논문 2006-43SD-2-11

타입 k 가우시안 정규기저를 갖는 유한체의 직렬곱셈 연산기

(A Serial Multiplier for Type k Gaussian Normal Basis)

김 창 한*, 장 남 수**

(Chang Han Kim and Nam Su Chang)

요 약

유한체의 H/W 구현에는 정규기저를 사용하는 것이 효과적이며, 특히 타입 I의 최적 정규기저를 갖는 유한체의 H/W 구현이 효율적이다. Massey-Omura등이 직렬곱셈 연산기를 제안한 이후 Agnew 등이 이를 개선하였으며 최근에 Reyhani-Masoleh 와 Hasan은 공간 복잡도는 크게 개선하였으나 Path Delay 가 조금 늘어난 연산기를 제안하였고, 2004년에는 Kwon 등이 Agnew등의 것과 같은 Path Delay를 가지나 공간 복잡도는 Reyhani-Masoleh 와 Hasan등의 것 보다 조금 더 큰 연산기를 제시하였다. 이 논문에서는 타입 (m,k) 인 가우스 주기를 갖는 유한체 중에서 $GF(mk+1)^* = \langle 2 \rangle$를 만족하는 유한체 $GF(2^m)$은 타입 I 최적 정규기저를 갖는 유한체인 $GF(2^{mk})$의 부분체인 것을 이용하여 Reyhani-Masoleh 와 Hasan의 직렬곱셈 연산기를 재구성하여 같은 면적 복잡도를 유지하면서 XOR Time Delay를 개선한 직렬곱셈 연신기를 구성하였다. 즉, k=4,6 인 경우는 Kwon등의 경우와 같은 Path Delay를 가지나 공간 복잡도 에서 효율적이고, k=10인 경우는 XOR Path Delay en 경우 보다 20% 개선되었고, 공간 복잡도는 Reyhani-Masoleh 와 Hasan의 것과는 같고 Kwon등의 것 보다는 XOR gate 가 32개 줄어든 효율적인 연산기 이다.

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 Gaussian normal basis of type k, which performs multiplication over $GF(2^m)$ in the extension field $GF(2^{mk})$ containing a type-I optimal normal basis. For k=2,4,6 the time and area complexity of the proposed multiplier is the same as tha of the best known Reyhani-Masoleh and Hasan multiplier[1,2].

Keywords: 유한체 연산, 직렬곱셈 연산기, 가우시안 정규기저, 최적정규기저

I. 서 론

유한체는 암호학과 코딩이론 등에 응용되고 있으며, 특히 최근들어 공개키 암호인 타원곡선암호(ECC), XTR, ElGamal 타입 암호등의 관련 응용 분야에 활발하게 사용되고 있는 관계로 유한체의 효율적인 연산 방법이 많은 관심의 대상이 되고 있다[1-2]. 유한체의 연산은 표현방법에 따라 달라지는데, 대표적으로 다항식 기저,[3-6] 정규기저[7-16]등을 이용한 것이고, 또 Noncon-vention 기저[17]를 이용한 것도 사용된다. 특히, H/W 구현에는 정규기저를 이용한 경우 제곱이 Cyclic Shift 에 의하여 이루어지는 등 많은 장점을 가지고 있다. 그 중에서도 기약 AOP(All One Polynomial)에 의해 생성되는 타입 I 최적 정규기저를 갖는 유한체가 가장 효과적으로 구현된다.[9,11,13] Massey-Omura[8]에 의하여 제안된 직렬곱셈 연산기는 병렬입력과 직렬출력(serial out)을 갖는 긴 Path Delay를 갖는 연산기이다. 그래서

* 정회원, 세명대학교 정보보호학과
(Dept. of Information Security, Semyung University)
** 학생회원 고려대학교 정보보호대학원
(Center for Information Security Technologies(CIST), Korea University)
† 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음
접수일자: 2005년10월12일 수정완료일: 2005년2월3일

Agnew 등[7]은 이것을 개선하여 Sequential Multiplier with Parallel Out(SMPO)를 갖는 연산기를 제안하였다. 최근 Reyhani-Masoleh와 Hasan[11,12,13]은 면적 복잡도는 줄었으나 Path Delay가 조금 증가된 SMPO를 제안하였다. 한편, 2004년에 Kwon 등[10]은 Agnew의 연산기를 개선하여 Path Delay는 유지하면서 면적 복잡도는 Reyhani-Masoleh 와 Hasan 의 것과 타입 II 최적 정규기저의 경우는 같고 다른 경우는 더 높은 SMPO를 제시하였다. 한편 Yang 등[16]은 Reyhani- Masoleh 과 Hasan 의 연산기에서 Type II 최적정규 기저를 갖는 경우 정규기저의 곱셈 행렬을 효율적으로 재구성함으로 Kwon 등의 연산기와 같은 Path Delay를 갖는 SMPO를 제안하였다.

본 논문에서는 Reyhani-Masoleh 와 Hasan 의 SMPO에서 Type I 최적 정규기저를 갖는 연산기를 바탕으로 하여 타입 (m, k)인 가우스 주기를 갖고, $GF(mk+1)^*=\langle 2\rangle$인 유한체 $GF(2^m)$가 타입 I65352의 최적 정규기저를 갖는 유한체인 $GF(2^{mk})$의 부분체인 것을 이용하여 SMPO 를 재구성 하였다.

m 이 8의 배수가 아니면 타입 (m,k) 의 가우스 주기를 갖는 k 가 항상 존재 한다[18]는 것은 잘 알려져 있으며, 기초 정수론을 이용하면 m이 홀수이고 $GF(2^m)$이 타입 4인 가우스 주기를 가지면 $GF(4m+1)^*=<2>$인 것을 쉽게 증명된다(참조 Lemma 1). 또한 표준문서 P1363[18], ANSI X9.63[19]의 자료에 수록된 2000이하의 홀수인 m 중에서 $GF(2^m)$이 타입 II, VI, X, XII 의 경우도 이러한 조건을 많이 만족하는 것을 알 수 있다.

그러므로 많은 경우의 유한체에 대하여 $GF(2^m)$의 연산기를 타입 I 확대체인 $GF(2^{mk})$의 연산기를 활용하여 구성할 수 있다. 기본 타입 I 연산기는 Reyhani-Masoleh 와 Hasan[11,12,13]의 연산기를 이용하였고, 타원곡선 암호를 비롯한 암호 응용에서는 m이 소수인 경우를 주로 사용하고 있어서 본 논문에서는 m이 홀수인 경우만 고려하였다.

