情報保護學會論文誌
第13券 第2號, 2003. 4

공개 파라메터 키 크기를 줄인 새로운 이산대수문제*

박 영 호**, 오 상 호***, 주 학 수****

A new discrete logarithm problem with public parameter key-size reduction

Young-Ho Park**, Sangho Oh***, Hak-Soo Ju****

요 약

본 논문은 유한체의 상군(quotient group)에서 이산대수문제를 고려한 새로운 공개키 시스템을 제안한다. 이 시스템은 기존의 공개키의 크기와 전송 데이터 양을 반으로 줄여 통신량의 부담을 줄일 뿐만 아니라 효율적인 승연산을 통해 계산비용을 줄일 수 있다. 특별히 DSA와 비교해서 같은 안전도를 갖는 이 시스템의 속도는 대략 50%정도 향상된다.

ABSTRACT

We introduce a new public key system based on the discrete logarithm Problem(DLP) in a quotient group of finite fields. This system achieves savings not only in communication overhead by reducing public key size and transfer data by half but also in computaional costs by performing efficient exponentiation. In particular, this system takes about 50 % speed-up, compared to DSA which has the same security.

Keyword : *Discrete Logarithm Problem, Quotient Group, Finite Field, Public Key Cryptosystem.*

Ⅰ. 서 론

엘가말(ElGamal) 암호시스템[5]과 DSA[15]와 같이 유한체의 곱세군에서 이산대수문제를 이용한 많은 시스템들이 암호학적 응용으로 유용하게 제안되었다. 이들은 소수체(prime field)의 부분군을 사용하며, 이들 시스템의 안전성은 큰 소수 위수의 부분군에서의 이산대수문제는 유한체의 전체 곱셈군의 이산대수문제만큼 어렵다는데 근거를 두고있다[11]. 하지만 최근에 소수체 대신에 확장체의 부분군을 사용하는 시스템들이 주목을 받고 있으며 LUC[3,14]와 XTR[9]이 공개키 암호법으로 소개되었다. 이 암호법들은 공개키 파라메터의 크기를 줄여 통신량을 절약하고 효율적인 연산방법들을 제시하였다. 유한체의 수열을 기반으로 하는 이 시스템들의 안전성은 확장체의 이산대수문제로 변형하여 이들의 안전성을 증명하였다[1,2,9]. 예를 들어 XTR 시스템의 경우, $q|p^2-p+1$인 소수 위수 q를 갖는 확장체 $GF(p^6)$의 부분군에서의 이산대수문제만큼 XTR-DL 문제가 안전하다고 증명하였다. 이들 시스템의 안전성은 확장체의 부분군에서의 이산대수문제는 그 부분군의 최소 포함체(surrounding field)의 것과 같다는 가정에 근거한다.

위 가정에 기반하여, 본 논문은 이차 확장체의 상군에서 이산대수문제를 기반한 새로운 공개키 암호시스템

* 본 연구는 한국정보보호진흥원 연구과제(2001-S-092) 지원으로 수행하였습니다.
** 세종사이버대학교, 컴퓨터공학부 (youngho@cybersejong.ac.kr)
*** 시큐어웍스테크놀러지 (gauss@cist.korea.ac.kr)
**** 한국정보보호진흥원 (hsju@kisa.or.kr)

(Quotient Group Cryptosystem : QGC)을 제안한다. 이 QGC의 안전성은 LUC와 같으며 다음과 같은 장점들을 갖고 있다. 첫째, LUC와 XTR 처럼 QGC는 공개키의 크기와 전송 테이터 양을 반으로 줄여 통신량의 감소시키는 이점이 있다. 공개키의 크기를 줄이는 것은 무선 통신과 PKI같은 실용적인 적용에서 매우 중요하다. 둘째, QGC의 스킴들은 기존의 유한체의 부분군 이산대수 시스템에서의 스킴들과 거의 비슷하다. 따라서 기존의 ElGamal 암호시스템, DSA, DH 키교환 스킴들을 이용한 모든 프로토콜들에 큰 수정없이 그대로 적용가능 하다. 또한 QGC는 LUC, XTR 에서는 수행하기 어려운, window방법과 선계산 방법을 사용하여 효율적인 승연산 뿐만 아니라 다승연산(multi-exponentiation)을 수행할 수 있다. 결과적으로 1024비트 소수체위의 DSA와 비교해서 같은 안전도를 갖는 QGC는 두 배나 효율적이다.

