通信情報保護學會論文誌
第 8 卷 第 2 號, 1998. 6

Modified 방법을 이용한 유한체의 연산

김 창 한 *, 오 상 호**, 임 종 인**, 서 광 석***, 윤 중 철**

Operations in finite fields using Modified method

Changhan Kim*, Sangho Oh**, Jongin Lim**, Kwangsuk Suh***, Joongchul Yoon**

요 약

최근들어 타원곡선 암호법(ECC)이 RSA 암호법을 대체할 것으로 기대되면서 ECC의 연산속도를 결정하는 중요한 요소인 유한체의 연산 속도에 관심이 고조되고 있다. 본 논문에서는 Modified 최적 정규 기저의 성질 규명과 $GF(q)(q=2^k,\ k=8$ 또는 16)위에서 $GF(q^m)(m$:홀수)의 Modified 최적 정규기저가 존재하는 m들을 제시하고, $GF(r^n)$위에서 $GF(r^{nm})$의 Modified 최적 정규기저와 Modified trinomial 기저를 이용한 연산의 회수와 각 기저를 이용한 유한체 $GF(q^m)$의 연산을 S/W화한 결과를 비교 하였다.

Abstract

Recently according as Elliptic Curve Cryptosystem(ECC) arises as the new alternative of Public-Key Cryptosystem(PKC), Our attention is concentrated on fast operations in finite fields, which are an important key to speeding up operations in ECC. In this paper we present the properties of modified optimal normal basis(MONB) and m, odd numbers satisfying that $\boldsymbol{GF}(q^m)$ has a MONB over $GF(q)$ $(q=2^k,\ k=8,\ 16)$ and compare the complexity of operations in $\boldsymbol{GF}(r^{nm})$ over a subfield $\boldsymbol{GF}(r^n)$ using MONB and MTB(modified trinomial basis) respectively. Also we present the implementation of operations in finite fields $\boldsymbol{GF}(q^m)$ using the two given method and the time-table.

1. 서 론

암호론은 역사적으로 오래된 흥미있는 문제이다. 1976년 Diffie 와 Hellman에 의하여 공개키 암호법이 제안된 이후로 정보통신의 시대를 맞이하여 암호학의 이용가치가 증대되고 있다. 특히 디지털서명등과 관련하여 공개키 암호시스템의 수요가 증대될 것으로 기대된다.

본 연구는 과학재단의 97년도 특정기초(97-0100-13-01-5)연구비를 지원 받아 수행 되었음

*세명대학교
**고려대학교
***서남대학교

공개키 암호법은 일방향 함수(one way function)에 근거를 두고 있으며 RSA와 ElGamal암호법으로 대표된다. RSA는 큰수의 소인수분해의 어려움에 바탕을 두고있는 암호법이고 ElGamal암호법은 순환군(cyclic group)의 이산대수(discrete logarithm) 문제의 어려움에 근거한 암호법이다. ElGamal암호법의 순환군은 Z_p^*와 $GF(q_n)^*$가 주로 사용된다. 또한 타원곡선 암호법(Elliptic curve cryptosystem, ECC)은 1985년 Kobliz[5]와 Miller[8]에 의하여 각각 독자적으로 제안된 것으로 유한체 $GF(q^n)$ 위에서 덧셈에 대한 타원곡선군의 이산대수 문제의 어려움에 바탕을 둔 암호법이다. 이와 같은 암호시스템은 유한체 $GF(q^n)$ 연산의 효율성에 많은 영향을 받는다. 이같은 효율성 관계로 실제로 쓰이는 유한체는 표수(characteristic)가 2인 $GF(2^n)$가 주로 쓰이고 있고, 최근들어 $GF(2^{kl})$의 형태가 더 효율적인 것으로 판정되고 있다[3]. 특히, 컴퓨터의 특성을 이용하기 위하여 k가 8 또는 16인 형태가 많이 활용되고 있다.[2, 9] 지금까지는 RSA가 공개키 암호시스템의 대표적인 역할을 하고있으나 최근들어 같은 난이도에서 키 길이를 $\frac{1}{4}$로 줄일 수 있는 타원곡선 암호시스템이 각광을 받으면서 유한체의 연산 속도에 더 많은 관심을 기울이고 있다. Harper등[3]에 의하여 Modified 다항식 기저를 이용한 연산법이 제안 되었고, 박일환등[11]은 Modified 정규기저를 이용한 연산법을, Win등[10]에 의하여 Modified trinomial 기저를 이용한 방법들이 제안 되었다.

