情報保護學會論文誌
第16卷 第4號, 2006. 8

타입 II 최적 정규기저를 갖는 유한체의 새로운 병렬곱셈 연산기*

김 창 한,[1†] 지 성 연,[2‡] 장 상 운,[3] 임 종 인[2]
[1]세명대학교 정보통신학부, [2]고려대학교 정보보호대학원, [3]국가기술보안연구소

A New Parallel Multiplier for Type II Optimal Normal Basis*

Chang Han Kim,[1†] Sung Yeon Ji,[2‡] Sang-Woon Jang[3], Jongin Lim[2]
[1]Information & Communication Systems, Semyung University,
[2]Graduate School of Information Security(GSIS), Korea University,
[3]National Security Research Institute

요 약

유한체의 H/W 구현에는 정규기저를 사용하는 것이 효과적이며, 특히 최적 정규기저를 갖는 유한체의 H/W 구현이 가장 효율적이다. 타입 I 최적 정규기저를 갖는 유한체 $GF(2^m)$은 m이 짝수이므로 암호학적으로 응용되지 못하는 단점이 있다. 그러나 타입 II 최적 정규기저를 갖는 유한체의 경우는 NIST에서 제안한 ECDSA의 권장 커브 중 $GF(2^{233})$위에 주어진 것이 있으며, 이 유한체가 타입 II 최적 정규기저를 갖는 등 여러 응용분야에 적용 되는바 효율적인 구현에 관한 연구가 활발하게 진행되고 있다. 본 논문에서는 타입 II 최적 정규기저를 갖는 유한체 $GF(2^m)$의 연산을 정규기저로 표현하여 확대체 $GF(2^{2m})$의 원소로 나타내어 연산을 하는 새로운 병렬곱셈 연산기를 제안하였으며, 제안한 연산기는 기존의 가장 효율적인 결과들과 동일한 공간 및 시간 복잡도를 갖는 효율적인 연산기이다.

ABSTRACT

In H/W implementation for the finite field, the use of normal basis has several advantages, especially, the optimal normal basis is the most efficient to H/W implementation in $GF(2^m)$. In this paper, we propose a new, simpler, parallel multiplier over $GF(2^m)$ having a type II optimal normal basis, which performs multiplication over $GF(2^m)$ in the extension field $GF(2^{2m})$. The time and area complexity of the proposed multiplier is same as the best of known type II optimal normal basis parallel multiplier.

Keywords : *유한체 연산, 병렬곱셈 연산기, 타입 II 최적 정규기저*

I. 서 론

유한체는 암호학과 코딩이론 등에 응용되고 있으며, 특히 최근 들어 공개키 암호인 타원곡선암호(ECC), XTR, ElGamal 타입 암호 등의 관련 응용 분야에 활발하게 사용되고 있는 관계로 유한체의 효율적인 연산 방법이 많은 관심의 대상이 되고 있다[1,2]. 유한체의 연산은 표현방법에 따라 달라지는데, 대표적으로 다항식기저[3,4], 정규기저[5-7] 등을 이용한 것이고 또 Noncomvention기저[8]를 이용한 것

접수일: 2006년 5월 3일; 채택일: 2006년 7월 5일
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 육성·지원사업의 연구결과로 수행되었음.
† 주저자, chkim@semyung.ac.kr
‡ 교신저자, jisy0522@cist.korea.ac.kr

