위계집단에서 효율적인 암호계의 안전성에 관한 소고

김용태*

A Study on Securities of Cryptosystems for Hierarchic Groups

Yong-Tae Kim*

요 약

1982년에 Akl 등이 준순서 집합으로 구성된 위계집단에서의 암호계를 제안하였는데, 키 생성 알고리즘이 사용자가 많아질 경우에는 안전하지 않기 때문에, 이 문제점을 극복하기 위해서 1985년에 MacKinnon 등이 협동 공격을 피하면서 그 암호계를 최적화할 수 있는 암호계를 제안하였다. 2005년에는 Kim 등이 복소 이차 비최대 order 의 Clifford 반군에 기반한 일방향 hash function을 이용한 키 분배 암호계를 제안하였다. 분 논문에서는 Kim 등이 제안한 암호계를 분석하여 그 취약점을 개선한 효율적인 암호계를 제안하려고 한다.

ABSTRACT

A cryptography for enforcing hierarchic groups in a system where hierarchy is represented by a partially ordered set was introduced by Akl et al. But the key generation algorithm of Akl et al. is infeasible when there is a large number of users. To overcome this shortage, in 1985, MacKinnon et al. proposed a paper containing a condition which prevents cooperative attacks and optimizes the assignment. In 2005, Kim et al. proposed the key management systems for using one-way hash function, RSA algorithm, poset dimension and Clifford semigroup in the context of modern cryptography, the key management system using Clifford semigroup of imaginary quadratic non-maximal orders. We, in this paper, show that Kim et al. cryptosystem is insecure in some reasons and propose a revised cryptosystem.

키워드

hierarchic group, key distribution, class semigroup, non-invertible ideal
위계집단, 키 분배, 류 반군, 비가역 이데알

I. 서 론

정부, 대사관이나 군대와 같은 위계성이 중요한 집단에서는 정보 흐름의 안전성이 매우 중요하다. 이러한 점을 감안하여 Akl 등[1]이 준순서 집합으로 구성된 위계집단에서의 암호계를 제안하였는데 키 생성 알고리즘이 사용자가 많아질 경우에는 안전하지 않기 때문에, 이 문제점을 극복하기 위해서 1985년에 MacKinnon 등[2]이 협동 공격을 피하면서 그 암호계를 최적화할 수 있는 암호계를 제안하였다. 2005년에는 Kim 등[3]이 복소 이차 비최대 order 의 Clifford 반군에 기반한 일방향 hash function을 이용한 키 분배 암호계를 제안하였다. 그 논문에 Kim 등은 분배되는 이데알 EK_0를 알 때 키 이데알 K_0을 복원하는 것이 매우 어렵다는 점에 기반한 암호계를 제안하였다. 복소 이차 비최대 order 의 Clifford 반군에 기반

* 광주교육대학교 수학교육과 교수(ytkim@gnue.ac.kr)
접수일자 : 2013. 01. 17 심사(수정)일자 : 2013. 03. 25 게재확정일자 : 2013. 04. 22

한 암호계는 수학적으로 안전하다는 사실은 널리 알려져 있지만 그의 응용분야가 아직은 넓지 않다. 따라서 위계집단에서의 메시지 전달체계에 복소 이차 비최대 order 의 Clifford 반군에 기반한 암호체계를 적용하는 것은 상당한 의미가 있다. 본 논문에서는 Kim 등의 암호계를 분석하여 그의 취약점을 도출하고, 이를 개선한 류 반군 위계집단에서의 $Cls(O)$ 위에서 효율적이고 안전한 암호계를 제안하려고 한다.

II. 위계집단에서의 암호계

위계집단에서의 암호계는 RSA 암호계[4]에 기반하여 키를 생성하는데, 생성과정에서 여러 가지 단점이 드러나게 되었다. 이러한 단점을 보완하여 1985년에는 Mackinnon 등[2]이 협동공격(cooperative attacks)을 방지하면서 알고리즘을 최적화하는 방법을 다음과 같이 제안하였다.

