복소 이차체위에서의 공개키 암호계에 관한 소고

김용태*

On the Public Key Cryptosystems over Imaginary Quadratic Fields

Yong-tae Kim*

요 약

1988년에 Buchmann 과 Williams이 처음으로 복소이차체의 최대 order을 이용한 키 분배암호계를 제안하였다. 그 후 Hűhnlein, Tagaki 등이 솟수 conductor를 갖는 비-최대 복소 이차 order의 class group에서 덫을 가지는 암호계를 발표하였다. 두 가지 방법의 공통점은 최대 oder 또는 비-최대 order의 가역 이데알의 특성을 이용하는 것이었다. 한편 2003년에 Kim and Moon은 복소 이차 비-최대 order의 class semigroup에 기반한 키분배암호계와 공개키 암호법을 소개하였다. 그런데 Kim and Moon의 암호계는 Zanardo등이 발표한 논문에서 동치이데알의 비-가역 이데알을 생성자로 택하여 비밀키를 그 이데알의 어떤 특성값으로 하는 암호계를 제안하였다. 본 논문에서는 이러한 암호계를 소개하고 그 암호계의 문제점, 효율성과 전망을 논하려고 한다.

ABSTRACT

In 1988, Buchmann et al. proposed a public key cryptosystem making use of ideals of the maximal orders in quadratic fields which may pave the way for a public key cryptosystem using imaginary quadratic non-invertible ideals as generators. Next year, Hűhnlein, Tagaki et al. published the cryptosystem with trapdoor and conductor prime p over non-maximal orders. On the other hand Kim and Moon proposed a public key cryptosystrem and a key distribution cryptotsystem over class semigroup in 2003. We, in this paper, introduce and analyze the cryptotsystems mentioned above.

키워드

public key cryptotsystem, non-maximal order, semigroup, conductor

Ⅰ. 서 론

공개키 암호학은 정보공학이나 전자상거래 등에 널리 사용되고 있다. 공개키암호계 중에서 최대 복소 이차체의 최대 order를 이용한 키분배 암호계를 처음으로 제안한 사람은 Buchmann and Williams[1] 이다. 그 후 Hűhnlein 등[3]이 솟수 conductor를 갖는 비-최대 복소 이차 order의 class group에서 덫을 가지는 암호계를 소개하였는데 이것은 비-최대 복소 이차 order의 class group에서는 이산대수문제가 어렵기 때문이라는 덫을 기반하여 만든 암호계이다. 즉 이 암호계들의 공통점은 최대 oder 또는 비-최대 order의 가역 이데알의 특성을 이용하는 것이었다. 그런데 Kim and Moon [8]은 복소 이차 비-최대 order의 class semigroup에 기반한 키분배암호계와 공개키 암호법을 소개하였다. 그런데 Kim and Moon의 암호계는 Zanardo등[9]이 발표한 논문에서 동치이데알의 비-가역 이데알을 생성자로 택하여 비밀키를 그 이데알의

* 광주교육대학교 수학교육과
접수일자 : 2009. 10. 17
심사완료일자 : 2009. 11. 23

어떤 특성값으로 하는 암호계를 제안하였는데, 이 암호계의 안전성을 비-최대 order의 류 반군구조를 계산하는데에 있어 비-가역 이데알이 유일하게 인수분해되지 않는 성질에 기반을 둔 것이었고, Zanardo등이 발표한 논문에서 동치이데알의 비-가역 이데알을 생성자로 택하여 비밀키를 그 이데알의 어떤 특성값으로 하는 암호계이었다. 본 논문에서는 복소 이차체위에서의 공개키 암호계를 개관하고, 그들의 취약점, 효율성과 전망을 논하고자 한다.

II. 공개키 암호계

공계키 암호계에서는 암호화하는 열쇠와 복호화하는 열쇠가 서로 다르며 암호화하는 열쇠는 공개하지만 복호화하는 열쇠는 비밀로 보관한다. 이러한 의미에서 공개키 암호체계를 비대칭 암호체계라고 부른다. 즉, 송수신자인 A(Alice)와 B(Bob)은 비밀키 K를 선택한다. 그런 다음 키 K를 이용하여 암호화규칙 e_K와 복호화규칙 d_K를 생성한다. 이때 e_K와 d_K는 다르다. 공개키 암호계의 배경 아이디어는 가 주어져 있는 경우에 d_K를 알아내는 데 계산적 실행이 힘들다는 것이다. 이 경우에는 e_K를 공개해도 안전하다. 공개키 암혹계의 장점은 비밀키를 전달하지 않고도 B에게 암호문을 안전하게 전달할 수 있다는 점이다. 이때 B는 자기만의 열쇠인 d_K만으로 암호문을 해독할 수 있다. 공개키 암호계는 1976에 처음으로 발표된후 1977년에 공개키 암호계인 RSA암호계가 실행되었다.

