복소 이차 류 반군위에서의 암호계의 안전성에 관한 소고

김용태*

On the Security of Cryptosystems Based on Imaginary Quadratic Class Semigroups

Yong-tae Kim*

요 약

본 논문에서는 비-최대 복소 이차 정수환(order)의 가역 이데알의 특성을 이용하는 암호계중에서 매우 중요한 이산대수문제(DLP)를 제안하고 그의 안전성을 분석하려고 한다. 우선 이러한 이산대수문제를 제안하게 된 수학적인 배경을 소개한 다음, $Cls(O)$위에서 안전한 이산대수문제를 구축 한다 . 또한 제안된 암호계의 안전성을 결정하는 최대 복소 이차 정수환의 류군(class group)의 류수(class number)와 비최대 류반군(class semigroup)의 류수를 비교하여 안전성이 증가하는 정도를 계산한다. 마지막으로 이데알의 소 이데알 인수분해 과정에서 유일인수분해의 가능성 문제를 기반으로 최대 order의 류군(class group)위에서의 DLP와 비최대 류반군(class semigroup)위에서의 DLP를 비교하면서, 본 논문에서 제안된 DLP의 안전성을 검증하고자 한다.

ABSTRACT

In this paper, we propose a new discrete logarithm problem(DLP) based on the class semigroups of imaginary quadratic non-maximal orders using the special character of non-invertible ideal and analysis its security. To do this, we first explain the mathematical background explicitly and prove some properties of $Cls(O)$ which relate to constructing the DLP and guaranteeing the security. To test the security of the proposed DLP, we compare the class number of the maximal order with that of the non-maximal order and investigate the unique factorization problems of ideals between class groups of the maximal orders and class semigroups of non-maximal orders to ensure the security of the cryptosystem.

키워드

discrete logarithm problem(DLP), class semigroup, non-invertible ideal, information security

I. 서 론

정보공학이나 전자상거래 등에 널리 사용되고 있는 공개키 암호계는 비밀키 암호계와는 달라서 빠져 나가기 힘든 덫(trapdoor)을 놓아 정보가 유출되는 경우에도 암호문을 해독하는 데에 많은 시간이 소요되기를 기대하는 암호학 분야이다. 따라서 RSA 암호계[7]와 같이 이론적으로는 쉬워 보이는 암호계가 있는가 하면, Lenstra[8]등이 제안한 ECC를 기반하는 암호계인 경우에는 상당한 수준의 수학적 지식을 요하기 때문에 대단히 유용한 암호계로 인정받고 있다. 그 후 Gauss[1]에 의해서 밝혀진 복소이차체의 이데알의 동

* 광주교육대학교 수학교육과(ytkim@gnue.ac.kr)
접수일자 : 2010. 11. 23 심사(수정)일자 : 2011. 01. 04 게재확정일자 : 2011. 02. 09

치류가 아벨군이 된다는 사실을 기반으로 키분배 암호계를 처음으로 제안한 사람은 Buchmann 등[2]이다. 그 후 Hűhnlein 등[3]이 솟수 conductor를 갖는 비-최대 복소 이차 order의 class group에서 덧을 가지는 암호계를 소개하였는데 이것은 비-최대 복소 이차 order의 class group에서는 이산대수문제가 어렵기 때문이라는 덧을 기반하여 만든 암호계이다. 즉 이 암호계들의 공통점은 최대 oder 또는 것이었다. 본 논문에서는 비-최대 order의 가역 이데알의 특성을 이용하는 암호계중에서 매우 중요한 이산대수문제(DLP)를 제안하고 그의 안전성을 알아보려고 한다. 우선 김용태[4]에서 논의했던 Kim and Moon[5]의 암호계의 취약점을 간단히 재조명하고, $Cls(O)$위에서 안전한 키 분배 암호계를 구축한 다음, 제안한 암호계가 안전한 이유를 설명하려고 한다. 복소 이차 류 반군을 이용하는 암호계는 대체로 이데알의 고차 곱을 수반하기 때문에 본 논문에서 분석하는 복잡도를 참고하면 도움이 되이라 믿는다.

II. 복소 이차 비최대 order의 류 반군(class semi-group)

본 장에서는 Kim et al.[6]을 참조하여 복소이차체에서 류반군을 구성하는 과정을 간단히 요약하고, 그 류반군의 구조를 설명하기로 한다.