이 논문에서는 Modified 최적 정규 기저의 성질 규명과 $GF(q)$ ($q=2^k$, $k=8$ 또는 16)위에서 $GF(q^m)$(m : 홀수)의 Modified 최적 정규기저가 존재하는 m들을 제시하고, $GF(r^n)$위에서 $GF(r^{nm})$의 Modified 최적 정규기저와 Modified trinomial 기저를 이용한 연산의 회수와 각 기저를 이용한 유한체 $GF(q^m)$의 연산을 S/W화한 결과를 비교 제시 하였다.

이 논문에서 $q=2^k$, k = 8 또는 16 이다.

2. 유한체의 표현

p를 소수, $r=p^l$, $l \in Z^+$ 라 하자. r 개의 원소를 갖는 유한체를 $GF(r)$ 라 하면 $GF(r^n)$ 는 다음과 같이 구성할 수 있다. $f(x) \in GF(r)[x]$를 n차의 monic인 기약다항식 이라 하면

$$GF(r^n) \cong GF(r)[x]/(f(x))$$

즉, $GF(r^n) = \{ a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \mid a_i \in GF(r) \}$ 이다. 한편 $f(\alpha)=0$라 하면

$$GF(r^n) = \{ a_0 + a_1 \alpha + \cdots + a_{n-1} \alpha^{n-1} \mid a_i \in GF(r) \}$$

와 같이 표현할 수 있다. 이와같이 표현하는 것을 다항식 기저를 사용한 표현이라 한다. 또한 $f(x)=x^n+a_t x^t+a_0$, $a_t, a_0 \in GF(r)$, $t \le \lfloor \frac{n}{2} \rfloor$ 일 때 Trinomial 기저라 한다. 우리는 특별히 $a_t = a_0 = 1$ 이고 $r=2$ 인 경우에 관심이 많다.

보조정리 2.1 $(m, n)=1$이고 $f(x)$가 $GF(r)[x]$에서 m차 기약다항식이면 $f(x)$는 $GF(r^n)$위에서도 기약다항식이다.[6]

따름정리 2.2 m이 홀수이고 $g(x)$가 $GF(2)$위에서 m차 기약다항식이면 $g(x)$는 $GF(q)$ 위에서 m차 기약다항식이다.

m, n이 서로소이고 $f(x)=x^m+x^t+1$, $t \le \lfloor m/2 \rfloor$가 $GF(r)$위에서 기약다항식이고 $f(\alpha)=0$ 이면 $A=\{1, \alpha, \cdots, \alpha^{m-1}\}$는 보조정리 [2.1]에 의하여 $GF(r^n)$ 위에서 $GF(r^{nm})$의 다항식 기저이다.

정 의 2.3 위의 A를 $GF(r^n)$위에서 $GF(r^{nm})$의 Modified trinomial 기저라 한다.

정 의 2.4 $GF(r^n)$의 부분집합 $A=\{\alpha\ \alpha^r, \alpha^{r^2}, \cdots, \alpha^{r^{n-1}}\}$가 $GF(r)$위에서 일차독립일 때 A를$GF(r)$위에서 $GF(r^n)$의 정규기저(normal basis)라 한다.

보조정리2.5 $(m, n)=1$이고 $B=\{\beta, \beta^r, \cdots, \beta^{r^{m-1}}\}$이$GF(r)$위에서 $GF(r^m)$의 정규기저이면 $GF(r^n)$위에서 $GF(r^{nm})$의 정규기저이다. [1]

정 의 2.6 $(m, n)=1$이고 $B=\{\beta, \beta^r, \cdots, \beta^{r^{m-1}}\}$이 $GF(r)$위에서 $GF(r^m)$의 정규기저일 때 B를 $GF(r^n)$위에서 $GF(r^{nm})$의 Modified 정규기저라 한다.

