情報保護學會論文誌
第16卷 第2號, 2006. 4

Type-Ⅱ 최적 정규기저에서 변형된 SMPO*

양 동 진,[1†] 장 남 수,[1] 지 성 연,[1] 김 창 한[2‡]
[1]고려대학교 정보보호대학원, [2]세명대학교 정보통신학부

Modified SMPO for Type-Ⅱ Optimal Normal Basis*

Dong Jin Yang,[1†] Nam Su Chang,[1] Sung Yeon Ji,[1] Chang Han Kim[2‡]
[1]Graduate School of Information Security(GSIS), Korea University,
[2]Information & Communication System, Semyung University

요 약

암호 활용과 코딩 이론은 유한체 $GF(2^m)$에서의 연산을 사용한다. 유한체 연산을 사용하는 분야에서 연산기의 공간, 시간 복잡도의 효율성은 메모리와 수행시간에 많은 영향을 미친다. 따라서 유한체 곱셈기를 효율적으로 구성하기 위한 노력은 계속 되고 있다. [11]에서 Massey-Omura는 정규기저를 사용하는 곱셈기를 제안했고, [1]에서 Agnew는 긴 지연시간을 갖는 Massey-Omura 곱셈기를 개선한 순차 곱셈기를 제안했다. Rayhani-Masoleh와 Hasan 그리고 S.Kwon은 Agnew의 곱셈기의 구조를 개선한 공간 복잡도를 줄인 곱셈기를 각각 제안했다[2,3]. [2]에서 Rayhani-Masoleh와 Hasan이 제안한 곱셈기의 구조는 [1]의 곱셈기보다 경로 지연시간은 약간 증가하였다. 하지만, [3]에서 S.Kwon는 [1]의 구조에서 시간 효율성의 감소가 없는 곱셈기의 구조를 제안했다. 본 논문에서는 type-Ⅱ 최적 정규기저에서 S.Kwon의 곱셈기와 시간과 공간 효율성이 같은 Rayhani-Masoleh와 Hasan의 구조를 변형한 곱셈기를 제안한다.

ABSTRACT

Cryptographic application and coding theory require operations in finite field $GF(2^m)$. In such a field, the area and time complexity of implementation estimate by memory and time delay. Therefore, the effort for constructing an efficient multiplier in finite field have been proceeded. Massey-Omura proposed a multiplier that uses normal bases to represent elements $GF(2^m)$ [11] and Agnew at al. suggested a sequential multiplier that is a modification of Massey-Omura's structure for reducing the path delay. Recently, Rayhani-Masoleh and Hasan and S.Kwon at al. suggested a area efficient multipliers for modifying Agnew's structure respectively[2,3]. In [2] Rayhani-Masoleh and Hasan proposed a modified multiplier that has slightly increased a critical path delay from Agnew at al.'s structure. But, In [3] S.Kwon at al. proposed a modified multiplier that has no loss of a time efficiency from Agnew's structure. In this paper we will propose a multiplier by modifying Rayhani-Masoleh and Hassan's structure and the area-time complexity of the proposed multiplier is exactly same as that of S.Kwon at al's structure for type-Ⅱ optimal normal basis.

Keywords : *Gaussian Normal Basis, Massey-Omura multiplier, finite field*

Ⅰ. 서 론

암호의 활용과 코딩 이론(Coding Theory)의 분야에서 유한체 연산은 매우 중요하다. 특히 $GF(2^m)$에서 곱셈 연산은 ECC, XTR, AES와 같은 암호

접수일: 2006년 1월 9일; 채택일: 2006년 3월 20일
* 본 연구는 정보통신부 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었습니다.
† 주저자 : djyang76@cist.korea.ac.kr
‡ 교신저자 : chkim@semyung.ac.kr

시스템에서 많이 사용되고 있다. 따라서 위와 같은 암호 시스템에서 연산 시간이 빠르고 공간 복잡도가 작도록 유한체 곱셈기를 구성하는 것은 주요 관심 대상이다. 최근에 공간 복잡도와 시간 복잡도를 효율적으로 구성하기 위하여 정규기저를 많이 사용한다[1-8,10]. 이와 같이 정규기저를 사용하면 하드웨어 구현에 적합하고 제곱 연산이 주기적인 쉬프트 연산(Shift Operation)을 통해서 수행되는 장점을 가진다.