결론적으로 본 논문에서는 n=mk 이고, 타입 I 최적 정규기저를 갖는 유한체 $GF(2^n)$의 부분체가 되는 타입 (m,k)인 가우스 주기를 갖는 유한체 $GF(2^m)$을 확대체 $GF(2^n)$에서 직렬곱셈 연산기를 작동하여 $GF(2^m)$의 곱셈을 수행하는 구조를 갖는 직렬곱셈 연산기를 제안하였으며, 타입 k= 4, 6, 10, 12등 모든 경우 공간 복잡도는 Reyhani-Masoleh 와 Hasan의 것과 같고 Kwon 등의 것 보다는 작다. XOR Path delay 는 모든 경우 Reyhani-Masoleh 과 Hasan 의 것 보다는 빠르고 k=4 의 경우는 Kwon 의 것과 같으며 k=10 의 경우는 20% 개선된 더 빠른 효과적인 연산기 이다.

II. 수학적 배경

1. 유한체의 정규기저를 이용한 표현과 곱셈

양의 정수 l 에 대하여 유한체 $GF(2)$위에서 $GF(2^l)$의 정규기저가 존재한다는 것은 잘 알려진 결과이다[2,20]. 즉, $\beta\in GF(2^l)$가 존재하여 $N=\{\beta, \beta^2, \dots, \beta^{2^{l-1}}\}$이 $GF(2)$위에서 $GF(2^l)$의 기저 일 때 N를 정규기저라 하고 β를 정규기저 생성자라 한다.

이 경우, $A\in GF(2^l)$ 에 대하여

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

로 표현되며 간단히 $A=(a_0, a_1, \dots, a_{l-1})$와 같이 좌표로도 표현한다. 또한 벡터(행렬)표현으로

$$A=\bar{a}\times\bar{\beta}^{\,T}=\bar{\beta}\times\bar{a}^{\,T},\ \bar{a}=(a_0\ a_1\ \dots\ a_{l-1})$$
$$\bar{\beta}=(\beta\ \beta^2\ \dots\ \beta^{l-1}).$$

그리고 T 는 행렬의 치환(Transpose)을 나타낸다. 그리고 정규기저의 특징이자 장점은 A^2 이 Right Cyclic Shift(RCS)에 의하여 주어진다는 것이다. 즉, $A^2=(a_{l-1}\ a_0, \dots, a_{l-2})$.

$A, B\in GF(2^l)$, $C=AB$ 라 하자. 그러면

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

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

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

A^2 이 cyclic shift 인 것을 이용하면 $C=AB=(c_0,$

$c_1, \ldots, c_{l-1}$)의 값은 다음과 같이 얻어진다.

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

이 같은 결과에 의하여 각 i 에 대하여 행렬 M_i 의 1의 개수는 모두 같음을 알 수 있고 이때 M_0 의 1의 개수를 정규기저 B 의 복잡도라 하고 C_N 으로 표시한다. 또한 Gao등은 다음과 같은 결과를 증명하였다[2,20].

정리 1. $C_N \geqq 2l-1$ [2,20].

이 논문에서는 모든 유한체는 정규기저에 의하여 표현되는 것으로만 고려한다.

2. 가우시안 정규기저

m, k 는 양의 정수, p = mk +1 $\neq$ 2 인 소수, 그리고 e 를 $GF(p)^*$ 에서 2의 위수(order), (mk/e, m) = 1 라 하자. 그리고 $GF(2^{mk})$에서 p의 원시근(a primitive nth root of unity)을 γ, kth root of unity를 τ 라 하고 $\beta = \gamma + \gamma^{\tau} + \gamma^{\tau^2} + \ldots + \gamma^{\tau^{k-1}}$로 놓으면 β는 $GF(2^m)$의 정규기저 생성자 이다[2,20]. 즉, $\{\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{m-1}}\}$는 GF(2) 위에서 $GF(2^m)$의 정규기저이다. 이때 β를 GF(2) 위에서 타입 (m, k)인 가우스 주기(Gauss period of type (m, k)) 라 한다.[18,19] 우리는 이 논문에서 $GF(2^m)$이 타입 (m,k)인 가우스 주기를 갖는 경우, $GF(2^m)$을 타입 k 라 한다. 정리1에서 $C_N = 2m-1$일 때 정규기저 N을 최적정규기저 (Optimal Normal Basis, ONB) 라 한다. 가우시안 정규기저에서 k= 1, 2인 경우 $C_N = 2m-1$을 만족하는 것은 잘 알려져 있다.[2,18,19,20] 이때 k=1인 경우를 타입 I 최적 정규기저, k=2인 경우를 타입 II의 최적 정규기저라 한다. 모든 계수가 1인 다항식을 All-One-Polynomial(AOP) $x^n + x^{n-1} + \ldots + x + 1$이라 한다.

정리2. (타입 I 최적 정규기저)

$GF(2)$위에서 $GF(2^n)$ 이 타입 I 의 최적 정규기저를 갖기 위한 필요충분조건은 n+1 이 소수이고 $GF(n+1)^* = \langle 2 \rangle$이다. 또는 n 차의 AOP $x^n + x^{n-1} + \ldots + x + 1$가 $GF(2)$위에서 기약다항식인 경우 AOP의 근이 최적 정규기저의 생성자이다[2,20].

Lemma 1. m 이 홀수이고 $GF(2^m)$이 타입 IV 이면 $GF(4m+1)^* = \langle 2 \rangle$ 이다.

증명. $GF(2^m)$이 타입 IV 이므로 $4m+1$은 소수이고 e 를 $GF(4m+1)^*$에서 2의 위수라 하면 (4m/e, m) = 1이다. 따라서 $e = m,\ 2m,\ 4m$ 이다. 그리고 $GF(4m+1)^* = \langle g \rangle$, $2 = g^t, 0 \leqq t < 4m$ 라 하면 $e = 4m/(t, 4m)$이다. 그러므로 $e = m, 2m$인 경우 t는 짝수이다. 즉, quadratic residue 이다. 그러나 m이 홀수이므로 $4m+1$은 $8k+5$ 이므로 2는 non-quadratic residue 이므로 모순이다. 따라서 2의 위수는 $4m$ 이다.

3. 부분체와 확대체와의 관계

n=mk 인 경우 유한체 $GF(2^m)$은 $GF(2^n)$ 의 부분체이다. 이 경우 $A \in GF(2^m)$가 $GF(2^n)$에서 어떻게 표현되는지 살펴보자. 유한체의 기본 성질에 의하면 $B \in GF(2^n)$ 인 경우, $B \in GF(2^m)$ 이기위한 필요충분조건은 $B^{2^m} = B$ 이다. 따라서 정규기저를 사용하여 표현할 경우 제곱이 Right Cyclic Shift(RCS)인 것을 이용하면 다음과 같은 결과를 얻을 수 있다. 앞으로 $A \in GF(2^n)$ 를 좌표로 표현하면

$$A = (a_0,\ a_1,\ \ldots,\ a_{n-1}), a_i \in GF(2)$$

와 같다.