3. $GF(r^n)$위에서 $GF(r^{nm})$에 관한 연산

m, n을 서로소라 하자. B가 $GF(r)$위에서 $GF(r^m)$의 Trinomial(정규) 기저이면 $GF(r^n)$위에서 $GF(r^{nm})$의 Modified Trinomial(정규) 기저를 이루고 이를 이용하여 표현하면 $GF(r^{nm})$의 연산은 부분체 $GF(r^n)$의 연산으로 표현된다.

3.1 Modified trinomial 기저를 이용한 연산

$(m, n)=1$ 이고 $f(x)=x^m+x^t+1$, $t\le \lfloor m/2 \rfloor$ 가 $GF(r)$위에서 기약다항식일 때$f(\alpha)=0$이면 $A=\{1, \alpha, \cdots, \alpha^{m-1}$은 $GF(r^n)$ 위에서 $GF(r^{nm})$의 Modified trinomial 기저를 이룬다. x, y가 $GF(r^{nm})$의 원소이면 $x=a_0+a_1\alpha+\cdots+a_{m-1}\alpha^{m-1}$, $y=b_0+b_1\alpha+\cdots+b_{m-1}\alpha^{m-1}$, $a_i, b_i \in GF(r^n)$와 같이 표현된다. $a^i\cdot a^j=a^{i+j}$를 기저 A를 사용하여 표현하여 보자. $k=i+j, 0\le i, j\le m-1$ 라하면 $0\le k\le 2m-2$이고

1) $0\le k<m$ 이면 $\alpha^{i+j}=\alpha^k$,

2) $m\le k<2m-t$ 이면

$$\alpha^{i+j}=\alpha^k$$
$$=\alpha^{k-m}\cdot\alpha^m$$
$$=\alpha^{k-m}+\alpha^{k-m+t}$$

3) $2m-t\le k\le 2m-2$인 경우

$$\alpha^{i+j}=\alpha^k$$
$$=\alpha^{k-m}\cdot\alpha^m$$
$$=\alpha^{k-m}+\alpha^{k-m+t},\ m\le k-m+t\le m-2+t$$
$$=\alpha^{k-m}+\alpha^{k-m+t}+\alpha^{k-2m+2t}$$

와 같이 표현된다.

정 리 3.1 $f(x)=x^m+x^t+1$, $t\le \lfloor m/2 \rfloor$ 가 $GF(r)[x]$에서 기약다항식 이면 $GF(r^{nm})$의 두원소 x, y의 곱을 하는데 $GF(r^n)$에서 m^2번의 곱셈과 $\frac{m(13m-6)}{8}$ 번이하의 덧셈이 필요하다.

증 명. $xy=\sum_{i,j=0}^{m-1} a_i b_j \alpha^{i+j}$ 이므로$GF(r^n)$에서 m^2번의 곱셈이 필요하다. 그리고 위에서 1)만족하는 i, j의 개수는 $\frac{m(m+1)}{2}$ 이고 3)의 경우

$$i=m-1 \quad j=m-t+1, \cdots, m-1 : t-1\text{개}$$
$$\vdots$$
$$i=m-t+1 \quad , \quad j=m-1 : 1\text{개}$$

이므로 $\frac{t(t-1)}{2}$개 이다. 따라서 2)를 만족하는 i, j의 개수는 $m^2-\frac{m(m+1)}{2}-\frac{t(t-1)}{2}$개다.

또 위에서 α^k는 1)의 경우 기저의 원소 하나로, 2)는 둘, 3)은 세 개로 표현되므로 $GF(r^n)$에서 덧셈의 회수는

$$\frac{m(m+1)}{2}+2\cdot[m^2-\frac{m(m+1)}{2}-\frac{t(t-1)}{2}]+3\cdot[\frac{t(t-1)}{2}]$$

$$= \frac{m(3m-1)+t(t-1)}{2}$$

$$\leq \frac{m(3m-1)+m/2(m/2-1)}{2}$$

$$\leq \frac{m(13m-6)}{8}$$

이다.

