연산을 의미한다. 그리고 단계 7에서 Circular_right_shift(z)는 레지스터의 오른쪽으로 한 비트 순환 쉬프트 연산을 의미한다.

PM을 위한 연산은 크게 레지스터 초기화 부분(단계1~단계3)과 연산 부분(단계4~단계7)로 나눌 수 있다. 단계1과 단계2, 그리고 단계 3에서 모든 레지스터를 초기화한다. 단계4~단계7 연산을 통해서 모듈러 곱셈 연산이 수행된다. PM 수행에 있어서 입력의 마지막 스텝과 연산의 첫 스텝은 병렬로 수행된다. 즉, 입력의 마지

막 스텝에 모든 레지스터의 값이 초기화 되고, 그 시점에 첫번째 결과값이 출력된다. 그림2의 제곱 부분에서 보여준 바와 같이 식 2의 모듈라 제곱 연산은 단순히 계수의 재배치에 의해서 계산된다. 또한, PM의 수행에 있어서 입력 상태와 처리 상태의 구별을 위해 하나의 제어 신호가 필요하다. 제어 신호는 입력을 위한 m+1비트의 1과 연산을 위한 m-1비트의 0이 필요하다. 그러나 입력의 마지막 클럭에 첫번째 연산의 결과를 출력할 수 있으므로 전체 m+1비트의 1과 m비트의 0, 즉, $2m$+1비트의 제어 신호가 필요하다.

그러나, PM의 AB^2연산 결과는 확장 필드상의 연산이기 때문에 추가적인 모듈라 감소 연산이 필요하다. 이 문제점을 해결하기 위한 다음 절에서는 새로운 알고리즘과 그 알고리즘에 기반 한 구조를 제시한다.

3.2 변형된 AB^2 곱셈기(MPM)

PM의 문제점을 해결하기 위해서 본 절에서는 먼저 그림1(b)의 알고리즘을 그림3과 같이 변형한다. 즉, 추가적인 모듈라 연산은 첫번째 결과값을 이용하여 그림3과 같이 계산할 수 있다.

a^3	a^2	a^1	a^0
P_4	P_4	P_4	P_4
A_3B_0	A_2B_0	A_1B_0	A_0B_0
A_2B_3	A_1B_3	A_0B_3	A_4B_3
A_1B_1	A_0B_1	A_4B_1	A_3B_1
A_0B_4	A_4B_4	A_3B_4	A_2B_4
A_4B_2	A_3B_2	A_2B_2	A_1B_2
p_3	p_2	p_1	p_0

그림 3 변형된 AB^2곱셈 알고리즘

그림3의 변형된 AB^2 곱셈 알고리즘 수행을 위해서는 곱셈 연산을 시작하기 전에 식3의 연산이 수행되어야 한다. 즉, 곱셈의 최상위 비트 결과 값이 곱셈을 수행하기 전에 계산 될 수 있어야 한다.

$$P_4 = A_4B_0+A_3B_3+A_2B_1+A_1B_4+A_0B_2 \quad (3)$$

그림4는 그림3에서 제시한 변형된 알고리즘에 기반 한 GF(2^4)상의 변형된 비트순차 AB^2곱셈기(Modified Power Multiplier, MPM)를 보여준다.

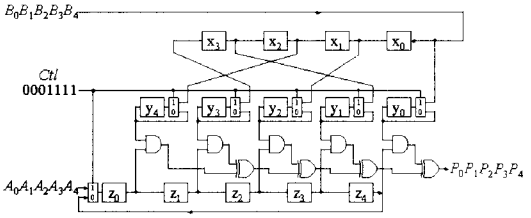


그림 4 변형된 비트순차 AB^2 곱셈기

그림4의 MPM구조는 m차의 구조로 쉽게 일반화 시킬 수 있다. 그림4의 오른쪽 강조된 부분이 추가적인 모듈라 연산을 위해서 추가된 부분이다. MPM은 다음 연산을 수행한다.

