유한체의 합성체위에서의 고속 연산기

김용태*

A Fast Multiplier of Composite fields over finite fields.

Yong-Tae Kim*

요 약

타원곡선 암호법(ECC)은 RSA나 ElGamal 암호법에 비하여 1/6정도의 열쇠(key) 크기로 동일한 안전도를 보장하므로, 메모리 용량이나 프로세서의 파워가 제한된 휴대전화기(cellular phone), 스마트카드, HPC (small-size computers) 등에 더욱 효과적인 암호법이다. 본 논문에서는 효과적인 타원곡선 암호법에 많이 사용되는 유한체위에서의 연산방법을 설명하고, Weil의 강하공격법(descent attack)에 안전하면서, 연산속도를 최대화하는 유한체의 합성체를 구축하여, 그 합성체위에서의 고속 연산기를 제안하려고 한다.

ABSTRACT

Since Elliptic Curve Cryptosystems(ECCs) support the same security as RSA cryptosystem and ElGamal cryptosystem with 1/6 size key, ECCs are the most efficient to smart cards, cellular phone and small-size computers restricted by high memory capacity and power of process. In this paper, we explicitly explain methods for finite fields operations used in ECC, and then construct some composite fields over finite fields which are secure under Weil's decent attack and maximize the speed of operations. Lastly, we propose a fast multiplier over our composite fields.

키워드

elliptic curve cryptosystem(ECC), multiplier, finite field, composite field, optimal normal basis

I. 서 론

유한체위에서의 연산은 타원곡선 암호법(ECC)과 이산대수문제(DLP)에 기반하는 암호법을 구현하는데 기본이 되는 연산으로서, 주로 유한체 $GF(2^n)$ 또는 유한체 $GF(p)$(p는 홀수인 소수)를 이용한다. 특히, ECC는 RSA나 ElGamal 암호법에 비하여 1/6정도의 열쇠(key) 크기로 같은 안전도를 제공하므로, 메모리 용량이나 프로세서의 파워가 제한된 휴대전화기(cellular phone), 스마트카드, HPC(small-size computers) 등에 더욱 효과적인 암호법이다. 그런데 유한체위에서의 연산은 그 유한체의 기저(basis)에 따라 암호시스템의 연산속도가 매우 다르게 되므로, 연산속도를 빠르게 하기 위해서는 유한체의 원소를 정규기저를 이용하여 표현하여서 연산하는 경우가 많다. 암호시스템의 연산속도는 중요한 문제이며, 속도를 높이는 요소인 공간과 연산시간의 맞교환(trade-off)을 적절하게 구사하는 일이 중요하다. 이 문제에 대하여 1998년에 Kaliski 등[1]은 기억용량을 줄인 효과적인 기저변환 방법을 제안하였다. 그러나 이 방법에는 기

* 광주교육대학교 수학교육과 교수(ytkim@gnue.ac.kr)
접수일자 : 2011. 04. 26 심사(수정)일자 : 2011. 05. 02 게재확정일자 : 2011. 06. 15

저변환 행렬과 그의 역행렬을 저장할 공간이 필요하게 되어 제한된 공간에서 효과적인 ECC의 특성에 결정적인 단점이 된다. 본 논문에서는 ECC위에서의 Weil의 강하공격법(descent attack)[2]에 안전하면서 기저변환이 필요치 않은 유한체의 합성체위에서의 연산속도를 최대화하는 유한체를 구성하고, 이를 이용한 고속 연산기를 제안한다.

II. 유한체

ECC 등에 사용되는 유한체 $GF(q^n)$에서의 연산의 효율성을 높이기 위해서는 관용기저(conventional basis)보다는 정규기저(normal basis)를 사용한다. 따라서 이 장에서는 정규기저를 가지는 유한체 $GF(q^n)$만을 대상으로 하며, q는 항상 소수(prime)이다.