도 사용된다. 특히, H/W 구현에는 정규기저를 이용할 경우 제곱이 Cyclic Shift에 의하여 이루어지는 등 많은 장점을 가지고 있다. 그 중에서도 최적 정규기저를 갖는 유한체가 가장 효율적으로 구현된다[5,7]. 최적 정규기저를 갖는 유한체는 2 가지 유형, 즉 타입 I과 타입 II가 있다[2]. 이 중 타입 I을 갖는 유한체 $GF(2^m)$은 m이 짝수인 관계로 효율성은 좋으나 암호학 분야를 비롯한 다양한 분야에 응용 되지 못하는 단점을 가지고 있다[9-11]. 그러나 타입 II 의 경우에는 NIST에서 ECDSA[11]의 권장 커브가 주어진 유한체 중 $GF(2^{233})$이 타입 II의 최적 정규기저를 갖는 등 응용분야에 다양하게 활용되므로 많은 연구가 이루어지고 있다. 특히 최근 2001년에 B. Sunar와 C.K. Koc[5]이 기존의 결과를 대폭 개선한 결과를 발표하였으며 2002년에는 M. Elia와 M. Leone[12] 그리고 A.Reyhani-Masoleh와 M.A. Hasan[7]이 Sunar등의 결과와 같은 곱셈기를 제안하였다. 본 논문에서는 타입 II 최적 정규기저를 갖는 유한체 $GF(2^m)$의 원소를 정규기저를 사용하여 표현할 경우 자연스럽게 $GF(2^m)$의 확대체인 $GF(2^{2m})$의 원소로 표시하여 곱셈을 수행하는 새로운 연산기를 제안하였으며, 제안하는 연산기는 기존의 가장 우수한 연산기와 같은 시간 및 공간 복잡도를 갖는 효율적인 병렬곱셈 연산기이다.

본 논문은 II장에서 수학적 배경을 설명 하였으며 III장에서 새로운 병렬곱셈 연산기를 제안하였고 IV장에서 제안된 연산기의 효율성과 기존의 결과와의 비교표를 제시하였으며 V장에서 결론을 제시한 형태로 구성 하였다.

II. 수학적 배경

1. 유한체의 정규기저를 이용한 표현과 곱셈

양의 정수 m에 대하여 유한체 $GF(2)$위에서 $GF(2^m)$의 정규기저가 존재한다는 것은 잘 알려진 결과이다[2][13]. 즉, $GF(2^m)$의 원소 β가 존재하여 $N=\{\beta,\beta^2,\cdots,\beta^{2^{m-1}}\}$이 $GF(2)$위에서 $GF(2^m)$의 기저 일 때 N을 정규기저라 하고, β를 정규기저 생성자라 한다. 이 경우, $A\in GF(2^m)$에 대하여

$$A=\sum_{i=0}^{m-1} a_i\beta^{2^i},\ a_i\in GF(2)$$

로 표현되며, 간단히 $A=(a_0,a_1,\cdots,a_{m-1})$과 같이 좌표로도 표현한다. 또한 벡터(행렬)표현으로 행렬의 치환(T : Transpose)을 사용하여 다음과 같이 표현 된다.

$$A=\bar{a}\times\bar{b}^T=\bar{b}\times\bar{a}^T,\ \bar{a}=[a_0 a_1 \cdots a_{m-1}],$$
$$\bar{b}=[b_0 b_1 \cdots b_{m-1}].$$

그리고 정규기저의 특징이자 장점은 A^2이 Right Cyclic Shift(RCS)에 의하여 주어진다는 것이다. 즉, $GF(2^m)$의 임의의 원소 $A=(a_0,a_1,\cdots,a_{m-1})$의 제곱은

$$A^2=(a_{m-1},a_0,\cdots,a_{m-2})$$

와 같이 표현된다. $A,B\in GF(2^m)$이고 $C=AB$ 라 하면, 다음과 같이 표현 할 수 있다.

$$C=(\bar{a}\times\bar{\beta}^T)(\bar{\beta}\times\bar{b}^T)=\bar{a}M\bar{b}.$$
$$M=\bar{\beta}^T\bar{\beta}=(\beta^{2^i+2^j}),0\le i,j\le m-1.$$

$\beta^{2^i+2^j}$를 기저 N을 사용하여 곱의 행렬 M을 다시 표현하면 다음과 같다.

$$M=M_0\beta+M_1\beta^2+\cdots+M_{m-1}\beta^{2^{m-1}}$$
$$M_i=Mat_{m\times m}(GF(2)).$$

A^2이 cyclic shift인 것을 이용하면 $C=AB=(c_0,c_1,\cdots,c_{m-1})$의 값은 다음과 같다.

$$c_i=\bar{a}M_i\bar{b}^T=\overline{a^{(i)}}M_0\overline{b^{(i)}},$$
$$\overline{a^{(i)}}=[a_i\ a_{i+1}\cdots a_{i-1}],$$
$$\overline{b^{(i)}}=[b_i\ b_{i+1}\cdots b_{i-1}].$$

이 같은 결과에 의하여 각 i에 대하여 행렬 M_i의 1의 개수는 모두 같음을 알 수 있고, 이때 M_0의 1의 개수를 정규기저 N의 복잡도라 하고 C_N으로 표시한다. 또한 Gao 등은 다음과 같은 결과를 증명하였다[2,13].