[알고리즘 3] MPM의 동작 알고리즘

입력: A, B

출력 : $P=AB^2 \bmod f(x)$

단계1 : for $i=m$ to 0

단계2 : Left_Shift(x, B_i), Right_Shift(z, A_i), $P_i = 0$

단계3 : if (i==0) $y_0 = x_0$, $y_1 = x_{m-2+1}$, $y_2 = x_1$,…, $y_{m-1} = x_m$, $y_m = x_{m/2}$

단계4 : for $i=m$ to 0

단계5 : for j=0 to m

단계6 : $P_i = P_i + y_{m-j} \times z_j$

단계7 : if (i==m) $z_{m+1} = P_i$

else $P_i = P_i + z_{m+1}$

단계8 : Circular_Right_Shift(z)

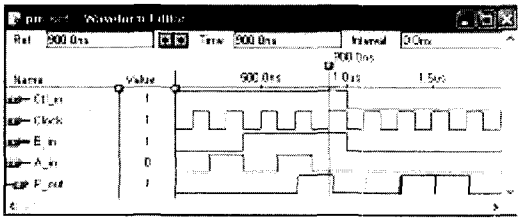
표 1 비트 순차 구조의 비교

구조 / 항목	Fenn et al. [15]		Kim et al. [13]	제안된 구조	
	AOPM	MAOPM		PM	MPM
연산	AB	AB	AB^2	AB^2	AB^2
기약다항식	AOP	AOP	Generalized	AOP	AOP
레지스터/래치	$2m$+2	$2m$+2	15m	$3m$+2	$3m$+3
AND	m+1	$2m$-1	4m	m+1	m+1
XOR	m	$2m$-2	4m	m	m+1
MUX	m+2	m+2	3m	m+2	m+3
Latency	$2m$+1	$2m$-1	3m-1	$2m$+1	$2m$+1
Critical path	1AND+ (log2m)XOR	1AND+ (log2m)XOR	1AND+2XOR	1AND+ (log2m)XOR	1AND+ (log2m)XOR

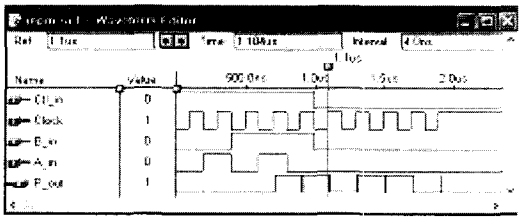
PM과의 가장 큰 차이점은 첫번째 연산의 결과 값을 바로 출력하지 않고, 그 값을 레지스터에 저장해 두고 두 번째 결과값부터는 첫번째 결과값을 이용하여 모듈라 감소 연산을 수행하는데 있다. 그렇게 함으로서 PM에서 요구되는 추가의 모듈라 감소 연산의 문제점을 해결하였다. MPM에서도 PM과 마찬가지로 곱셈기의 수행에 있어서 입력 상태와 처리 상태의 구별을 위해서 $2m+1$ 비트의 제어 신호가 필요하다.

4. 시뮬레이션 및 분석

본 장에서는 지금까지 제안된 구조의 시뮬레이션 결과를 제시하고, 제안한 구조와 기존의 구조를 비교 분석한다. 본 논문에서 제안한 구조의 검증을 위해서는 Altera 사의 MAX+PLUS를 이용하여 시뮬레이션 하였다. 그림 5는 PM과 MPM의 시뮬레이션 결과를 보여준다. 그림 5에서 확인할 수 있듯이 PM에서는 입력의 마지막 시점에 첫 번째 결과가 출력된다. 그러나 MPM에서는 계산의 두 번째 시점부터 AB^2연산의 결과를 출력한다



(a) PM 시뮬레이션 결과



(b) MPM 시뮬레이션 결과

그림 5 GE(2^4)상에서의 시뮬레이션 결과

기존의 연구에서 LFSR구조를 기반으로 하는 AB^2연산 구조는 없었다. 따라서 본 논문에서는 AB곱셈을 위한 Fenn et al. [15]의 LFSR구조와 AB^2연산을 위한 Kim et al. [13]의 시스톨릭 구조를 대상으로 비교 분석한다. 표 1은 본 논문에서 제안한 구조와 기존의 구조에 대한 비교를 자세히 보여준다.

