이차 복소 order에서의 계산 복잡도에 관한 소고

김용태*

Computational Complexity in Imaginary Quadratic Order

Yong-Tae Kim*

요 약

본 논문에서는 류수 계산의 복잡성과 소인수분해의 어려움을 덫으로 하는 IQC(Imaginary Quadratic Cryptosystem)에 기반을 둔 새로운 암호계를 제안한 다음, 그의 암호화와 복호화 시간을 줄이는 효율적인 알고리즘을 제시하기로 한다. 또한 제안하는 암호계의 안전성을 쉽게 알 수 있도록, 그 암호계의 가장 간단한 예를 들어 그 암호계에 사용되는 공개키 또는 비밀키의 복잡도와 안전성을 분석하고 제안된 암호계의 작동과정을 소개하기로 한다.

ABSTRACT

In this paper, we propose a new cryptosystem based on the IQC depended on the complexity of class number and intractibility of factoring integer, and introduce two algorithm which reduce encryption and decryption times. To recognize the security of the cryptosystem, we take a simple example to analyze the complexities of public key and secret key and then introduce the operating process of the cryptosystem.

키워드

imaginary quadratic cryptosystem(IQC), class number, discrete logarithm problem(DLP), computational complexity.
이차 복소 암호계, 류수, 이산대수문제, 계산복잡도

I. 서 론

이차복소 orded의 류군에 기반을 둔 암호계(IQC)는 1988년에 Buchman[1]에 의해서 소개되었으므로 Koblitz[2]가 제안한 ECC(elliptic curve cryptography)와 동시대에 사용되기 시작한 암호계이지만 상대적으로 덜 사용되어 왔다. 그 이유는 IQC에서 사용되는 scheme이나 공개키 또는 비밀키를 선정하는 형식을 갖춘 이론이 미약했기 때문이다. 그런데 2000년에 Hühnlein[3]이 이차복소 비최대 order에 기반을 둔 암호계를 발표하면서 다시 IQC에 기반을 둔 NICE(New Ideal Coset Encryption) 등의 암호계가 부활되어 현재에는 다양한 암호계가 소개되고 있다. 본 논문에서는 IQC를 기반으로 구축한 이산대수문제(DLP)와 ElGamal 등에 꼭 필요한 이차복소체의 류수(class number)를 분석하고, 류수 계산의 복잡도와 소인수분해의 어려움을 배경으로 하는 IQC에 기반을 둔 새로운 암호계를 제안하기로 한다. 이를 위하여 제 II 장에서는 이차복소체의 류수에 관하여 논의한 다음, 제 III 장에서는 IQC에 기반을 둔 새로운 암호계를 제

* 광주교육대학교 수학교육과 교수(ytkim@gnue.ac.kr)
접수일자 : 2012. 05. 08 심사(수정)일자 : 2012. 05. 25 게재확정일자 : 2012. 06. 07

안하고, 그 암호계의 가장 간단한 예를 들어 그 암호계에 사용되는 공개키 또는 비밀키의 복잡도와 안정성을 분석하고 제안된 암호계의 작동과정을 소개하기로 한다.

II. 이차 복소체의 류수

이차 복소체, 이차 복소 최대 order O_K와 류군(class group) $Cl(D)$, 이차 복소 비최대(Imaginary quadratic non-maximal) order(IQ_NMO)와 류 반군(class semigroup) $Cls(O_f)$, 이데알 I를 속(lattice) I=(A,B)로 표현하는 등의 이차체의 기본적인 성질은 [4]를 참고하면 된다.

2.1. IQ_NMO에서의 암호계에서는 IQ_NMO의 가역이데알(invertible ideal)의 집합인 Picard 군(group) $Pic(O_f)$의 크기와 비가역 이데알(non-invertible ideal)의 정체를 밝히는 일이다. 류반군 $Cls(O_f)$의 구성과정에서 명백히 $Cl(D) \subset Pic(O_f)$이다.

2.2. 판별식이 크면 이차 복소 최대 order인 O_K의 류수 역시 커지며, Gauss[5]에 의하면 판별식이 D인 O_K의 평균 류수는 $\overline{h(D)} = c_1\sqrt{D}, c_1 \approx 0.46$ 이고, 그 류수의 계산 복잡도는 다음과 같다[6].

판별식이 $D<0$인 모든 이차체에서 O_K의 류수 $h(D)$의 크기는 $h(D) > C(\epsilon)|D|^{\frac{1}{2}-\epsilon}$ 이며, 확장된 리만가설(ERH)이 성립한다면

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

이므로 $h(D) \approx \sqrt{|D|}$인 것으로 기대하게 되었다. 한편 Cox[7]는 두 conductor f인 비최대 order O_f의 류수 $h(D_f)$와 $h(D)$ 사이에는 다음과 같은 관계가 있음을 증명하였다.