정리 1. $C_N\ge 2m-1$[2].

2. 타입 II 최적 정규기저

정리 1에서 $C_N=2m-1$일 때 정규기저 N을 최

적정규기저(Optimal Normal Basis, ONB)라 한다. 그리고 $GF(2)$위에서 최적 정규기저는 다음과 같이 타입 I, 타입 II 인 경우만 존재한다는 것은 잘 알려진 사실이다. 모든 계수가 1인 다항식을 All One Polynomial(AOP : $x^m+x^{m-1}+\cdots+x+1$) 이라 한다.

정리 2. (타입 I 최적 정규기저) $GF(2)$위에서 $GF(2^m)$이 타입 I의 최적 정규기저를 갖기 위한 필요충분조건은 $m+1$이 소수이고 $GF(m+1)^*=<2>$이다. 또는 m차의 AOP $x^m+x^{m-1}+\cdots+x+1$가 $GF(2)$위에서 기약다항식인 경우 AOP의 근이 최적 정규기저의 생성자 이다[2][13].

정리 3. (타입 II의 최적 정규기저) $2m+1$은 소수이고, $GF(2m+1)^*=<2>$이다. 또는 $2m+1 \equiv 3 \bmod 4$을 만족하고 $GF(2m+1)^*=<-1,2>$이면 $\beta=\gamma+\gamma^{-1}$는 $GF(2)$위에서 $GF(2^m)$의 최적 정규기저 생성자이다. 여기서 γ는 $GF(2^{2m})$에서 $2m+1$의 원시근이다[2,13].

본 논문에서는 m을 $GF(2^m)$이 타입 II의 최적 정규기저를 갖는 경우로 제한한다. 이러한 경우 γ 는 $GF(2^{2m})$의 원소라는 것과

$$\begin{aligned} N &= \{\beta,\beta^2,\cdots,\beta^{2^{m-1}}\} \\ &= \{\gamma+\gamma^{-1},\gamma^2+\gamma^{-2},\cdots,\gamma^m+\gamma^{-m}\} \end{aligned} \qquad (*)$$

인 것은 잘 알려진 사실이다[2]. $A\in GF(2^m)$인 경우 A를 확대체 $GF(2^{2m})$에서 표현하면 다음과 같다. $\beta=\gamma+\gamma^{-1}$는 $GF(2)$ 위에서 $GF(2^m)$ 의 정규기저 생성자이다. 따라서 원소 $A\in GF(2^m)$는 (*) 에 의하여

$$\begin{aligned} A &= a_0\beta+a_1\beta^2+a_2\beta^{2^2}+\cdots+a_{m-1}\beta^{2^{m-1}} \\ &= A_0(\gamma+\gamma^{-1})+A_1(\gamma^2+\gamma^{-2})+\cdots \\ &\quad +A_{m-1}(\gamma^m+\gamma^{-m}) \end{aligned}$$

와 같이 표현된다. 여기서 A_i는 a_j의 재배열에 의하여 얻어진다. 그러므로 A_i를 구하기 위하여 a_j의 재배열을 하면 $A\in GF(2^m)$는 확대체 $GF(2^{2m})$의 원소로 다음과 같이 표현 된다.

$$\begin{aligned} A = {} & A_0\gamma+A_1\gamma^2+A_2\gamma^3+\cdots+A_{m-1}\gamma^m \\ & +A_{m-1}\gamma^{m+1}+A_{m-2}\gamma^{m+2}+\cdots+a_0\gamma^{2m}, \\ & A_j\in GF(2^2). \end{aligned}$$

참고 1. $\gamma,\gamma^2,\cdots,\gamma^{2m}$은 일반적으로 유한체 $GF(2)$위에서 확장체 $GF(2^m)$의 기저가 되지 않는다. $GF(2m+1)^*=<2>$인 경우만 기저가 된다.