2.1. 이산대수 문제(Discrete Logarithm Problem)

p가 솟수인 경우에, 유한체 $\mathbb{Z}_p$ 의 곱셈군 $\mathbb{Z}_p{}^*$는 순환군이 되고 $\mathbb{Z}_p{}^*$의 모든 원소는 한 원소(생성자, 원시원소)의 멱으로 표현된다.

i) 이 때 그 생성자(generator) 즉 원시원소를 α라 하면 $2 \le \alpha \le p-2$이다.

ii) 임의의 $\beta \in \mathbb{Z}_p{}^*$는 적당한 지수 $a \in \mathbb{Z}_p$가 존재하여 $\alpha^a \equiv \beta \bmod p$이다.

이 때 a를 $\log_\alpha \beta$로 표기한다.

iii) 이와 같이 주어진 β에 대하여 α의 지수 a를 구하는 문제를 유한체 $\mathbb{Z}_p$에서의 이산 대수문제(DLP)라고 한다.

솟수 p를 주의 깊게 선택하면 a를 구하는 문제가 대단히 어렵다고 알려져 있다.

2.2. ElGamal 암호계

1985년에 T. ElGamal은 이산대수문제의 어려움에 기반한 다음과 같은 공개키 암호를 개발하였다.

i) p가 솟수이고 유한체 $\mathbb{Z}_p$에서의 DLP가 어렵다(intractible)고 하자.

ii) $\alpha \in \mathbb{Z}_p{}^*, \mathcal{S} = \mathbb{Z}_p{}^*, \quad = \mathbb{Z}_p{}^* \times \mathbb{Z}_p{}^*$ 이라 하고

$= \{(p, \alpha, a, \beta) : \alpha^a \equiv \beta \bmod p\}$ 라 하자.

iii) 여기에서 p, α, β는 공개키이고, a는 비밀키이다.

iv) 멧시지 S를 변환한 정수를 x라고 하자. 그러면 어떤 원소 (p, α, a, β)를 정하고 임의의 (비밀인) 수 $k \in \mathbb{Z}_{p-1}$를 택하여, 암호화규칙을 다음과 같이 정의한다.

$$e_k(x,k) = (y_1, y_2), y_1 = \alpha^k \bmod p,$$
$$y_2 = x\beta^k \bmod p.$$

v) 또한 $y_1, y_2 \in \mathbb{Z}_p{}^*$에 대하여 복호화규칙을 다음과 같이 정의한다.

$$d_k = (y_1, y_2) = y_2 (y_1^a)^{-1} \bmod p.$$

그러면 비밀키 a를 알고 있는 B는 α^k로부터 β^k를 계산하게 된다. 그런 다음 y_2를 β^k로 나누어서 암호문인 x를 복원하게 된다.

III. 복소 이차 체에서 order의 류 반군(class semi-group)

본 장에서는 Kim et al.[7]을 참조하여 복소이차체에서 류반군을 구성하는 과정을 간단히 요약하고, 그 류반군의 구조를 설명하기로 한다.

$D_1 < 0$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 $D_f = f^2 D$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 O의0이 아닌 주 이데알이라 할 때, $Cls(O) = I(O)/P(O)$를 order O의 류 반군이라고 정의한다. 그러면 다음의 정리를 얻게 된다.

정리 1. ([5]의 정리 3.4 참조)류반군 $Cls(O) = \dot{\bigcup}_{k|f} G_k$, 단 G_k는 $\gcd(A) = k$인 모든 $O-$이데알 A를 포함하는 집합이다.

그러면 중요한 성질인 다음의 보조정리를 얻게 된다

보조정리 1. O의 두 이데알 류 $\overline{A}, \in G_k, \overline{B} \in G_h$에 대하여 그들의 이데알 곱 $\overline{AB} \in G_l$, 단 $l = \mathrm{lcm}(k,h)$.