정리 3. $B = (b_0, b_1, \ldots, b_{n-1}) \in GF(2^n)$라 하자. 그러면 $B \in GF(2^m)$ 이기위한 필요충분조건은 $0 \leqq i, t < mk$ 에 대하여 $i \equiv t \ mod\ m$ 이면 $b_i = b_t$ 이다.

즉, $(b_0, b_1, \ldots, b_{m-1}, \cdots, b_0, b_1, \ldots, b_{m-1})$.

앞으로 이 논문에서는 m 은 홀수, n = mk, n+1 은 소수 이고 $GF(n+1)^* = \langle 2 \rangle$ 인 경우 만 고려하자. 이때 γ를 n+1 의 원시근 이라 하면 정리2 에 의하

여 γ는 $GF(2^n)$의 타입 I 의 최적정규 기저 생성자이다. 그리고 이 경우 e = mk, τ = 2^m 이므로 (m, k)는 가우스 주기이고

$$\beta = \gamma + \gamma^{2^m} + \gamma^{2^{2m}} + \ldots + \gamma^{2^{m(k-1)}}$$

는 GF(2) 위에서 $GF(2^m)$ 의 정규기저 생성자이다. 그러므로 원소 A $\in GF(2^m)$는

$$A = A_0\beta + A_1\beta^2 + A_2\beta^{2^2} + \ldots + A_{m-1}\beta^{2^{m-1}},$$
$$A_i \in GF(2)$$

와 같이 표현된다. 그리고 $GF(2^m)$는 $GF(2^n)$의 부분체이므로

$$\begin{aligned} A = &A_0\gamma + A_1\gamma^2 + A_2\gamma^{2^2} + \ldots + A_{m-1}\gamma^{2^{m-1}} \\ &+ A_0\gamma^{2^m} + A_1\gamma^{2^{m+1}} + \ldots + A_{m-1}\gamma^{2^{2m-1}} \\ &+ \ldots + \\ &+ A_0\gamma^{2^{m(k-1)}} + A_1\gamma^{2^{m(k-1)+1}} + \ldots + A_{m-1}\gamma^{2^{mk-1}} \\ &\in GF(2^n) \end{aligned}$$

이다. 그리고

$$A = a_0\gamma + a_1\gamma^2 + a_2\gamma^{2^2} + \ldots + a_{mk-1}\gamma^{2^{mk-1}} \in GF(2^n)$$

라 하면

$$a_{i+mj} = A_i,\ 0 \leqq i \leqq m-1,\ 0 \leqq j \leqq k-1 \quad (2)$$

이다. 마찬가지로

$$B = B_0\beta + B_1\beta^2 + B_2\beta^{2^2} + \ldots + B_{m-1}\beta^{2^{m-1}} \in GF(2^m)$$

라 하고

$$B = b_0\gamma + b_1\gamma^2 + b_2\gamma^{2^2} + \ldots + b_{mk-1}\gamma^{2^{mk-1}} \in GF(2^n)$$

라 하면 (2) 식과 같은 성질을 만족한다.

Ⅲ. Reyhani-Masoleh and Hasan의 AOP를 이용한 직렬 곱셈기

Ⅲ장에서는 Reyhani-Masoleh 와 Hasan[11,12,13]의 연산기 에서 AOP의 경우에 적용한 유한체의 직렬 곱셈기의 구조를 살펴보고자 한다. $GF(2^n)$이 타입 I 의 최적정규기저인 경우에 적용한 직렬 곱셈기를 살펴보자. 즉, $GF(2^n)$은 기약다항식 AOP $x^n + x^{n-1} + \cdots + x + 1$에 의하여 생성된 유한체이고 AOP의 근을 γ라 하면 γ는 $GF(2^n)$의 타입 I 의 최적 정규기저를 생성한다. 이 경우 n 은 짝수이고 $\delta_i = \gamma^{1+2^i}$, $i = 1, 2, \cdots, v = n/2$ 라 하자. 그러면 γ 가 AOP의 근인 성질을 이용하여 다음과 같은 Lemma를 얻을 수 있다.

Lemma 2.

$$\delta_i = \begin{cases} \gamma^{2^{k_i}}, & i = 1, 2, \cdots, n/2 - 1 \\ 1 = \sum_{j=0}^{n-1} \gamma^{2^j} & , i = v = n/2 \end{cases},$$

여기서 k_i는 $2^i + 1 \equiv 2^{k_i} \ mod\ n+1$을 만족하는 값이다.

Ⅱ장에서와 같이 $GF(2^n)$에서의 곱 $C = AB$ 를 계산하는 경우를 고려하자. Reyhani-Masoleh 와 Hasan은 유한체의 곱의행렬 $M = (\beta^{2^i + 2^j})$과

$$\delta_i = \beta^{1+2^i},\ i = 1, 2, \cdots,\ v = \lfloor l/2 \rfloor$$

와 β^{2^j}, $0 \leq j \leq m-1$ 를 이용하여 다음의 Lemma를 제시 하였다. 이 논문에서는 $<< i >>$는 $i\ mod\ n$을 $((i))$는 $i\ mod\ m$을 나타낸다.

Lemma 3. $GF(2^n)$은 타입 I의 최적 정규기저를 갖는 유한체이고 γ 를 이 정규기저의 생성자라 하자. 그리고 $A, B \in GF(2^n)$, $C = AB$ 라 하면

$$C=\sum_{j=0}^{n-1} a_{j-g} b_{j-g}\gamma^{2^j}+\sum_{i=1}^{v-1}\left(\sum_{j=0}^{n-1} x_{j,i}\gamma^{2^j}\right)^{2^{k_i}}$$
$$+\sum_{j=0}^{n-1}\left(\sum_{i=1}^{v-1} x_{i,v}\right)\gamma^{2^j},\ v=n/2\ ,$$
$$x_{j,i}=\begin{cases} a_j b_{\ll i+j \gg}+a_{\ll i+j \gg} b_j & \text{if } g=1 \\ (a_j+b_{<<i+j\gg})(b_j+b_{<<i+j\gg}) & \text{if } g=0 \end{cases}$$

Ⅳ. 타입 (m,k)의 가우시안 정규기저를 갖는 유한체의 연산기

1. 새로운 연산기

Ⅲ 장에서 언급한 바와 같이 $GF(2^m)$은 타입 k 인 가우시안 정규 기저를 갖고 $GF(n+1)^*=<2>$, n=mk 인 경우를 고려한다. 여기서 m이 홀수인 경우만 고려하므로 k는 짝수이다. 우리의 생각은 $GF(2^m)$의 원소 A, B 를 확대체인 타입 I 의 최적 정규기저를 갖는 $GF(2^n)$의 부분체의 원소로 생각하여 Ⅲ장의 연산기에 적용하여 A, B 의 곱셈 연산기를 구현하고자 한다.