2.1. 이차체의 구성

$D_1<0$을 제곱인수가 없는 정수라 할 때, $D=4D_1/r^2$, 단, $D_1\equiv 1 \bmod 4$ 이면 $r=2$, $D_1\equiv 2,3 \bmod 4$ 이면 $r=1$ 이라고 한다면, $K=\mathbb{Q}(\sqrt{D_1})$은 판별식이 D인 복소 이차체이다. 이제 $\alpha,\beta\in K$에 대하여 $[\alpha,\beta]=\alpha\mathbb{Z}+\beta\mathbb{Z}$로 정의하고, $\alpha\in K$에 대하여 $\alpha', N(\alpha), T(\alpha)$를 각각 α의 공액복소수, 노름, 트레이스로 정의하고, K안에서 conductor가 f이고 판별식이 $D_f=f^2D$인 order를 $O=[1, fw]$, 단 $w=(D+\sqrt{D})$, O의 임의의 이데알은 $A=[a,b+c\gamma]$, $\gamma=fw$, $a,b,c\in\mathbb{Z}$, $a>0, c>0$, $c|a$, $c|b$ 그리고 $ac|N(b+c\gamma)$이다. 또한 O의 두 이데알 A,B가 $\alpha,\beta\in K$에 대하여 $(\alpha)A=(\beta)B$이면 '동치'라고 정의하고 기호로는 $A\sim B$로 표기하고, 이데알 A의 동치류를 $\overline{A}$로 표기한다. $I(O)$를 O의 0이 아닌 분수 이데알, $P(O)$를 O의 0이 아닌 주 이데알(principle ideal)이라 할 때, $Cls(O)=I(O)/P(O)$를 order O의 류 반군(class semigroup)이라고 정의한다. 그런데 류반군의 구조를 알기 위해서는 다음 사항이 중요하다. $Cls(O)$를 구성하는 군 G_k들과 관련된 성질을 명확히 밝히고 $Cls(O)$의 구조를 설명하고자 한다. 우선, 잘 알려진 바와 같이 $Cls(O)$는 유한집합이다 [9, 9.6]. 반군(semi-group) S가 다음의 동치 명제를 만족하면 Clifford 반군이라고 한다[10].

(C1) S에 속하는 모든 원소 x는 S의 한 군 G_k에 속한다.

(C2) S에 속하는 모든 원소 x는 정규적(regular)이다, 즉 S의 원소 y 가 존재하여 $x=xyx$ (그러한 x를 von Neumann regular라고 한다) ,

(C3) $Cls(O)$ 는 S의 군들의 semilattice이다.

또한, 반군 S가 Clifford 반군이면, e 가 S의 idempotent원소이고 G_e = { $x\in S$ | $xe=x$이고 $xy=e$, $y\in S$ }일 때, S는 군 G_e들의 분할이 됨을 상기하자. 그러면 $Cls(O)$에 속하는 모든 idempotent 는 order O의 0아닌 이데알 E 에 대하여, $E^2=\lambda E$, $\lambda\in K^*$즉, $Cls(O)$의 원소로서 $\overline{E}$가 idempotent 일 때 E를 idempotent원소라고 함을 상기하자. 그러므로 O와 $E_k=[k, f\omega]$, 단 $k|f$, 는 idempotent이다. 따라서 $Cls(O)$의 부분군 G_1은 O의 모든 가역 이데알의 집합이므로 Picard 군이다.

임의의 O-이데알 $I=[a,b+\gamma]$에 대하여 $\gcd(I)=\gcd(a, Tr(b+\gamma), N(b+\gamma))$로 정의한다.

2.2. 동치류 반군 $Cls(O)$의 구조

본 절에서는 Cox[11, Lemma 7.5]를 일반화하여 positive definite 이차형식에 대응하는 비가역(non-invertible) 이데알을 구축하고, $Cls(O)$를 구성하는 군 G_k를 설명한 후에, $Cls(O)$의 구조를 밝히고자 한다. 또한 기호표현의 편의상 이차형식 $u(x,y)=ax^2+bxy+cy^2$ 을 (a,b,c) 로 표기하고, 만일 $u(\eta,1)=0$ 이고 η 가 상부 반평면 위에 있을 때 η 를 이차형식 $u(x,y)$의 근이라고 한다.