2.1. 다중수준 암호계

1) 한 집단 내의 컴퓨터 사용자를 서로 소인 집합(security classes), $U_1, U_2, \cdots, U_n$ 으로 나눈다.

2) 집합족 $S=\{U_1, U_2, \cdots, U_n\}$ 위에 준순서 관계 $\leq$ 를 다음과 같이 정의한다. 준순서 집합 $(S, \leq)$ 에서 관계 $U_i \leq U_j$ 는 U_i 의 안전도가 U_j 의 안전도 이하임을 뜻한다. 다시 말하면 U_j 는 U_i 의 정보를 알아낼 수 있지만, 반대로는 되지 않는다는 것을 의미한다.

3) 중앙통제소(CA)가 집단내의 구성원에게 저장시키거나 배포하려는 어떤 정보를 x_m 라고 하자. 여기에서 첨자 m 은 U_m 과 그이상의 집단 $(U_m \leq) U_i$ 만이 정보 x_m 에 접근 가능함을 뜻한다.

2.2 다중수준 암호계의 solution

Akl 등[1]은 다음과 같이 세 단계의 다중수준 암호계의 solution을 제시하였다.

1 단계 : CA는 n 개의 복호 키 $K_1, K_2, \cdots, K_n$ 을 생성한다.

2 단계 : 각각의 키 $K_i\,(i=1,2,\cdots,n)$ 를 모든 사용자 U_i 에게 나누어 주고 안전하게 보관하도록 한다.

3 단계 : 모든 사용자 $(U_i \leq) U_j, (i,j=1,2,\cdots,n)$ 는 키 K_i 를 알게 한다.

2.3 암호화, 복호화 protocol

E_K 와 D_K 를 각각 암호 키 K 를 사용한 암호화, 복호화 과정이라고 하자.

1) 저장하거나 배포할 정보 x_m 을 비밀 키 K_m 을 이용하여 암호문 $x' = E_{K_m}(x_m)$ 을 계산하고, 순서쌍 $[x', m]$ 을 저장하거나 배포한다.

2) 비밀 키 K_m 을 소유한 사용자만이 $x_m = D_{K_m}(x')$ 를 계산하여 정보 x_m 을 얻게 된다.

그런데 여러 명의 사용자가 협동하여 할당받지 않은 비밀 키를 계산해낼 가능성이 있다. 이러한 단점을 보완하기 위하여 Mackinnon 등[2]이 poset의 긴 가지(longest chain)를 제거하는 알고리즘을 제안하였는데 본 논문의 내용과는 무관하므로 그 과정을 생략하기로 한다.

III. 복소 이차 order 의 류 반군

본 장에서는 김용태[5]를 참조하여 복소이차체에서 류 반군을 구성하는 과정을 간단히 요약하고, 그 류 반군의 구축과정을 설명하기로 한다.

3.1. 류 반군의 구축

$D_1 < 0$ 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 D 인 복소이차체이다. 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 α 의 공액복소수, 노름, 트레이스로 정의하고, K 안에서 conductor가 f 이고 판별식이 $D_f = f^2 D$ 인 order를 $O=[1, fw]$, 단 $w=(D+\sqrt{D})$, O 의 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 O 의 두 이데알 A, B 가 $\alpha, \beta \in K$ 에 대하여 $(\alpha)A = (\beta)B$ 이면 '동치' 라고 정의하고 기호로는 $A \sim B$ 로 표기하고, 이데알 A 의 동치류를 $\overline{A}$ 로 표기한다. $I(O)$ 를 O 의 0이 아닌 분수 이데알, $P(O)$ 를 O 의 0이 아닌 주 이데알(principal ideal)이라 할 때,

$Cls(O)=I(O)/P(O)$를 order O의 류 반군(class semigroup)이라고 정의한다.

그런데 류 반군의 구조를 알기 위해서는 다음 사항이 중요하다.

$Cls(O)$를 구성하는 군 G_k들과 관련된 성질을 명확히 밝히고 $Cls(O)$의 구조를 설명하고자 한다.