먼저 ς_i 를 정의 하자.

정의1. n=mk, n+1 은 소수, $GF(n+1)^*=<2>$라 하고 k_i 는 Lemma 2의 값이라 하자. 이때 $1 \leqq i_0 \leqq u=(m-1)/2$에 대해

$$i \in \{i_0,\ m-i_0,\ m+i_0,\ \ldots,\ km/2-i_0\}$$

인 경우 다음과 같이 ς_i 를 정의 한다.

$$\varsigma_i=\begin{cases} k_i \ mod\ m, & i \equiv i_0 \ mod\ m \\ k_i+i_0 \ mod\ m, & i \equiv -i_0 \ mod\ m \end{cases} \quad (3)$$

이것을 이용하여 다음의 정리를 얻을 수 있다.

정리 4. $GF(2^m)$은 타입(m, k)인 가우스 주기를 갖고, n = mk, $GF(n+1)^*=<2>$ 라 하자. 이 경우 $A, B \in GF(2^m) \subset GF(2^n)$, $C=AB$ 이면

$$C=\sum_{j=0}^{m-1} A_{j-g} B_{j-g}\beta^{2^j}$$
$$+\sum_{i_0=1}^{u}\left(\sum_{w=0}^{k/2-1}\left(\sum_{j=0}^{m-1} x_{j,i_0}\beta^{2^j}\right)^{2^{\varsigma_{wm+i_0}}}\right.$$
$$\left.+\sum_{w=1}^{k/2}\left(\sum_{j=0}^{m-1} x_{j,i_0}\beta^{2^j}\right)^{2^{\varsigma_{wm-i_0}}}\right),$$
$$x_{j,i}=\begin{cases} A_j B_{((i+j))}+A_{((i+j))} B_j & \text{if } g=1 \\ (A_j+A_{((i+j))})(B_j+B_{((i+j))}) & \text{if } g=0 \end{cases}$$

증명. g=1인 경우 만 증명하자. A, B $\in GF(2^m) \subset GF(2^n)$ 라 하자. 그러면 (2)에서와 같이

$$a_j=A_{((j))},\ b_j=B_{((j))},\ 0 \leqq j \leqq n-1.$$

먼저, $a_i b_i=A_{((i))}B_{((i))}$, $0 \leqq i \leqq n-1$ 이므로 n 개를 계산하여야 하나 (2) 식에 의하여 m개인 A_iB_i, $0 \leqq i \leqq m-1$만 계산하면 된다.

두 번째로 $i=wm,\ 1 \leqq w \leqq km/2$ 인 경우

$$\begin{aligned} x_{j,i} &= (a_j b_{\ll i+j \gg})+(a_{\ll i+j \gg} b_j) \\ &= A_{((j))}B_{((wm+j))}+A_{((wm+j))}B_{((j))} \\ &= A_{((j))}B_{((j))}+A_{((j))}B_{((j))} \\ &= 0. \end{aligned}$$

그리고 마지막으로

$$\begin{aligned} x_{j\,i} &= (a_j b_{\ll j+i \gg})+(a_{\ll j+i \gg} b_j) \\ &= (A_j B_{((j+i))}+(A_{((j+i))}B_j) \\ &= x_{((j)),((i))} \end{aligned}$$

이다.

따라서 $1 \leqq i \leqq (m-1)/2$ 에 대해,

$$\sum_{j=0}^{n-1} x_{j,i}\gamma^{2^j}=\sum_{t=0}^{k-1}\left(\sum_{j_0=0}^{m-1} x_{j_0,i}\gamma^{2^{j_0}}\right)^{2^{tm}}$$
$$\equiv \sum_{j_0=0}^{m-1} x_{j_0,i}\beta^{2^{j_0}} \quad \text{이므로}$$

$$\sum_{i=1}^{v-1}\left(\sum_{j=0}^{n-1}x_{j,i}\gamma^{2^j}\right)^{2^{k_i}}=\sum_{i=1}^{v-1}\left(\sum_{j_0=0}^{m-1}x_{j_0,i}\gamma^{2^{j_0}}\right)^{2^{tm}}$$
$$=\sum_{j_0=0}^{m-1}\left(\sum_{i=1}^{v-1}x_{j_0,i}\beta^{2^{k_i}}\right)^{2^j}$$

$1 \leqq i_0 \leqq u=(m-1)/2$에 대해

1) $i=wm+i_0,\ 0 \leqq w \leqq k/2-1$,

2) $i=wm-i_0,\ 1 \leqq w \leqq k/2$

인 경우로 나누어 생각하자.

1)의 경우

$$\begin{aligned}x_{j,i} &= x_{j,\,wm+i_0}\\ &= a_j b_{\ll j+wm+i_0 \gg}+a_{\ll j+wm+i_0\gg}b_j\\ &= A_{((j))}B_{((j+i_0))})+A_{((j+i_0))}B_{((j))}\\ &= x_{((j)),i_0}\end{aligned}$$

2)의 경우

$$\begin{aligned}x_{j,i} &= x_{j,\,wm-i_0}\\ &= a_j b_{\ll j+wm-i_0 \gg}+a_{\ll j+wm-i_0\gg}b_j\\ &= A_{((j))}B_{((j-i_0))})+A_{((j-i_0))}B_{((j))}\\ &= x_{((j-i_0)),i_0}\ .\end{aligned}$$

그러므로

$$AB=C$$
$$=\sum_{j_0=0}^{m-1}A_{j-g}B_{j-g}\beta^{2^j}+\sum_{j_0=0}^{m-1}\left(\sum_{i=1}^{v-1}x_{j,i}\beta^{2^{k_i}}\right)^{2^j}$$
$$=\sum_{j_0=0}^{m-1}A_{j-g}B_{j-g}\beta^{2^j}+$$
$$\sum_{j=0}^{m-1}\left(\sum_{i_0=1}^{u}x_{j,i}\left(\sum_{w=0}^{k/2-1}\beta^{2^{k_{wm+i_0}}}+\sum_{w=1}^{k/2}\beta^{2^{k_{wm-i_0}+i_0}}\right)\right)^{2^j}.$$

위 정리에서

$$G_j(A,B)=A_{j-g}B_{j-g}\beta$$
$$+\sum_{i_0=1}^{u}x_{j,i_0}\left(\sum_{w=0}^{k/2-1}\beta^{2^{k_{wm+i_0}}}+\sum_{w=1}^{k/2}\beta^{2^{k_{wm-i_0}+i_0}}\right)$$ 라 하면

$$C=((G_{m-1}^2+G_{m-2})^2+\cdots+G_1)^2+G_0,$$
$$G_{m-t}(A,B)=G_{m-1}(A^{2^{t-1}},B^{2^{t-1}})$$

