AB^2 세미시스톨릭 곱셈기

이형목[0], 김현성, 전준철, 유기영
경북대학교 컴퓨터공학과
(hmh101[0], hskim, jcjeon33, yook)@purple.knu.ac.kr

AB^2 Semi-systolic Multiplier

Hyung-Mok Lee[0], Hyun-Sung Kim, Jun-Cheol Jeon, Kee-Young Yoo

Dept. of Computer Engineering at Kyungpook national university

요 약

본 논문은 유한 체 GF(2^m)상에서 AB^2 연산을 위해 AOP(All One Polynomial)에 기반한 새로운 MSB(Most Significant bit) 우선 알고리즘을 제시하고, 제시한 알고리즘에 기반하여 병렬 입출력 세미시스톨릭 구조를 제안한다. 제안된 구조는 표준기저(standard basis)에 기반하고 모듈라(modular) 연산을 위해 다항식의 계수가 모두 1인 m차의 기약다항식 AOP를 사용한다. 제안된 구조에서 AND와 XOR게이트의 딜레이(delay)를 각각 D_{AND2}와 D_{XOR2}라 하면 각 셀 당 임계경로는 $D_{AND2}+D_{XOR2}$이고 지연시간은 $m+1$이다. 제안된 구조는 기존의 구조보다 임계경로와 지연시간 면에서 보다 효율적이다. 또한 구조 자체가 정규성, 모듈성, 병렬성을 가지기 때문에 VLSI구현에 효율적이다. 더욱이 제안된 구조는 유한 체 상에서 지수 연산을 필요로 하는 Diffie-Hellman 키 교환 방식, 디지털 서명 알고리즘 및 ElGamal 암호화 방식과 같은 알고리즘을 위한 기본 구조로 사용될 수 있다. 이러한 알고리즘을 응용해서 타원 곡선(elliptic curve)에 기초한 암호화 시스템(Cryptosystem)의 구현에 사용될 수 있다.

1. 서 론

에러 교정 코드(Error-Correcting Codes)[1], 디지털 신호 처리(Digital Signal Processing)[2] 및 암호학(Cryptography) [3]의 응용에서 갈로아 체(Galois field, GF)[4]연산은 아주 중요하다. 이러한 유한 체 중에서 특별한 관심을 가지는 유한 체 GF(2^m)은 2^m개의 원소를 가진다. 그리고 이 원소들은 0과 1로 이루어진다. 유한 체 GF(2^m)은 0과 1로 이루어진 속성 때문에 컴퓨터 구조를 구현하기 위한 계산에 적당하다. 본 논문에서는 기저의 변환이 필요 없는 표준기저에 초점을 맞추었다.

1984년에 Yeh[5]는 일반적인 GF(2^m)상에서 $AB+C$의 연산을 수행하여 병렬 시스톨릭 어레이 구조를 구현하였다. 표준기저상에서 구현한 세미시스톨릭 어레이 구조가 논문 [6]에 제시되었다. 그리고 그 후에도 많은 비트 단위 병렬 시스톨릭 곱셈기들이 제안되었으나 시스템의 복잡도 때문에 이러한 곱셈기들은 암호화 시스템구성에 효과적이지 못했다. 이러한 시스템의 복잡도를 줄이기 위해서 Itoh와 Tsujii[7]가 GF(2^m)상에서 m차의 기약 AOP(All One Polynomial)에 기초한 곱셈기와 m차의 기약다항식 ESP(Equally Spaced Polynomial)에 기초한 곱셈기를 설계하였다. 이렇게 설계된 두개의 곱셈기는 작은 시스템 복잡도를 가졌다. 이 후에 Hasan[8]은 처리기로서 AOP에 기초한 작은 크기의 병렬 곱셈기를 제안하고, 이를 이용하여 ESP에 기초한 병렬 곱셈기로 발전시켰다. 또한, 타원 곡선(elliptic curve) 기반의 공개키 암호화시스템의 구현에 있어서 GF(p)나 GF(2^m)상에서 효율적인 지수 연산이 필요하다. 이러한 지수 연산을 효율적으로 계산하는 알고리즘을 Knuth[9]가 제안하였다. 지금까지의 연구에서 효율적인 구조들이 제안되었지만 보다 효율적인 구조 설계에 관한 연구가 필요하다.