반군(semi-group) S가 다음의 동치 명제를 만족하면 Clifford 반군임을 상기하자[5, pp. 94-95, Theorem 2.1]);

(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 군G_e들의 분할이 됨을 상기하자. 그러면 $Cls(O)$에 속하는 모든 idempotent는 order O의 0 아닌 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.

3.2. $Cls(O)$의 구조

우선 다중수준 암호계를 구축하는데 필요한 $Cls(O)$의 특징을 몇 가지 소개하기로 한다. Gauss[6]의 설명을 이용하여 이들의 사실을 이해하거나 증명하는데 다음의 표기법이 필요하다.

양의 definite 이차형식 $u(x,y)=ax^2+bxy+cy^2$을 간단하게 (a,b,c)로 표기하고, $u(\eta,1)=0$ 이면 η는 $u(x,y)$의 근이고 상부반평면의 점으로 간주한다.

정리 1. k가 conductor f의 약수이면 idempotent $E_k=[k,\gamma]$ 이다.

(증명) 이차형식 $u(x,y)=(k, kb_1, kc_1)$의 판별식이 D_f이고 $f=kd$라 하자. 그러면 b_1과 dD가 same parity 이므로 $k\eta-\gamma \in k\mathbb{Z}$이다. 따라서 $[k, k\eta]=[k,\gamma]$ 이다. Q.E.D.

정리 2. 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 놓으면 Gauss[6, 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. 이러한 사실을 바탕으로 $Cls(O)$의 구조를 다음과 같이 알 수 있게 된다.

정리 3. ([7], 정리 4 참조) 류 반군 $Cls(O)=\dot{\bigcup_{k|f}} G_k$, 단 G_k, $k|f$,는 $\gcd(A)=k$인 모든 $O-$이데알 A를 포함하는 집합이고 서로 소이다.

다음에는 Clifford semigroup $Cls(O)$의 서로 소인 군 G_k들 사이에서 주어지는 bonding homomorphism의 정의를 이용하여 Zanardo 등[8]이 증명한 정리를 소개한다.

정리 4. ([8], Proposition 16, 17] 참조) k가 conductor f의 약수일 때, $E_k=[k,\gamma]$는 idempotent이고, I를 $\overline{I} \in G_k$ 인 $O-$이데알이라 하자. 그러면 가역 이데알 $J \in G_1$이 존재하여 $I \sim JE_k$이다.

따라서 정리 4에 의하면 Clifford semigroup $Cls(O)$의 모든 bonding homomorphism은 전사(surjective)이다.

IV. Kim 등의 암호계의 안전성 분석

2005년에 Kim 등[3]은 $Cls(O)$에서의 다중수준 키 관리 체제를 제안하였다. 이절에서는 Kim 등[3]의 암호계를 분석하여 암호계 취약성을 찾아내기로 한다.

4.1. Kim 등의 암호계

Kim 등 $Cls(O)$위에서 위계집단의 다중수준 키 관리 체제를 다음과 같이 제안하였다.

1) 충분히 큰 conductor f를 선택한다.

2) f의 어떤 약수 k를 선택하여 정리 1에 의해서 이데알 $E=[k,\gamma]$의 idempotent인 동치류 $\overline{E} \in Gls(O)$를 만든다.

3) 비밀키인 이데알 $K_0 \in G_k$를 선택한다.

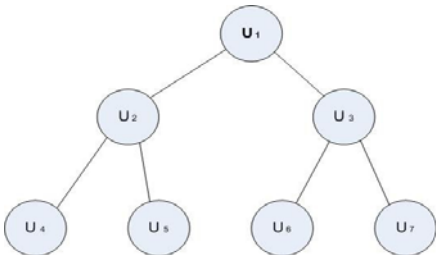
($k \neq 1$이면 이데알 K_0는 비가역적이다.)

