Regular paper http://dx.doi.org/10.13067/JKIECS.2014.9.4.409

최적정규기저를 갖는 유한체위에서의 저 복잡도 비트-병렬 곱셈기

김용태*

A Low Complexity Bit-Parallel Multiplier over Finite Fields with ONBs

Yong-Tae Kim*

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 m 이 짝수이기 때문에 어떤 암호계에는 응용되지 못하는 단점이 있다. 그러나 타입 II 최적 정규기저를 갖는 유한체의 경우는 NIST 에서 제안한 ECDSA 의 권장 커브가 주어진 $GF(2^{233})$이 타입 II 최적 정규 기저를 갖는 등 여러 응용분야에 적용 되므로, 이에 대한 효율적인 구현에 관한 연구가 활발하게 진행되고 있다. 본 논문에서는 타입 II 최적 정규기저를 갖는 유한체 $GF(2^m)$의 연산을 정규기저를 이용하여 표현하여 확대체 $GF(2^{2m})$의 원소로 표현하여 연산을 하는 새로운 비트-병렬 곱셈기를 제안하였으며, 기존의 가장 효율적인 곱셈기들보다 블록 구성방법이 용이하며, XOR gate 수가 적은 저 복잡도 곱셈기이다.

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 $GF(2^m)$. The finite field $GF(2^m)$ with type I optimal normal basis(ONB) has the disadvantage not applicable to some cryptography since m is even. The finite field $GF(2^m)$ with type II ONB, however, such as $GF(2^{233})$ are applicable to ECDSA recommended by NIST. In this paper, we propose a bit-parallel multiplier over $GF(2^m)$ having a type II ONB, which performs multiplication over $GF(2^m)$ in the extension field $GF(2^{2m})$. The time and area complexity of the proposed multiplier is the same as or partially better than the best known type II ONB bit-parallel multiplier.

키워드

Finite Field, Finite Field Arithmetic, Optimal Normal Basis, Bit-Parallel Multiplier
유한체, 유한체 연산, 최적정규기저, 비트-병렬 곱셈기

I. 서 론

유한체는 암호학과 코딩이론 등에 응용되고 있으며, 특히 공개키 암호인 타원곡선암호(ECC), XTR, ElGamal 타입 암호등의 관련 응용 분야에 활발하게 사용되고 있기 때문에 유한체의 효율적인 연산 방법이 많은 관심의 대상이 되고 있다[1-2]. 유한체의 연산은 원소의 표현방법에 따라 달라지는데, 원소의 대

* 광주교육대학교 수학교육과 교수(ytkim@gnue.ac.kr)
접수일자 : 2014. 01. 10 심사(수정)일자 : 2014. 03. 07 게재확정일자 : 2014. 04. 11

표적인 표현방법으로는 다항식 기저[3-4], 정규기저[5-7]등을 사용하거나 nonconvention 기저[8]를 사용한다. 또한 유한체 $GF(2^m)$에서 기저표현에 필요한 이진수열을 생성하는 방법에 관한 연구[9-10]가 최근에 진행되고 있다. 특히, H/W 구현시에 정규기저를 이용하면 제곱은 단순한 Cyclic Shift 에 의하여 이루어지는 등 많은 장점을 가지고 있으며, 그 중에서도 최적 정규기저를 갖는 유한체가 효율성이 가장 높다[5],[7]. 최적 정규기저를 갖는 유한체는 2 가지 유형, 즉 타입 I 과 타입 II 가 있다[2]. 이 중 타입 I 을 갖는 유한체 $GF(2^m)$은 m 이 항상 짝수이기 때문에 효율성은 좋으나 암호학 분야를 비롯한 여러 분야에 응용되지 못하는 단점을 가지고 있다[11]. 그러나 타입 II 의 경우는 NIST에서 ECDSA의 권장 커브가 주어진 유한체 중 $GF(2^{233})$ 이 타입 II 의 최적 정규기저를 갖는 등 응용분야에 다양하게 활용되므로 이에 대한 많은 연구가 이루어지고 있다[11]. 특히 2001년에 Sunar 와 Koc[5] 이 기존의 결과를 대폭 개선한 결과를 발표하였으며 2002년에는 Elia 와 Leone[12] 그리고 Reyhani-Masoleh 와 Hasan[7] 이 Sunar등[5]의 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 표시되어 곱셈을 수행하는 새로운 연산기를 제안하였으며, 이 제안한 연산기는 기존의 가장 효율적인 곱셈기들과 공간 및 시간 복잡도가 동일하거나 부분적으로는 저복잡도인 연산기이다. 본 논문의 II 장에서는 유한체 위에서의 연산과정을 설명 하였으며 III 장에서는 새로운 비트-병렬 곱셈기를 제안하였고 IV 장에서는 제안된 곱셈기의 효율성과 기존의 결과와의 비교표를 제시하였다.