본 논문은 유한 체 GF(2^m) 상에서 AB^2 연산을 위해서 AOP에 기반한 새로운 MSB(Most Significant bit)우선 알고리즘을 제시하고, 제시한 알고리즘에 기반하여 병렬 입출력 세미시스톨릭 곱셈기를 제안한다. 제안된 구조는 표준기저에 기반하고 모듈라(modular) 연산을 위해 다항식의 계수가 모두 1인 m차의 기약다항식 AOP의 성질을 사용한다. 제안된 구조에서 2-입력 AND와 XOR게이트의 딜레이(delay)를 D_{AND2}와 D_{XOR2}라 하면 각 셀 당 임계경로는 $D_{AND2}+D_{XOR2}$이고 지연시간은 $m+1$이다. 제안된 구조는 기존의 구조보다 임계경로와 지연시간 면에서 보다 효율적이다. 또한 구조 자체가 정규성, 모듈성, 병렬성을 가지기 때문에 VLSI구현에 효율적이다.

2. AOP에 기반한 곱셈 알고리즘

유한 체 GF(2^m)은 GF(2)상에서 m차의 기약다항식에 의해 생성된 유한 확대 체이다. 유한 체 GF(2^m)에서 0이 아닌 모든 원소들은 세 가지 기저에 의해서 표현된다. 즉, 표준, 정규 및 이원기저에 의해서 표현된다. 정규와 이원기저는 기저의 변환을 필요로 한다. 그러나 표준기저는 기저의 변환이 필요 없다. 그러므로 본 논문에서는 유한 체 GF(2^m)상에서 모듈라 연산을 위해 표준기저에 초점을 맞추었다. 유한 체 GF(2^m)상에서 만약 다항식 $f(x)=f_mx^m+f_{m-1}x^{m-1}+\cdots+f_1x+f_0$의 근이 상수 다항식이거나 자기 자신이면 이 다항식 $f(x)$를 기약다항식이라고 한다. 또한, 유한 체 GF(2^m)상에서 만약 다항식 $f(x)=f_mx^m+f_{m-1}x^{m-1}+\cdots+f_1x+f_0$의 계수 f_i ($0\le i\le n$)가 모두 1이면 이 다항식 $f(x)$를 AOP(All One Polynomial)이라고 한다. 다항식 AOP에서 $m+1$이 소수이고 2가 모듈라 $m+1$에 대해서 원시 근이 되면 이 AOP는 기약 다항식이 된다. 다항식 AOP는 모듈라 감소 연산을 위해서 매우 특별한 성질을 가진다. 그러므로, 본 논문에서는 지금부터 AOP의 성질을 모듈라 감소 연산을 위해서 사용한다. 모듈라 다항식으로 AOP의 성질을

사용하기 위해서는 기저의 확장이 요구된다. 그래서 본 논 문은 표준기저에서 확장된 기저를 사용한다. 다항식 $F(x)=x^m+x^{m-1}+\cdots+x+1$를 m차의 기약 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 만족하고 $\alpha^m=\alpha^{m-1}+\cdots+\alpha+1$로 나타낼 수 있고 양변에 α를 곱하고 정리하면 다음 방정식을 만족한다.

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

이제 AOP의 속성이 적용된 $P=\alpha^{m+1}$를 모듈라로 사용해서 GF(2^m)상의 확대 체 상에서의 원소 A 와 B^2의 곱 즉, $AB^2 \bmod P$ 연산을 수행한다. 이렇게 곱셈한 연산의 결과 역시 확대 체 상의 원소가 된다. 이 곱셈 $AB^2 \bmod P$연산의 결과를 $R=r_m\alpha^m+r_{m-1}\alpha^{m-1}+\cdots+r_1\alpha+r_0$라 할 때, 기약다항식 AOP의 성질을 이용해서 본 논문에서 제안한 AB^2를 계산하는 새로운 MSB알고리즘은 다음과 같다.

$$\begin{aligned} R &= AB^2 \bmod P \\ &= A(b_m\alpha^m+b_{m-1}\alpha^{m-1}+\cdots+b_1\alpha+b_0)^2 \bmod P \\ &= A(b_m\alpha^{2m}+b_{m-1}\alpha^{2m-2}+\cdots+b_1\alpha^2+b_0) \bmod P \\ &= (Ab_m\alpha^{2m}+Ab_{m-1}\alpha^{2m-2}+\cdots+Ab_1\alpha^2+Ab_0) \bmod P \\ &= r_m\alpha^m+r_{m-1}\alpha^{m-1}+\cdots+r_1\alpha+r_0 \end{aligned} \quad (2)$$