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

증명) [7, 정리 7.25] 참조

단 O_K는 최대 order이고 $(\frac{D}{p})$는 Kronecker 기호이다. 즉, 이 정리에 의해서 류 반군 $Cls(O_f)$의 가역(invertible) 이데알의 집합인 Picard 부분군 $Pic(O_f)$의 위수인 $h(D_f)$는 최대 order의 류수인 $h(D)$의 배수인 사실을 알게 되었다. 현재에는 $h(D_f)$를 계산하는 정밀한 고속 알고리즘이 많이 등장하였지만, $D<0$ 인 경우에는 가우스 축소법[5]을 사용하는 것이 가장 효율적이며, 계산 속도를 향상시키기 위해서 현재까지 알려져 있는 이데알의 계산에 가장 효율적인 프로그램인 PARI패키지에서 GP언어를 이용하여 다음과 같은 이데알 축소법을 사용하면 기약(reduced) 이데알을 생성하는 계산 속도를 줄이게 된다.

2.3. 이데알 축소법

```
bqf(D)=
{
 local(b0=D%2, fv,a,c,zv);
 if(D>=0 || D%4>1, return([])'
 fv=[[1,b0,(b0^2-D)/4]];
 forset(b=b0, floorsqrt(-D/3), 2
    zv=divisors((b^2-D)/4);
    n=length(zv);
    forstep(j=(n+1)/2, 2, -1,
      a=zv[j] ; if (a<b, break) ;
      c=zv[n-j+1];
      if(gcd(gcd(a,b),c) !=, next);
      fv=concat(fv,[[a,b,c]]);
      if(b&&a != b && a != c,
fv=concat(ft,[[a,-b,c]]))) ;
 fv
 }
```

GP언어는 [8]을 참조하고, GP언어의 기초에 관해서는 [9]를 참조하면 된다.

III. IQ_NMO에서의 암호계

이 장에서는 IQ_NMO위에서 새로운 암호계를 구축한 다음, 그 암호계에 대한 계산 복잡도와 안전성을 논하기로 한다.

3.1. O_K의 이데알과 비최대 order O_f의 이데알

Cox[7]는 최대 order O_K의 이데알과 비최대 order O_f의 이데알 사이의 관계를 다음과 같음을 증명하였다.

정리 2. O_f의 모든 가역 이데알의 집합을 $\mathcal{I}$, O_K의 모든 가역 이데알의 집합을 $\mathcal{P}$라고 하면 다음이 성립한다.

1) 만일 $J\in\mathcal{P}$이면 $I=J\cap O_f\in\mathcal{I}$이고 $N(I)=N(J)$이다.
2) 만일 $I\in\mathcal{I}$이면 $J=IO_K\in\mathcal{P}$이고 $N(J)=N(I)$이다.
3) 사상 $\psi : J\mapsto J\cap O_K$ 는 동형사상 $\mathcal{P}\simeq\mathcal{I}$을 만들고, 이 사상의 역은 $\psi^{-1} : I\mapsto IO_K$이다.

증명) [7, Proposition 7.20 참조]

정리 2에서 사상 ψ는 전단사이므로 정의구역과 공변역을 바꾸어 $\psi^{-1}=\phi$로 놓으면, O_f의 비가역 이데알 I에 대하여 $J=IO_K$는 O_K의 가역 이데알이 되며, 두 이데알 I,J의 norm 은 같다. 마찬가지로 J가 O_K의 가역 이데알이면 $I=J\cap O_f$이고 $N(I)=N(J)$이다. 따라서 사상 $\phi : I\mapsto IO_K$는 두 집합 $\mathcal{I},\mathcal{P}$ 사이에 동형사상이 되며, ϕ의 역사상은 $\phi^{-1} : J\mapsto I=J\cap O_K$ 가 된다. 따라서 다음의 따름 정리가 성립한다.

따름정리 1. 만일 $I\in\mathcal{I}$가 기약이데알이면 $\phi(I)\in\mathcal{P}$도 기약이데알이다.

따름정리 2. 만일 $I\in\mathcal{I}$의 norm이 $\sqrt{|D|/4}$보다 작으면 $\phi(I)\in\mathcal{P}$는 기약이데알이다.

위의 사실을 이용하여 사상 ϕ를 빠르게 계산하기 위한 알고리즘은 다음과 같다.

3.1.1. 사상 ϕ의 계산알고리즘

O_K의 이데알 J의 기약이데알과 O_f의 이데알의 기약이데알을 각각 $Red_{O_K}(J)$, $Red_{O_f}(I)$로 표기하기로 한다.