Massey-Omura가 제안한 곱셈기는 병렬로 입력을 받아서 순차적으로 결과 값을 출력하는 구조로 임계 경로 지연(Critical path delay)이 매우 오래 걸렸다[12]. 따라서 Agnew는 [3]에서 Massey-Omura 곱셈기를 개선하여 복잡도를 줄인 순차 곱셈기(Sequential Multiplier with Parallel Output, SMPO)를 제안했다. 최근에 Reyhani-Masoleh, Hasan과 S.Kwon은 [2]에서 제안된 방법을 개선하여 공간 복잡도를 줄이는 SMPO를 각각 [3]와 [4]에서 제안했다. [3]에서는 [2]에서보다 경로 지연 시간은 증가하지만, 공간 복잡도를 줄인 곱셈기를 제안했다. 예를 들어 type-II 최적 정규기저(Optimal Normal Basis, ONB)를 사용할 때, $GF(2)$에서 $GF(2^m)$의 확장 차수는 m이고, T_A와 T_X는 각각 두개의 입력 값에 대한 AND게이트와 XOR게이트의 경로 지연 일 때, [1]에서 제안된 곱셈기의 시간 복잡도가 $m(T_A+2T_X)$ 인 반면 [3]에서 제안된 곱셈기의 시간 복잡도는 $m(T_A+3T_X)$ 이다. [4]에서 S.Kwon은 [2]에서 제안된 SMPO의 경로 지연의 증가 없이 공간 복잡도를 줄인 곱셈기를 제안했다. 따라서 [4]에서 제안된 SMPO가 [3]에서 제안된 SMPO와 비교하였을 때 공간 복잡도는 같지만 시간 효율성은 크다. 그러므로 알려진 SMPO들 중에서 [4]에서 제안된 SMPO가 시간과 공간 복잡도에서 가장 효율적이라고 알려졌다.

본 논문에서는 [3]에서 제안된 곱셈기의 구조를 변형한 $GF(2^m)$에서 type-II ONB를 사용하는 순차 곱셈기를 제안 한다. 제안하는 순차 곱셈기의 임계 경로 지연은 [3]의 곱셈기보다 줄어들었고 [4]에서 제안된 곱셈기의 임계 경로 지연과 정확하게 같다. 그리고 제안하는 곱셈기의 공간 복잡도는 [3]에서 제안된 곱셈기의 공간 복잡도와 같다. 따라서 제안하는 곱셈기는 $k=2$일 때 [4]에서 제안된 곱셈기와 같은 복잡도 가진다.

II. 기존의 곱셈기

1. type-II 최적 정규기저

$GF(2^m)$에서 type-II ONB는 $1\le i<2m+1$ 에 대하여 $\gamma^{2m+1}=1$이고 $\gamma^i\neq 1$을 만족하는 즉, 원시근 γ 에 대하여, 표준 원소 $\alpha=\gamma+\gamma^{-1}$ 을 사용하여 구성된다.

type-II ONB는 $p=2m+1$이 소수이고 다음 두 조건 중에서 하나를 만족하면 구성할 수 있다[14].

1) 2는 Z_{2m+1}의 원시근(Primitive)이다.
2) $2m+1\equiv 3 \bmod 4$ 이고 2는 Z_{2m+1}에서 이차 잉여(Quadratic residues)를 생성한다.

두 번째 조건은 (-1)은 모듈러 p에 대하여 이차 잉여를 생성하지 않고, 2는 모듈러 p 에 대하여 이차 잉여를 생성한다는 것을 의미한다.

최적 정규기저를 사용하면 하드웨어에서 ECC의 효율적인 구현이 가능하다. 따라서 ECC의 효율적인 구성인 가능한 확장 차수 m에 대하여 ANSI는 type-II ONB의 경우($m=191$ $EX4,5$ 와 $m=239$ $EX4,5$) 들을 추천하였고 NIST는 하나의 type-II ONB ($m=233$)를 추천했다[13,14].