본 논문의 구성은 다음과 같다. II장에서 유한체의 2차 확장체에서의 상군을 설명한다. 그리고 III장에서 상군에서 이산대수문제를 기반으로 하는 QGC를 소개한다. IV, V장에서 QGC의 안전성을 분석하고 QGC와 LUC를 비교한다. 마지막으로 VI장에서는 QGC의 효율적인 구현에 대한 방법들을 살펴볼 것이다.

II. 상군(Quotient Group)

양의 정수 n와 소수 p에 대해 $l=p^n$라 놓자. F_l를 l 개의 원소를 갖는 유한체라하고, $F_l(\omega)$를 F_l에서 기약다항 x^2+Ax+B 의 근 ω로 확장한 유한체라 하자. 이때 $F_l(\omega)$는 F_l 위에서 차수 2인 벡터공간으로 $\{1,\omega\}$는 바탕이 된다. 따라서 $F_l(\omega)$의 모든 원소는 다음과 같은 일차결합으로 표현된다:

$$a=a_0+a_1\omega,\quad a_0,a_1\in F_l\ .$$

$F_l(\omega)^*$는 위수가 l^2-1인 곱셈군으로 부분군 F_l^*를 포함하며 $|F_l(\omega)^*/F_l^*|=l+1$이다. $F_l(\omega)^*$의 곱으로 유도된 연산을 갖는 F_l^*의 상군(quotient group)를 $G=F_l(\omega)^*/F_l^*$라 하자. 더 명확하게, $a\in F_l(\omega)^*$를 포함하는 류(class)를 $[a]$라 표시하자. 여기서, $[a]=[b]\in G \Leftrightarrow ab^{-1}\in F_l^*$ 임을 알 수 있다. 그리고 G에서 연산을 $[a][b]=[ab]$로 정의한다.

[정리 1]

(1) G는 $F_l(\omega)^*$의 곱으로 유도된 연산을 갖는 위수가 $l+1$인 순환군이다.

(2) 만일 $a\in F_l(\omega)^*$ 이고 $a\notin F_l$ 이면 유일한 원소 $a\in F_l$가 존재하여 $[a]=[a+\omega]$ 이다.

증명) (1)은 유한체와 군이론으로부터 자명하다.

$a=a_0+a_1\omega\in F_l(\omega)^*$이면 $a\notin F_l^*$ 이므로 $a_1\neq 0$이고 $[a]=[a_0+a_1\omega]=[a_1(a_0a_1^{-1}+\omega)]=[a_0a_1^{-1}+\omega]$ 이다. 따라서 $a=a_0a_1^{-1}$로 놓으면 (2)의 증명이 성립한다. □

위 정리1로부터 일대일 대응함수 $\phi: G\setminus[1]\ \rightarrow\ F_l$를 정의할 수 있다.

$$\phi([a_0+a_1\omega])=a_0a_1^{-1}.$$

또한 $\phi([1])=id$ 로 정의하므로서 함수 ϕ는 G의 모든 원소로 확장된다. 따라서 함수 ϕ는 상군의 모든 원소를 $F_l\ \cup\ id$ 로 표현할 수 있다.

III. 상군 암호시스템 (QGC)

본 장에서는 상군 $G=F_l(\omega)^*/F_l^*$에서 이산대수문제를 논하자. 상군에서 이산대수문제는 $[\beta]=[\alpha]^k$인 두 원소 $[\alpha],[\beta]\in G$에서 정수 k를 결정하는 문제이다. 앞으로 간단하게 상군 이산대수문제를 기반으로 하는 공개키 암호법을 QGC(quotient group cryptosystem)이라 하자.

지금부터 본 논문을 통해 다음과 같은 기호들을 사용한다. q를 $l+1$를 나누는 소수라 하고, G의 생성원를 $[\gamma]$라 하자. 또한 $[\delta]:=[\gamma]^{\frac{l+1}{q}}$ (또는 $[\gamma^{\frac{l+1}{q}}]$)라 놓고 $[\delta]$로 생성된 G의 부분군을 H라 하자.

QGC는 파라메터 생성과정에서 주요한 네 개의 성분 F_l, $F_l(\omega)$, q, 와 $[\delta]$ 들을 포함한다. 이들 공개키 정보중에서 $[\delta]$는 표현함수 ϕ를 사용하여 $[\delta]$ 대신에 $g:=\phi([\delta])$를 사용하므로서 크기를 반으로 줄일 수 있다. 같은 방법으로 $[\delta]$로 생성된 모든 공개키들의 크기를 반으로 줄일 수 있다.

본 장에서 파라메터 선택을 언급하고, 상군의 몇 가지 암호학적 적용을 자세히 설명한다. 3.2에서 Diffie- Hellman key agreement를, 3.3에서 ElGamal encryption를 그리고, 3.4에서 Digital Signature를 설명할 것이다.