II. ONB를 이용한 유한체위에서의 연산

이 장에서는 유한체의 원소를 정규기저를 이용하여 표현하는 방법과 ONB를 이용한 원소들의 곱셈법을 설명하기로 한다.

2.1. 유한체의 정규기저를 이용한 원소의 표현과 곱셈

양의 정수 m 에 대하여 유한체 $GF(2)$위에서 $GF(2^m)$의 정규기저가 존재한다는 것은 잘 알려진 결과이다[14]. 즉, $\beta \in GF(2^m)$가 존재하여 $N=\{\beta, \beta^2, ..., \beta^{2^{m-1}}\}$ 이 $GF(2)$위에서 $GF(2^m)$의 기저 일 때 N를 정규기저라 하고 β를 정규기저 생성자라 한다. 이 경우, $A \in GF(2^m)$ 는

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

로 표현되며, 간단히 $A=(a_0, a_1, ..., a_{m-1}))$와 같이 좌표로 표현하거나, 벡터(행렬)표현으로

$$A = \bar{a} \times \bar{\beta}^{\ T} = \bar{\beta} \times \bar{a}^{\ T},\ \bar{a} = [a_0\ a_1\ ...\ a_{m-1}], \tag{2}$$

$\bar{\beta} = [\beta\ \beta^2\ ...\ \beta^{m-1}]$, T는 행렬의 전치, (2)와 같이 표현하기도 한다.

이러한 정규기저의 특징이자 장점은, A^2 은 $A=(a_0, a_1, ..., a_{m-1}))$를 한 번의 Right Cyclic Shift(RCS)를 수행하면 된다는 것이다. 즉,

$$A^2 = (a_{m-1}\ a_0, ..., a_{m-2}) \tag{3}$$

이제, $A, B \in GF(2^m)$, $C=AB$라 하자. 그러면

$$C = (\bar{a}\bar{\beta}^{\ T})(\bar{\beta}\bar{b}^{\ T}) = \bar{a}M\bar{b}\ ,$$
$$M = \bar{\beta}^{\ T}\bar{\beta} = (\beta^{2^i+2^j}),\ 0 \leqq i,j \leqq m-1. \tag{4}$$

$\beta^{2^i+2^j}$ 를 정규기저 $N=\{\beta, \beta^2, ..., \beta^{2^{m-1}}\}$ 을 사용하여 곱의 행렬 M을 다시 표현하면 다음과 같다.

$$M = M_0\beta + M_1\beta^2 + ... + M_{m-1}\beta^{2^{m-1}},$$
$$M_i \in Mat_{m\times m}(GF(2)). \tag{5}$$

A^2 이 RCS 인 사실을 이용하면 $C=AB=(c_0, c_1, ..., c_{m-1})$의 값은 다음과 같이 얻어지게 된다.

$$c_i = \bar{a} M_i \bar{b}^{\ T} = \bar{a}^{(i)} M_0 \bar{b}^{(i)^T},$$
$$\bar{a}^{(i)} = [a_i,\ a_{i+1}, ..., a_{i-1}],$$
$$\bar{b}^{(i)} = [b_i,\ b_{i+1}, ..., b_{i-1}] \quad (6)$$

따라서 각 i 에 대하여 행렬 M_i 의 1의 개수는 모두 같음을 알 수 있고 이때 M_0 의 1의 개수를 정규기저 N 의 복잡도라 하고 C_N 으로 표시하며, Gao등은 다음과 같은 결과를 증명하였다[2],[13].