따름정리 3.2 $f(x)=xm+x^t+1$, $t \leq \lfloor m/2 \rfloor$ 가 $GF(r)[x]$에서 기약다항식 이면 $GF(r^{nm})$의 x의 제곱을 하는데 $GF(r^n)$에서 m번의 제곱과 $\frac{7}{4}m$ 번 이하의 덧셈이 필요하다.

증 명

$$x^2 = \{a_0+a_1\alpha+\cdots+a_{m-1}\alpha^{m-1}\}^2$$
$$= a_0^2+a_1^2\alpha^2+\cdots+a_{m-1}^2\alpha^{2(m-1)}$$

이므로 $GF(r^n)$에서 m번의 제곱이 필요하다. 그리고 $k=2i$, $i=0, 1, \cdots, m-1$에 대해서

$$0 \leq k < m \quad , \quad m \ \frac{m}{2} \leq i\text{의 개수} \leq \frac{m+1}{2}$$

$$2m-t \leq k \leq 2m-2, \qquad i\text{의 개수} = \frac{t}{2}$$

이므로 $m \leq k < 2m-t$일 때 i의 개수는 $\frac{m-1}{2} - \frac{t}{2} \leq i$ 의 개수 $\leq \frac{m}{2} - \frac{t}{2}$ 이므로 덧셈의 개수 T는

$$T \leq \frac{m}{2} + 2 \cdot [\frac{m}{2} - \frac{t}{2}] + 3 \cdot \frac{t}{2}$$
$$= \frac{3}{2}m + \frac{t}{2}$$
$$\leq \frac{3}{2}m + \frac{m/2}{2}$$
$$= \frac{7}{4}m$$

이다.

역원은 Euclidean알고리즘을 이용하여 구할 수 있다.

3.2 Modified 최적 정규기저를 이용한 연산

유한체 $GF(r^n)$의 원소 x, y를 정규기저 $A=\{\alpha, \alpha^r, \alpha^{r^2}, \cdots, \alpha^{r^{n-1}}\}$를 사용하여 나타내면 다음과 같다.

$$x = a_0\alpha + a_1\alpha^r + \cdots + a_{n-1}\alpha^{r^{n-1}},$$
$$a_i \in GF(r)$$
$$y = b_0\alpha + b_1\alpha^r + \cdots + b_{n-1}\alpha^{r^{n-1}},$$
$$b_i \in GF(r)$$

x를 r승하면 $\alpha^{r^n} = \alpha$을 이용하여

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

를 구할 수 있다. 즉, $x=(a_0, a_1, \ldots, a_{n-1})$로 표현하면 x를 r승하는 것은 x를 오른쪽으로 한번 쉬프팅하는 것과 같다는 것이다. 즉 $r=2$ 인 경우는 제곱은 오른쪽으로 1번 쉬프팅하는 것과 같다. 그리고 xy 곱의 경우

$$z = [a_0\alpha + a_1\alpha^r + \cdots + a_{n-1}\alpha^{r^{n-1}}][b_0\alpha + b_1\alpha^r + \cdots + b_{n-1}\alpha^{r^{n-1}}]$$
$$= c_0\alpha + c_1\alpha^r + \cdots + c_{n-1}\alpha^{r^{n-1}}$$

라할 때 $c_0 = f(a_0, \cdots, a_{n-1}, b_0, \cdots, b_{n-1})$라 하면 $z^r = c_{n-1}\alpha + c_0\alpha^r + \cdots + c_{n-2}\alpha^{r^{n-1}}$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 $c_i=f(a_{n-i}, \cdots, a_{n-i-1}, b_{n-i}, \cdots, b_{n-i-1})$, *where* $a_k=a_r$, $b_k=b_r$, *if* $k \equiv r \bmod n$.

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

$$c_0 = f(a_0, \cdots, a_{n-1}, b_0, \cdots, b_{n-1})$$
$$= \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} a_i b_j l_{ij}, \qquad l_{ij} = l_{ij}^{(0)} \in GF(r) \qquad (*)$$

로 놓으면

$$c_k = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_{i+k} b_{j+k} l_{ij}$$ (모든 index는 modulus n 으로 줄임)

이다. 이때 $M=(l_{ij})$를 $GF(r)$위에서 $GF(r^n)$에 대한 A의 곱의 행렬이라 한다. M은 대칭행렬이고 $r=2$일 경우 l_{ij} 는 0 또는 1이다.