3.1 파라메터 생성

먼저 $n=1$ 또는 $n=2$로 놓자. 이 제한은 단지 설명의 편의를 위한 것이며 모든 n으로 일반화 할 수 있다. 1024비트 RSA와 같은 안전성을 얻기 위해 p는 $n=1$일 때는 약 512비트로, $n=2$일 때는 약 256비트로 선택한다. 그리고, 작은 크기의 부분군 공격(small subgroup attack)를 피하기 위해 q는 160비트 이상으로 선택한다.

1) $l=p$인 경우

DSA에서와 같이 p와 q는 $q|p+1$를 만족하게 선택한다. p와 q를 선택하는 효율적인 방법 중 하나는 다음과 같다.

(알고리즘 2)

(1) 160비트 소수 q를 선택한다.

(2) $p=qk-1$, $p\equiv 2 \bmod 3$이면서 p가 512비트 소수가 되는 k를 결정한다.

여기서 $p\equiv 2 \bmod 3$ 조건은 x^2+x+1이 ω의 최소 다항식(minimal polynomial)을 주기 때문에, $F_p(\omega)$에서 빠른 연산을 유도한다. (보조정리 6 참조.)

2) $l=p^2$인 경우

여기서 $q|p^2+1$을 만족하는 p와 q를 선택하는 효율적인 알고리즘을 설명한다.

(알고리즘 3)

(1) 160비트 소수 $q\equiv 1 \bmod 4$를 선택한다. 이 조건은 적당한 p에 대해 $q|p^2+1$이기 위한 필요조건이다.

(2) F_q^*의 원시원소 r를 찾아 다음을 계산한다.

$$\lambda_i=(-1)^i\, r^{\frac{q-1}{4}} \bmod q \quad (i=1 \text{ 또는 } 2).$$

(3) $p=\lambda_i+kq$가 256비트 소수이고, $p\equiv \pm 2 \bmod 5$인 k를 결정한다.

p와 q를 선택한 후에, $p\equiv \pm 2 \bmod 5$ 이므로 $F_{p^2}(\omega)$를 정의하는 다항식으로 F_p위에서의 기약 다항식 $f(x)=x^4+x^3+x^2+x+1$를 취한다. 따라서 $F_{p^2}(\omega)$는 F_p위에서 정규기저를 가지므로 효율적인 연산을 실행할 수 있다. (보조정리 9 참조.)

마지막으로, 위수가 q인 군 H의 생성원 $[\delta]$를 찾자. 먼저 임의의 원소 $\gamma\in F_l(\omega)^*$를 취하고 $\delta=\gamma^{(l+1)/q}$를 계산한 후 $[\delta]=[1]$ 인지를 확인한 후 $[\delta]\neq[1]$이면 $[\delta]$를 H의 생성원으로 찾는다.

3.2 Diffie-Hellman 키교환 (QGC-DH)

Alice와 Bob은 공개정보 $l, q, g=\phi([\delta])\in F_l$를 알고, K를 공동키로 공유하기를 원한다. 기존의 Diffie-Hellman 프로토콜은 그대로 QGC에 적용가능하다.

- Alice는 $[2, q-1]$에서 선택한 임의의 k_1에 대해 $h_1=\phi([(g+\omega)^{k_1}])$를 계산하여 Bob에게 보낸다.
- Bob도 $[2, q-1]$에서 선택한 임의의 k_2에 대해 $h_2=\phi([(g+\omega)^{k_2}])$를 계산하여 Alice에게 보낸다.
- Alice 와 Bob은 서로에게 받은 h_2와 h_1를 사용하여 비밀키 $K=\phi([(h_2+\omega)^{k_1}])=\phi([(h_1+\omega)^{k_2}])$를 공유한다.

3.3 ElGamal 암호기법 (QGC-ELG)

Bob은 Alice의 비밀키 $1<d<q$에 대한 공개키 $e=\phi([(g+\omega)^d])$를 가지고 자신의 메시지 m를 암호해서 Alice에게 보내기를 원한다고 가정하자. m F_l의 원소로 표현되었다고 가정하자. ElGamal 암호 프로토콜의 여러 형태들은 아래와 같은 QGC으로 묘사될 수 있다.