보조정리 1([11, Proposition 7.4]참조) O를 복소 이차체 K의 order, A를 $O-$이데알이라고 하자. 그러면

$\{\beta\in K \mid \beta A\subset A\} = O$ 일 필요충분조건은 A가 가역 이데알인 것이다. 보조정리 3.1을 이용하여 Cox[11, Lemma 7.5]를 일반화하면 다음과 같다.

보조정리 2. $u(x,y)=(a,b,c)$를 판별식이 D_f이고 positive definite인 이차형식이라 하자. $k=\gcd(a,b,c)$이고 η를 $u(x,y)$의 근이라고 하자. 그러면 $[a, a\eta]$는 $k=1$ 이면 order $O=[1,\gamma]$의 가역 이데알이고, $k>1$ 이면 비가역 이데알이다.

(증명) $a\eta$ 가 대수적 정수이므로 $[1, a\eta]$는 K의 order이다. 지금 $[a, a\eta]$가 $[1, a\eta]$의 가역 이데알이 될 필요충분조건은 $k=1$임을 보이자. 임의의 $\beta\in K$ 대하여, $\beta[a, a\eta]\subset[a, a\eta]$가 될 필요충분조건은 $\beta a\in[a, a\eta]$이고, $\beta(a\eta)\in[a, a\eta]$인 것이다. $\beta a\in[a, a\eta]$이면, 정수 m 과 n이 존재하여 $a\beta= ma+n(a\eta)$이다. 따라서 $\beta=m+n\eta$이다. 역으로, 임의의 정수 m과 n에 대하여, 분명히 $a\eta(m+n\eta)\in[a, a\eta]$이다. 또한, $\beta(a\eta) = ma\eta + na\eta^2 = ma\eta + n(-b\eta-c) = -nc + (ma-nb)\eta$ 이다. 따라서 $\beta(a\eta)\in[a, a\eta]$일 필요충분조건은 $a|nc$이고 $a|nb$인 것이다. 만일 $k=1$이면, $a|n$이다. 그러나 만일 $k>1$이면, $\gcd(a,b)$와 $\gcd(a,c)$는 k이상이 된다. 따라서 임의의 정수 m과 a의 자명하지 않은 공약수 s 가 존재하여 $a\eta(m+s\eta)\in[a, a\eta]$이다. 즉,

$\{\beta\in K\mid \beta[a, a\eta]\subset[a, a\eta]\} = [1, a\eta]$ 일 필요충분조건은 k=1이다. 따라서 보조정리 1에 의해서, 만일 $k=1$이면 $[a, a\eta]$ 는 $[1, a\eta]$의 가역 이데알이고 $k>1$이면 $[a, a\eta]$는 비가역 이데알이다. 또한, f 는 판별식이 D_f인 order O 의 conductor 이므로 $a\eta = -(b+fD)/2 +\gamma$이다. 그런데 fD와 b는 same parity이므로, $-(b+fD)/2\in\mathbb{Z}$이다. 그러므로 $[1, a\eta]= [1,\gamma]$이고, 따라서 $O=[1,\gamma]$이고

$[a, a\eta]= [a, -(b+fD)/2+\gamma]$는 O-이데알이다.

Q.E.D.

특히, $a=k$이면, module $[k, k\eta]$를 E_k로 표기한다. 또한 모든 이차형식 $u(x,y)$는 $k=\gcd(a,b,c)$일 때 $u(x,y)=(ka_1, kb_1 , kc_1)= ku_1(x,y)$로 표기하기로 한다.

따름정리 3. k가 f의 약수이면, $E_k= [k, \gamma]$이고 $E_k^2 = kE_k$이다. 즉, $\overline{E_k}^2=\overline{E_k}$이다.

(증명) $f=kd$, $k=\gcd(k,b,c)$이고 이차형식 $v(x,y)=(k, kb_1 , kc_1)$의 판별식이 D_f라고 하자. 그러면 b_1과 dD는 same parity 이므로 $k\eta -\gamma \in\mathbb{Z}$이다. 따라서 $[k, k\eta] =[k, \gamma]$이다. 또한 $k|N(\gamma)$ 이므로 E_k는 O-이데알이다. 또한 $k|Tr(\gamma)$이므로 $E_k = E_k'$이다. 그리고 $k^2|N(\gamma)$이므로

$E_k^2 = E_kE'_k = [k,\gamma][k,\gamma'] = [k^2, k\gamma, k\gamma', N(\gamma)] = k[k,\gamma] = kE_k$이다. 따라서 $\overline{E_k^2} = \overline{E_k}$이다.