을 만족 한다. 그리고 각 j 에 대하여 i_0당 k 번의 β^{2^t}가 등장하므로 최대 $ku+1$개의 항이 생길 수 있다. 그러나 i_0당 같은 β^{2^t}가 나타날 경우는 같은 값을 두 번 더하는 것이므로 삭제하면 된다. 그러므로 위의 정리에서 M =

$$|\{\beta\}|+\sum_{i_0=1}^{u}|\{\beta^{2^{\varsigma_{i_0}}},\beta^{2^{\varsigma_{m-i_0}}},\beta^{2^{\varsigma_{m+i_0}}},\cdots,\beta^{2^{\varsigma_{(k/2)m-i_0}}}\}|+\epsilon u,$$
$$\epsilon=\begin{cases}1 & if\ \ g=1\\ 2 & if\ \ g=0\end{cases}$$

이 serial 곱셈기의 XOR의 개수를 나타내고 $l=Max_{j=0,m-1}M_j+1$,

$$M_j=|\{wm+i_0|\varsigma_{wm+i_0}=j,0\leqq w<k/2\}|$$
$$+|wm-i_0|\varsigma_{wm-i_0}=j,1\leqq w\leqq k/2|+t,$$
$$t=\begin{cases}1 & if\ j=0\\ 0 & if\ j\neq 0\end{cases}$$

이 XOR 의 Path Delay를 결정하므로 l 값을 작게 하기 위하여 다음과 같은 보조정리를 생각하자.

Corollary 1. $GF(2^m)$은 타입(m, k)인 가우스 주기를 갖고, n = mk, $GF(n+1)^*=<2>$라 하자. $A,B\in GF(2^m)\subset GF(2^n)$, $C=AB$ 이면

$$C=\sum_{j=0}^{m-1}\left(A_{j+j_0-g}B_{j+j_0-g}\beta^{2^{j_0}}\right)^{2^j}$$
$$+\sum_{j=0}^{m-1}\left(\sum_{i_0=1}^{u}x_{j+j_{i_0},i_0}\left(\sum_{w=0}^{k/2-1}\beta^{2^{\varsigma_{wm+i_0}+j_{i_0}}}\right.\right.$$
$$\left.\left.+\sum_{w=1}^{k/2}\beta^{2^{\varsigma_{wm-i_0}+j_{i_0}}}\right)\right)^{2^j},$$
$$x_{j,i}=\begin{cases}A_jB_{((i+j))}+A_{((i+j))}B_j & \text{if } g=1\\ (A_j+A_{((i+j))})(B_j+B_{((i+j))}) & \text{if } g=0\end{cases}$$

증명. 각 i_0에 대하여 j_{i_0}, 그리고 j_0 만큼의 쉬프팅을

하면

$$C=\sum_{j=0}^{m-1}(A_{j-g}B_{j-g}\beta^{2^{j_{i_0}}})^{2^{j-j_{i_0}}}+\sum_{i_0=1}^{u}(\sum_{j=0}^{m-1}x_{j,i_0}(\sum_{w=0}^{k/2-1}\beta^{2^{\varsigma_{wm+i_0}+j_{i_0}}}+\sum_{w=1}^{k/2}\beta^{2^{\varsigma_{wm-i_0}+j_{i_0}}})^{2^{j-j_{i_0}}}.$$

이므로 $j-j_{i_0}$ 를 다시 j 로 정리하면 Corollary 가 얻어진다.

$$G_j(A,B)=A_{j+j_0-g}B_{j+j_0-g}\beta^{2^{j_{i_0}}}+\sum_{i_0=1}^{u}x_{j+j_{i_0},i_0}(\sum_{w=0}^{k/2-1}\beta^{2^{\varsigma_{wm+i_0}+j_{i_0}}}+\sum_{w=1}^{k/2}\beta^{2^{\varsigma_{wm-i_0}+j_{i_0}}})$$

라 하면 보조정리에 의하여

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

이 경우 l 에서 β 의 쉬프팅은 각 i_0에 대한 쉬프팅 수행을 통한

$$l'=Max_{j=0,m-1}M_j+1,$$
$$M_j=|wm+i_0|\varsigma_{wm+i_0}+j_{i_0}=j,0\le w<k/2|$$
$$+|\{wm-i_0|\varsigma_{wm-i_0}+j_{i_0}=j,1\le w\le k/2\}|$$

의 값을 구한 다음 $j_0\ne l'$ 인 j_0를 선택하면 되므로 Path Delay를 결정하는 값은 l' 이다.

2. 최적화

실제적 구현시 $1\le i_0\le u=(m-1)/2$에 대하여

$$i=i_0,m-i_0,\ m+i_0,\dots,km/2-i_0 \tag{4}$$

인 경우 정리 4에서 i 에 대하여 ς_i 중 2개의 같은 경우 S_i 의 출력값이 같으므로 그 2개를 삭제하여도 결과가 같다. 이같은 사항을 고려하여 구현할 경우 XOR gate 수와 Path Delay를 줄일 수 있다. 즉, 위의 각 i_0 에 대하여 모든 i 에 대한 ς_i 가 같은 것이 있는지 확인 한다. 다음의 $GF(2^m)$ 은 k 타입의 가우시안 정규기저를 갖고 $GF(km+1)^*=<2>$ 를 만족한다.

1) k =4 인 경우를 살펴보자.

Lemma 4. (k=4인 경우) m이 홀수, p=4m+1 은 소수, $GF(p)^*=<2>$ 라 하자.

그리고 u = (m-1)/2 에 대하여, $Z_p^*=<2>$에서

$$\begin{cases}2^u+1=2^{k_1}, & 2^{m-u}+1=2^{k_2},\\ 2^{m+u}+1=2^{k_3}, & 2^{2m-u}+1=2^{k_4}\end{cases}$$

라 하면 다음 두식 중 하나가 성립한다.

$$k_1=k_2+u \ mod\ m,\ k_3=k_4+u\ mod\ m\ .$$

증명. $(1+2^m)^2=2^{m+1}=(2^{u+1})^2$ 이므로 $1+2^m=\pm 2^{u+1}$. 먼저 이것을 이용하여 $2^{m+u}-2^u=\pm 1$이 됨을 증명하자.