- Bob은 $k\in_R[2, q-1]$를 선택하여 $c_0=\phi([(g+\omega)^k])$, $c_1=\phi([m+\omega][(e+\omega)^k])$를 계산한다. 그리고 암호문 $c=(c_0, c_1)$를 Alice에게 보낸다.
- Bob의 암호문 c에서 메시지 m를 얻기 위해 Alice는 $\phi([c_1+\omega]\ [(c_0+\omega)^d]^{-1})$를 계산한다.

3.4 전자서명, QGC-DSA

Alice는 임의의 길이인 메시지 m에 서명을 하기 원하고, Bob은 Alice의 공개키인 e로 서명을 확인하기 원한다.

- Alice는 임의로 선택한 $1<k<q$에 대해

$$r\equiv\phi([(g+\omega)^k]) \bmod q$$
$$s\equiv k^{-1}\{h(m)+dr\} \bmod q$$

를 계산하여 서명 (r, s)를 Bob에게 보낸다. 여기서

r, s는 q보다 작은 양의 정수이고, $h(\cdot)$는 정수값을 갖는 해쉬함수이다.

- Bob은 $t=s^{-1} \bmod q$를 계산한 후 $u_1=t\cdot h(m) \bmod q$, $u_2=r\cdot t \bmod q$, $v=\phi([(g+\omega)^{u_1}][(e+\omega)^{u_2}])$를 계산한 후 (r,s)를 확인한다. $v\equiv r \bmod q$인 경우에만 서명을 받아들인다.

Ⅳ. QGC의 안전성

4.1 상군에서의 이산대수문제

현재까지 큰 소수체(prime field)의 모든 곱셈군에 대해 이산대수문제를 푸는 다항식 시간의 알고리즘이 발견되지 않았으므로 이 문제를 기반으로 하는 공개키 시스템들은 안전성을 신뢰받을 수 있었다. 또한 Schnorr[11]는 충분히 큰 소수 위수의 순환 부분군에서의 이산대수문제는 전체 곱셈군에서의 것만큼 어렵다고 지적하였다. 이에 근거한 ElGamal 암호법이나 DSA와 같은 시스템들이 사용되고 있다. 최근에 확장체의 부분군에서의 이산대수문제는 그 부분군의 최소 포함체(surrounding field)의 것과 같다는 가정에 근거한 공개키 시스템들이 소개되었다[6,8,9].

F_l의 이차 확장체 $F_l(\omega)$의 상군 $G=F^*_{l(\omega)}/F^*_l$을 고려하자. 여기서 $l+1$이 큰 소인수 q($\approx$160비트)를 갖는다하자. $l=p$ 또는 $l=p^2$ 경우

$$q|l+1 \Rightarrow q|p+1 \text{ 또는 } q|p^2+1$$

을 만족한다. 이 경우 상군 G는 위수가 $l+1$인 순환으로 $F_l(\omega)^*$의 위수 $l+1$인 순환부부군과 동형이다. 또한 위수 $l+1$인 부분군은 $F_l(\omega)$의 어떠한 부분체에도 포함되지 않는다. 그러므로 G의 위수가 q인 부분순환군 H에서 이산대수문제는 Schnorr 와 Lenstra의 가정에 근거하여 안전하다. 추가적으로 160비트 소수 q의 선택은 H의 이산대수문제가 작은 부분군 공격(small subgroup attack)을 피하게 한다.

아래의 정리 4는 G의 이산대수문제와 $F_l(\omega)^*$의 이산대수문제 사이의 중요한 관계를 설명한다.

(정리 4) 만약 G에서의 이산대수문제를 효율적으로 푼다면, $F_l(\omega)^*$의 이산대수문제를 F_l^*의 이산대수문제로 유도할 수 있다.

(증명)

$\alpha^n=\beta$라 하자. 상군의 연산정의에 의해 $[\alpha]^n=[\beta]$를 얻는다. 가정에 의해 $r\equiv n \bmod l+1$을 만족하는 $r\le l+1$를 얻는다. 따라서 적당한 정수 t가 존재하여 $n=(l+1)t+r$를 만족하고, α^{l+1}는 F_l에 속하므로 $a=\alpha^{l+1}$, $b=\beta\alpha^{-r}$로 놓는다면 $a^t=b\in F_l$를 얻는다. 따라서 t를 구하면 n의 값을 알수 있다. □

위의 정리 4의 역으로, 만일 F_l^*에서의 이산대수문제가 취약하다고해서 반드시 $F_l(\omega)^*$에서의 이산대수문제가 취약한 것은 아니다. 다만 G에서의 이산대수문제를 푸는 효율적인 알고리즘이 주어지고 현재 공격에서 F_l^*에서의 이산대수문제가 취약하다면, $F_l(\omega)^*$은 안전하지 않다는 것이다.