2.1. 유한체 $GF(q^n)$위에서의 연산

이 절에서는 유한체에 관한 이론은 Menezes[3]를, 정규기저에 관한 이론은 Gao and Lenstra[4]를, ECC에 관한 이론은 Blake등[5]을 따르면서, 정규기저를 사용한 유한체 $GF(q^n)$위에서 원소들의 연산방법을 소개하기로 한다. 유한체 $GF(q^n)$의 임의의 두 원소 x, y 를 정규기저 A={ $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}$}를 사용하여 나타내면 다음과 같다.

$$x=\sum_{i=0}^{n-1} a_i q^{i-1},\ y=\sum_{j=0}^{n-1} b_j q^{j-1},\ a_i,b_j \in GF(p).$$

그런데 $\alpha^{q^n}=\alpha$이므로

$$\begin{aligned} x^q &= (a_0\alpha + a_1\alpha^q + \cdots + a_{n-1}\alpha^{q^{n-1}})^q \\ &= a_0^q\alpha^q + a_1^q(\alpha^q)^r + \cdots + a_{n-1}^q(\alpha^{q^{n-1}})^q \\ &= a_{n-1}\alpha + a_0\alpha^q + \cdots + a_{n-2}\alpha^{q^{n-1}} \end{aligned}$$

를 구할 수 있다. 즉,

$x=(a_0,a_1,\cdots,a_{n-1})$ 로 표현하면 x를 r승하는 것은 x를 오른쪽으로 한번 쉬프팅(shifting)하는 것과 같다는 것이다. 즉 q = 2 인 경우는 제곱은 오른쪽으로 1번 쉬프팅하는 것과 같다.

그리고 곱 xy의 연산에서는

$$\begin{aligned} z &= [a_0\alpha + a_1\alpha^q + \cdots + a_{n-1}\alpha^{q^{n-1}}] \times \\ &\quad [b_0\alpha + b_1\alpha^q + \cdots + b_{n-1}\alpha^{q^{n-1}}] \\ &= c_0\alpha + c_1\alpha^q + \cdots + c_{n-1}\alpha^{q^{n-1}} \end{aligned}$$

라고 할 때 $c_0 = f(a_0,\cdots,a_{n-1},b_0,\cdots,b_{n-1})$이라고 놓으면,

$z^q = c_{n-1}\alpha + c_0\alpha^q + \cdots + c_{n-2}\alpha^{q^{n-1}}$이므로

$c_{n-1} = f(a_{n-1},a_0,\cdots,a_{n-2},b_{n-1},b_0,\cdots,b_{n-2})$이다. 따라서,

$$c_i = f(a_{n-i},\cdots,a_{n-i-1},b_{n-i},\cdots,b_{n-i-1}),$$

$$a_k = a_r,\ b_k = b_t,\ k \equiv r \bmod n$$

이다. 즉, $\alpha^{q^i}\cdot\alpha^{q^j} = l_{ij}^{(0)}\alpha + \cdots + l_{ij}^{(n-1)}\alpha^{q^{n-1}}$이면

$$\begin{aligned} c_{n-1} &= f(a_0,\cdots,a_{n-1},b_0,\cdots,b_{n-1}) \\ &= \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} a_i b_j l_{ij},\ l_{ij} = l_{ij}^{(n-1)} \in GF(q) \quad \cdots (1) \end{aligned}$$

로 놓으면,

$c_{n-k} = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} a_{i-k} b_{j-k} l_{ij}$ 이다. 이때 $M=(l_{ij})$를 $GF(q)$위에서 $GF(q^n)$에 대한 A의 곱의 행렬이라 한다. 그러면 M은 대칭행렬이고, r = 2일 경우 행렬 M의 모든 성분 l_{ij} 는 0 또는 1이다.

2.2. 최적 정규기저를 사용한 연산 방법

A={ $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}$}를 $GF(q)$위에서 $GF(q^n)$의 정규기저라 할 때 A의 곱의 행렬 M의 요소 중 0이 아닌 것의 개수를 C_N이라 하면 $C_N \geqq 2n-1$ 이다[4]. 또한 $GF(q^n)$의 정규기저 A={ $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}$}가 $C_N = 2n-1$인 경우에, A를 최적 정규기저(optimal normal basis)라 한다. 특히 $\gcd(m,n)=1$인 경우, B ={ $\beta, \beta^q, \cdots, \beta^{q^{m-1}}$}이 $GF(q)$위에서 $GF(q^n)$의 정규기저이면 B={ $\beta, \beta^q, \cdots, \beta^{q^{m-1}}$}를 $GF(q^n)$위에서 $GF(q^{nm})$의 수정된 정규기저라고 한다. 2000년의 IEEE 규준에 의거한 표기법[6]에 따르고, $x, y \in GF(q^{mn})$을 수정된 정규기저 B를 사용하여 표현하면 다음과 같다.