정 리 3.3 A를 $GF(r)$위에서 $GF(r^n)$의 정규기저라할때 A의 곱의행렬 M의 요소중 0이 아닌 것의 개수를 C_N이라 하면 $C_N \geq 2n-1$이다.[7]

정 의 3.4 A가 $GF(r^n)$의 정규기저이고 C_N이 $2n-1$일 때 A를 최적 정규기저(optimal normal basis)라 한다.

$(m, n)=1$이고 $B=\{\beta, \beta^r, \cdots, \beta^{r^{m-1}}\}$ 이 $GF(r)$위에서 $GF(r^n)$의 정규기저이면 B는 $GF(r^n)$위에서 $GF(r^{nm})$의 Modified 정규기저이다. $x, y \in GF(r^{nm})$을 B를 사용하여 표현하면 다음과 같다.

$$x = a_0\beta + a_1\beta^r + \cdots + a_{m-1}\beta^{r^{m-1}}$$
$$y = b_0\beta + b_1\beta^r + \cdots + b_{m-1}\beta^{r^{m-1}}$$
$$, a_i, b_i \in GF(r^n)$$

그리고

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

이므로 $xy = c_0\beta^r + c_1\beta^r + \cdots + c_{m-1}\beta^{r^{m-1}}$
일 때
$c_0 = f(a_0, \cdots, a_{m-1}, b_0, \cdots, b_{m-1})$
$$= \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_i b_j l_{ij}, \quad l_{ij} = l_{ij} \in GF(r^n) \qquad (**)$$

라 하면

$$c_k = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_{i+k} b_{j+k} l_{ij}, \quad k=0, n, 2n, \cdots, (m-1)n \ Mod\ m$$

이다. 이때 $L=(l_{ij})$를 $GF(r^n)$ 위에서 $GF(r^{nm})$에 대한 B의 Modified 곱의 행렬이라 한다.

정 리 3.5 $B=\{\beta, \beta^r, \cdots, \beta^{r^{m-1}}\}$가 $GF(r)$위에서 $GF(r^n)$의 정규기저이고 $(m, n)=1$ 이면 $GF(r)$위에서 $GF(r^n)$에대한 B의 곱의 행렬 M 과 $GF(r^n)$위에서 $GF(r^{nm})$에대한 B의 Modified 곱의 행렬 L은 일치한다.

증 명. $GF(r^n)$이 $GF(r^{nm})$의 부분체이므로 M, L의 구성 정의 (*), (**)에 의하여 명백하다.

따름정리 3.6 B를 $GF(r^n)$위에서 $GF(r^{nm})$의 Modified 정규기저이면 곱의행렬 M의 요소중 0이 아닌 것의 개수 $2m-1$보다 크거나 같다.

증 명. 정리[3.3]과 **정리[3.5]**에 의하여 성립한다.

정 의 3.7 $B=\{\beta, \beta^r, \cdots, \beta^{r^{m-1}}\}$가 $GF(r^n)$위에서 $GF(r^{nm})$의 Modified 정규기저이고 Modified 곱의 행렬의 0아닌요소의 개수가 $2m-1$일 때 Modified 최적 정규기저라 한다.

$GF(2)$위에서 $GF(2^m)$의 최적 정규기저는 구성 방법에 따라 I타입과 II타입으로 구분되고 모든 m에 대하여 최적 정규기저가 존재하는 것은 아니고 m이 홀수이면 II타입의 최적 정규기저 이다.[7]

정 리 3.8 $(m, n)=1$ 이고 $B=\{\beta, \beta^r, \cdots, \beta^{r^{m-1}}\}$이 $GF(r)$위에서 $GF(r^m)$의 최적 정규기저이면 $GF(r^n)$위에서 $GF(r^{nm})$의 Modified 최적 정규기저이다.

증 명. 보조정리[2.5]와 정리[3.5]에 의하여 B는 $GF(r^n)$위에서 $GF(r^{nm})$의 Modified 최적 정규기저이다.