또한 유한체 곱셈군의 이산대수문제의 강력한 공격법인 index-calculus 공격을 상군인 G에 직접 적용하는 것은 현재로서 효율적인 방법을 알 수가 없다.

4.2 상군에서의 Diffie-Hellman 문제

QGC-DH의 안전성은 이산대수문제에 의존하는 것이 아니라 생성자 $[\delta]$, $[\delta]^{k_1}$ 와 $[\delta]^{k_2}$가 주어졌을 때 $[\delta]^{k_1k_2}$를 찾는 Diffie-Hellman 문제[4]에 기반 한다. 4.2절에서와 같은 방법으로 G와 $F_l(\omega)^*$에서의 Diffie-Hellman 문제 사이의 관계를 쉽게 유도할 수 있다.

(정리 5)
만약 QGC-DH 문제를 푸는 효율적인 알고리즘이 존재하면, $F_l(\omega)^*$의 DH 문제를 F_l^*의 이 DH 문제로 유도할 수 있다.

Ⅴ. QGC와 LUC의 비교

이 장에서 Lucas 수열을 간단히 살펴보고, QGC와 LUC의 중요한 차이점을 논하자.

P, Q을 정수, σ 를 $K=Q(\sqrt{\xi})$위의 x^2-Px+Q의 근이라 하자. 여기서 $\xi=P^2-4Q$는 제곱수가 아닌 원소이고 σ는 이차체 K의 대수적정수 O_K (the ring of integers) 의 원소이다. 그리고 $\sigma=\frac{v+u\sqrt{\xi}}{2}$ 인 정수 $v=v(\sigma)$와 $u=u(\sigma)$가 존재한다. 비슷한 방법으로 정수 $v_k=v(\sigma^k)=v_k(\sigma)$와 $u_k=u(\sigma^k)=u_k(\sigma)$

에 대해 $\sigma^k=\frac{v_k+u_k\sqrt{\xi}}{2}$라 할 수 있다. $u_0=0$, $v_0=2$인 순환하는 관계 u_k와 v_k를 Lucas 수열이라 부른다. 암호학적인 적용은 p의 법에서 정의된다. 즉, σ^k의 정수계수는 Z/pZ의 원소로 고려되고, ξ는 Z/pZ에서 제곱수가 아닌 것으로 가정된다.

먼저, Lucas 수열 기반의 시스템과 QGC를 비교하기 위해서, Lucas 시스템은 유한체의 확장체에서 부분군에서 이산대수시스템으로 변형시키는 방법을 고려하자[1,2]. 더 정확하게 기저 σ와 σ^k에서 이산대수문제와 같이 $O_K/p\cong F_{p^2}$의 σ와 Z/pZ의 v_k에서 k를 결정하는 문제를 고려하자. 이 두 문제들은 계산적으로 같은 복잡도를 갖는다[1]. 두 가지 추가되는 조건, $Q\equiv 1 \bmod p$와 $p+1$를 나누는 적당한 k에 대해 $v_k(\sigma)\neq 2 \bmod p$에 의해, v_k에서 k를 찾는 문제는 F_{p^2}위에 위수가 $p+1$인 순환부분군 $\langle\sigma\rangle$에서 이산대수문제로 변형된다. Lucas 시스템에서 개인키 k에 대응되는 공개키 v_k의 크기는 p보다 작다. 또한 키 크기를 줄이는 방법도 변형된 시스템으로 사용할 수 있다. 예를 들어, Bob은 공개키 σ^k 대신에 $\sigma^k+\sigma^{-k}$를 공개하고, Alice는 Z/pZ에서 이차방정식을 계산하여 공개키 σ^k를 얻는다. 일반적으로 v_k 계산량은 σ^k의 계산량 보다 적다. 그러나 기존의 군에서의 이산대수문제에 여러 가지 프로토콜[10]에 적용함에 있어 약간의 제약이나 변형이 필요하다.

QGC의 경우에, 통신량을 반으로 줄이는 이익은 Z/pZ에서 한번의 역원과 한번의 곱셈의 추가적인 연산만으로 얻을 수 있다. 또한 계산량을 줄이기위해 일반적인 효율적인 승연산 기법들이 모두 적용될 수 있다.

그러므로 QGC는 일반적인 부분군의 이산대수문제에 기반한 반면에 LUC는 수열의 연산을 기반으로 하고 있으며 실제의 승연산을 수행하지 않는다. 따라서 QGC는 LUC, XTR 에서는 수행하기 어려운, window방법과 선계산방법을 사용하여 효율적인 승연산 뿐만 아니라 다승연산(multi-exponentiation)을, 예를들어 $a^kb^lc^md^n$등과 같은 연산, 수행할 수 있다.