$x = a_0\beta + a_1\beta^q + \cdots + a_{m-1}\beta^{q^{m-1}}$

$y = b_0\beta + b_1\beta^q + \cdots + b_{m-1}\beta^{q^{m-1}}$,

$a_i, b_j \in GF(q^n)$.

그런데 $\beta^{q^m} = \beta$ 이므로,

$z = xy = c_0\beta + c_1\beta^q + \cdots + c_{m-1}\beta^{q^{m-1}}$ 로 놓으면,

$$z^q = x^q y^q$$

$$= (a_{m-1}^q\beta + a_0^q\beta^q + \cdots + a_{m-2}^q\beta^{q^{m-1}}) \times (b_{m-1}^q\beta + b_0^q\beta^q + \cdots + b_{m-2}^q\beta^{q^{m-1}})$$

$$= (c_{m-1}^q\beta + c_0^q\beta^q + \cdots + c_{m-2}^q\beta^{q^{m-1}})$$

이다. 따라서

$$c_{m-2}^q = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_{i-1}^q b_{j-1}^q l_{ij} = (\sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_{i-1} b_{j-1} l_{ij})^q$$

이고, $GF(q^n)$ 위에서는 $u^q = v^q \Leftrightarrow u = v$ 이므로

$$c_{m-1-k} = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_{i-k}\, b_{j-k}\, l_{ij} = x^{(k)}\, T\, y^{(k)t},$$

단, $x^{(k)} = (a_{m-k}, \cdots, a_{m-1-k})$,
$y^{(k)t} = (b_{m-k}, \cdots, b_{m-1-k})^t$

이고, t는 벡터의 전치(transpose)를 뜻한다. 그러한 경우에, $T = (l_{ij})$를 $GF(q^n)$ 위에서 $GF(q^{nm})$에 대한 B의 수정된 곱의 행렬이라 한다.

정리 1. $B=\{\beta, \beta^q, \cdots, \beta^{q^{m-1}}\}$가 $GF(q)$ 위에서 $GF(q^n)$의 정규기저이고 gcd(m, n) = 1이면 $GF(q)$ 위에서 $GF(q^m)$에 대한 B의 곱의 행렬 M 과 $GF(q^n)$ 위에서 $GF(q^{nm})$에 대한 B의 수정된 곱의 행렬 T는 일치한다.

(증명) $GF(q^m)$이 $GF(q^{nm})$의 부분체이므로 M, T의 구성과정에 의하여 명백하다.

정의 2. $B=\{\beta, \beta^q, \cdots, \beta^{q^{m-1}}\}$가 $GF(q^n)$ 위에서 $GF(q^{nm})$의 수정된 정규기저이고 수정된 곱의 행렬의 0아닌 성분의 개수가 $2m-1$일 때 수정된 (Modified) 최적 정규기저라 한다.

$GF(2)$위에서 $GF(2^m)$의 최적 정규기저는 구성방법에 따라 type I과 type II로 구분되며, 모든 자연수 m에 대하여 최적 정규기저가 존재하는 것은 아니지만, m 이 홀수인 경우에는 type II의 최적 정규기저가 된다[4].

정리 3. $\gcd(m,n) = 1$이고 $B=\{\beta, \beta^q, \cdots, \beta^{q^{m-1}}\}$이 $GF(q)$위에서 $GF(q^m)$의 최적 정규기저이면 $GF(q^n)$ 위에서 $GF(q^{nm})$의 수정된 최적 정규기저이다.

(증명) 정리 2 에 의하여 B는 $GF(q^n)$위에서 $GF(q^{nm})$의 수정된 최적 정규기저인 것이 자명하다.

따름정리 4. m이 홀수이고 $B=\{\beta, \beta^q, \cdots, \beta^{q^{m-1}}\}$가 $GF(2)$위에서 $GF(2^m)$에 관한 최적 정규기저이면 B는 $GF(q)$위에서 $GF(q^m)$의 수정된 최적 정규기저이고 $GF(q)$위에서 $GF(q^m)$에 관한 B의 곱의 행렬 L의 성분은 0 또는 1이다.