정리 1. $C_N \geqq 2m-1$.

2.2. 최적 정규기저

정리 1에서 $C_N = 2m-1$일 때 정규기저 N을 최적정규기저(Optimal Normal Basis, ONB)라고 부르며, $GF(2)$ 위에서 최적 정규기저는 다음과 같이 타입 I, 타입 II 인 경우만 존재한다는 것은 잘 알려진 사실이다[2],[13]. 모든 계수가 1인 다항식 $x^m + x^{m-1} + ... + x + 1$ 을 All-One-Polynomial(AOP)이라 한다.

정리 2. (타입 I 최적 정규기저)

$GF(2)$위에서 $GF(2^m)$ 이 타입 I 의 최적 정규기저를 갖기위한 필요충분 조건은 m+1 이 소수이고 $GF(m+1)^* = <2>$이다. 또는 m 차의 AOP인 $x^m + x^{m-1} + ... + x + 1$가 $GF(2)$위에서 기약다항식인 경우 AOP의 근이 최적 정규기저의 생성자 이다[2],[13].

정리 3. (타입 II의 최적 정규기저)

$2m+1$이 소수이고, $GF(2m+1)^* = <2>$ 이거나 또는 $2m+1 \equiv 3 \bmod 4$이고 $GF(2m+1)^* = <-1, 2>$ 이면 $\beta = \gamma + \gamma^{-1}$ 는 $GF(2)$ 위에서 $GF(2^m)$의 최적 정규기저의 생성자이다. 단, γ는 $GF(2^{2m})$에서 $2m+1$의 원시근이다[2],[13].

앞으로 본 논문에서는 m 을 유한체 $GF(2^m)$가 타입 II의 최적 정규기저를 갖는 경우로 제한한다. 이 경우에는 γ 는 $GF(2^{2m})$의 원소가 되며,

$$N = \{\beta,\ \beta^2, ...,\ \beta^{2^{i-1}}\}$$
$$= \{\gamma + \gamma^{-1},\ \gamma^2 + \gamma^{-2}, \cdots,\ \gamma^m + \gamma^{-m}\} \quad (7)$$

인 것은 잘 알려진 사실이다[2]. 임의의 원소 $A \in GF(2^m)$ 는 확대체 $GF(2^{2m})$에서 다음과 같이 표현된다[14]. 즉, $\beta = \gamma + \gamma^{-1}$는 $GF(2)$ 위에서 $GF(2^m)$ 의 정규기저 생성자 이므로 원소 $A \in GF(2^m)$는 식 (7) 에 의하여

$$\begin{aligned} A &= a_0\beta + a_1\beta^2 + a_2\beta^{2^2} + ... + a_{m-1}\beta^{2^{m-1}} \\ &= A_0(\gamma + \gamma^{-1}) + A_1(\gamma^2 + \gamma^{-2}) + ... \\ &\quad + A_{m-1}(\gamma^m + \gamma^{-m}) \end{aligned} \quad (8)$$

와 같이 표현되며, A_i 는 계수 a_j 를 재배열하여 얻어진다. 그러므로 재 정열을 하면 $A \in GF(2^m)$는 확대체 $GF(2^{2m})$의 원소로 다음과 같이 표현된다. 즉,

$$\begin{aligned} A &= A_0\gamma + A_1\gamma^2 + A_2\gamma^3 + ... + A_{m-1}\gamma^m \\ &\quad + A_{m-1}\gamma^{m+1} + A_{m-2}\gamma^{m+2} + ... + A_1\gamma^{2m} \\ &\quad ,\ A_j \in GF(2^2) \end{aligned} \quad (9)$$