따름정리 3.9 m이 홀수이고 B 가 $GF(2)$위에서 $GF(2^m)$에 관한 최적 정규기저이면 B는 $GF(q)$위에서 $GF(q^m)$의 modified 최적 정규기저이고 $GF(q)$위에서 $GF(q^m)$에 관한 B의 곱의 행렬 L의 요소는 0 또는 1이다.

증 명. m이 홀수 이므로 정리[3.8]에 의하여 B는 $GF(q)$ 위에서 $GF(q^m)$에 관한 Modified 최적 정규기저이다. 그리고 정리[3.5]에 의하여 $GF(2)$위에서 $GF(2^m)$에 관한 B의 곱의 행렬M 과 L이 일치하므로 요소는 0 또는 1 이다.

정 리 3.10 m이 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.

증 명. 따름정리[3.9]와 [7,p. 100]에 의하여 명백하다.

$GF(r^n)$위에서 $GF(r^{nm})$의 Modified 최적 정규기저를 사용하여 $GF(r^{nm})$의 원소의 곱을 하는데 $GF(r^n)$에서 $m(2m-1)$번의 곱셈과 $m(2m-2)$번의 덧셈이 필요하다.

그러나 따름정리[3.9]에 의하여 $r^n=q(2^8$또는 $2^{16})$인 경우 $GF(q)$에서 $m(2m-1)$번의 곱셈과 $2m(m-1)$번의 덧셈이 필요하고 제곱의 경우

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

이므로 1번의 쉬프팅과 $GF(q)$에서 m번의 제곱이 필요하다. 역원의 계산은 $x^{-1}=x^{q^m-2}$를 이용하여 구할 수 있다.[4]

4. GF(q)위에서 GF(q^m)의 연산회수와 실행결과의 비교

$GF(q)$위에서 $GF(q^m)$를 Modified trinomial 기저와 Modified 최적 정규기저를 이용하여 표현할 경우 1회의 곱셈과 제곱을 할 경우 $GF(q)$에서 각 연산의 회수는 다음표와 같다.

기저 / 연산	modified trinomial 기저	Modified 최적 정규기저
곱 셈	곱 셈 : m^2 덧 셈 : $\frac{m(13m-6)}{8}$	곱 셈 : $m(2m-1)$ 덧 셈 : $m(2m-2)$
제 곱	곱 셈 : m 덧 셈 : $\frac{7m}{4}$	제 곱 : m 쉬프팅 : 1

$q=2^8$인 경우 $GF(q)$의 각 원소를 1바이트에 표현하여 덧셈 연산은 1바이트의 bitwise XOR 이고 곱셈은 $0 \leq i, j, \leq 254$, $i+j \equiv t \mod 255$ 의 연산으로 주어진다.

그리고 $GF(q)$위에서 $GF(q^m)$를 Modified trinomial 기저와 Modified 최적 정규기저로 표현하여 S/W화 하여 각 1만회의 곱셈, 제곱, 역원을 계산한 시간을 비교한 표는 다음과 같다.

(초/10000회 , k = 8)

유한체 / 기저 / 연산	$GF(q^{23})$		$GF(q^{33})$	
	Modified trinomial 기저	Modified 최적 정규기저	Modified trinomial 기저	Modified 정규 정규기저
곱 셈	5.50	15.50	9.60	33.00
제 곱	0.60	0.53	0.80	0.67
역 원	40.00	370.00	80.03	671.50

여기서 사용한 Trinomial 기저는 $x^{23}+x^5+1$, $x^{33}+x^{13}+1$ 이고 펜티엄 166 CPU와 비주얼 C++ 5.0을 사용하여 계산한 결과이다. 그리고 Modified 최적 정규기저를 사용하여 역원을 계산할 경우 Itoh[4]방법을 사용하는데 각각 12, 11번의 곱셈과 186, 338번의 제곱을 해야한다