위의 식 (2)에서 $AB^2 \bmod P$ 연산은 곱셈 연산과 모듈라 감소 연산으로 이루어진다. 곱셈은 일반 정수 상에서의 곱셈 연산과 동일하고, 모듈라 감소 연산은 2-비트 순환 시프트(2-bit circular shift) 연산에 의해 수행될 수 있다. 또한, 식 (2)에서 각각의 중간 결과 값 R_i는 다음과 같이 계산된다.

$$\begin{aligned} R_0 &= Ab_m\alpha^{2m} \\ &= \sum_{k=0}^{m} (a_kb_m\alpha^k)\,\alpha^{2m} \\ &= \sum_{k=0}^{m} (C^0_k\,\alpha^k)\,\alpha^{2m} \\ &= \sum_{k=0}^{m} [C^0_k\,\alpha^k\alpha^2]\,\alpha^{2m-2} \\ &= [(C^0_m\,\alpha^{m+2}+C^0_{m-1}\,\alpha^{m+1}+\cdots+C^0_1\,\alpha^3+C^0_0\,\alpha^2)]\alpha^{2m-2} \\ &= [C^0_{m-2}\,\alpha^m+C^0_{m-3}\,\alpha^{m-1}+\cdots+C^0_1\,\alpha^3+C^0_0\,\alpha^2+C^0_m\,\alpha \\ &\quad +C^0_{m-1}]\alpha^{2m-2} \\ &\quad , C^0_k=a_kb_m \quad k=0,1,\cdots,m \end{aligned}$$

$$\begin{aligned} R_1 &= [C^1_{m-4}\,\alpha^m+C^1_{m-5}\,\alpha^{m-1}+\cdots+C^1_{m-1}\,\alpha^2+C^1_{m-2}\,\alpha+C^1_{m-3}]\,\alpha^{2m-4} \\ &\quad , C^1_k=a_kb_{m-1} \quad k=0,1,\cdots,m \end{aligned}$$

$$\begin{aligned} R_i &= [C^i_{m-2i}\,\alpha^m+C^i_{m-2i-1}\,\alpha^{m-1}+\cdots+C^i_{m-2i-2}\,\alpha+C^i_{m-2i-1}]\,\alpha^{2m-2i} \\ &\quad , C^i_k=a_kb_{m-i} \quad k=0,1,\cdots,m \end{aligned}$$

$$\begin{aligned} R_m &= [C^m_m\,\alpha^m+C^m_{m-1}\,\alpha^{m-1}+\cdots+C^m_1\,\alpha+C^m_0] \\ &\quad , C^m_k=a_kb_0 \quad k=0,1,\cdots,m \end{aligned}$$

식 (2)를 기반으로 하여 중간 결과 값 R_i를 계산하는 식을 정규 방정식으로 나타내면 다음과 같다.

$$\begin{aligned} R_i &= [C^i_{m-2i}\,\alpha^m+C^i_{m-2i-1}\,\alpha^{m-1}+\cdots+C^i_{m-2i-2}\,\alpha+C^i_{m-2i-1}]\,\alpha^{2m-2i} \\ &\quad , C^i_k=a_kb_{m-i} \; k=0,1,\cdots,m \end{aligned} \quad (3)$$

위의 정규 방정식의 연산 처리는 중간 결과 값을 구하고, 구한 결과 값에서 α의 계수를 2-비트 순환 시프트 함으로써 다음 결과 값을 얻는다. 즉, 모듈라 감소 연산을 수행한다. 이러한 특성은 기약다항식으로 AOP의 특성을 사용했기 때문에 가능하다. 일반 기약다항식을 사용해서 모듈라 감소 연산을 하는 것은 본 논문에서 제안한 방법 보다 아주 큰 연산 복잡도를 가진다.

다음 장에서는 정규방정식 (3)에 기반한 곱셈기를 제안한다.

3. 제안된 병렬 입출력 세미시스톨릭 곱셈기

유한 체 GF(2^4)의 원소 A, B, 및 B^2는 확장된 기저상에서 각각

$$\begin{aligned} A &= a_4\alpha^4+a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0 \\ B &= b_4\alpha^4+b_3\alpha^3+b_2\alpha^2+b_1\alpha+b_0 \\ B^2 &= b_4\alpha^8+b_3\alpha^6+b_2\alpha^4+b_1\alpha^2+b_0 \end{aligned}$$

로 표현된다. 유한 체 GF(2^4)상의 원소 A와 B^2의 확장된 기저 상에서의 곱, $AB^2 \bmod \alpha^5+1$ 연산은 식 (2)에 의해 다음과 같이 계산된다.