정리 4. $A,B\in GF(2^m)$인 경우에 A,B를 확대체 $GF(2^{2m})$의 원소로 표현하여 $C=AB$를 계산할 경우 $\gamma,\gamma^2,\cdots,\gamma^m$의 계수만 구하면 된다.

증명. $GF(2^{2m})$ 의 원소 X 가

$$\begin{aligned} X = {} & X_0\gamma+X_1\gamma^2+X_2\gamma^3+\cdots+X_{m-1}\gamma^m \\ & X_{m-1}\gamma^{m+1}+X_{m-2}\gamma^{m+2}+\cdots+X_0\gamma^{2m} \end{aligned}$$

와 같이 표현되면 X는 $GF(2^m)$에서 다음과 같이 표현된다. 즉, (*)에 의하여 계수를 조정하면

$$\begin{aligned} X &= X_0(\gamma+\gamma^{-1})+X_1(\gamma^2+\gamma^{-2})+\cdots \\ &\quad +X_{m-1}(\gamma^m+\gamma^{-m}) \\ &= X_0'\beta+X_1'\beta^2+\cdots+X_{m-1}'\beta^{2^{m-1}} \end{aligned}$$

한편 A,B는 $GF(2^m)$의 원소 이므로 $GF(2^{2m})$의 원소로 표현하면

$$\begin{aligned} A = {} & A_0\gamma+A_1\gamma^2+A_2\gamma^3+\cdots+A_{m-1}\gamma^m \\ & +A_{m-1}\gamma^{m+1}+A_{m-2}\gamma^{m+2}+\cdots+A_0\gamma^{2m} \\ B = {} & B_0\gamma+B_1\gamma^2+B_2\gamma^3+\cdots+B_{m-1}\gamma^m \\ & +B_{m-1}\gamma^{m+1}+B_{m-2}\gamma^{m+2}+\cdots+B_0\gamma^{2m} \end{aligned} \qquad (**)$$

이다.

$\gamma^{2m+1}=1$를 이용하면

$$\begin{aligned} & B_{j-1}\gamma^jA+B_{j-1}\gamma^{2m-j+1} \\ = {} & B_{j-1}(A_{j-2}\gamma+\cdots+A_0\gamma^{j-1}+0 \\ & +A_0+\gamma^{j+1}+\cdots+A_{m-1}\gamma^{m+j} \\ & +A_{m-1}\gamma^{m+j+1}+\cdots+A_j\gamma^{2m}) \\ & +B_{j-1}A_{j-1}+B_{j-1}(A_j\gamma+\cdots \\ & +A_{m-1}\gamma^{m-j}+A_{m-1}\gamma^{m-j+1}) \\ & +\cdots+A_0\gamma^{2m-j}+0+A_0\gamma^{2m-j+2} \\ & +\cdots+A_{j-2}\gamma^{2m})+B_{j-1}A_{j-1} \end{aligned}$$

$$\begin{aligned} &= B_{j-1}((A_{j-2}+A_j)\gamma+\cdots \\ &\quad +(A_0+A_{2j-2})\gamma^{j-1}+A_{2j-1}\gamma^j \\ &\quad +(A_0+A_{2j})\gamma^{j+1}+\cdots \\ &\quad +(A_{m-j-1}+A_{m-j})\gamma^m \\ &\quad +(A_{m-j}+A_{m-j-1})\gamma^{m+1} \\ &\quad +\cdots+(A_0+A_{2j+1})\gamma^{2m-j} \\ &\quad +A_{2j-1}\gamma^{2m-j+1} \\ &\quad +(A_0+A_{2j-2})\gamma^{2m-j+2} \\ &\quad +\cdots+(A_j+A_{j-2})\gamma^{2m}) \end{aligned} \quad (***)$$

즉, γ^m 과 γ^{m+1}을 중심으로 좌우 대칭인 계수를 가지므로 $GF(2^m)$의 원소 $\gamma, \gamma^2, \cdots, \gamma^m$의 계수만 구하면 된다. □