개인적은 교류에서 Eric Verheul은 LUC은 QGC와 같다고 지적했다. 왜냐하면, 앞에서 언급한 것처럼, LUC는 F_{p^2}의 위수가 $p+1$인 순환부분군에서 암호시스템이 설계될 수 있고, 군 연산의 측면에서, F_{p^2}의 상군과 같은 계산량을 갖는다. 그러나 QGC는 앞에서 서술한 것과 같은 장점들을 지니고 있다.

Ⅵ. 효율적인 구현

본 장은 상군 G에서 수행할 수 있는 효율적인 승연산 방법을 논한다. $F_l(\omega)^*$에 있는 임의의 원소 a와 임의의 정수 k에 대해 $[a]^k$를 계산한다고 가정하자. $[a]^k=[a^k]$이기 때문에, G에 있는 원소의 승연산은 이차체 $F_l(\omega)$에 있는 원소의 승연산으로 변형할 수 있다. 우리는 상군을 기반으로 하는 공개키 암호 시스템의 $F_l(\omega)$에서의 승연산 속도가 얼마나 향상되는지 관심이 있다.

6.1 이차 확장체

512비트 소수 $p\equiv 2 \bmod 3$에 대해 소수체 F_p의 이차 확장체 $F_p(\omega)$는 F_p위의 기약다항식 X^2+X+1를 사용한다. 확장체에서 효율적인 연산을 위해 다항식기저(polynomial basis) 대신에 non-conventional 기저$\{\omega,\omega^2\}$를 사용할 것이다. $F_p(\omega)$위의 연산을 아래 보조정리 6에 의해 소수체위의 연산으로 유도할 수 있다([9]참고).

(보조 정리 6)

$F_p(\omega)$에서 제곱과 곱은 각각 F_p에서 두 번과 세 번의 곱으로 얻을 수 있다. 또한 이 기저를 사용하면, p승 연산으로 G의 원소의 역원을 쉽게 계산할 수 있다. 사실,

$$a^p=(a\omega+b\omega^2)^p=a\omega^p+b\omega^{2p}=b\omega+a\omega^2$$

이다. 따라서 아래의 결과를 얻는다.

(보조 정리 7)

$[a]=[a\omega+b\omega^2]$가 G의 원소라면, $[a]$의 역원은 $[a]^{-1}=[b\omega+a\omega^2]$에 의해 쉽게 얻는다.

보조 정리 7에 의해 상군 G의 원소의 역원은 원소의 성분을 바꾸는 것으로 얻을 수 있으므로 계산량이 없다. 보조 정리 7은 G에서 빠른 승연산을 위해 signed binary 방법을 사용할 수 있게 해준다. 보조 정리 6와 함께 NAF window 방법을 사용하면 같은 안전도를 갖는 소수체에서의 원래 승연산 보다 40%의 속도 향상을 이끈다.

6.2 사차 확장체

256비트 소수 $p \equiv \pm 2 \bmod 5$라 하자. 즉 F_5에서 p는 원시원소이다. 간단하게 $p \equiv 2 \bmod 5$라 가정하자. 다항식 $(x^5-1)/(x-1)=x^4+x^3+x^2+x+1$의 근의 집합 $T:=\{\zeta, \zeta^p, \zeta^{p^2}, \zeta^{p^3}\}$는 $F_p(\zeta)$에서 최적정규기저를 형성한다. $\zeta^i=\zeta^{i \bmod 5}$ 이므로, $a \in F_p(\zeta)$는 기저 T에 대해 F_p의 선형결합으로 표현할 수 있다.

$$a=a_1\zeta+a_2\zeta^2+a_3\zeta^3+a_4\zeta^4$$

여기서 a_i는 F_p의 원소이다. $F_p(\zeta)$에서 효율적인 곱셈연산을 위해 F_p위에서 $F_p(\zeta)$의 다른 기저 $S:=\{1, zetz+\zeta^{-1}, \zeta, \zeta(\zeta+\zeta^{-1})\}$를 소개한다. T에서 S로의 전환행렬이 non-singular 행렬이므로 S가 기저임을 쉽게 보일 수 있다. 이 행렬의 0이 아닌 성분은 ± 1이다. 두 기저 사이의 전환은 거의 무시할 만큼의 시간에 가능하다. $\omega=\zeta+\zeta^{-1}$라 하면, ω는 F_p위의 기약다항식 x^2+x-1의 근이므로 ω에 의해 생성된 $F_p(\omega)$는 F_p위의 차수가 2인 중간체이다. 상군 $G=F_p(\zeta)^*/F_p(\omega)$는 위수가 p^2+1인 순환군이다. $F_p(\zeta)$에서 곱연산과 제곱연산은 다항식 전개와 $F_p(\omega)$를 경유한 $\zeta^5=1$를 사용하여 수행된다.