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

정리 4. $A, B \in GF(2^m)$ 인 경우에 A, B 를 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

$$\begin{aligned} X &= X_0\gamma + X_1\gamma^2 + X_2\gamma^3 + ... + X_{m-1}\gamma^m \\ &\quad + X_{m-1}\gamma^{m+1} + X_{m-2}\gamma^{m+2} + ... + X_1\gamma^{2m} \end{aligned} \quad (10)$$

와 같이 표현되면 A 는 $GF(2^m)$에서 다음과 같이 표현된다. 식 (7)에 의하여 계수를 조정하면

$$\begin{aligned} X &= X_0(\gamma+\gamma^{-1})+X_1(\gamma^2+\gamma^{-2})+\ldots \\ &\quad +X_{m-1}(\gamma^m+\gamma^{-m}) \\ &= X'_0\beta+X'_1\beta^{2^2}+\cdots X'_{m-1}\beta^{2^{m-1}} \end{aligned} \tag{11}$$

이 되고, A,B는 $GF(2^m)$의 원소이므로 $GF(2^{2m})$ 의 원소로 표현하면

$$\begin{aligned} A &= A_0\gamma+A_1\gamma^2+A_2\gamma^3+\ldots+A_{m-1}\gamma^m \\ &\quad +A_{m-1}\gamma^{m+1}+A_{m-2}\gamma^{m+2}+\ldots+A_1\gamma^{2m} \\ B &= B_0\gamma+X_1\gamma^2+B_2\gamma^3+\ldots+B_{m-1}\gamma^m \\ &\quad +B_{m-1}\gamma^{m+1}+B_{m-2}\gamma^{m+2}+\ldots+B_1\gamma^{2m} \end{aligned} \tag{12}$$

이다. 이때 위의 식에서 $\gamma^{2m+1}=1$ 임을 이용하면

$$\begin{aligned} & B_{j-1}\gamma^j A+B_{j-1}\gamma^{2m-j+1} \\ = & B_{j-1}(A_{j-2}\gamma+\cdots+A_0\gamma^{j-1}+0+A_0\gamma^{j+1}+\cdots+A_{m-1}\gamma^{m+j} \\ & +A_{m-1}\gamma^{m+j+1}+\cdots+A_j\gamma^{2m})+B_{j-1}A_{j-1} \\ + & B_{j-1}(A_j\gamma+\cdots+A_{m-1}\gamma^{m-j}+A_{m-1}\gamma^{m-j+1}+\cdots \\ & A_0\gamma^{2m-j}+0+A_0\gamma^{2m-j+2}+\cdots+A_{j-2}\gamma^{2m})+B_{j-1}A_{j-1} \\ = & B_{j-1}((A_{j-2}+A_j)\gamma+\cdots+(A_0+A_{2j-2})\gamma^{j-1} \\ & +A_{2j-1}\gamma^j+(A_0+A_{2j})\gamma^{j+1}+\cdots \\ & +(A_{m-j-1}+A_{m-j})\gamma^m+(A_{m-j}+A_{m-j-1})\gamma^{m+1} \\ & +\cdots+(A_0+A_{2j+1})\gamma^{2m-j}+A_{2j-1}\gamma^{2m-j+1} \\ & +(A_0+A_{2j-2})\gamma^{2m-j+2}+\cdots+(A_j+A_{j-2})\gamma^{2m}). \end{aligned} \tag{13}$$

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

앞으로 본 논문에서는 $A\in GF(2^m)$를 $GF(2^{2m})$의 원소로 표현할 경우 다음과 같이 벡터 모양으로 표현하기로 한다.

$$\begin{aligned} A &= A_0\gamma+A_1\gamma^2+A_2\gamma^3+\ldots+A_{m-1}\gamma^m \\ &\quad +A_{m-1}\gamma^{m+1}+A_{m-2}\gamma^{m+2}+\ldots+A_1\gamma^{2m} \\ &\equiv (A_0,\cdots,A_{m-1},A_{m-1},\cdots,A_0). \end{aligned} \tag{14}$$

(14)

또한, 필요한 경우 원소 A의 앞의 m 개의 성분만을 이용하여

$$\overline{A}\equiv A = (A_0,A_1,\cdots,A_{m-1}) \tag{15}$$

로 나타내기로 한다.