Fenn et al.은 AOP를 이용한 LFSR 구조에 기반 한 AB연산을 수행하는 두 가지의 곱셈기를 제안하였다. Fenn et al.의 구조에서 AOPM은 확장된 필드상의 연산을 MAOPM은 원래의 필드상의 연산을 수행한다. Fenn et al.의 AOPM구조와 제안된 PM구조를 비교해 보면 PM은 단지 m 개의 레지스터 추가로 AB^2연산을 수행할 수 있다. 반면에 MAOPM과 MPM을 비교해보면 본 논문에서 제안한 MPM이 상당한 구조적 장점을 가짐을 확인할 수 있다. Kim et al.은 AB^2연산을 위한 비트 순차 시스톨릭 어레이 구조를 제시하였다. 두 구조를 비교하면 본 논문에서 제안한 구조가 구조적 복잡도 면에서 현저한 장점을 보임을 확인 할 수 있다. 그러나 시간 복잡도 측면을 살펴보면, 지연(Latency) 측면에서는 본 논문에서 제안한 구조가 Kim et al. 구조에 비해서 장점을 보이나 기본 셀의 임계경로(Critical path)를 살펴보면 시스톨릭 어레이 구조가 LFSR 구조에 비해서 더 효율적임을 확인 할 수 있다.

5. 결 론

본 논문에서는 GF(2^m)상에서 AB^2연산을 위한 두 가지 새로운 알고리즘과 구조를 제안하였다. 먼저 LFSR 구조기반의 새로운 AB^2연산 알고리즘과 비트 순차 AB^2 곱셈기(Power Multiplier, PM)를 설계하였다. PM구조는 확장된 필드상의 연산이므로 연산 후 추가적인 모듈라 감소 연산이 필요했다. 그러한 문제를 해결하기 위해서 PM 구조로부터 변형된 변형 AB^2 곱셈기(Modified Power Multiplier, MPM)를 제안하였다. 시뮬레이션 결과 제안된 구조가 구조복잡도면에서 기존의 구조들보다 훨씬 효율적임을 알 수 있었다. 제안된 곱셈기는 공개키 암호의 핵심이 되는 지수기의 구현을 위한 효율적인 기본구조로 사용될 수 있을 것이다.

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] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," *Comm. ACM*, vol. 21, pp. 120-126, 1978.
[8] A.J. Menezes, *Elliptic Curve Public Key Cryptosystems*, Boston, MA: Kluwer Academic Publishers, 1993.
[9] R. Lidl, H. Niederreiter, and P. M. Cohn, *Finite Fields (Encyclopedia of Mathematics and Its Applications)*, Cambridge University Press, 1997.
[10] D. E. Knuth, *The art of Computer Programing. Volume 2: Seminumerical Algorithms*, Addison-Wesley, Reading, Massachusetts, 2nd edition, 1997.
[11] C. L. Wang and Y. H. Guo," New Systolic for AB^2+C, Inversoin and Division in GF(2m)," *IEEE Trans. on Computres*, Vol.49, No.10, pp.1120-1125, Otc. 2000.
[12] S.-W. Wei, VLSI architectures for computing exponentiations, multiplications, multiplicative inverses, and divisions in $GF(2^m)$, *IEEE Trans. Circuit & Syst.-: Analog and Digital Signal Processing*, vol.44, no.10, pp.847-855, Oct. 1997.
[13] N. Y. Kim, H. S. Kim, and K. Y. Yoo, Efficient Systolic Architectures for AB^2 Multiplication in $GF(2^m)$, Will be published to LNCS, May 2002.
[14] T. Itoh and S. Tsujii, Structure of parallel multipliers for a class of fields $GF(2^m)$, *Info. Comp.*, vol. 83, pp. 21-40, 1989.
[15] S.T.J. Fenn, M.G. Parker, M. Benaissa, and D. Tayler, Bit-serial multiplication in $GF(2^m)$ using irreducible all-one opolynomial, *IEE Proc. Comput. Digit. Tech.*, vol. 144, no.6 pp. 391-393, 1997.
[16] C.H. Liu, N.F. Huang, and C.Y. Lee, Computation of AB^2 Multiplier in $GF(2^m)$ Using an Efficient Low-Complexity Cellular Architecture, *IEICE Trans. Fundamentals*, vol. E83-A, no.12, pp. 2657-2663, 2000.
[17] H.S. Kim, *Bit-Serial AOP Arithmetic Architecture for Modular Exponentiation*, Ph.D. Thesis, Kyungpook National University, 2002.

김 현 성
1996년 2월 : 경일대학교 컴퓨터공학과 공학사. 1998년 2월 : 경북대학교 컴퓨터공학과 공학석사. 2002년 2월 : 경북대학교 컴퓨터공학과 공학박사. 2002년 3월~현재 : 경일대학교 컴퓨터공학과 교수. 관심분야는 정보보호, 암호칩 설계, IDS, PKI

유 기 영
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. 관심분야는 정보보호, 암호학, 암호칩 설계, 스마트카드보안