Q.E.D.

정리 4. ([4], 정리 1 참조) 류반군 $Cls(O)=\dot{\bigcup_{k|f}} G_k$, 단 G_k는 $\gcd(A)=k$인 모든 O-이데알 A를 포함하는 집합이고, 서로 소이다.

정리 5. 두 O-이데알 I, J가 모두 판별식이 D_f이고 $\gcd(I)=k_1$, $\gcd(J)=k_2$이라면,

$\gcd(IJ)=lcm(k_1, k_2)$이다.

(증명) 두 이차형식 $u(x,y)$와 $v(x,y)$는 각각 이데알 I, J에 대응하는 양의 definite이고 판별식이 모두 D_f이라고 하자. 또한 $k_1=\gcd(u(x,y))$, $k_2=\gcd(v(x,y))$ 라고 할 때, $u_1(x,y)=\frac{1}{k_1}u(x,y)$, $v_1(x,y)=\frac{1}{k_2}v(x,y)$으로 정의하자. 그러면 $f=k_1d_1=k_2d_2$일 때, $u_1(x,y)$과$v_1(x,y)$은 원시 이데알이고 판별식은 각각 d_1^2D, d_2^2D이다. 따라서 $d=\gcd(d_1, d_2)$로 놓으면Gauss[1, art. 236]에 의해서 $u_1(x,y)$과$v_1(x,y)$의 직접적인 곱(direct composition) $U_1(x,y)$의 판별식은 d^2D가 된다. 그러면 $k=lcm(k_1,k_2)$로 놓으면 간단한 계산에 의해서 $f=kd$ 가 된다. 따라서 $U(x,y)$을 $u(x,y)$와 $v(x,y)$의 직접적인 곱이라 하면 $\gcd(U(x,y))=k=lcm(k_1,k_2)$ 이다. Q.E.D.

정리 6. ([10, 정리 16] 참조) $k|f$이고 $E_k=[k,\gamma]$는 idempotent, I는 그의 동치류 가 $\bar{I}\in G_k$인 O-이데알이다. 그러면 가역이데알 J이 존재하여 $JE_k=kI$이다. 이 때 가역이데알 J의 동치류 $\bar{J}$는 G_1의 원소임을 상기하자.

III. $Cls(O)$에서의 ElGamal 암호계의 안전성

이 절에서는 우선 김용태[4]에서 논의했던 Kim and Moon[9]의 암호계의 취약점을 간단히 재조명하고, $Cls(O)$위에서 안전한 이산대수문제(DLP)에 기반하는 암호계를 제안하고, 그 암호계를 안전하게 운용하는 방법을 논하려고 한다.

3.1. $Cls(O)$에서의 Kim and Moon의 ElGamal 암호계

$Cls(O)$에서의 Kim and Moon[5]이 제안한 ElGamal암호계의 비밀키는 다음과 같이 생성한다. 두 명의 사용자 A(Alice)와 B(Bob)는 절대 값의 크기가 10^{200} 정도인 정수 D와 conductor f, 비최대 order O의 비가역이데알 I를 선택하여 $D_f = f^2 D$를 공개한다.

* 공개키(public key) : 판별식 D_f, 비가역 이데알 $I \in G_k$ (생성자), 단 $1 < k|f$.

i) A는 임의의 정수 x를 선택하여 $J \sim I^x$인 기약이데알 J를 계산하여 B에게 보낸다.

ii) B는 임의의 정수 y를 선택하여 $M \sim I^y$ 인 기약이데알 M를 계산하여 A에게 보낸다.

iii) A는 기약 이데알 $U_1 \sim M^x$을 계산하고, B는 기약 이데알 $U_2 \sim J^y$를 계산한다.

그러면 $U_1 \sim M^x \sim (I^y)^x = (I^x)^y \sim J^y \sim U_2$ 이다.

이데알 $U_1=[L(U_1), \alpha_1]$, $U_2=[L(U_2), \alpha_2]$ 라고하면, A와 B는 각각

* $\gcd(L(U_1),\ N(\alpha_1)/L(U_1), T(\alpha_1))=\gcd(L(U_2),\ N(\alpha_2)/L(U_2), T(\alpha_2))$를 계산하여 비밀키(private key)로 사용한다.