예 1. $m=5$ 이고 $j=2$ 인 경우

$$\begin{aligned} & B_1\gamma^2A+B_1\gamma^9A \\ = & B_1(A_0+A_2,A_3,A_0+A_4,A_1+A_4,A_2+A_3, \\ & A_2+A_3,A_1+A_4,A_0+A_4,A_3,A_0+A_2). \end{aligned} \tag{16}$$

III. 제안하는 ONB를 갖는 $GF(2^m)$의 비트-병렬 곱셈기

이장에서는 제안하는 타입 II 최적 정규기저를 갖는 유한체 $GF(2^m)$ 의 원소를 확대체 $GF(2^{2m})$의 원소로 표시하여 곱셈하는 곱셈기에 대하여 설명하고, 간단한 예를 들어 기존의 곱셈기와 복잡도를 비교하기로 한다.

정리 5. $A,\ B\in GF(2^m)$이고 $C=AB$라 $\overline{A}=(A_0,A_1,\cdots,A_{m-1})$, $\overline{B}=(B_0,B_1,\cdots,B_{m-1})$ $\overline{C}=(C_0,C_1,\cdots,C_{m-1})$ 라 하면

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

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

$$\begin{aligned} A[j] = (& A_{j-2}+A_j,\cdots,A_0+A_{2j-2},A_{2j-1}, \\ & A_0+A_{2j},\cdots,A_{m-j-2}+A_{m-j}, \\ & A_{m-j-1}+A_{m-j}) \text{ if } 2<j \text{ and } 2j\leqq m \end{aligned}$$

$$\begin{aligned} A[j] = (& A_{j-2}+A_j,\cdots,A_{2j-m-1}+A_{m-1}, \\ & A_{2j-m-2}+A_{m-1},\cdots,A_0+A_{2m-2j+1}, \\ & A_{2m-2j},\cdots,A_{m-j-1}+A_{m-j}) \text{ if } 2j>m \end{aligned} \tag{17}$$

단, 모든 index는 m을 법으로 계산한 값이다.

(증명) A,B를 식(12)과 같이 표현한 다음, 식 (13)과 같이 계산하면,

$$
\begin{aligned}
C = AB &= \sum_{j=1}^{m} B_{j-1}(A\gamma^{j} + A\gamma^{2m-j+1}) \\
&= \sum_{j=1}^{m} B_{j-1}((A_{j-2}+A_j)\gamma + \cdots + (A_0 + A_{2j-2})\gamma^{j-1} \\
&\quad + A_{2j-1}\gamma^{j} + (A_0 + A_{2j})\gamma^{j+1} + \cdots \\
&\quad + (A_{m-j-1} + A_{m-j})\gamma^{m} + (A_{m-j} + A_{m-j-1})\gamma^{m+1} \\
&\quad + \cdots + (A_0 + A_{2j+1})\gamma^{2m-j} + A_{2j-1}\gamma^{2m-j+1} \\
&\quad + (A_0 + A_{2j-2})\gamma^{2m-j+2} + \cdots + (A_j + A_{j-2})\gamma^{2m})
\end{aligned} \tag{18}
$$

가 된다. 그런데, $j=1$인 경우 에는

$$B_0(A_1, A_0 + A_2, \cdots, A_{m-3} + A_{m-1}, A_{m-2} + A_{m-1}), \tag{19}$$

$1 < j$ 이고 $2j < m$ 인 경우에는

$$
\begin{aligned}
B_{j-1}(\, & A_{j-2} + A_j, \cdots, A_0 + A_{2j-2}, A_{2j-1}, A_0 + \\
& A_{2j}, \cdots, A_{m-j-2} + A_{m-j}, A_{m-j-1} + A_{m-j}),
\end{aligned} \tag{20}
$$

$2j > m$ 인 경우에는

$$
\begin{aligned}
B_{j-1}(\, & A_{j-2} + A_j, \cdots, A_{2j-m-1} + A_{m-1}, A_{2j-m-2} \\
& + A_{m-1}, \cdots, A_0 + A_{2m-2j+1}, A_{2m-2j}, \cdots, \\
& A_{m-j-1} + A_{m-j})
\end{aligned} \tag{21}
$$

이므로 정리가 증명되었다.