$2^{2m}=-1$ 인 것을 이용하면

$$\begin{aligned}2^{m+u}-2^u&=2^{m+u}+2^{2m+u}\\&=2^{m+u}(1+2^m)\\&=\begin{cases}2^{m+2u+1}, & if\ 1+2^m=2^{u+1}\\ -2^{m+2u+1}, & if\ 1+2^m=-2^{u+1}\end{cases}\\&=\begin{cases}-1, & if\ 1+2^m=2^{u+1}\\ 1, & if\ 1+2^m=-2^{u+1}\end{cases}.\end{aligned}$$

다음은 $1+2^m=2^{u+1}$ 와 $1+2^m=-2^{u+1}$ 인 경우로 나누어 Lemma를 증명하자.

1) $1+2^m=-2^{u+1}$인 경우, $2^u+1=2^{m+u}$이므로

$$2^{m-u}+1=2^{u+1}+1=-(2^m+1)+1=-2^m=2^{3m}.$$

2) $1+2^m=2^{u+1}$ 인 경우, $2^{m+u}+1=2^u$이므로

$$2^{2m-u}+1=2^{m+u+1}+1=2^m2^{u=1}+1=2^{m(1+2^m)}+1=2^m.$$

그러므로 Lemma가 성립한다.

따라서 g=1인 경우 타입 4 는 $M=(5m-7)/2$ 개의 XOR gate 가 필요하다. 한편 최적의 l' 값을 계산하기 위하여 각 $i_0 \neq u$ 에 대해 4개의 서로 다른 $\varsigma_{i_0}, \varsigma_{m-i_0}, \varsigma_{m+i_0}, \varsigma_{2m-i_0}$ 가 $i_0 = u$인 경우는 2개가 존재하므로 전체는 $2m-4$이다. 즉 $\sum_{i=1}^{u} M_i - 1 =$. $2m-4$. 이것을 m 개의 열에 보조정리 1 과 같이 각 i_0 를 j_{i_0} 만큼의 쉬프팅을 한 후의 최적의 l' 값을 고려하면 2보다 작을 수는 없다. 그리고 $\beta^{2^{j_0}}$ 의 경우 l'보다 작은 1을 갖는 j_0 열을 선택하면 된다. 기존의 결과에 의하면 type k 인 경우 $l=k+1$ 이고 Path Delay는 $\lceil \log l' \rceil$ 이므로 l'=4 가 최적의 값이다. 2000 이하의 모든 대상인 m 은 이것을 만족하는 $j_0, j_{i_0}, i_0 = 1, \cdots, u$ 를 갖는다는 것을 확인 하였다.

2) k=6인 경우를 살펴보자.

타입 k=6을 만족하는 2000 이하의 m 대하여 (4)식의 i 에 대한 ς_i 가 같은 쌍이 4개 나타난다. 먼저 i_0 에 대하여 (4)식의 i_1, i_2에 대한 ς_i 가 같을 때를 $\{i_0, i_1, i_2, \varsigma_i\}$ 로 표현하자. 그러면 m=103인 경우,

$$\{1, 2*103-1, 2*103+1, 89\},$$
$$\{14, 14, 103-14, 14\},$$
$$\{14, 103+14, 2*103-14, 15\},$$
$$\{15, 15, 103-15, 14\}$$ 이다.

이것을 이용하여 다음의 Conjecture 1을 얻을 수 있다.

Conjecture 1.(k=6인 경우) m이 홀수, p=6m+1 은 소수, $GF(p)^* = < 2 >$ 라 하자. $1 \leq i_0 \leq u = (m-1)/2$에 대하여, $i = i_0, m-i_0, m+i_0, ..., km/2 - i_0$ 일 때 ς_i 가 같은 쌍이 4개 존재 한다.

그러므로 타입 6의 경우는 $M=(7m-13)/2$ 개의 XOR gate 가 필요하다. 그리고 타입 4의 경우와 같이 $\sum_{i=1}^{u} M_i - 1 = 3m - 11$이고 또한 $l = 7$ 이므로 $l' = 3$인 경우가 최적이나 얻어지지 않으므로 l' = 5,6,7 이 같은 Path Delay를 가지므로 무엇이든 같다.

3) k=10, 12 인 경우 m 을 보자.

타입 k=10, 12를 만족하는 2000 이하의 m 대하여 (4)식의 i 에 대한 ς_i 가 같은 쌍이 각각 16, 25개 나타난다.

Remark 1. (k=10, 12인 경우) m이 홀수, p=10m+1 또는 12m+1이 소수, $GF(p)^* = < 2 >$ 인 경우를 살펴보며.

$1 \leq i_0 \leq u = (m-1)/2$에 대하여, $i = i_0$, $m - i_0,\ m + i_0, ..., km/2 - i_0$ 일 때

ς_i 가 같은 쌍이 k=10이면 16 개, k=12 이면 25개 존재한다. 따라서 타입 10의 경우 $M=(11m-41)/2$, 12의 경우 $M=(13m-61)/2$개의 XOR gate 가 필요하다. 그리고 타입 10의 경우 $\sum_{i=1}^{u} M_i - 1 = 5m - 37$ 이므로 $l' = 8$인 경우가 적당한 값이며 2000 이하에 대하여 모두 존재하는 것을 확인 하였다. 또한 비슷한 방법으로 type k 인 경우도 계산할 수 있다.

V. 복잡도 계산

정리 4와 Corollary 1을 중심으로 구성한 serial multiplier의 복잡도를 살펴보면 다음과 같다.

정리5. 정리 4와 Corollary 1을 이용한 직렬곱셈 연산기의 복잡도의 최대값은 다음과 같다.

a) g=1 인 경우 : m AND gate 그리고 $(k+1)(m-1)/2 + 1$ XOR gate.

a)' g=0 인 경우 : $(m+1)/2$ AND gate, 그리고 $(k+2)(m-1)/2 + 1$ XOR gate.

b) $T_A + (1 + \lceil \log_2 l' \rceil) T_X$, T_A 는 AND delay, T_X 는 XOR Delay 이다.

증명. a) 먼저 AND gate 수를 살펴보면 $A_{j-1}B_{j-1}$계산에 1번, 각 $1 \leq i_0 \leq u = (m-1)/2$ 에 대하여 x_{j,i_0} 계산에 2번 즉 $m-1$번 이므로 전체는 m 번이 필요하다. 그리고 XOR gate는 각 $1 \leq i_0 \leq u = (m-1)/2$ 에 대하여 x_{j,i_0} 계산에 각 1번 즉, $(m-1)/2$번이 필요하고 $G_j(A,B)^2 + G_{j-1}(A,B)$에서 x_{j,i_0}의 계산은 제외하고 계산하는데 $1 + k(m-1)/2$ 번의 연산이 필요하므로 전체는 $(k+1)(m-1)/2 + 1$개의 XOR gate 가 필요하다.

a)' AND gate 는 y_{j,i_0}에 $(m-1)/2$번 A_jB_j에 1번 따라서 전체는 $(m+1)/2$ 번이다. 그리고 XOR gate 는 $1 \leqq i_0 \leqq u = (m-1)/2$ 에 대하여 x_{j,i_0} 계산에 각 1번 즉, $(m-1)/2$번이 필요하고 $G_j(A,B)^2 + G_{j-1}(A,B)$에서 x_{j,i_0}의 계산은 제외하고 계산하는데 $1+k(m-1)/2$ 번의 연산이 필요하므로 전체는 $(k+2)(m-1)/2+1$개의 XOR gate 가 필요하다.

b) Path Delay의 경우는 AND gate는 1번에 이루어지고 XOR gate는 x_{j,i_0} 에 1번, 그리고 $G_j'(A,B)^2+G_{j-1}'(A,B)$ 에서 x_{j,i_0}의 계산은 제외하고 기저 β^{2^j}에서 최대 XOR 의 개수가 l' 이므로 전체 XOR Path Delay는 $1+\lceil log_2 l' \rceil$ 이다.