3.2. $Cls(O)$위에서의 ElGamal 암호계의 재분석

이 문제에 대한 분석(analysis 또는 attack)은 김용태[4]에서 개괄적으로 이루어졌으나, 정확한 근거를 제시하여 재분석을 하려고 한다. [4. 정리 5]에 의하면 $\gcd(U_1) = \gcd(U_2)$일 필요충분조건은 U_1, U_2의 동치류가 같은 군 G_i에 속하는 것이다. 그런데 위의 암호계에 나타나는 이데알은 모두 군 G_k에 포함되므로 그들의 gcd 는 모두 k이다. 따라서

$\gcd(U_1) = \gcd(L(U_1), N(\alpha_1)/L(U_1), T(\alpha_1))$

$= \gcd(L(U_2), N(\alpha_2)/L(U_2), T(\alpha_2)) = \gcd(U_2)$를 비밀키로 사용하는 것은 암호계로서 의미가 없다. 따라서 다음 장에서는 $Cls(O)$에 기반한 의미 있는 암호계를 제안하려고 한다.

IV. $Cls(O)$에서의 DLP

이 장에서는 III장에서 논의한 $Cls(O)$의 구조와 이데알의 특성을 이용하여 안전하고 새로운 DLP를 제안하려고 한다.

4.1. $Cls(O)$에서의 새로운 DLP

판별식 D, conductor f, D_f는 3.1 에서와 같다.

i) $1 < k|f$인 $Cls(O)$의 부분군 G_k 안에서 항등원인 idempotent E_k와 다른 두 비가역 이데알 동치류 $\overline{I}, \overline{J}$를 선택한다.

ii) $J \sim I^x$ 인 $x \in \mathbb{Z}$를 구한다.

4.2. 제안된 DLP의 배경

i) 정리 4에서의 Clifford semigroup $Cls(O)$의 서로 소인 군 G_k들 사이에서 주어지는 bonding homomorphism의 정의와 정리 6 에 의해서 두 이데알 I, J의 동치류 $\overline{I}, \overline{J}$의 bonding homomorphism ϕ_k 하에서의 원상(preimages)을 $\overline{S}$, $\overline{T}$라고하면, $\phi_k(\overline{I}) = \overline{S}$ 이고 $\phi_k(\overline{J}) = \overline{T}$이다.

ii) Picard group G_1에서 만일 $y \in \mathbb{Z}$가 존재하여 $S \sim T^y$가 된다면, ϕ_k가 준동형사상(homomorphism)이므로 $I \sim J^y$ 가 되므로, y역시 G_k에서의 DLP의 해가 된다.

iii) 그러한 y를 쉽게 찾지 못한다면 정리 6을 이용하여 iii)에서와 같이 I, J의 원상을 구하게 되는데, ϕ_k가 전사(surjective)이므로 ϕ_k의 원상은 유일하지 않다.

4.3. 새로운 DLP의 안전성

암호계의 안전성은 H/W 구현시의 복잡도(complexity)에 의존한다. 따라서 이 절에서는 이데알

곱셈, 류수의 계산, DLP를 H/W에서 구현할 때 발생하는 복잡도를 계산하여 암호계의 안전성을 검증하기로 한다.

4.3.1. 이데알 곱셈 알고리즘의 복잡도

3.1에서 구하는 기약 이데알을 구하기 위해서는 효율적인 곱셈 알고리즘을 찾아야 한다. 지금 $Q_1 = rL(U_1)$, $Q_2 = rL(U_2)$ 라 하자. 단, r은 2.1절의 상수이다.

Algorithm (이데알의 곱셈)

Input : 원시이데알 U_1=[$\frac{Q_1}{r}$, $\frac{P_1+\sqrt{D_f}}{r}$] 과

U_2=[$\frac{Q_2}{r}$, $\frac{P_2+\sqrt{D_f}}{r}$]

Output : 원시이데알 U_3=[$\frac{Q_3}{r}$, $\frac{P_3+\sqrt{D_f}}{r}$],

단, $U_1 U_2 = (m) U_3$, $m \in \mathbb{Z}$.