정리 5를 이용한 유한체의 H/W 구현에 필요한 architecture를 다음과 같이 구성할 수 있다. 먼저 $A[j]$에서 $A_i + A_j$, $0 \leq i < j \leq m-1$ 를 구하는 XOR Block 과 이 결과와 B_t 를 곱하는 AND 1 Block, 그리고 $B_j A_i$ 를 구하는 AND 2 Block 와 각 좌표 별로 XOR 를 하는 BTX(Binary Tree XOR) Block 로 구성하면, 그림 1과 같다.

제안하는 곱셈기를 각 Block 별로 구체적으로 설명하면 다음과 같다. 먼저 XOR Block 은 m개의 $A[j]$ 대하여 각 $m-1$ 개의 XOR 이 구성 되므로 XOR 의 개수는 $m(m-1)$ 개다.

그러나 A_i, $0 \leq i \leq m-1$에 대하여,

$$A_i + A_j,\ 0 \leq i < j \leq m-1,$$

$$
\begin{aligned}
& A_0 + A_1, A_1 + A_2, \cdots, A_{m-2} + A_{m-1} \\
& A_0 + A_2, A_1 + A_3, \cdots, A_{m-3} + A_{m-1} \\
& \quad \vdots \\
& A_1 + A_{m-2}, A_2 + A_{m-1} \\
& A_1 + A_{m-1}
\end{aligned} \tag{22}
$$

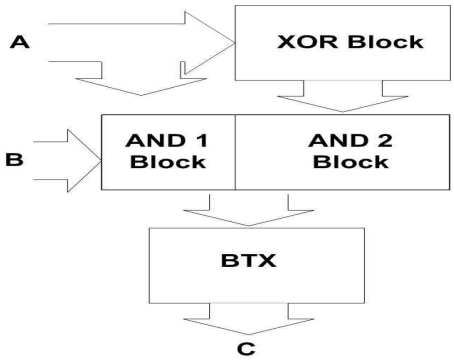

그림 1. 타입 II ONB를 갖는 유한체 $GF(2^m)$의 비트-병렬 곱셈기

Fig. 1 The block diagram of Type II ONB bit-parallel multiplier for $GF(2^m)$

이므로 $m(m-1)/2$ 개 이다. 따라서 이 중 동일한 원소의 개수는 적어도 $m(m-1)/2$ 개 이다. 그러므로 XOR Block 에서는 최대 $m(m-1)/2$ 개의 XOR 게이트가 필요하다. 또한, AND 1 Block 에서는 m 이 홀수인 경우에는

$$B_0 A_1, B_1 A_3, \cdots, B_{(m-1)/2} A_{m-1}, \text{를}, \\ B_{(m+1)/2} A_{m-2}, \cdots, B_{m-1} A_0$$

짝수인 경우에는

$$B_0 A_1, B_1 A_3, \cdots, B_{(m-2)/2} A_{m-1}, \text{를} \\ B_{m/2} A_{m-2}, \cdots, B_{m-1} A_0$$

계산하면 된다. 그리고 AND 2 Block 에서는 XOR Block 계산 값과 B_j 의 곱이 필요한 부분의 연산으로 정리 5에 의하여, 각 j 별로 $m-1$ 개의 곱이 필요하기 때문에 최대한 $m(m-1)$개의 AND 연산이 필요하므로, 전체 AND 연산은 m^2 개 이다. 마지막으로 BTX 는 각 m 개의 좌표별로 m 개의 값을 XOR 해야 하므로, XOR 게이트 수는 $m(m-1)$개이다. 따라서 전체 XOR 게이트는 $3m(m-1)/2$ 개가 필요하다.