4) 키 관리체제 작동과정

i) 두 이데알 E, F가 idempotent 이고, semilattice에서 관계 $E < F$가 주어지면, bonding homomorphism ϕ_{FE}: $G_E \rightarrow G_F$은 $\phi_{FE}(K_0) = EK_0$ 가 된다.

ii) CA는 idempotent E_{k_i} (단, $k_i | f$)를 각각의 사용자인 U_i에게 분배한다. 예를 들면 CA(U_1)는 비밀키 K_0와 E_{k_i}의 곱을 계산하여 $E_{k_2}K_0$, $E_{k_3}K_0$을 각각 U_2, U_3 에게 분배한다. 또한 CA는 $E_{k_2}E_{k_4}K_0$를 계산하여 U_4에게 보낸다. 이러한 방법으로 CA는 모든 사용자에게 키를 보낸다.

iii) 그러면, 상위의 사용자는 자기보다 하위의 사용자의 키를 모두 계산할 수 있게 된다.



4.2. Kim 등의 암호계의 취약성

1) bonding homomorphism하에서 원상의 계산

Kim 등은 bonding homomorphism ϕ_{FE}: $G_E \rightarrow G_F$은 $\phi_{FE}(K_0) = EK_0$ 에서, $J = EK_0$ 를 알아내는 경우에 K_0를 복원하는 일은 $E_k \sim O$인 경우를 제외하면 불가능할 것이라고 하였다. 편의상 order O에서 부분군 G_k에로의 bonding homomorphism을 ϕ_k: $G_1 \rightarrow G_k$로 정의하자. 일반적으로 ϕ_k하에서 G_k의 이데알 J의 원상의 개수는 기껏해야 $|Ker(\phi_k)|$이며, 아주 작은 수이므로 정리 4에서, $Cls(O)$의 부분군 G_k의 원소인 동치류 $\overline{J}$가 주어지면 이데알 J의 $|Ker(\phi_k)|$이하의 원상을 random 하게 선택하여 그 이데알의 bonding homomorphism하에서 상인 $\overline{J}$를 찾을 수 있으며, 실패하는 경우에는 이 과정을 몇 번 반복하면 된다.

2) conductor f

만일 conductor f를 쉽게 소인수분해 할 수 있다면, 류 반군 $Cls(O)$에서의 키 관리 체제는 상대적으로 안전성이 취약한 류 군(class group) $Cl(O)$안에서의 키 관리 체제가 되기 때문에 conductor f의 소인수 약수에 대응하는 몇 개의 유한체에서의 키 관리 체제로 회귀하게 되며, $Cls(O)$의 구조가 알려지게 되어 $Cls(O)$에서의 모든 암호계가 완전히 깨어지게 된다.

4.3. $Cls(O)$에서 안전한 위계집단의 암호계

이 절에서는 Kim 등[3]의 암호계를 개선하여 안전한 새로운 $Cls(O)$위에서 위계집단의 다중수준 암호계를 제안하려고 한다. Zanardo와 Zannier의 논문[8]에서 증명이 된 정리 4의 증명과정에서 conductor f의 약수에 대한 중국인의 나머지 정리(CRT)를 적용하는 부분이 핵심이 되어 bonding homomorphism하에서 원상의 계산이 가능하게 되며, 위에서 분석한 바와 같이 conductor f가 쉽게 소인수분해 된다면 류 반군 $Cls(O)$에서의 키 관리 체제가 류 군(class group) $Cl(O)$ 또는 작은 소수 몇 개에 대응하는 유한체에서의 키 관리체제로 회귀하게 된다.