(증명) m이 홀수이므로 $B=\{\beta, \beta^q, \cdots, \beta^{q^{m-1}}\}$는 $GF(q)$ 위에서 $GF(q^m)$에 관한 수정된 최적 정규기저이다. 그리고 정리 1에 의해서 $GF(2)$위에서 $GF(2^m)$에 관한 B 의 곱의 행렬 M 과 T가 일치하므로 모든 성분은 0 또는 1 이다.

정리 5. m 이 3, 9, 11, 23, 29, 33, 35, 39, 41, 51, 53, 65, 69, 81, 83, 89, 95, 99, 105, 113, 119, 131, 135, 155, 173, … 등에 대하여 $GF(q)$위에서 $GF(q^m)$에 관한 곱의 행렬의 요소가 0 또는 1인 최적 정규기저가 존재한다.

(증명) 따름정리 4와 [3, p. 100]에 의하여 명백하다.

III. 합성체(Composite fields)연산의 H/W 구현

이 장에서는 정리 5에 적합한 합성체를 구축하고 그 합성체 위에서의 고속 연산이 가능한 곱셈기를 제안하기로 한다.

3.1. $GF(2)$위에서의 합성체의 곱셈기 구축

최적 정규기저는 type I, II가 있다[4]. 합성체 $GF(q^{nm})$는 $GF(2)$ 위에서 $GF(2^n)$가 type I 또는 II가 되느냐에 따라서 다음과 같이 하드웨어(H/W)를

각각 구현한다. 합성체의 곱셈기에서는 부분체 $GF(2^n)$는 type Ⅱ의 최적정규기저를, 확대체 $GF(2^{nm})$는 type Ⅰ의 최적정규기저를 사용한다. $B=\{\beta,\beta^q,\cdots,\beta^{q^{m-1}}\}$가 $GF(2)$위에서 $GF(2^m)$의 type Ⅰ 최적정규기저이면 $B=\{\beta,\beta^q,\cdots,\beta^{q^{m-1}}\}$는 $GF(2^n)$위에서 $GF(2^{nm})$의 수정된(modified) 최적 정규기저이다. 예를 들면 $GF(2^4)$, $GF(2^3)$은 각각 type Ⅰ, Ⅱ 의 최적 정규기저를 갖는다. 이 경우 $GF(2^3)$을 부분체로 하고 $GF(2^{12})$를 확대체로 본다. 이때 $GF(2)$ 위에서 $GF(2^4)$의 type Ⅰ의 최적정규기저를 이용하여 $GF(2^3)$위에서 $GF(2^{12})$의 원소를 표현한다. 그리고 type Ⅰ의 정규기저의 곱의 행렬 T 는 다음과 같이 두 개의 행렬의 합으로 표현된다. 즉 $T=P+Q$이고 아래의 그림은 내적(Inner Product, IP), 순환(Cyclic Shift, CS), 덧셈기(Adder)로 구성되어있다. IP는 $GF(2^n)$위에서 m 개의 벡터의 내적으로 구성되어있다. CS는 Rewiring으로 구성된다. 덧셈기는 $GF(2^n)$의 덧셈(XOR)으로 구성되어 있다.

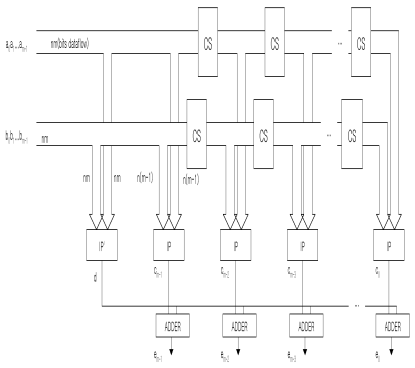

그림 1. 행렬의 덧셈기
Fig. 1 Adder of a matrix

따라서 위의 덧셈기를 활용하는 c_i의 계산과정은 다음과 같다.

$$\begin{aligned} c_{m-1-k} &= x^{(k)}Ty^{(k)t} \\ &= x^{(k)}(P+Q)y^{(k)t} \\ &= d+x^{(k)}Qy^{(k)t} \\ &= d+d_{m-1-k},\ \mathrm{d},\ \mathrm{d_{m-1-k}} \in \mathrm{GF}(2^n) \end{aligned}$$