1. $G = \gcd(Q_1/r, Q_2/r)$를 계산하고, 확장된 유크리트 호제법을 이용하여 일차합동식 $\frac{Q_1}{r}x_1 \equiv G \bmod \frac{Q_2}{r}$의 해 x_1을 구한다.
2. $H = \gcd(\frac{P_1+P_2}{r}, G)$를 계산하고, 확장된 유크리트 호제법을 이용하여 일차합동식 $\frac{P_1+P_2}{r}x_2 + Gy_2 \equiv H$의 해 x_2, y_2를 구한다.

또 다음과 같이 설정한다.

3. $X \equiv y_2 x_1 (P_2 - P_1) + x_2 \frac{D_f - P_1^2}{Q_1} \bmod \frac{Q_2}{H}$.
4. $Q_3 = \frac{Q_1 Q_2}{rH^2}$ 그리고 $P_3 \equiv P_1 + X\frac{Q_1}{rH} \bmod Q_1$.

이 방법은 Buchmann et al.[2]에 의하면, U_3 를 계산하기 위해서는 $O(\log m \log|D_f|)$기본연산이 필요하게 된다.

4.3.2. 류수(class number)와 DLP의 복잡도 (complexity)

이 절에서는 $Cls(O)$에서의 키분배 암호계의 안정성에 영향을 미치는 Picard 군 즉, 가역이데알의 동치류인 류군(class group)의 위수와 이산대수문제(DLP)의 복잡도를 논하기로 한다.

a) 류수

$Cls(O)$에서의 류수는 실제로는 군 G_1의 원소의 개수이다. 류수의 관념은 Gauss[1 ,art. 302]는 복소이차 체에서 순전히 계산에 의해서 류수를 구하였지만, 1930년까지는 완전한 증명을 하지 못하였다. 그 후 Siegel[12]은 $\lim_{D\to-\infty} \frac{\log h(D)}{\log |D|} = \frac{1}{2}$ 임을 증명하여, 주어진 $\epsilon > 0$에 대하여 상수 $C(\epsilon)$이 존재하여, 판별식이 $D < 0$인 모든 이차 체에서

$h(D) > C(\epsilon)|D|^{\frac{1}{2}-\epsilon}$ 임을 알게 되었다. 또한 Littlewood[13]는 확장된 리만가설(ERH)이 성립한다면

$$\frac{\pi(1+o(1))\sqrt{|D|}}{12e^{\gamma}\log\log|D|} < h(D) < \frac{2(1+o(1))\sqrt{|D|}\log\log|D|}{\pi}$$

임을 증명하였다. 따라서 $h(D) \approx \sqrt{|D|}$인 것으로 기대하게 되었다. 한편 Cox[11 ,정리 7.25]는 두 류수 $h(D_f)$와 $h(D)$ 사이에는 다음과 같은 관계가 있음을 증명하였다.

$$h(D_f) = \frac{h(D) f}{[O_K^*: O^*]} \Pi_{p|f} (1 - (\frac{D}{p})\frac{1}{p}),$$

단 O_K는 최대 order이다. 즉, 이 정리에 의해서 류 반군의 Picard 부분군의 위수인 $h(D_f)$는 최대 order의 류수인 $h(D)$의 배수인 사실을 알게 되었다.

b) $C(O_K)$에서의 이산대수문제

Buchmann 등[2]은 최대 order O_K의 류군 $C(O_K)$에서 판별식 D와 이데알 H, I, J는 알려져 있고 x 또는 y 를 모를 때, 이데알 U_1또는 U_2를 결정할 때의 복잡도를 계산하여 $C(O_K)$에서의 이산대수문제는 안전하다는 사실을 증명하였다.

c) $Cls(O)$에서의 이산대수문제

Adams[9, 정리 4(Fundamental Theorem)]에 의하면 최대 order O_K의 류군 $C(O_K)$의 모든 이데알은 소이데알(prime ideal)의 곱으로 유일하게 인수분해 되지만, 비 최대 order O의 류반군 $Cls(O)$의 비가역이데알은 소 이데알의 곱으로 유일인수분해가 되지 않는다. 또한 order O의 류수인 $h(D_f)$는 O_K의 류수인 $h(D)$의 배수이므로, 비가역 이데알을 생성자로 사용하는 $Cls(O)$에서의 이산대수문제는 $C(O)$에서

의 이산대수문제보다 복잡도가 훨씬 커지기 때문에 더욱 안전한 것을 알 수 있다.