4.3.1. 수정된 암호계

류 반군 $Cls(O)$위에서의 암호계가 류 군 $Cl(O)$위에서의 암호계보다 상대적으로 안전한 이유는 $Cl(O)$의 이데알은 소이데알의 곱으로 소인수분해가

유일한 반면, $Cls(O)$의 이데알은 소이데알의 곱으로 소인수분해가 유일하지 않다는 사실과, $Cl(O)$의 구조는 잘 알려져 있으나 $Cls(O)$의 구조는 아직도 명확하게 드러나지 않다는 점이다. 사상 ϕ에 관한 계산 복잡도에 관하여 김용태[9]는 다음과 같이 설명하였다. 사상 ϕ는 전사이며 핵 $Ker(\phi)$는 $Cls(D_f)$의 부분군이다. 따라서 $Cl(D)$의 임의의 가역(invertible) 이데알의 원상은 $h(D_f)/h(D)$개 씩 나타나기 때문에 이 원상들에서 유일한 기약 이데알을 다음과 같이 이데알의 norm의 크기를 이용하여 찾아낸다. $Cl(D)$의 임의의 기약이데알 J에 대하여 $I=\phi^{-1}(J)=J\cap O_K$는 원시(primitive) 가역 이데알이고 $N(J)=N(I)$이다.

따라서 $N(I)>\sqrt{|D|/4}$이 되도록 비 가역 이데알 I를 신중하게 선택하고, conductor f가 충분히 크고 보관이 잘 된다면 IQ_NMO 암호계의 안전성에 의하여 대단히 안전하다. 따라서 Kim 등의 암호계를 수정 보완하기 위해서는 conductor f를 신중하게 선택하여 비가역 이데알의 bonding homomorphism을 ϕ_k하에서의 원상을 찾기 어렵게 하는 것과, 그에 대응하는 위계집단의 수를 효율적으로 조절할 필요가 있다.

1) 정리 3에 의하여 위계집단을 서로 소인 집합(security classes) $U_1, U_2, \cdots, U_n$으로 나누고 각각 부분군 $G_1, G_2, \cdots, G_n$에서 이데알 곱셈을 하게 한다.

2) $S=\{U_1, U_2, \cdots, U_n\}$위에 준순서 관계 $\leq$ 를 다음과 같이 정의한다. 준순서 집합 $(S, \leq)$에서 관계 $U_i \leq U_j$는 U_i의 안전도가 U_j의 안전도 이하임을 뜻한다. 다시 말하면 U_j는 U_i의 정보를 알아낼 수 있지만, 반대로는 되지 않는다는 것을 의미한다.

3) 중앙통제소(CA)가 집단내의 구성원에게 저장시키거나 배포하려는 어떤 정보를 $I_m \in G_m$라고 하자.

여기에서 첨자 m은 U_m과 그이상의 집단 $(U_m \leq) U_i$만이 정보 I_m에 접근 가능함을 뜻한다.

4.3.2. 위계집단 $S=\{U_1, U_2, \cdots, U_n\}$에서의 효율적인 암호계

1) 충분히 큰 소인수를 가지는 conductor f를 선택한다.

2) f의 큰 소인수 k를 선택하여 비가역(non-invertible) 이데알 $E=[k,\gamma]$의 idempotent인 동치류 $\overline{E} \in Cls(O)$를 만든다.

3) 비밀키인 비가역 이데알 $K_0 \in G_k$를 선택한다.

4) 키 관리체제 작동과정

i) 두 이데알 E, F가 idempotent 이고, semilattice에서 관계 $E < F$가 주어지면, bonding homomorphism ϕ_{FE}: $G_E \rightarrow G_F$은 $\phi_{FE}(K_0)=EK_0$ 가 된다.

ii) CA는 idempotent E_{k_i} (단, $k_i | f$)를 각각의 사용자인 U_i에게 분배한다. 예를 들면 CA(U_1)는 비밀키 K_0와 E_{k_i}의 곱을 계산하여 $E_{k_2}K_0$, $E_{k_3}K_0$을 각각 U_2, U_3 에게 분배한다. 또한 CA는 $E_{k_2}E_{k_4}K_0$를 계산하여 U_4에게 보낸다. 이러한 방법으로 CA는 모든 사용자에게 키를 보낸다.

iii) 그러면, 상위의 사용자는 자기보다 하위의 사용자의 키를 모두 계산할 수 있게 된다.

5) 비밀키인 비가역 이데알 $K_0 \in G_k$의 정수부분을 이진수인 GMW 수열[10] 또는 Zeng 수열[11]로 변환하여 복잡도를 높인다.