2. Reyhani-Masoleh, Hasan's 곱셈기

α 는 1절에서와 같이 정의 된 type-II ONB의 표준 원소라 하고 $\alpha_0,\alpha_1,\cdots,\alpha_{m-1}$ 는 $GF(2^m)$에서 $\alpha_i=\alpha^{2^i}$을 만족하는 정규기저라 하자. 그러면 $GF(2)$의 λ_{ij}에 대하여 다음이 성립한다.

$$\alpha\alpha_i=\sum_{j=0}^{m-1}\lambda_{ij}\alpha_j$$

[2]에서 Agnew가 $\alpha_i\alpha_j$를 사용하여 구성한 반면 [3]에서 Reyhani-Masoleh, Hasan은 $\alpha\alpha_i$사용하여 $\alpha\alpha_i$와 $\alpha\alpha_{m-i}$ 사이의 대칭 성질을 사용했다. 그리고 임계 경로 지연은 같지만 구조가 다른 XESMPO (XOR Efficient SMPO)와 AESMPO(AND Efficient SMPO)를 제안했다. 따라서 XESMPO에 대하여 살펴보고 AESMPO에 대하여 논하도록 한다.

[3]에서 $A=\sum_{i=0}^{m-1}a_i\alpha_i$ 와 $B=\sum_{j=0}^{m-1}b_j\alpha_j$ 의 곱 C는 다

음과 같이 계산된다.

$$C=\sum_{ij} a_i b_j \alpha_i \alpha_j$$
$$=\sum_{i=0}^{m-1} a_i b_i \alpha_{i+1} + \sum_{i=0}^{m-1}\sum_{j\neq i} a_i b_j (\alpha\alpha_{j-i})^{2^i}$$
$$=\sum_{i=0}^{m-1} a_i b_i \alpha_{i+1} + \sum_{i=0}^{m-1}\sum_{j\neq 0} a_i b_{j+i} (\alpha\alpha_j)^{2^i}.$$

위의 식 우변에서 두 번째 항은 $v=\lceil \frac{m-1}{2} \rceil$ 즉, $m=2v+1$ 또는 $m=2v+2$ 에 대하여 다음과 같다.

m이 홀수일 때,

$$\sum_{i=0}^{m-1}\sum_{j=1}^{v} a_i b_{j+i} (\alpha\alpha_j)^{2^i} + \sum_{i=0}^{m-1}\sum_{j=m-v}^{m-1} a_i b_{j+i} (\alpha\alpha_j)^{2^i}.$$

m이 짝수일 때,

$$\sum_{i=0}^{m-1}\sum_{j=1}^{v} a_i b_{j+i} (\alpha\alpha_j)^{2^i} + \sum_{i=0}^{m-1}\sum_{j=m-v}^{m-1} a_i b_{j+i} (\alpha\alpha_j)^{2^i}$$
$$+\sum_{i=0}^{m-1} a_i b_{v+1+i} (\alpha\alpha_{v+1})^{2^i}.$$

ANSI와 NIST에서 추천한 경우들과 같이 m을 홀수로 제안할 수 있다. 따라서 홀수 m에 대하여 다음과 같은 식이 성립한다.([3] 참고),

$$\sum_{i=0}^{m-1}\sum_{j=m-v}^{m-1} a_i b_{j+i} (\alpha\alpha_j)^{2^i}$$
$$=\sum_{i=0}^{m-1}\sum_{j=1}^{v} a_i b_{m-j+i} (\alpha\alpha_{m-j})^{2^i}$$
$$=\sum_{i=0}^{m-1}\sum_{j=1}^{v} a_{i+j} b_i (\alpha\alpha_{m-j})^{2^{i+j}}$$
$$=\sum_{i=0}^{m-1}\sum_{j=1}^{v} a_{i+j} b_i (\alpha\alpha_j)^{2^i}.$$

따라서 C는 다음과 같다.

$$C=\sum_{i=0}^{m-1} a_i b_i \alpha_{i+1} + \sum_{i=0}^{m-1}\sum_{j=1}^{v} (a_i b_{j+i} + a_{j+i} b_i)(\alpha\alpha_j)^{2^i}$$
$$=\sum_{i=0}^{m-1} (a_i b_i \alpha_1 + \sum_{j=1}^{v} (a_i b_{j+i} + a_{j+i} b_i)\alpha\alpha_j)^{2^i}$$
$$=\sum_{i=0}^{m-1} (F_i)^{2^i}.$$