여기서 k에 관계없이 d의 값은 일정하고 P는 m개의 1로 구성되어 있고 Q 는 m-1개의 1로 구성되어 있다[4]. 그러므로 type Ⅰ 합성체 의 하드웨어 구현은 부분체는 type Ⅱ 최적정규기저 하드웨어 구현 방법인 MO_Multiplier[7]를 사용하고 확대체는 Reyhani-Masoleh와 Hasan[8]이 제안한 type Ⅰ 합성체의 구현 방법인 MMO_multiplier를 사용한다.

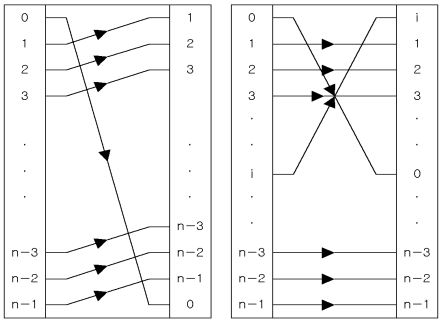

그림 2. 순환 이동기(CS), 교환기의 구조
Fig. 2 Cyclic Shifter & Exchanger

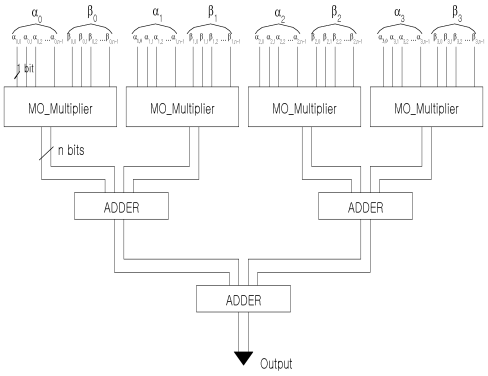

그림 3. 곱셈기의 기본구조
Fig. 3 Fundamental structure of the multiplier

3.2. 곱셈기의 복잡도(Complexity)

위의 그림은 내적(Inner Product, IP), 순환(Cyclic Shift, CS), Adder로 구성되어있다. IP는 $GF(2^n)$위에서 m 개의 벡터의 내적으로 구성되어있다. CS 는 Rewiring으로 구성된다. Adder 는 $GF(2^n)$의 덧셈(XOR)로 구성되어 있다. 부분체 $GF(2^n)$에서 곱셈 1

번에 필요한 연산은 n^2AND gates,$2n^2-2n \veebar$ gates, $D_A+(1+\lceil \log_2 n \rceil)D_x$Delays(MO_ Multiplier)가 필요하다. 따라서 먼저 d를 구하는데 길이가 m인 벡터를 $GF(2^n)$위에서 내적하는 것이므로 필요한 연산은

mn^2AND gates, $m(2n^2-2n)+n(m-1) \veebar$ gates, $D_A+(1+\lceil \log_2 n \rceil + \lceil \log_2(m-1) \rceil)D_x$ Delays 이다. 또한 각 d_i 를 구하는데 m-1개의 벡터를 내적하는 것이므로, 필요한 연산은

$(m-1)n^2$AND gates,
$(m-1)(2n^2-2n)+n(m-2) \veebar$ gates,
$D_A+(1+\lceil \log_2 n \rceil + \lceil \log_2(m-2) \rceil)D_x$Delays
이다. 그런데 $c_i = d+d_i$ 이므로 $z=xy$를 구하는데 필요한 연산은

m^2n^2AND gates, $n(2m^2n-m^2-1) \veebar$ gates, $D_A+(2+\lceil \log_2 n \rceil + \lceil \log_2(m-1) \rceil)D_x$Delays 이다. 또한 따름정리 4에 의하여 구성한 합성체 $GF(2^{n\times 4})$의 곱셈기의 구조는 다음과 같다.