Corollary 2. Corollary 1의 연산기 에서 타입 4 의 최적 정규 기저를 갖는 유한체 $GF(2^m)$의 복잡도는 다음과 같다.

a) g=1 인 경우 : m AND gate, $(5m-7)/2$ XOR gate.

a)' g=0 인 경우 : $(m+1)/2$ AND gate, 그리고 $3m-4$ XOR gate.

b) $T_A + (1+\lceil \log_2 l' \rceil)T_X = T_A + 3T_X$.

증명. a) Lemma 3에 의하여 $i_0 = u$인 경우 β^{i_0} 와 β^{m-i_0} 또는 β^{m+i_0} 와 β^{2m-i_0}가 같으므로 XOR gate 수는

$$(4+1)(m-1)/2+1-2 = (5m-7)/2$$
$$= (C_N+1)/2 + \lfloor m/2 \rfloor .$$

a)' a)와 비슷하게 얻어진다.

b) III.2의 최적화에 의하여 $l' = 3$이 되도록 Corollary 1과 같이 쉬프팅이 가능하므로 Path Delay는 $T_A + 3T_X$ 이다.

Corollary 3. Corollary 1의 연산기에서 타입 6 의 최적

표 1. Type k를 갖는 유한체의 정규 기저에 의한 직렬곱셈 연산기의 복잡도 비교(l' 은 $IV.1$에 주어짐)
Table 1. Comparison of Sequential Multipliers for type k Gaussian Normal Basis(l' is defined in $IV.1$).

Multipliers		#AND	#XOR	Critical Path Delay
MO [8]		C_N	$\leqq (C_N-1)$	$T_A + \lceil log_2(mk) \rceil T_X$
Agnew등 [7]		m	$\leqq C_N$	$T_A + (1+\lceil log_2 k \rceil T_X$
Reyhani-Masoeh and Hasan[13](g=1)	General	m	$\leqq (C_N+1)/2 + \lfloor m/2 \rfloor$	$T_A + (1+\lceil log_2(k+1) \rceil T_X$
	Type IV	m	$(5m-7)/2$	$T_A + 4T_X$
	Type X	m	$(11m-73)/2$	$T_A + 5T_X$
Reyhani-Masoeh and Hasan[13](g=0)	General	$(m+1)/2$	$\leqq (C_N+2m-1)/2$	$T_A + (1+\lceil log_2(k+1) \rceil T_X$
	Type IV	$(m+1)/2$	$3m-4$	$T_A + 4T_X$
	Type X	$(m+1)/2$	$6m-37$	$T_A + 5T_X$
Kwon등 [10]	General	m	$\leqq m+(k-1)(m-1)/2$	$\leqq T_A + \lceil \log_2 k \rceil T_X$
	Type IV	m	$(5m-3)/2$	$T_A + 3T_X$
	Type X	m	$(11m-9)/2$	$T_A + 5T_X$
제안한 연산기(g=1)	General	m	$\leqq (k+1)(m-1)/2+1$	$\leqq T_A + (1+\lceil log_2 l' \rceil) T_X$
	Type VI	m	$(5m-7)/2$	$T_A + 3T_X$
	Type X	m	$(11m-73)/2$	$T_A + 4T_X$
제안한 연산기(g=0)	General	$(m+1)/2$	$\leqq (k+2)(m-1)/2+1$	$\leqq T_A + (1+\lceil log_2 l' \rceil) T_X$
	Type IV	$(m+1)/2$	$3m-4$	$T_A + 3T_X$
	Type X	$(m+1)/2$	$6m-37$	$T_A + 4T_X$

정규기저를 갖는 유한체 $GF(2^m)$의 복잡도는 다음과 같다.

a) g=1 인 경우 :m AND gate, $(7m-21)/2$ XOR gate.

a)′ g=0 인 경우 : $(m+1)/2$ AND gate, 그리고 $4m-11$ XOR gate.

b) T_A+(1+$\lceil \log_2 7 \rceil$)T_X = T_A+4T_X.

증명. a) Conjecture 1에 의하면 갓 i_0 에 대한 4쌍의 기저가 같으므로 XOR gate 수는

$$(6+1)(m-1)/2+1-8=(7m-21)/2$$
$$=(C_n+1)/2+\lfloor m/2 \rfloor .$$

Corollary 4. Corollary 1의 연산기 에서 타입 10 의 가우시안 정규기저를 갖는 유한체 $GF(2^m)$의 복잡도는 다음과 같다.

a) g=1 인 경우 : m AND gate, $(11m-73)/2$ XOR gate.

a)′ g=0 인 경우 : $(m+1)/2$ AND gate, 그리고 $6m-37$ XOR gate.

b) T_A+4T_X.

증명. a) i_0에 대g k s 16쌍의 기저가 같으므로 XOR gate 수는

$$(10+1)(m-1)/2+1-32=(17m-73)/2.$$

b). Remark 1과 같이 $l'=8$이 되도록 Corollary 1 과 같은 쉬프팅을 구할 수 있다.

Remark 2. 타입 II 최적 정규기저의 경우, Yang 등[16] 쉬프팅 되는 것을 수학적으로 증명 하여 재구성한 거의 일부가 되어 결과적으로 같은 복잡도를 얻게 된다. 그리고 k=12, 14, 등의 경우에 대하여도 이와 같이 분석 할 수 있다.

기존의 연산기와 제안한 연산기의 구체적인 비교는 표1에서 제시하였다.