위의 식에서 $\delta_j = \alpha\alpha_j$와 $g\in 0,1$ 에 대하여 $F_i(A,B) = a_{i-g} b_{i-g}\alpha + \sum_{j=1}^{v} z_{ij}\delta_j$ 이고, $1\le j\le v$에 대하여 z_{ij}는 다음과 같이 결정한다.

$$z_{ij}=\begin{cases}(a_i+a_{i+j})(b_i+b_{i+j}), & g=0;\\ a_i b_{j+i}+a_{j+i}b_i, & g=1.\end{cases}$$

$g=1$ 인 경우, XESMPO라 부르고 $g=0$ 인 경우 AESMPO라 부른다. $F_{m-t}=F_{m-1}(A^{2^{t}},B^{2^{t}})$, 이므로 곱 $C=AB$는 $\sum_{i=0}^{m-1} F_i^{2^i}$ 을 통해서 계산할 수 있다. 이 성질을 이용하여, Reyahni-Masoleh, Hasan은 다음과 같은 정리 1을 증명했다.

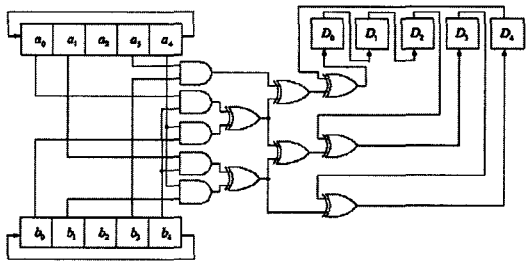

그림 1. $GF(2^5)$ 에서 (2)의 XESMPO

정리 1. ([3]) A와 B를 $GF(2^m)$ 의 원소라 하고 $C=AB$라 하자. 그러면 다음을 만족한다.

$$C=(((F_{m-1}^2+F_{m-2})^2+F_{m-3})^2+\cdots+F_1)^2+F_0.$$

예를 들면, $m=5$일 경우 type-II ONB를 사용하는 [2]에서 제안된 곱셈기의 XESMPO는 그림 1.과 같다. 그림 1.에서 XESMPO는 Z-array와 XOR-array 두 개의 부분으로 구성 된다. Z-array에서는 z_{ij}를 계산하고 XOR-array에서는 $\sum_{j=1}^{v} z_{ij}(\alpha\alpha_j)^{2^i}$ 를 계산한다. 그리고 결과를 저장 공간 D에 저장한다. Z-array에 따라서 XESMPO와 AESMPO로 나누어 진다.

III. 기존의 곱셈기

1. 제안하는 곱셈기

[3]에서 제안한 SMPO는 II장 2절에서 기술한 z_{ij}, δ_j와 같이 정의하여 다음과 같은 식을 사용한다.

$$C=\sum_{i=0}^{m-1}a_ib_i\alpha_{i+1}+\sum_{i=0}^{m-1}\sum_{j=1}^{v}z_{ij}(\delta_j)^{2^i}.$$

따라서 II장 2절의 곱셈 행렬 (λ_{ij})에 의하여 δ_j값이 결정된다. 곱셈기를 제안하기 전에 몇 개의 기호를 정의한다. 첫 번째, type-II ONB를 사용하므로 (λ_{ij})의 첫 번째 행과 첫 번째 열을 제외한 모든 행과 열에 정확하게 두개의 1이 있다. 따라서 $l(i)$를 (λ_{ij})에서 i번째 행에서 1들의 거리로 정의하자. 여기서 거리는 두개의 1사이의 0의 개수를 의미한다. m이 홀수이기 때문에 만약 $l(i)$가 홀수면 $l(i)$는 $m-l(i)$ 값으로 결정하고, $l(i)$가 짝수면 $l(i)$값으로 결정한다. 따라서 짝수 값을 가지는$l(i)$를 구할 수 있다. 두 번째 기호를 정의하기 전에 보조정리 1을 소개한다.

보조정리 1. $GF(2^m)$의 type-II ONB를 사용하면, $1\le i\ne j\le v$에 대하여 $l(i)\ne l(j)$이다.