본 논문에서 $A \in GF(2^m)$를 $GF(2^{2m})$의 원소로 표현할 경우 다음과 같이 벡터 형태로 표현하도록 한다.

$$\begin{aligned} A = &\ A_0\gamma+A_1\gamma^2+A_2\gamma^3+\cdots+A_{m-1}\gamma^m \\ &+A_{m-1}\gamma^{m+1}+A_{m-2}\gamma^{m+2}+\cdots+A_0\gamma^{2m} \\ \equiv &\ (A_0,\cdots,A_{m-1},A_{m-1},\cdots,A_0) \end{aligned}$$

그리고 필요한 경우 앞의 m개의 벡터로 표현하고,

$$\overline{A} \equiv A = (A_0, A_1, \cdots, A_{m-1})$$

로 나타내도록 한다.

예 1. $m=5$ 이고 $j=2$ 인 경우

$$\begin{aligned} &B_1\gamma^2 A + B_1\gamma^9 A \\ &= B_1(A_0+A_2, A_3, A_0+A_4, A_1+A_4, A_2+A_3, \\ &\qquad A_2+A_3, A_1+A_4, A_0+A_4, A_3, A_0+A_2) \end{aligned}$$

이다.

III. 타입 II 최적 정규기저를 갖는 병렬곱셈 곱셈기

III장 에서는 타입 II 최적 정규기저를 갖는 유한체 $GF(2^m)$의 원소를 확대체 $GF(2^{2m})$의 원소로 표시하여 곱셈하는 연산기에 대하여 설명하도록 한다.

정리 5. $A, B \in GF(2^m)$이고 $C=AB$를 구하기 위하여

$$\overline{A} = (A_0, A_1, \cdots, A_{m-1}),$$
$$\overline{B} = (B_0, B_1, \cdots, B_{m-1}),$$
$$\overline{C} = (C_0, C_1, \cdots, C_{m-1})$$라 하면

$$\overline{C} = \sum_{j=1}^{m} B_{j-1} A[j],$$

$$\begin{aligned} A[1] = &\ (A_1, A_0+A_2, \cdots, \\ &\ A_{m-3}+A_{m-1}, A_{m-2}+A_{m-1}), \\ A[j] = &\ (A_{j-2}+A_j, \cdots, A_0+A_{2j-2}, \\ &\ A_{2j-1}, A_0+A_{2j}, \cdots, A_{m-j-2}+A_{m-j}, \\ &\ A_{m-j-1}+A_{m-j}), \\ &\ \text{if} \quad 1<j \quad \text{and} \quad 2j \le m \\ A[j] = &\ (A_{j-2}+A_j, \cdots, A_{2j-m-1}+A_{m-1}, \\ &\ A_{2j-m-2}+A_{m-1}, \cdots, A_0+A_{2m-2j+1}, \\ &\ A_{2m-2j}, \cdots, A_{m-j-1}+A_{m-j}), \\ &\ \text{if} \quad 2j>m. \end{aligned}$$

단, 모든 index는 modular m에 관한 값이다.

증명. A, B를 (**)와 같이 표현하여 (***)와 같이 계산하면

$$\begin{aligned} \overline{C} = \overline{A}\overline{B} &= \sum_{j=1}^{m} B_{j-1}(\overline{A}\gamma^j+\overline{A}\gamma^{2m-j+1}) \\ &= \sum_{j=1}^{m} B_{j-1}((A_{j-2}+A_j)\gamma+\cdots+(A_0 \\ &\quad +A_{2j-2})\gamma^{j-1}+A_{2j-1}\gamma^j+(A_0+A_{2j})\gamma^{j+1} \\ &\quad +\cdots+(A_{m-j-1}+A_{m-j})\gamma^m+(A_{m-j} \\ &\quad +A_{m-j-1})\gamma^{m+1}+\cdots+(A_0+A_{2j+1})\gamma^{2m-j} \\ &\quad +A_{2j-1}\gamma^{2m-j+1}+(A_0+A_{2j-2})\gamma^{2m-j+2} \\ &\quad +\cdots+(A_j+A_{j-2})\gamma^{2m}) \end{aligned}$$