V. 결 론

2000년대에 들어와서 복소 이차 체에 기반한 몇 가지 암호계가 제안되었는데 그 중에는 많은 결함이 발견되어 폐기된 것도 있어왔다. 이산대수문제는 통상 p가 솟수인 경우에, 유한체 $\mathbb{Z}_p$ 의 곱셈군 $\mathbb{Z}_p^*$에서 사용되어왔으나, 현재에는 수학적 배경이 좀 더 난해한 ECC 또는 $Cls(O)$에 기반한 DLP문제가 논의되고 있다. 본 논문에서는 $Cls(O)$위에서 DLP를 제안하게 된 수학적인 배경을 소개하였다. 특히, 비-최대 order의 비-가역 이데알의 특성을 이용하는 암호계중에서 매우 중요한 이산대수문제(DLP)를 제안하고 그의 안전성을 알아보았다.. 이 내용은 키분배[14]의 문제와도 밀접한 관계가 있으므로 후에 다시 논의할 예정이다. 또한 제안된 암호계의 안전성을 결정하는 최대 order의 류군(class group)의 류수(class number)와 비 최대 류반군(class semigroup)의 류수를 비교하여 안전성에 미치는 정도를 계산하였다. 마지막으로 최대 order의 류군(class group)위에서의 DLP와 비 최대 류반군(class semigroup)위에서의 DLP를 비교하면서, 본 논문에서 제안된 DLP는 안전함을 검증하였다.

감사의 글

본 논문은 광주교육대학교 2010년도 학술진흥장학재단의 후원으로 수행되었음.

참고 문헌

[1] K. F. Gauss, Disquisitiones Arithmeticae, translation A. C. Clarke, S.J., Yale Univ. Press, 1966.

[2] J. Buchmann, H. C. Willams, A key exchange system based on imaginary quadratic fields, J. Cryptology 1, pp.107-118, 1988.

[3] D. Hűhnlein, J. J. Jr. Michael, S. Paulus and T. Tagaki, A cryptosystem based on the non-maximal imaginary quadratic orders with fast decryption, in Advanced Cryptology Eurocrypt '98, LNCS 1403, Springer-Verlag, Berlin, pp. 294-307,1989.

[4] 김용태, 복소이차체 위에서의 공개키 암호에 관한 소고, 한국전자통신학회논문지, 제4권, 4호, pp. 270-273, 2009.

[5] H. Kim, S. Moon, Public-Key Cryptosystems based on Class Semigroups of Imaginary Quadratic Non-maximal Orders, ASISP 2, 2004.

[6] Yongtae Kim, Chang-han Kim, On the public key cryptosystems over class semigroups of imaginary quadratic non-maximal orders, Commun. Korean Math. Soc., 21, no. 3, pp.577-586, 2006.

[7] R. L. Rivest, A. Shamir, L. Adelman, A Method for Obtaining Digital Signatures and Public Key Cryptosystems, Comm. of ACM21 pp. 120-126, 1978.

[8] H. W. Lenstra, Factoring integers with elliptic curves, Ann. of Math. 126, pp.649-673, 1987.

[9] W. Adams, L. J. Goldstein, Introduction to Number Theory, Prentice-Hall, 1976.

[10] P. Zanardo, U. Zannier, The class semigroup of orders in number fields, Math.Proc. Camb.Phil. Soc. 115, pp. 379-391,1994.

[11] Cox, Primes of the form x^2+ny^2, New York, 1989.

[12] C. L. Siegel, Űber die Classenzahl quadratischer, Acta Arithmetica 1, pp.83-86, 1935.

[13] J. Littlewood, On the class number of the corpus $P\sqrt{-k}$, Proc. London Math. Soc. 27, pp358-372, 1928.

[14] H. Kim, B. Park, J. Ha, B. Lee, D. Park, New Key Management Systems for Multilevel Security, ICCSA 2005, LNCS 3481, pp.245-253, 2005.

저자 소개

김용태(Yong-tae Kim)

1976년 공주사범대학 수학교육과 졸업(이학사)
1986년 고려대학교 대학원 수학과 졸업(이학석사)
1991년 고려대학교 대학원 수학과 졸업(이학박사)
2000년 서울대학교 대학원 수학교육과 졸업 (교육학석사)
2008년 서울대학교 대학원 수학교육과 수료 (교육학박사)
1992년~현재 광주교육대학교 수학교육과 교수
※ 관심분야 : ECC, 정수론적 암호학, 공개키암호학