증명) 보조정리 1의 명제는 $1\le i\ne j\le v$를 만족하는 모든 i, j에 대하여 $(\alpha\alpha_i)^{(2^s)}=(\alpha\alpha_j)$를 만족하는 정수 s가 존재하지 않는다는 것과 동치이다. 따라서 위의 조건을 만족하는 i와 j가 존재한다고 가정하고, 이 때 명제가 모순이 되는 것을 이용한다. 1절에서 정의한 type-II ONB를 사용하여 $\alpha=\gamma+\gamma^{-1}$라 하면 다음식이 성립한다.

$$(\alpha\alpha_i)^{(2^s)}=(\alpha\alpha_j)$$
$$((\gamma+\gamma^{-1})(\gamma^{2^i}+\gamma^{-2^i}))^{(2^s)}=(\gamma+\gamma^{-1})(\gamma^{2^j}+\gamma^{-2^j})$$

따라서 다음과 같이 전개할 수 있다.

$$(\gamma^{1+2^i}+\gamma^{-(1+2^i)})^{(2^s)}+(\gamma^{-(1-2^i)}+\gamma^{1-2^i})^{(2^s)}$$
$$=(\gamma^{1+2^j}+\gamma^{-(1+2^j)})+(\gamma^{-(1-2^j)}+\gamma^{1-2^j}).$$

위 식에 의하여

$$\begin{cases}(1+2^i)2^s\equiv\pm(1+2^j)\\(1-2^i)2^s\equiv\pm(1-2^j)\end{cases}\qquad(1)$$

또는

$$\begin{cases}(1+2^i)2^s\equiv\pm(1-2^j)\\(1-2^i)2^s\equiv\pm(1+2^j)\end{cases}\qquad(2)$$

을 만족한다.

식 (1)을 다르게 표현하면 다음과 같다.

$$\frac{1+2^i}{1+2^j}\equiv\pm\frac{1-2^i}{1-2^j}$$
$$(1+2^i)(1-2^j)\equiv\pm(1-2^i)(1+2^j)$$

$2^{i+1}\equiv-2^{j+1}$ 또는 $2\equiv2^{(i+j+1)}$. $1\le i\ne j\le v$ 이고 $Z^*_{2m+1}=\leftarrow1,2>$ 에서 $o(2)$값은m이 되고, $Z^*_{2m+1}=<2>$ 에서 $o(2)$값은 $2m$이 되므로 두식이 모두 성립하지 않는다. 따라서 식 (1)을 만족하는 s는 존재하지 않는다. 유사한 방법으로 식 (2)는 다음과 같이 표현된다.

$$2^{i+1}\equiv-2^{j+1}\quad\text{또는}\quad2\equiv-2^{(i+j+1)}.$$

식 (1)과 동일한 이유로 식 (2)는 성립하지 않는다. 따라서 $(\alpha\alpha_i)^{(2^s)}=(\alpha\alpha_j)$를 만족하는 s는 존재하지 않는다. □

다음 따름정리에서 두 번째 기호를 소개한다.

따름정리 1. γ_i를 모든 $1\le i\le v$에 대하여 행렬(λ_{ij})에서 i번째 행을 오른쪽 쉬프트 연산한 횟수라 하자. 만약 (λ_{ij})에서 모든 i번째 행에 각각γ_i만큼 쉬프트 연산을 수행하면 $(\lambda_{ij})_{1\le i\le v,\ 0\le j\le m-1}$ 에서 마지막 열을 제외한 모든 열에 1은 하나씩만 존재한다.

보조정리 1에 의하여 $l(i)$값은 짝수이고 서로 다르다는 것을 알 수 있다. 그러므로 행렬(λ_{ij})의 첫 번째 행부터 v번째 행까지 모든 행에 정확하게 두개의 1이 있고 $l(i)$는 서로 다른 짝수 값을 가지므로 모든 열에 1이 하나씩 존재하도록 곱셈 행렬의 절반 이상 쉬프트 연산을 수행할 수 있다. $\lambda_i=(\lambda_{i0},\lambda_{i1},\cdots,\lambda_{i\,m-1})$ 이고 $(\lambda_i\to\gamma_i)$는 γ_i만큼 오른쪽 쉬프트 연산을 수행한 λ_i라고 하면, 모든 $1\le i\le v$에 대하여 (λ_{ij})의 i번째 행을 γ_i만큼 쉬프트 연산을 수행하여 행렬 (λ_{ij}')을 구할 수 있다:

$$(\lambda_{ij})=\begin{pmatrix}\lambda_0\\\lambda_1\\\vdots\\\lambda_v\\\lambda_{v+1}\\\vdots\\\lambda_{m-1}\end{pmatrix}\Rightarrow(\lambda_{ij}')=\begin{pmatrix}\lambda_0\\(\lambda_1\to\gamma_1)\\\vdots\\(\lambda_v\to\gamma_v)\\\lambda_{v+1}\\\vdots\\\lambda_{m-1}\end{pmatrix}=\begin{pmatrix}\lambda_0\\\underbrace{(\cdots1\ \ 0s\ \ 1\cdots0)}_{l(1)}\\\vdots\\\underbrace{(\cdots1\ \ 0s\ \ 1\cdots0)}_{l(v)}\\\lambda_{v+1}\\\vdots\\\lambda_{m-1}\end{pmatrix}$$

결과적으로 변형된 행렬$(\lambda_{ij}')_{1\le i\le v,\ 0\le j\le m-1}$의 마지막 열의 원소들은 모두 0이 되고, (λ_{ij}')의 첫 번째 행은 $(010\cdots0)$과 같이 표현된다. 그러므로 γ_0 값을 $m-2$로 한다. 위와 같이 쉬프트 연산을 수행한 행렬 $(\lambda_{ij}')_{1\le i\le v,\ 0\le j\le m-1}$은 모든 열에 하나의 1을 가진다.

정리 2. type-II ONB를 사용하면 모든 $0\le i\le v$에 대하여 γ_i를 구할 수 있다.

증명) 보조정리 1과 따름정리 1에 의하여 명제는 자명하다.

알고리즘 1. [2]에서 제안된 구조의 변형된 알고리즘

입력 : $A=(a_0,a_1,\cdots,a_{m-1})$, $B=(b_0,b_1,\cdots,b_{m-1})$
출력 : $C=(c_0,c_1,\cdots,c_{m-1})$

1. $(\lambda_{ij}')_{0\le i\le v,0\le j\le m-1}$의 모든 열 $0\le i\le v$에서 1의 개수가 하나가 되는 적당한 γ_i를 찾는다.
2. A, B를 m비트 저장 공간에 저장 하고,$D_0,D_1,\cdots,D_{m-1}$을 0으로 초기화 한다.
3. $i=0$부터 $m-1$까지 다음과 같이 한다.
   3.1. $D=D^2+G_i(A,B)$.
   3.2. $A\leftarrow A^2$, $B\leftarrow B^2$.
4. m번째 반복 연산하면 모든 $0\le i\le m-1$에 대하여 $AB=\sum_{i=0}^{m-1}c_i\alpha_i$를 만족하는 $D_i=c_i$를 구할 수 있다.

정리 2를 이용 하여 [2]의 방정식을 다음과 같이 수정할 수 있다.

$$\begin{aligned}C&=\sum_{i=0}^{m-1}a_ib_i\alpha_{i+1}+\sum_{i=0}^{m-1}\sum_{j=1}^{v}z_{ij}\cdot\delta_j^{2^i}\\&=\sum_{i=0}^{m-1}a_{i+\gamma_0}b_{i+\gamma_0}\alpha_{i+\gamma_0+1}+\sum_{i=0}^{m-1}\sum_{j=1}^{v}z_{i+\gamma_j,j}\cdot\delta_j^{2^{i+\gamma_i}}\\&=\sum_{i=0}^{m-1}(a_{i+\gamma_0}b_{i+\gamma_0}\alpha_{\gamma_0+1}+\sum_{j=1}^{v}z_{i+\gamma_j,j}\cdot\delta_j^{2^{\gamma_i}})^{2^i}.\end{aligned}$$

$G_i(A,B)$를 다음과 같이 정의하자.

$$G_i(A,B)=a_{i+\gamma_0}b_{i+\gamma_0}\alpha_{\gamma_{0+1}}+\sum_{j=1}^{v}z_{i+\gamma_j,j}\cdot\delta_j^{2^{\gamma_i}}$$

따라서 C는 다음과 같이 표현된다.

$C=((G_{m-1}^2+G_{m-2})^2+\cdots+G_1)^2+G_0$.