예 2. $GF(2^5)$ 상에서의 비트-병렬곱셈기

$\overline{A}=(A_0,A_1,A_2,A_3,A_4)$, $\overline{B}=(B_0,B_1,B_2,B_3,B_4)$라 놓으면,

$$\begin{aligned}\overline{C} &= \overline{A}\,\overline{B} \\ &= B_0(A_1,A_0+A_2,A_1+A_3,A_2+A_4,A_3+A_4) \\ &\quad B_1(A_0+A_2,A_3,A_0+A_4,A_1+A_4,A_2+A_3) \\ &\quad B_2(A_1+A_3,A_0+A_4,A_4,A_0+A_3,A_1+A_2) \\ &\quad B_3(A_2+A_4,A_1+A_4,A_0+A_3,A_2,A_0+A_1) \\ &\quad B_4(A_3+A_4,A_2+A_3,A_1+A_2,A_0+A_1,A_0)\end{aligned} \tag{23}$$

와 같이 표현 되므로, XOR Block에서는

$$A_0+A_1,A_1+A_2,A_2+A_3,A_3+A_4,A_0+A_2,$$
$$A_1+A_3,A_2+A_4,A_)+A_3,A_1+A_4,A_0+A_5$$

를 계산하고 AND 1 Block에서는

$B_0A_1,B_1A_3,B_2A_4,B_3A_2,B_4A_0$를 계산한다.

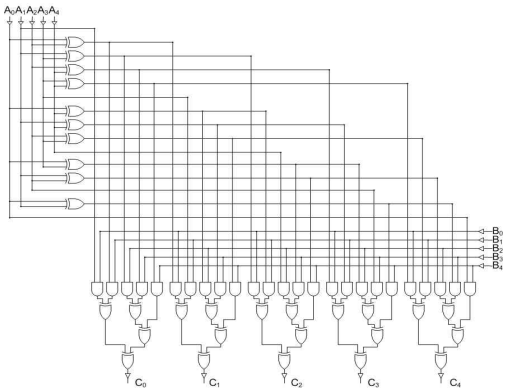

그림 2. $GF(2^5)$상에서의 비트-병렬곱셈기
Fig. 2 The bit-parallel multiplier over $GF(2^5)$

IV. 복잡도

III장에서 제안한 타입 II 최적 정규기저를 갖는 유한체 $GF(2^m)$의 비트-병렬 곱셈기의 복잡도는 다음 정리와 같이 계산된다.

정리 7. 유한체 $GF(2^m)$의 비트-병렬 곱셈기의 최대 복잡도는 다음과 같다.

1) m^2 AND gates와 $3m(m-1)/2$ XOR gates,

2) $1T_A+(1+\lceil \log_2 m \rceil)T_X$.

(증명) 1)은 III 장에서 증명하였다. 2) AND 1, AND 2 Block에서 병렬로 AND 연산을 함으로 1번의 D_A (AND Delay) 가 일어나고, XOR Block에서 병렬로 A_i+A_j, $0 \leq i < j \leq m-1$, 를 계산함으로 1번의 D_X 가 일어나고 BTX에서 각 좌표별로 m 개의 XOR 를 하여야 함으로 $\lceil \log m \rceil D_X$번의 Delay 가 발생한다.

따라서 전체는 $1T_A+(1+\lceil \log_2 m \rceil)T_X$ 번의 Delay 가 발생한다.

제안하는 곱셈기와 기존의 곱셈기와의 복잡도의 비교는 표 1에 제시하였다.