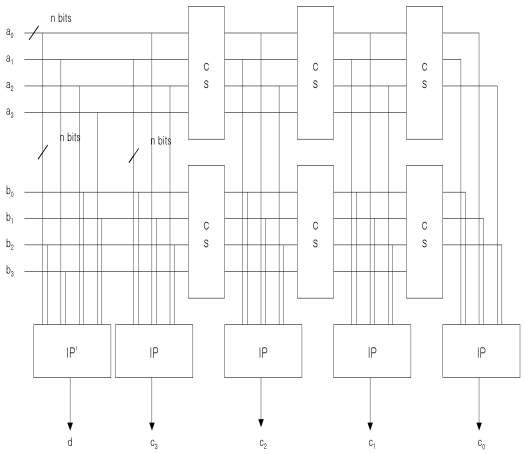

그림 4. $GF(2^{n\times 4})$의 곱셈기 구조
Fig. 4 Multiplier of $GF(2^{n\times 4})$

계산과정에서 제곱 연산은 다음과 같이 Rewiring으로 주어진다.

$$x^2=(a_0\beta+a_1\beta^q+\cdots+a_{m-1}\beta^{q^{m-1}})^2$$
$$= a_0^2\beta^2+a_1^2\beta^{q^2}+\cdots+a_{m-1}^2\beta^{q^m}$$
$$= (a_{m-1}^2,a_0^2,\ldots,a_{m-2}^2)$$

여기서 a_i는 $GF(2^n)$의 원소이므로 a_i^2 역시 Rewiring으로 구해진다.

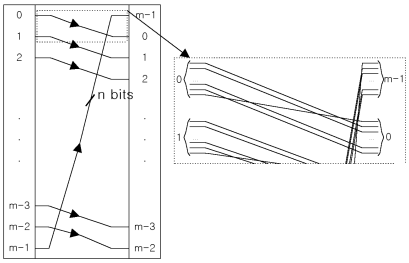

그림 5. 제곱기
Fig. 5 Squaring

3.3. 제안하는 합성체 곱셈기

부분체는 type Ⅰ 최적정규기저를 갖는 $GF(2^n)$이고 확대체는 type Ⅱ 최적정규기저를 갖는$GF(2^{nm})$인 경우이다. $B=\{\beta,\beta^q,\cdots,\beta^{q^{m-1}}\}$가 $GF(2)$위에서 $GF(2^m)$의 type Ⅱ 최적 정규기저이면 $B=\{\beta,\beta^q,\cdots,\beta^{q^{m-1}}\}$는 $GF(2^n)$위에서 $GF(2^{nm})$의 수정된 최적 정규기저가 된다. 따라서

$$c_{m-1-k}=x^{(k)}Ty^{(k)t}, k=0,1,\ldots,m-1$$

에서 행렬 T는 (m-1)m 열을 제외하고는 1인 성분은 각각 2개 존재하고 m-1 열의 1의 성분은 1개이다. 그러므로 준(Quasi) IP는 m-1개의 Adder와 IP로 구성되어 있다. 또한 부분체위에서 한 번의 곱셈에 필요한 시간은
n^2AND,$n^2-1 \veebar$,$D_A+(1+\lceil \log_2(n-1) \rceil)$Delays 가 필요하다. 그러므로 type Ⅰ 합성체위에서 한 번의 곱셈을 하기 위해서는
m^2n^2AND gates, $m^2(n^2+2n-1)+2mn$ XOR gates와 $D_A+(2+\lceil \log_2(n-1) \rceil + \lceil \log_2(n-1) \rceil$Delays가 필요하다. 다음 절에서는 3차 확대체의 예를 들어 확대체의 곱셈기를 구체적으로

제안하기로 한다.

3.4. $GF(2^{n\times 3})$의 곱셈기

유한체 $GF(2^3)$를 계수가 모두 1인(All-in-One) 다항식 x^3+x^2+1에 의하여 구성할 경우 β를 $x^3+x^2+1=0$의 근이라고 하면 정리 5에 의해서 $\{\beta,\beta^2,\beta^{2^2}\}$은 $GF(2)$위에서 $GF(2^3)$의 type Ⅱ 최적 정규기저를 형성하고, 행렬 T는 다음과 같다.

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

이때, $GF(2^{n\times 3})$의 두 원소를 type Ⅱ 최적정규기저 $\{\beta,\beta^2,\beta^{2^2}\}$로 표현한 벡터 행렬을 각각 $(a_0,a_1,a_2),(b_0,b_1,b_2),a_i,b_j\in GF(2^n)$라고 하면 곱셈기의 구조는 다음과 같다.