$G_{m-t}(A,B)=G_{m-1}(A^{2^{t-1}},B^{2^{t-1}})$에 의하여 곱셈 알고리즘을 얻을 수 있다.

2. 예제

$k=2$일 경우

예를 들어, $GF(2^5)$에서 type-II ONB를 사용하는 경우를 살펴보자. [3]에서 S.Kwon은 $\alpha\alpha_i$를 쉽게 계산하는 방법을 제안했다. 그 방법에 의하여 곱셈 행렬 (λ_{ij})를 구할 수 있다:

$0\le i\le 2$에 대하여 γ_i는 다음과 같다.

$$(\lambda_{ij})=\begin{pmatrix}01000\\10010\\00011\\01100\\00101\end{pmatrix}\rightarrow(\lambda_{ij}')=\begin{pmatrix}00001\\10010\\01100\\01100\\00101\end{pmatrix}$$

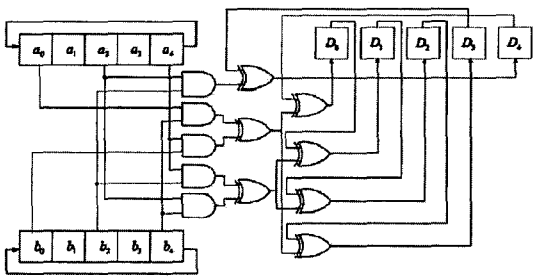

그림 2. 제안하는 변형된 Reyhani-Masoleh, Hasan의 XESMPO

$$\gamma_i=\begin{cases}3, & \text{if } i=0;\\0, & \text{if } i=1;\\3, & \text{if } i=2.\end{cases}$$

$m-1=4$이고 $v=2$이므로 앞 절에서 정의한 식 $G_i(A,B)$는 다음과 같다.

$G_4(A,B)=a_2b_2\alpha_4+z_{4,1}\cdot\delta_1+z_{2,2}\cdot\delta_2^{2^3}$.

[3]에서는 $z_{4,1}$, $z_{4,2}$를 먼저 계산했지만 제안하는 곱셈기는 $z_{4,1}$, $z_{2,2}$를 먼저 계산하고 결과들을 순차적으로 저장한다. 따라서 제안하는 곱셈기의 구조는 그림 2와 같다.

Ⅳ. 복잡도 분석

제안하는 곱셈기는 [3]의 곱셈기와 동일한 공간 복잡도를 가진다. 그리고 type-II ONB를 사용할 경우 제안하는 방법은 [3]의 곱셈기보다 시간 효율성이 향상된다. 따라서 제안하는 방법은 [2]에서 제

안된 곱셈기와 동일한 시간 효율성을 가지지만 많은 공간 효율성을 가진다. 그리고 [4]에서 제안된 곱셈기와 공간 복잡도와 시간 복잡도가 같다. 결과적으로 표 1과 같은 복잡도를 구할 수 있다.

표 1. type-II ONB의 경우 SMPO 곱셈기의 복잡도 분석

	임계 경로 지연	AND	XOR	flip-flop
[2]의 곱셈기	T_A+2T_X	m	$2m-1$	$3m$
[3]의 곱셈기	T_A+3T_X	m	$\frac{3m-1}{2}$	$3m$
[4]의 곱셈기	T_A+2T_X	m	$\frac{3m-1}{2}$	$3m$
제안한 방법	T_A+2T_X	m	$\frac{3m-1}{2}$	$3m$

V. 결 론

유한체 $GF(2^m)$의 type-II ONB에서 [3]에서 제안된 Reyhani-Masoleh, Hasan의 곱셈기를 보다 시간 효율적인 곱셈기를 구성하였다. 제안하는 곱셈기는 [4]의 S.Kwon 곱셈기와 시간과 공간에서 같은 효율성을 가진다. 제안하는 곱셈기를 $k=2$일 경우 뿐 만 아니라 일반적인 type-k에 대하여 확장하여 적용할 수 있기를 기대한다. 하지만 일반적인 type-k에 확장 적용하기 위해서 행렬 $(\lambda_{ij}')_{0\le i\le v0\le j\le m-1}$ 의 각 열에서 1의 개수가 가장 작도록 구성할 수 있다는 것을 보여야 한다.