Ⅳ. $Cls(O)$에서의 공개키 암호계

Zanardo 등[9]은 Howie[2]에서 힌트를 얻어 류 반군의 구조를 설명하였는데, 다시 Kim and Moon[8]은 Zanardo 등[8]의 논문을 토대로 하여 다음과 같은 $Cls(O)$에서의 ElGamal암호계의 비밀키를 다음과 같이 생성한다고 발표하였다.

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

i) A는 임의의 정수 x를 선택하여 $J \sim I^x$인 기약 이데알 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 비밀키로 사용한다.

4.2. 그런데 Jacobson[4]은 이 과정을 다음과 같이 분석하였다.

1) 생성자 I의 이데알 류 $\overline{I}$는 G_k 에 속하기 때문에 $\gcd(I) = k$이다. 그리고 I를 거듭제곱한 이데알은 다시 G_k 에 속하기 때문에의 그 이데알의 gcd 역시 k이다. 따라서 비밀키의 의미가 없다.

2) Zanardo 등[9]의 정리 16에 의하면 이데알 $I \in G_k$의 bonding homomorphism 에 의한 G_1에서의 원상은 쉽게 구해지기 때문에 공격에 취약하다.

4.3. 그러나 Jacobson[4]의 주장 2)에서 Zanardo 등[9]의 정리 16에 의해서 '$I \in G_k$의 bonding homomorphism 에 의한 G_1에서의 원상은 쉽게 구해지기 때문에' 는 그 증명과정에서 중국인의 나머지정리(CRT)를 이용하는 과정에서 conductor f를 완전하게 소인수분해를 할 수 있다는 전제가 중요한 내용이었다. 잘 아는바와 같이 자연수의 소인수 분해 문제는 intractible 이기 때문에 '복소 이차 비-최대 order의 class semigroup에 기반한 키분배암호계와 공개키 암호법'은 아직도 유효한 방법이다.

V. 결 론

이산대수문제는 통상 p가 솟수인 경우에, 유한체 $\mathbb{Z}_p$ 의 곱셈군 $\mathbb{Z}_p^*$에서 사용되어왔으나 생성자를 좀더 구성이 어려운 복소 이차 비-최대 order의 비가역 이데알을 이용하면 이산대수문제의 복잡도가 증가하게 된다. 따라서 $Cls(O)$에 기반한 이산대수문제를 좀더 적극적으로 활용하는 방안을 모색해야 되겠으며, 정부, 외교와 군사의 정보를 효율적으로 보호하기 위한 multilevel cryptosystem[6] 에도 적용이 가능하기 때문에 장차 많은 연구가 필요하겠다.

참고 문헌

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

[2] J. M. Howie, "An introduction to semigroup theory", Academic Press, New York, 1976.

[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] Jr. Michael Jacobson, "The security of cryptosystems based on class semigroups of imaginary quadratic non-maximal orders", ASISP 2004, LNCS 3108, pp.149-156, 2004.

[5] Yongtae Kim, "The multilevel Security Problem over Class Semigroups of Imaginary Quadratic Non-maximal Orders", Honam Mathematical J., No.2, pp.185-196, 2006.

[6] Yongtae Kim, C. H. Kim and T. Y. Youn, "On the Security of Multilevel Cryptosystems over Class semigroups of Imaginary Quadratic Non-maximal Orders", 3rd European PKI Workshop, Turin, Italy, LNCS 4043, pp.92-100, 2006.

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

[8] H. Kim and S. Moon, "Public-Key Cryptosystems based on Class Semigroups of Imaginary Quadratic Non-maximal Orders", ASISP 2003, LNCS 2727, pp.488-497, 2003.

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

저자 소개

김용태(Yong-tae Kim)

1976년 2월: 공주사범대학 수학교육과(이학사)

1986년 2월: 고려대학교 대학원 수학과 (이학석사)

1991년 2월: 고려대학교 대학원 수학과(이학박사)

2000년 8월: 서울대학교 대학원 수학교육과(교육학석사)

2008년 2월: 서울대학교 대학원 수학교육과(박사과정 수료)

1992년 3월 ~ 현재 : 광주교육대학교 수학교육과 교수

※관심분야 : ECC, 정수론적 암호학, 공개키암호학