5. 결 론

정보통신의 시대를 맞이하여 암호학의 가치가 증대되고 ECC가 공개키 암호시스템의 중요한 역할을 할 것으로 기대 되면서 유한체 연산의 속도에 관심이 고조되고 있다. Modified 최적 정규기저를 사용한 경우 유한체 $GF(q^m)$의 역원을 계산하는데 q^m-2를 2진법으로 나열하면 곱셈을 많이 해야하는 형태로 표현되므로 비효율적인 것을 볼 수 있다. 그러므로 컴퓨터의 특성을 이용하기 위하여 유한체 $GF(q^m)$를 Modified 기저를 사용할 경우 Modified trinomial 기저가 더 효율적이다. 그리고 본 논문에서 Modified 기저를 이용한 유한체의 연산을 이론적으로 규명하고 S/W화 하였으므로 ECC와 ElGamal암호법 기타 유한체의 연산을 필요로하는 여러 분야에 활용할 수 있을 것으로 기대된다.

참 고 문 헌

[1] 박일환, 임종인, 조인호, 이상진, " 유한체 GF(2n)위의 고속 연산 방법 ", 한국통신정 보보호학회논문지, v.5 n.2 pp. 37-44, 1995.

[2] J. Guajardo and C. Paar, " Efficient algorithms for elliptic curve crytosystems", Crypto 97, Springer-Verlag, pp. 342-356, 1997.

[3] G. Harper, A. Menezes and S. Vanstone, " Public-Key Cryptosystems with very small Key length", Eurocrypt'92, Springer-Verlag, pp. 163-173, 1992.

[4] T. Itoh, O. Teechai and S. Tsuji, "A fast algorithm for computing multiplicative inverses in GF(2t) using normal bases"(in Japanese), J. Society for Electronic Communications (Japan), 44 pp. 31-36, 1986.

[5] N. Koblitz, "Elliptic curve cryptosystems", Mathematics of Computation, 48, pp. 203-209, 1987.

[6] R. Lidl, and H. Niederreiter, " Introduction to finite fields and their applications ", Revised edition, Cambridge Unversity press, Cambridge, 1994.

[7] A.J. Menezes, "Applications of finite fields", Kluwer academic publishers, Boston, 1993.

[8] V.S. Miller, " Use of elliptic curve in cryptography", Crypto'85, Springer-Verlag, pp. 417-426, 1986.

[9] R. Schroeppel, H. Orman, S. O'Malley, and O. Spatscheck, " Fast key exchange with elliptic curve systems", Crypto 95, Springer-Verlag, pp 43-56, 1995.

[10] E. De Win, A. Bosselaers, S. Vandenberghe, P. De Gersem, and J. Vandewalle, " A fast sofrware implementation for arithmetic operations in GF(2t)", Asiacrypt 96, Springer-Verlag, pp 65-76, 1996.

□ 著者紹介

김 창 한

1985년 2월 고려대학교 수학과 학사
1987년 8월 고려대학교 수학과 석사
1992년 2월 고려대학교 수학과 박사
1992년 3월 ~ 현재 세명대학교 전산정보학부 조교수

오 상 호

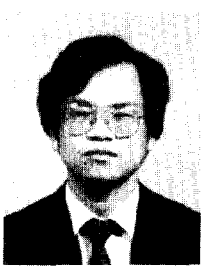
1993년 2월 고려대학교 수학과 졸업
현재 고려대학교 수학과 암호학연구실

※ 주관심분야 : Algebraic Number Theory, Cryptography

임 종 인

1980년 2월 고려대학교 수학과 학사
1982년 2월 고려대학교 대학원 수학과 석사
1986년 2월 - 고려대학교 대학원 수학과 이학박사
1986년 8월 - **현재** 고려대학교 수학과 교수

※ 주관심분야 : 응용대하학 및 정수론, 암호론



서 광 석

고려대 수학과 학사(1978)
고려대 수학과 석사(1982)
고려대 수학과 박사(1989)
1991년 서남대 수학과 부교수

※ 주관심 분야 : 전산수론 및 암호학

윤 중 철

1993년 2월 고려대학교 수학과 학사
1995년 8월 고려대학교 대학원 수학과 석사
1995년 9월 - **현재** 고려대학교 대학원 수학과 박사과정 재학중

※ 주관심분야 : **정수론, 공개키 암호시스템**