참 고 문 헌

[1] 정석원, 윤중철, 이선옥 "GF(2^n)에서의 직렬-병렬 곱셈기 구조", 정보보호학회지, 제 13권 3호, pp.27-34, 2003.6.

[2] G.B. Agnew, R.C. Mullin, I. Onyszchuk, and S.A. Vanstone, "An implementation for a fast public key cryptosystem," *J. Cryptology*, Vol.3, pp.63-79, 1991.

[3] A. Reyhani-Masloeh and M.A. Hasan, "Efficient Digit-Serial Normal Basis Multipliers over Binary Extension Fields," *ACM Trans. on Embedded Computing Systems(TECS), Special Issue on Embedded Systems and Security*, pp.575-592, Vol.3, Issue 3, August 2004.

[4] S. Kwon, K. Gaj, C.H. Kim, C.P. hong, "Efficient Linear Array for Multiplication in $GF(2^m)$ Using a Normal Basis for Elliptic Curve Cryptography," *CHES 2004*, LNCS 3156, pp. 76-91, 2004.

[5] E.R. Berlekamp, "Bit-serial Reed-Solomon encoders," *IEEE Trans.* Imform. Theory, Vol. 28, pp. 869-874, 1982.

[6] H. Wu, M.A. Hasan, I.F. Blake, and S. Gao, "Finite field multiplier using redundant representation," *IEEE. Trans. Computers*, Vol 51, pp. 1306-1316, 2002.

[7] A. Reyhani-Masloeh and M.A. Hasan, "A new construction of Massey-Omura parallel multiplier over $GF(2^m)$," *IEEE Trans. Computers*, Vol. 51, pp. 511-520, 2002.

[8] A. Reyhani-Masloeh and M.A. Hasan, "Efficient multiplication beyond optimal normal bases," *IEEE Trans. on Computers*, Vol. 52, pp. 428-439, 2003.

[9] A. Reyhani-Masloeh and M.A. Hasan, "Low Complexity Word-Level Sequential Normal Basis Multipliers," *IEEE Trans. on Computers*, pp 98-110, Vol. 54, no. 2, February 2005.

[10] C. Paar, P. Fleischmann, and P. Roelse, "Efficient multiplier architectures for Galois fields $GF(2^{4n})$," *IEEE Trans. Computers*, Vol. 47, pp. 162-170, 1988.

[11] B. Sunar and C.K. Koc, "An efficient optimal normal basis type-II multiplier," *IEEE Trans. Computers*, Vol. 50, pp. 83-87, 2001.

[12] J.L. Massey and J.K. Omura, "Computational method and apparatus for finite field arithmetic," *US Patent* no. 458627, 1986.

[13] NIST, "Digital Signature Standard," *FIPS Publication*, 186-2, February, 2000.

[14] ANSI, "Public Key Cryptography for the Financial Services Industry: The

Elliptic Curve Digital Signature Algorithm(ECDSA)," *ANSI* x9.62, 1988.
[15] S. Gao, "*Normal Bases over Finite Fields*," A thesis for Doctor of Philosophy, 1993.
[16] Soonhak Kwon, Chang Hoon Kim and Chun Pyo Hong, "Efficient Exponentiation for a Class of Finite Fields Determined by Gauss Periods," *CHES 03*, LNCS, pp. 228-242.

〈著者紹介〉

양 동 진 (Dong Jin Yang) 정회원
1999년 2월: 고려대학교 수학과 졸업
2002년 9월: 고려대학교 정보보호대학원 석사
2005년 2월~현재: 삼성전자 정보통신 총괄
〈관심분야〉 정보보호, 공개키 암호이론, 무선 통신, 암호칩 설계

장 남 수 (Nan Su Chang) 학생회원
2002년 2월: 서울시립대 수학과 학사
2005년 2월: 고려대학교 정보보호대학원 석사
2005년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 공개키 암호 알고리즘, 무선 LAN 기술, 암호칩 설계 기술

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

김 창 한 (Chang Han Kim) 정회원
1985년 2월: 고려대학교 수학과 학사
1987년 2월: 고려대학교 수학과 석사
1992년 2월: 고려대학교 수학과 박사
1992년 3월~현재: 세명대학교 정보보호학과, 정보통신학부 교수
〈관심분야〉 정수론, 공개키 암호, 암호 프로토콜