[9]에서 비슷한 접근으로 기저$\{1, \omega\}$를 사용하여 $F_p(\omega)$에서 곱연산과 제곱연산을 각각 F_p에서 3번의 곱연산과 2번의 곱연산으로 계산할 수 있다. 그러므로 그러므로 아래의 보조정리를 얻는다.

(보조정리 8) $F_p(\zeta)$에서 곱연산과 제곱연산은 각각 F_p에서 12번의 곱연산과 7번의 곱연산으로 계산할 수 있다.

앞에서와 같이, $F_p(\zeta)$위에서 p승연산은 기저 T를 사용하여 추가적인 비용을 들이지 않는다. 사실 이것은 $F_p(\zeta)$의 원소 표현 성분의 교환으로 얻을 수 있고, 아래와 같이 쉽게 증명된다.

(보조정리 9)

G에 있는 원소 $[a]=[a_1\zeta+a_2\zeta^2+a_3\zeta^3+a_4\zeta^4]$에 대해,

(1) $[a]^p=[a_3\zeta+a_1\zeta^2+a_4\zeta^3+a_2\zeta^4]$

(2) $[a]^{-1}=[a_4\zeta+a_3\zeta^2+a_2\zeta^3+a_1\zeta^4]$

상군 G에서 승연산의 속도를 향상하는 두가지 방법을 설명하기 위해 보조정리 9를 사용한다. 이차체인 경우처럼, 보조정리 9(2)를 사용하여 signed binary method(NAF)를 G에 적용한다. 이것은 원래 승연산보다 15%의 속도향상을 줄 수 있다.

또 다른 효율적인 방법은 타원곡선 위의 군 G 의 위수가 q인 부분군 H 에 적용하는 [7]의 아이디어를 변형한 것이다. 우선 $\lambda:=p \bmod q$를 만든다. q가 p^2+1를 나누기 때문에 p의 거의 모든 경우에 λ는 160비트 수이다. H의 원소 $[\beta]$에 대하여, $[\beta^\lambda]=[\beta^p]$ 이므로 $[\beta]^\lambda$를 계산하는 비용은 없다. $[1, q]$에서 균일하게 선택한 k에 대해 H안의 $[\beta]^k$를 효율적으로 계산하기 위해, k를 λ항에 대해 k의 길이의 반인 두 성분으로 분해해서 사용한다. k를 $[0, \sqrt{q}]$의 적당한 원소 k_1와 k_2로 $k=k_1+k_2\lambda$같이 표현할 수 있다고 가정하자. 그때 $[\beta]^k=[\beta]^{k_1+k_2\lambda}=[\beta]^{k_1}[\beta^\lambda]^{k_2}$를 얻는다. 그래서 앞의 승연산을 병렬로 처리할 수 있다[3]. 타원곡선(elliptic curves)에서처럼, p승연산의 비용이 없으므로 승연산의 속도향상이 기대된다. 계산실험으로 기존의 방법보다 50%의 개선을 확인할 수 있었다. 마침내 이 방법의 효율성은 임의의 k에 대해 효율적이고 빠르게 $k=k_1+k_2\lambda$로 표현하는 방법에 의존한다. k를 분해하는 문제는 [7]에서 설명한 알고리즘으로 효율적으로 해결된다. H위에서 승연산에 대한 앞의 분석은 동시에 두 방법을 사용하여 기존의 1024비트 소수체에서의 승연산 보다 거의 50 %향상시킨다.

Ⅶ. 결 론

[표 1]에서 $F_{p_0}(\zeta)$, $F_{p_1}(\omega)$와 F_{p_2}에서 160비트 승연산을 비교하였다. 여기서 p_0, p_1 와 p_2는 각각 256, 512 와 1024비트 소수들이고, ζ, ω는 각각 F_{p_0}위의 이차 기약다항식 $x^4+x^3+x^2+x+1$와 F_{p_1}위의 기약다항식 x^2+x+1의 근들이다. 소수체 연산은 NTL 4.0를 사용하였다[12]. 소스코드는 Visual C 5.0에서 설계되었고, 연산속도는 Pentium III 650MHz에서 측정되었다.