$$\begin{aligned} R &= AB^2 \bmod \alpha^5+1 \\ &= A(b_4\alpha^4+b_3\alpha^3+b_2\alpha^2+b_1\alpha+b_0)^2 \bmod \alpha^5+1 \\ &= A(b_4\alpha^8+b_3\alpha^6+b_2\alpha^4+b_1\alpha^2+b_0) \bmod \alpha^5+1 \\ &= r_4\alpha^4+r_3\alpha^3+r_2\alpha^2+r_1\alpha+r_0 \end{aligned} \quad (4)$$

각각의 중간 결과값 계수 R_i는 정규방정식 (3)에 의해서 다음과 같이 계산된다.

$$\begin{aligned} R_0 &= C^0_2\,\alpha^4+C^0_3\,\alpha^3+C^0_4\,\alpha^2+C^0_0\,\alpha+C^0_1 \\ R_1 &= C^1_4\,\alpha^4+C^1_0\,\alpha^3+C^1_1\,\alpha^2+C^1_2\,\alpha+C^1_3 \\ R_2 &= C^2_1\,\alpha^4+C^2_2\,\alpha^3+C^2_3\,\alpha^2+C^2_4\,\alpha+C^2_0 \\ R_3 &= C^3_3\,\alpha^4+C^3_4\,\alpha^3+C^3_0\,\alpha^2+C^3_1\,\alpha+C^3_2 \\ R_4 &= C^4_0\,\alpha^4+C^4_1\,\alpha^3+C^4_2\,\alpha^2+C^4_3\,\alpha+C^4_4 \end{aligned} \quad (5)$$

정규방정식 (3)에 기반하여 C^i_k 에 관해 계산한 결과를 A, B의 계수 a_j, $b_i(0\le i,j\le m)$로 표현하면 다음과 같이 나타낼 수 있다.

$$\begin{aligned} R_0 &= a_2b_4\alpha^4+a_3b_4\alpha^3+a_4b_4\alpha^2+a_0b_4\alpha+a_1b_4 \\ R_1 &= a_4b_3\alpha^4+a_0b_3\alpha^3+a_1b_3\alpha^2+a_2b_3\alpha+a_3b_3 \\ R_2 &= a_1b_2\alpha^4+a_2b_2\alpha^3+a_3b_2\alpha^2+a_4b_2\alpha+a_0b_2 \\ R_3 &= a_3b_1\alpha^4+a_4b_1\alpha^3+a_0b_1\alpha^2+a_1b_1\alpha+a_2b_1 \\ R_4 &= a_0b_0\alpha^4+a_1b_0\alpha^3+a_2b_0\alpha^2+a_3b_0\alpha+a_4b_0 \end{aligned} \quad (6)$$

식 (5-6)은 $AB^2 \bmod \alpha^5+1$ 연산의 중간 계산 값을 나타낸다. 방정식 (3)에 기초해서, 그림 1은 유한 체 GF(2^4)상의 병렬 입출력 세미시스톨릭 구조를 보여준다. 제안된 구조는 $(m+1)^2$개의 기본 셀을 갖는 병렬 입출력 구조이다. 또한, 제안된 구조는 a_j값과 b_i 값($0\le i,j\le m$)이 동시에 입력되는 배열 구조이다. 그리고, 첫 번째 행의 마지막 셀에 입력되는 값은 0으로 초기화 한다. a_j값들은 같은 열(column)에 있는 인접 셀들간에 전송되지만 b_i값들은 한 번에 같은 행(row)에 있는 모든 셀에 전송(broadcasting)되는 세미시스톨릭 어레이 속성을 갖는다[6]. 결국 $AB^2 \bmod \alpha^5+1$ 연산은 식 (6)의 결과에서 같은 차수의 α의 계수의 합을 구함으로써 수행된다. 또한, 한 행에 있는 모든 열들 간에는 의존성 (dependency)이 없으므로 같은 행에 있는 각각의 셀들은 병렬로 수행될 수 있다. 제안한 구조의 분석을 위해서 2-입력 AND와 XOR 게이트(gate)의 딜레이(delay)를 각각 D_{AND2}와 D_{XOR2}라 하면 각 셀 당

임계경로는 $D_{AND2}+D_{XOR2}$이고 지연시간은 $m+1$이다. 그리고 전체 게이트 수는 각각 $(m+1)^2$개의 AND와 XOR 게이트를 갖는다. 그림 1로부터 GF(2^m)상에서 제안된 구조를 m=4에서 뿐만 아니라, 모든 m에 대해서도 확장 시킬 수 있다.