4.3.3. 안전성

복소 이차 비최대 order 의 Clifford 반군에 기반한 암호체계 안전성은 Hũnlein[12]의 검증과 김용태[7]의 주장을 토대로 하면서, 제안하는 암호계의 안전성은 다음과 같은 사실에 근거하고 있다.

1) conductor f는 큰 소인수를 가지므로, 비밀키 K_0는 안전하다.

2) 비최대 order에서 비가역 이데알을 찾는 일은 매우 어렵다.

3) 위계의 상위자는 집단의 모든 정보의 흐름을 장악하게 되며, 위계의 하위자는 상위자의 정보를 알 수 없게 된다.

V. 결 론

위계집단에 안전한 암호계는 RSA가 안전하다는 배경으로 구축되었다. 본 논문에서는 Kim 등[5]이 제안한, 분배되는 이데알 EK_0를 알 때 키 이데알 K_0을 복원하는 것이 매우 어렵다는 점에 기반한 암호계를 분

석하여 그의 취약점을 개선, 보완한 효율적이고 안전한 암호계를 제안하였다. 이 암호계는 conductor f를 완전하게 소인수분해 하거나 또는 류 반군 $Cls(O)$의 구조를 완전히 파악하지 않는 한 위계집단에서는 안전한 암호계이다. 특히 비밀키인 비가역 이데알 $K_0 \in G_k$의 정수부분을 이진 수열로 변환한다면 키이데알과 idempotent 이데알의 상호상관관계가 낮아지기 때문에 [13] 더욱 안전하게 될 것이다.

감사의 글

이 논문은 2013년도 광주교육대학교 학술연구비 지원에 의한 것임

참고 문헌

[1] Selim G. Akl, Peter D. Talor, "Cryptographic Solution to a Multilevel Security Problem," CRYPTO 1982, pp. 237-249, 1982.
[2] S. J. MacKinnon, P. D. Taylor, H. Meijer, S. G. Akl, "An Optimal Algorithm for Assignment Cryptographic Keys to Control Access in a Hierarchy", IEEE Trnas. Computers Vol. 34, No. 9, pp. 797-802, 1985.
[3] 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.
[4] R. L. Rivest, A. Shamir, L. Adelman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", Comm. of ACM21 pp. 120-126, 1978.
[5] 김용태, "복소 이차체 위에서의 공개키 암호계에 관한 소고", 한국전자통신학회논문지, 4권, 4호, pp. 270-273, 2009.
[6] K. F. Gauss, "Disquisitiones Arithmeticae", translation A. C. Clarke, S.J., Yale Univ. Press, 1966.
[7] 김용태, "복소이차 류 반군위에서의 암호계의 안전성에 관한 소고", 한국전자통신학회논문지, 6권, 1호, pp. 90-96, 2011.
[8] P. Zanardo, U. Zannier, "The class semigroup of orders in number fields", Math. Proc.. Camb. Phil. Soc. 115, pp. 379-391, 1994.
[9] 김용태, "이차 복소 order에서의 계산 복잡도에 관한 소고", 한국전자통신학회논문지, 7권, 3호, pp. 545-551, 2012.
[10] 조성진, 임지미, 김진경, 김석태, "GMW 수열과 No 수열에 의해서 생성된 수열의 확장수열", 한국전자통신학회논문지, 7권, 2호, pp. 271-277, 2012.
[11] 김한두, 조성진, 권민정, 안현주, " 확장 Zeng 수열의 상호상관 함숫값에 대한 연구", 한국전자통신학회논문지, 7권, 1호, pp. 61-67, 2012.
[12] D. Hùnlein, "Cryptosystems based on quadratic orders", PhD-thesis, TU-Darmstadt, Germany, 2000.
[13] 최언숙, 조성진, 권숙희,"확장된 비선형 이진수열의 상호상관관계 분석", 한국전자통신학회논문지, 7권, 2호, pp. 263-270, 2012.

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