표 1. 정규기저를 갖는 유한체의 병렬 곱셈 연산기의 복잡도 비교
Table 1. Comparison of normal basis multipliers

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

제안하는 곱셈기는 Sunar, RR_MO와 Elia 등이 제안한 곱셈기와 비교하여 AND gate의 수와 Time Delay는 동일하며, 기존의 곱셈기의 XOR gate 수는 정확하게 $\frac{3m(m-1)}{2}$개인 반면에 제안하는 XOR gate 수는 $\frac{3m(m-1)}{2}$ 이하로 나타났으며, 특히 그림 1의 블록 구성방법이 다른 곱셈기보다 용이하다.

V. 결 론

유한체가 암호학적 분야에 응용되면서 유한체의 연산에 많은 관심을 가지고 있으며, 유한체 연산에 필요

한 이진수열을 생성하는 방법에 관한 연구도 진행되고 있다[15]. H/W 구현은 유한체의 원소를 정규기저를 이용하여 표현할 때 가장 효율적이며, 특히 타입 II 최적 정규기저를 갖는 유한체의 경우에는 구현도 효율적이며, 암호프로토콜을 비롯한 많은 암호학 관련 분야에 응용된다. 본 논문에서는 타입 II 최적 정규기저를 갖는 유한체 $GF(2^m)$ 의 원소를 정규기저를 사용하여 표현할 경우 확대체 $GF(2^{2m})$의 원소로 간단하게 표현되는 성질을 이용하여 곱셈기를 구현한 결과, 기존의 가장 효율적인 곱셈기들보다 블록 구성방법이 다른 곱셈기보다 용이하며, XOR gate 수가 적은 저 복잡도인 곱셈기이므로 유한체와 관련된 응용분야에 활용할 수 있을 것으로 기대된다.

감사의 글

본 논문은 광주교육대학교 2014년도 학술연구비 지원에 의한 것임

참고 문헌

[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 finite fields.* Kluwer Academic, 1993.

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

[4] A. Reyhani-Maslleh and M. H. Hasan, "Efficient Digit Serial Normal Basis Multiplier over Binary Extension Fields," *ACM Trans. Embedded Systems and Security,* vol. 3, 2004, pp. 575-592.

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

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

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

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

[9] S.-J. Cho, J.-G. Kim, U.-S. Choi, and S.-T. Kim, "Cross-correlation of linear and nonlinear GMW-sequences generated by the same primitive polynomial on $GF(2^p)$," *The Korea Institute of Electronic Communication Sciences 2011 Spring Conf.,* vol. 5, no. 1, 2011, pp. 155-158.

[10] H.-D. Kim, S.-J. Cho, M.-J. Kwon, and H.-J. An, "A study on the cross sequences," *J. of The Korea Institute of Electronic Communication Sciences,* vol. 7, no. 1, 2012, pp. 61-67.

[11] Y. Kim, "Fast Sequential Optimal normal Bases Multipliers over finite fields," *J. of The Korea Institute of Electronic Communication Sciences,* vol. 8, no. 8, 2013, pp. 1207-1212.

[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, 2002. pp. 346-351.

[13] S. Gao Jr. and H. W. Lenstra, "Optimal normal bases," *Designs, Codes and Cryptography,* vol. 2, 1992, pp. 315-323.

[14] Y. Kim, "A Fast Multiplier of Composite fields over finite fields," *J. of The Korea Institute of Electronic Communication Sciences,* vol. 6, no. 3, 2011, pp. 389-395.

[15] U.-S. Choi and S.-J. Cho, "Design of Binary Sequence with optimal Cross-correlation Values," *J. of The Korea Institute of Electronic Communication Sciences,* vol. 6, no. 4, 2011, pp. 539-544.

저자 소개

김용태(Yong-Tae Kim)

1976년 2월 공주사범대학 수학교육과(이학사)
1986년 2월 고려대학교 대학원 수학과(이학석사)
1991년 2월 고려대학교대학원 수학과(이학박사)
2000년 8월 서울대학교 대학원 수학교육과(교육학석사)
2008년 2월 서울대학교 대학원 수학교육과(박사과정수료)
1992년 3월~현재 광주교육대학교 수학교육과 교수
※ 관심분야 : ECC, 정수론적 암호학, 공개키암호학