를 구할 수 있다. 그러나 $j=1$인 경우

$$B_0(A_1, A_0+A_2, \cdots, A_{m-3}+A_{m-1}, A_{m-2}+A_{m-1})$$

이다. 그리고 $1<j$ 이고 $2j<m$ 인 경우

$$\begin{aligned} B_{j-1}(&A_{j-2}+A_j, \cdots, A_{2j-m-1}+A_{m-1}, \\ &A_{2j-m-2}+A_{m-1}, \cdots, A_0+A_{2m-2j+1}, \\ &A_{2m-2j}, \cdots, A_{m-j-1}+A_{m-j}) \end{aligned}$$

이다. 또한 $2j>m$인 경우

$$\begin{aligned} B_{j-1}(&A_{j-2}+A_j, \cdots, A_{2j-m-1} \\ &+A_{m-1}, A_{2j-m-2}+A_{m-1}, \\ &\cdots, A_0+A_{2m-2j+1}, A_{2m-2j}, \cdots, \\ &A_{m-j-1}+A_{m-j}) \end{aligned}$$

이므로 정리가 성립한다. □

정리 5를 이용한 유한체의 하드웨어 구현의 아키텍처를 다음과 같이 구성할 수 있다. 즉 먼저 $A[j]$에서

$A_i+A_j, 0 \leqq i < j \leqq m-1$을 구하는 XOR Block과 이 결과와 B_t를 곱하는 AND 1 Block, 그리고 B_jA_i 를 구하는 AND 2 Block과 각 좌표 별로 XOR를 하는 BTX(Binary Tree XOR) Block으로 구성 할 수 있다. 즉 그림 1과 같이 구성 된다.

각 Block 별로 구체적으로 살펴보자. 먼저 XOR Block은 m개의 $A[j]$대하여 각 $m-1$개의 XOR로 구성 되므로 XOR의 개수는 $m(m-1)$개 이다. 그러나 $A_i, 0 \leqq i \leqq m-1$에 대하여

$A_i+A_j, 0 \leqq i < j \leqq m-1$의 개수는

$$\begin{array}{l} A_0+A_1, A_1+A_2, \cdots, A_{m-2}+A_{m-1} \\ A_0+A_2, A_1+A_3, \cdots, A_{m-3}+A_{m-1} \\ \quad\vdots \\ A_1+A_{m-2}, A_2+A_{m-1} \\ A_1+A_{m-1} \end{array}$$

이므로 $m(m-1)/2$개 이다. 따라서 다른 것과 일치하는 것이 적어도 $m(m-1)/2$개 이다. 그러므로 최대로 XOR Block에서는 $m(m-1)/2$개의 XOR 게이트가 필요하다.

AND 1 Block에서 m이 홀수 인 경우

$$B_0A_1, B_1A_3, \cdots, B_{(m-1)/2}A_{m-1}, B_{(m+1)/2}A_{m-2}, \cdots, B_{m-1}A_0$$

이고 짝수인 경우는

$$B_0A_1, B_1A_3, \cdots, B_{(m-2)/2}A_{m-1}, B_{m/2}A_{m-2}, \cdots, B_{m-1}A_0$$

를 계산하면 된다. 그리고 AND 2 Block은 XOR Block 계산 값과 B_j의 곱이 필요한 부분의 연산으로 정리 5에서 보면 각 j별로 $m-1$개의 곱이 필요하므로 최대 $m(m-1)$개의 AND 연산이 필요하다. 결과적으로 전체 AND 연산은 m^2개 이다.

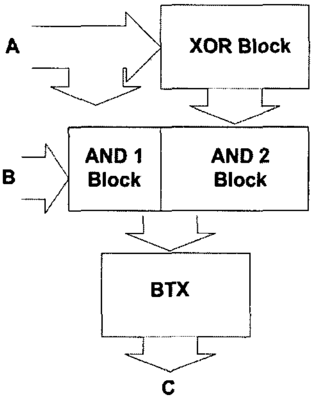

그림 1. 타입 II 최적 정규 기저를 갖는 유한체의 병렬 곱셈 연산기

마지막으로 BTX는 각 m개의 좌표별로 m개의 값을 XOR 해야 하므로 $m(m-1)$개의 XOR 게이트를 필요로 한다. 결과적으로 XOR 게이트는 전체적으로 $3m(m-1)/2$개가 필요하다.