VI. 예 제

g=1, m =37, k = 4 이면 n = 146, p = 147 이므로 $GF(147)^*=<2>$ 이다.

$$G_j(A,B)=A_{j-1}B_{j-1}\beta + \sum_{i_0=1}^{u} x_{j,i_0}\Big(\sum_{w=0}^{k/2-1}\beta^{2^{\varsigma_{wm+i_0}}}+\sum_{w=1}^{k/2}\beta^{2^{\varsigma_{wm-i_0}}}\Big)$$

이므로 각 행 $1 \le i_0 \le u$ 에 대하여

$2^j=2^{\varsigma_{wm+i_0}}$, $2^{\varsigma_{wm-i_0}} \in GF(211)^*$ 인 경우 j 열의 값을 1로하고 나머지는 0으로 하는 행렬을 M 이라 하

$$\begin{pmatrix}
1&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&1&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&1&0&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1\\
0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&1&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0\\
0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1\\
0&1&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&1&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}$$

그림 1. $GF(2^{37})$에 대한 M의 행렬

Fig. 1. The Matrix M for $GF(2^{37})$.

면 그림 1과 같다. 그리고 Corollary 1에 의하여 16행을 오른쪽으로 2번 쉬프팅 하면 M (그림 2) 와 같은 행렬이 나타나며 한열에 1의 수는 최대 3이다. 그러므로 $j_0 = 0,\ i_0 \neq 16$인 경우 $j_{i_0} = 0$, 그리고 $j_{16} = 2$ 이다.

Ⅳ. 결 론

유한체가 암호학적 분야에 응용되면서 유한체의 연산에 많은 관심을 가지고 있으며, 하드웨어 구현은 정규기저를 이용하여 표현할 경우 효율적으로 구현할 수 있다. 특히 타입 I의 최적정규기저를 갖는 유한체가 가장 효과적으로 구현된다. 그리고 양의 정수 m 이 8의 배수가 아니면 타입 (m, k)인 가우스 주기가 되는 k 가 존재한다는 것도 알려진 사실이다. 그리고 m 이 홀수이고 $GF(2^m)$이 type Ⅳ 의 가우스 주기를 가지면 $GF(4m+1)^* = < 2 >$인 것을 Lemma 1에서 증명하였다. 이와 같이 $GF(2^m)$이 타입 (m, k)인 가우스 주기를 갖고 $GF(mk+1)^* = < 2 >$ 인 유한체가 많이 존재한다. 본 논문에서는 이러한 경우 $GF(2^{mk})$는 타입 I 의 최적 정규 기저를 갖는 $GF(2^{mk})$의 부분체인 것을 이용하여 $GF(2^m)$의 직렬곱셈 연산기를 타입 I 최적 정규기저를 갖는 $GF(2^{mk})$에 적용하여 제안하였으며, 그러한 결과 암호학적으로 많이 응용되는 유한체인 k= 4, 10 의 경우 지금까지 알려진 것 중 공간 복잡도 면에서 가장 효율적인 Reyhani-Masoleh과 Hasan[11,12,13]의 연산기와 같은 공간 복잡도를 가지면서 XOR Path Delay는 개선되었고, XOR Path Delay 면에서 가장 효율적인 Kwon 등[15] 의 연산기와 k=4, 6은 같은 XOR Path Delay를 가지나 공간복접도 면에서 XOR gate 수가 2, 8개 줄었고, k=10인 경우는 Kwon 등[10] 의 연산기 보다 XOR Path Delay 는 20% 개선되고 공간 복잡도는 XOR gate가 32 개 줄어든 개선된 연산기 이다. 따라서 관련 응용 분야의 H/W 구현에 유용하게 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] T. Itoh and S. Tsujii, "Structure of parallel multipliers for a class of fields $GF(2^m)$", information and Computation, vol. 83, pp. 21-40, 1989.

[4] C.K. Koc and B. Sunar, "Low-complexity bit-parallel canonical and normal basis multipliers

$$
\begin{pmatrix}
1&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&1&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&1&0&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1\\
0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&1&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0\\
0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1\\
0&1&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&1&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&1&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}
$$

그림 2. $GF(2^{37})$에 대한 행렬 M′

Fig. 2. The matrix M′ for $GF(2^{37})$.

for a class of finite fields", IEEE Trans. vol. 47, no. 3, pp. 353-356, Mar, 1998.

[5] 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.

[6] 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.

[7] 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.

[8] J.L Massey and J.K. Omura, Computational method and apparatus for finite field arithmetic, US Patent No. 4,587,627, to OMNET Assoc., Sunnyvale CA, Washington, D.C.: Patent Trademark Office, 1986.

[9] M.A. Hasan, M.Z. Wang, and V.K. Bhargava, "A modified Massey-Omura parallel multiplier for a class of finite fields", IEEE Trans. vol. 42, no. 10, pp. 1278-1280, Oct, 1993.

[10] 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.

[11] A. Reyhani-Masoleh and M.A. Hasan, "Low complexity sequential normal basis multipliers over $GF(2^m)$," 16th IEEE Symposium on Computer Arithmetic, vol. 16, pp. 188-195, 2003.

[12] A. Reyhani-Masoleh and M.A. Hasan, "Efficient Digit-Serial Normal Basis Multipliers over Binary Extension Fields," ACM Trans. on Embedded $m(m+1)/2$ed Computing Systems (TECS), Special Issue on Embedded Systems and Security, pp. 575-592, vol. 3, Issue 3, August 2004.

[13] A. Reyhani-Masolleh and M.H. Hasan, "Low Complexity Word-Level Sequential Normal Basis Multipliers", IEEE Trans. vol. 54, no. 2, pp. 98-110, February, 2005.

[14] 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.

[15] A. Reyhani-Masolleh and M.H. Hasan, "Efficient multiplication beyond optimal normal bases", IEEE Trans. vol. 52, no. 4, pp. 428-439, April, 2003.

[16] D.J. Yang, C.H. Kim, Y. Park, Y. Kim, and J. Lim, "Modified Sequential Normal Basis Multipliers for Type II Optimal Normal Bases", ICCSA 2005, LNCS 3481, pp. 647-656, 2005.

[17] 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.

[18] IEEE P1363, Standard specifications for public key cryptography, Draft 13, 1999.

[19] ANSI X 9.63, Public key cryptography for the financial services industry: Elliptic curve key agreement and transport protocols, draft, 1998.

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

저 자 소 개

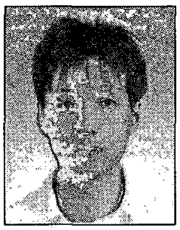
김 창 한(정회원)

1985년 고려대학교 수학과 학사 졸업.

1987년 고려대학교 수학과 석사 졸업.

1992년 고려대학교 수학과 박사 졸업.

<주관심분야 : 정보보호, 공개키 암호, 병렬연산>



장 남 수(학생회원)

2002년 서울시립대학교 수학과 학사 졸업.

2005년 고려대학교 정보보호대학원 석사 졸업.

2005년 ~ 현재 고려대학교 정보보호대학원 박사과정.

<주관심분야 : 공개키 암호, 암호칩 설계 기술, 부채널 공격>