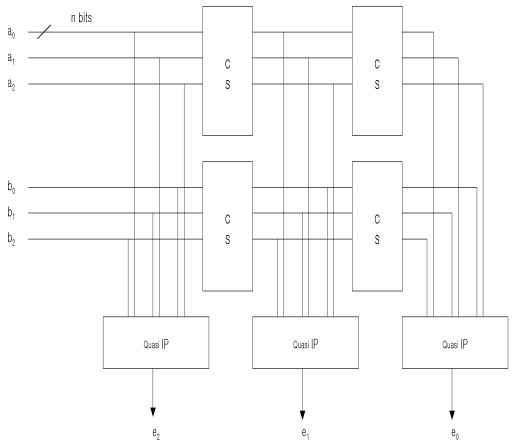

그림 6. $GF(2^{n\times 3})$의 곱셈기 구조
Fig. 6 Multiplier of $GF(2^{n\times 3})$

또한 위의 곱셈기에서의 내적연산은 다음의 준내적(Quasi Inner Product) 연산기가 사용된다.

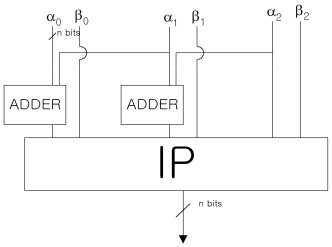

그림 7. 길이가 3인 벡터의 준내적기
Fig. 7 Quasi Inner Product of Length 3

Ⅳ. 결 론

$GF(2^n)$위에서의 타원곡선 암호시스템을 컴퓨터를 이용하여 구현할 경우에는, S/W는 다항식기저, H/W는 정규기저를 사용한다. 따라서 서로 다른 기저를 사용한 타원곡선 암호시스템 사이의 통신이 불가피하므로 암호시스템의 속도를 지연하는 원인이 되고, 더구나 기저변환행렬을 저장해야하는 것은 더 심각한 문제이다. 본 논문에서는, H/W 구현에 효과적인 type Ⅰ의 최적 정규기저를 가지는 유한체의 희귀성을 감안하여, 합성체위에서의 H/W 구현에 적합한 다양한 유한체를 구성하는 방법을 제공하였으며, 특히 $q=2$인 경우, 즉 $GF(2)$의 합성체인 $GF(2^{m\times k})$위에서 구축한 몇 가지 곱셈기의 구조를 제안하였다.

감사의 글

본 논문은 광주교육대학교 2011년도 학술진흥장학재단의 후원으로 수행되었음.

참고 문헌

[1] B.S. Kaliski Jr and Y.L. Yin, "Storage-Efficient Finite Field Basis Conversion," SAC' 98, 1998.
[2] S. Galbraith and N. Smart, "A cryptographic application of Weil descent, Codes, and Cryptography," LNCS 1746, pp. 191-200, 1999.
[3] A.J. Menezes, "Applications of finite fields," Kluwer Academic Publishers,1993.
[4] S. Gao, H.W. Lenstra Jr., "Optimal Normal

Bases, Designs, Codes, and Cryptography," Vol. 2, pp. 315-323, 1992.
[5] I. F. Blake, G. Seroussi, N. P. Smart," Elliptic Curves in Cryptography," London Mathematical Society Lecture Note Series, 265, Cambridge Univ. Press, 1999.
[6] IEEE 1363-2000," IEEE Standard Specification for Public Key Cryptography," 2000.
[7] M.A. Hasan, M.Z. Wang and V.K. Bhargava, "A modified Massey-Omura parallel multiplier for a class of finite fields, IEEE Transactions on Computers, Vol. 42, No. 10, pp. 1278-1280, Oct., 1993.
[8] A. Reyhani-Masoleh, M.A. Hasan, "Efficient Multiplication Beyond Optimal Normal Bases," IEEE Trans. on Computers, Vol. 52, No. 4, pp. 428-439, 2003.
[9] A. Reyhani-Masoleh, M.A. Hasan, "Efficient Digit-Serial Normal Basis Multipliers over Binary Extension Fields," ACM Trans. on Embedded Computing Systems, Vol. 3, No. 3, pp. 575-592, 2004.

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