예 2. $GF(2^5)$ 인 경우를 살펴보면 $\overline{A}=(A_0,A_1,A_2,A_3,A_4)$, $\overline{B}=(B_0,B_1,B_2,B_3,B_4)$ 인 경우

$$\begin{aligned} \overline{C} &= \overline{A}\overline{B} \\ &= B_0(A_1, A_0+A_2, A_1+A_3, A_2+A_4, A_3+A_4) \\ &\quad + B_1(A_0+A_2, A_3, A_0+A_4, A_1+A_4, A_2+A_3) \\ &\quad + B_2(A_1+A_3, A_0+A_4, A_4, A_0+A_3, A_1+A_2) \\ &\quad + B_3(A_2+A_4, A_1+A_4, A_0+A_3, A_2, A_0+A_1) \\ &\quad + B_4(A_3+A_4, A_2+A_3, A_1+A_2, A_0+A_1, A_0) \end{aligned}$$

와 같이 표현 되므로 XOR Block에서는

$$\begin{array}{l} A_0+A_1, A_1+A_2, A_2+A_3, A_3+A_4, A_0+A_2, \\ A_1+A_3, A_2+A_4, A_1+A_3, A_1+A_4, A_0+A_5 \end{array}$$

표 1. 타입 II 최적 정규기저에 의한 유한체의 병렬곱셈 연산기의 복잡도 비교

Multipliers	#AND	#XOR	Time Delay
Sunar[5]	m^2	$3m(m-1)/2$	$T_A+(1+\lceil \log_2 m \rceil)T_X$
RR_MO[7]	m^2	$3m(m-1)/2$	$T_A+(1+\lceil \log_2 m \rceil)T_X$
Elia[12]	m^2	$3m(m-1)/2$	$T_A+(1+\lceil \log_2 m \rceil)T_X$
제안한 연산기	m^2	$\leq 3m(m-1)/2$	$T_A+(1+\lceil \log_2 m \rceil)T_X$

를 계산하고 AND 1 Block에서는

$$B_0A_1, B_1A_3, B_2A_4, B_3A_2, B_4A_0$$

를 계산한다.

Ⅳ. 타입 II 최적 정규기저를 갖는 유한체 연산기의 복잡도

Ⅲ장에서 제안한 타입 II 최적 정규기저를 갖는 유한체 $GF(2^m)$의 복잡도는 다음 정리와 같다.

정리 6. 유한체 $GF(2^m)$의 병렬 곱셈 연산기(그림 1) 의 최대 복잡도는 다음과 같다. 과적으로 전체 AND 연산은 m^2개 이다.

1) m^2 AND gate 와 $3m(m-1)/2$ XOR gate
2) $T_A+(1+\lceil \log_2 m \rceil)T_X$

증명. 1)은 Ⅲ 장에서 언급하였다.

2) AND 1, AND 2 Block에서 병렬로 AND 연산을 함으로 1번의 T_A(AND 지연시간)가 일어나고, XOR Block에서 병렬로 $A_i+A_j, 0 \le i < j \le m-1$를 계산하므로 한 번의 T_X(XOR 지연시간)가 일어나고 BTX에서 각 좌표별로 m개의 XOR를 수행하므로 $\lceil \log m \rceil T_X$의 지연시간이 발생한다. 따라서 곱셈을 수행하기 위하여 $T_A+(1+\lceil \log_2 m \rceil)T_X$의 지연시간이 소요된다.

기존의 결과와의 비교는 표 1에서 제시하였다.

Ⅴ. 결 론

유한체가 암호학적 분야에 응용되면서 유한체의 연산에 많은 관심을 가지고 있으며, 하드웨어 구현은 정규기저를 이용하여 표현할 경우 효율적으로 구현할 수 있다. 특히 타입 II 최적 정규기저를 갖는 유한체의 경우 구현도 효율적이고 암호 프로토콜을 비롯한 많은 관련 분야에 응용된다. 본 논문에서는 타입 II 최적 정규기저를 갖는 유한체 $GF(2^m)$의 원소를 정규기저를 사용하여 표현 할 경우 확대체 $GF(2^{2m})$의 원소로 간단하게 표현되는 성질을 이용하여 곱셈기를 구현한 결과 기존의 곱셈기 중 가장 효과적인 것과 같은 시간 및 공간 복잡도를 갖는 병렬곱셈 연산기로 구현되며, 따라서 타입 II 최적 정규기저를 갖는 유한체와 관련된 응용분야에 많이 활용할 수 있을 것으로 기대된다.