본 논문에서 확장체의 상군에 기반한 QGC라는 새로운 공개키 시스템을 소개하고, 이 시스템들의 안

〔표 1〕 유한체에서 승연산

	160-비트 승연산
$F_{p_0}(\zeta)$	21.13 (ms)
$F_{p_1}(\omega)$	30.77 (ms)
F_{p_2}	42.84 (ms)

전성을 분석하였다. 이 시스템들은 기존의 부분군에서의 이산대수를 기반으로 하는 시스템에 비해 통신량과 계산량을 감소시키는 장점을 가지고 있다. 통신량의 관점에서 공개키 크기와 전송테이터 양을 반으로 감소시키며 이 과정에서 추가로 필요한 계산비용은 무시할 만큼 적다. 계산량의 관점에서 QGC는 소수체 위에서 이산대수 시스템과 비교하여 승연산이 30~50%의 향상되었다. 특히, QGC가 LUC와 LUC로 변형된시스템들과의 중요한 차이점들을 논하였다.

참 고 문 헌

[1] D.Bleichenbacher, W.Bosma, A.Lenstra, "Some Remarks on Lucas-Based Cryptosystems", Crypto'95, Springer-Verlag, pp. 386~396.

[2] A.E. Brouwer, R. Pellikaan, E.R. Verheul, "Doing more with fewer bits", Proceedings Asiacrypt99, LNCS 1716, Springer-Verlag 1999, pp. 321~332.

[3] Ian Blake, Gadiel Seroussi and Nigel Smart: 'Elliptic Curves in Cryptography', London Mathematical Society Lecture Note Series. 265, Cambridge University Press, 1999.

[4] W. Diffie, M. Hellman, "New directions in cryptography" IEEE Trans. on Information Theory, vol. IT-22, 1976, 644~654.

[5] T. ElGamal, "A Public Key Cryptosystem and a Signature scheme Based on Discrete Logarithms", IEEE Trans. on Information Theory 31(4), 1985, 469~472.

[6] T. ElGamal, "A Subexponential-Time Algorithm for Computing Discrete Logarithms over $GF(p^2)$", IEEE Trans. on Information Theory 31(4), 1985, 473~481.

[7] R. Gallant, R. Lambert and S. Vanstone, "Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms", CRYPTO' 2001, LNCS 2139, Springer-Verlag 2001, pp 190~200.

[8] A.K. Lenstra, "Using Cyclotomic Polynomials to Construct Efficient Discrete Logarithm Cryptosystems over Finite Fields", Proceedings ACISP97, LNCS 1270, Springer-Verlag 1997, pp 127~138.

[9] A.K. Lenstra and E.R. Verheul, "The XTR public key system" Crypto 2000, LNCS 1880, Springer-Verlag 2000, pp 1~19.

[10] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, "Handbook of applied cryptography", pp.162~163, CRC press.

[11] C.P. Schnorr, "Efficient signature generation by smart cards", Journal of Cryptology, 4, pp. 161~174 (1991).

[12] V. Shoup, "Fast consturction of irreducible polynomials over finite fields", Journal of symbolic computation, 17(1994), 371~391.

[13] V. Shoup, "NTL 4.0", available at www.shoup.net

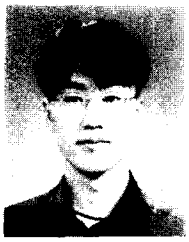
[14] P. Smith and C. Skinner, "A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms", Asiacrypt'94, pp. 298~306.

[15] American National Standard, NIST.

〈著者紹介〉

박 영 호 (Young-Ho Park) 종신회원
1990년 2월 : 고려대학교 수학과 학사
1993년 2월 : 고려대학교 수학과 석사
1997년 2월 : 고려대학교 수학과 박사
2001년3월~2002년 2월 : 고려대 정보보호기술연구센터 객원조교수
2002년 3월~현재 : 세종사이버대학교 조교수
<관심분야> 정수론, 공개키 암호, 암호 프로토콜

오 상 호 (Sangho Oh)
1993년 2월 : 고려대학교 수학과 학사
2001년 3월~현재 : 고려대학교 정보보호대학원 석사 과정
2002년 2월~현재 : 시큐어웍스 테크놀러지 선임연구원
<관심분야> 정수론, 공개키 암호 , 암호 프로토콜



주 학 수 (Hak-Soo Ju)
1997년 8월 : 고려대학교 수학과 학사
1999년 8월 : 고려대학교 수학과 석사
2001년 8월 : 고려대학교 수학과 박사과정 수료
2001년 9월~현재 : 한국정보보호진흥원 연구원
<관심분야> ECC, 워터마킹, PKI