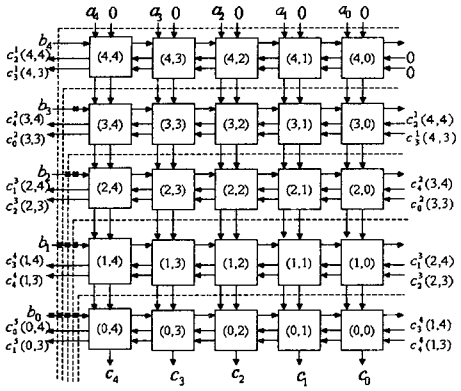

그림 1. GF(2^4)상의 병렬 입출력 세미시스톨릭 구조

그림 2는 제안된 구조의 기본 셀을 보여준다. 제안된 구조의 기본 셀을 하나의 AND와 XOR로 이루어지는 효율적인 구조이다.

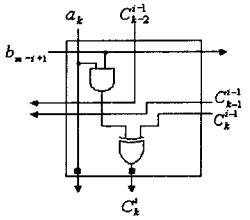

그림 2. 제안된 구조의 기본 구조

4. 비교 및 분석

본 논문에서는 AB^2 연산을 위한 병렬 입출력 세미시스톨릭 구조를 유한 체 GF(2^m)에서 제안하였다. 역원/나눗셈을 위한 병렬 입출력 세미시스톨릭 구조와 시스톨릭 파워 썸(power-sum)구조가 논문 [6]과 [10]에 제안되었다. 표1은 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. 먼저 논문 [6]에서 AND와 XOR게이트는 각 2-입력이고 임계경로는 $D_{AND2}+D_{XOR2}$이고 지연시간은 $m+1$ 이다. 그리고 논문 [10]에서는 AND게이트는 2-입력이고 XOR게이트는 4-입력이다. 그리고 지연시간은 $2m+m/2$이고 임계경로는 $D_{AND2}+D_{XOR4}$이다. 본 논문에서 제안된 구조는 AND와 XOR게이트는 각각 2-입력이다. 제안된 구조의 임계경로는 $D_{AND2}+D_{XOR2}$이고 지연시간은 $m+1$이다. 결국 본 논문에서 제안된 구조가 논문 [6]과 비교할 때, AB^2를 계산하는 본 구조와 지연시간과 임계경로 면에서는 같고 셀 복잡도 면에서는 본 구조가 향상됨을 확인 할 수 있다. 그리고 논문 [10]과 비교하면, 셀 복잡도 및 지연시간과 임계경로 면에서 아주 효율적이었다. 따라서 본 구조가 더 효율적임을 알 수 있다. 제안된 구조는 Altera MAX Plus II 시뮬레이션 툴을 이용하여 시뮬레이션 되었다.

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

표1. 구조의 성능 비교

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

5. 결 론

본 논문에서는 GF(2^m) 상의 AB^2를 계산하는 새로운 MSB알고리즘과 병렬 입출력 세미시스톨릭 곱셈기를 제안하였다. 일반 기약다항식을 사용하는 것 보다 기약다항식으로 AOP의 속성을 사용함으로써 제안된 구조는 전체 지연시간으로는 $m+1$을 가졌고 각 셀 당 $D_{AND2}+D_{XOR2}$의 임계경로를 가졌다. 그러므로 본 논문에서 제안된 구조는 기존의 구조보다 지연시간과 임계경로 면에서 보다 효율적이다. 이 구조는 일반 기약다항식을 사용할 때 보다 구조가 더 간단해지고 시스템의 복잡도를 줄일 수 있는 장점을 제공한다. 따라서 제안된 구조를 기반으로 하여 보다 효율적이고 안전한 공개키 암호화시스템을 구현할 수 있다.

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] E.R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill,1986.

[5] 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.

[6] S. K. Jain and L. Song, "Efficient Semisystolic Architectures for finite field Arithmetic," *IEEE Trans. on VLSI Systems*, vol.6, no.1, Mar. 1998.

[7] T. Itoh and S. Tsujii, "Structure of parallel multipliers for a class of finite fields GF(2^m)," *Info. Comp.*, vol.83, pp.21-40, 1989.

[8] M. A. Hasan, M. Z. Wang and V. K. Bhargava, "Modular Construction of low complexity parallel multipliers for a class of finite fields GF(2^m)," *IEEE Trans. On Computers.*, vol.8, pp.962-971, Aug. 1992.

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

[10] 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.