참 고 문 헌

〔1〕 R. Lidl and H. Niederreiter, *Introduction to finite fields and its applications*, Cambridge Univ. Press, 1994.

〔2〕 A.J. Menezes, I.F. Blake, X. Gao, R.C. Mullin, S.A. Vanstone, and T. Yaghoobian, *Applications of finitr fields*, Kluwer Academic, 1993.

〔3〕 C.K. Koc and B. Sunar, "Low-complexity bit-parallel canonical and normal basis multipliers for a class of finite fields", *IEEE Trans.* vol.47, no.3, pp. 353-356, Mar, 1998.

〔4〕 H. Wu and M.A. Hasan, "Low Complexity bit-parallel multipliers for a class of finite fields", *IEEE Trans.* vol.47, no.8, pp. 883-887, Aug., 1998.

〔5〕 B. Sunar and C.K. Koc,"An efficient optimal normal basis type II multiplier", *IEEE Trans.* vol.50, no.1, pp. 83-88, Jan., 2001.

〔6〕 C.C Wang, T.K. Truong, H.M. Shao, L.J. Deutsch, J.K. Omura, and I.S. Reed,"VLSI architectures for computing multiplications and inverses in $GF(2^m)$", *IEEE Trans.* vol.34, no.8, pp. 709-716, Aug., 1985.

〔7〕 A. Reyhani-Masolleh and M.H. Hasan, "A new construction of Massey-Omura parallel multiplier over $GF(2^m)$", *IEEE Trans.* vol.51, no.5, pp. 512-520, May, 2002.

〔8〕 C.H. Kim, S. Oh, and J. Lim,"A new hardware architecture for operations in $GF(2^n)$", *IEEE Trans.* vol.51, no.1, pp. 90-92, Jan, 2002.

〔9〕 IEEE P1363, *Standard specifications for public key cryptography*, Draft 13,

1999.
[10] ANSI X 9.63, *Public key cryptography for the financial services industry*: Elliptic curve key agreement and transport protocols, draft, 1998.
[11] Nat'l Inst. of Standard and Technology, Digital Signature Standard, FIPS 186-2, Jan. 2000.
[12] M. Elia and M. Leone, "On the Inherent Space Complexity of Fast Parallel Multipliers for $GF(2^m)$", IEEE Trans. Computers, Vol. 51, no. 3, pp.346-351, Mar. 2002.
[13] S. Gao Jr. and H.W. Lenstra, "Optimal normal bases", *Designs, Codes and Cryptography*, vol. 2, pp.315-323, 1992.

〈著者紹介〉

김 창 한 (Chang Han Kim) 평생회원
1985년 2월: 고려대학교 수학과 학사
1987년 2월: 고려대학교 수학과 석사
1992년 2월: 고려대학교 수학과 박사
2000년 2월~현재: 세명대학교 정보통신학부 부교수
〈관심분야〉 정수론, 공개키 암호, 암호 프로토콜

지 성 연 (Sung Yeon Ji) 학생회원
2005년 2월: 한신대학교 수학과 학사
2005년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 공개키 암호, 암호 칩 설계 기술, 부채널 공격

장 상 운 (Sang-woon Jang) 정회원
2002년 2월: 고려대학교 수학과 학사
2004년 2월: 고려대학교 정보보호대학원 석사
2004년 2월~현재: 국가기술보안연구소
〈관심분야〉 정보보호, 암호이론

임 종 인 (Jongin Lim) 정회원
1980년 2월: 고려대학교 수학과 학사
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
1999년 2월~현재: 고려대학교 정보보호대학원 원장, CIST 센터장
〈관심분야〉 암호이론, 정보보호정책