Algorithm 1

Input : $Cls(O_f)$의 기약이데알 I, $Cls(D_f)$의 판별식 D_f, $Cl(D)$의 판별식 D, conductor f.

Output : $J=\phi(I)$.

1. A← a
2. $b_O \leftarrow D \bmod 2$
3. Solve $1=\mu f+\nu a$ for $\mu,\nu\in\mathbb{Z}$ using extended Euclidean algorithm
4. $B \leftarrow b\mu+ab_O\nu \mod 2a$
5. ideal (A,B) ← Red_{O_K}(A,B)
6. RETURN (A,B)

이 알고리즘의 매 단계에는 $O((\log\sqrt{|D|})^2)$ 비트 연산이 필요하기 때문에 이 알고리즘은 이차적 이므로 계산속도가 빠르다.

3.1.2. 역 사상 ϕ^{-1}의 계산 알고리즘

사상 ϕ는 전사이며 핵 $Ker(\phi)$는 $Cls(D_f)$의 부분군이다. 따라서 $Cl(D)$의 임의의 기약이데알의 원상은 $h(D_f)/h(D)$개 씩 나타나기 때문에 이 원상들에서 유일한 기약이데알을 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. 이때 따름정리 2,3에 의해서 만일 $Cls(D_f)$의 가역 이데알 I의 norm $N(I)<\sqrt{|D|/4}$이면 I,J 모두 기약이데알이 된다. 그러므로 $Cls(D_f)$의 모든 가역 이데알 I의 norm $N(I)<\sqrt{|D|/4}$으로 한정하면, $\phi(I)\cap O_K$는 기약이데알이 되므로 사상 ϕ의 유일한 역상을 계산할 수 있게 된다. 이렇게 조건이 제한된 역사상 ϕ^{-1}의 효율적인 계산 알고리즘은 다음과 같다.

Algorithm 2

Input : 기약이데알 $J=(A,B)\in Cl(D)$, 단 $N(I)<\sqrt{|D|/4}$, f는 conductor

Output : 기약이데알 $I\in Cls(D_f)$, $\psi^{-1}(J)=I=(a,b)$.

1. a ← A
2. b ←Bf mod 2a
3. RETURN (a,b)

이 알고리즘 역시 매 단계에는 $O((\log\sqrt{|D|})^2)$ 비트 연산이 필요하기 때문에, 이 알고리즘은 이차적 이다. 또한 위의 알고리즘의 효과적인 H/W 실행에 고속 연산기[10]를 적용하면 암호화와 복호화를 더욱 빠르게 할 수 있다.

3.2. 제안하는 IQ_NMO 암호계

$D<0, f$는 D_f를 소인수분해 할 수 없는 충분히 큰 conductor f를 선택한다.

전송할 메시지 M은 norm 이 $\sqrt{|D|/4}$보다 작은 $Cl(D)$의 기약이데알이다.

1. 키 생성

비트 길이가 $\lfloor \sqrt{|D|/4} \rfloor$ 와 $\frac{h(D_f)}{h(D)}$사이의 두 정수 k,l와 $\phi(P)$가 O_K에서 principal 이데알이 되는 이데알 $P\in Cls(D_f)$ 를 선택한다. 이 때, (P, D_f, k, l)이 암호계의 매개변수이며 D, f는 비밀키이다.

2. 암호화

평문(plaintext) M은 $Cls(D_f)$에서 기약이데알이고 $\log_2 N(M) < k$인 기약이데알이면, 임의로 $l-1$ 비트인 정수 r을 선택하여

$C = Red_{D_f}(MP^r)$을 계산한 후에 C를 암호문으로 보낸다.

3. 복호화

비밀키 D, f를 이용하여 받은 암호문 C를 Algorithm 1으로 계산하여 기약이데알 $\mathcal{R}$을 계산한 다음, $\mathcal{R}$을 Algorithm 2 로 계산하여 평문 M을 복원한다.

4. 암호계의 정당화

암호화는

$\phi(MP^r) = \phi(M)\phi(P^r) = \phi(M)O_K = \phi(M)$ 으로

계산되며, 복호화는 $M = \phi^{-1}(\phi(M))$이다.

5. 평문(plaintext)의 이데알화

비밀문장을 수로 바꾼 메시지를 x라 하고 길이가 $k-2-\lfloor \log_2 x \rfloor$ 인 임의의 정수를 t라고 하자.

x와 t의 비트고리를 $x \bullet t$로 표기하자. 그러면 $(D_f/l) = 1$이고 $x \bullet t$보다 큰 가장 작은 솟수 l을 정할 수 있다. 또한 $-l < b < l$이면서 $D_f \equiv b^2 \bmod 4l$이 되는 정수 b를 계산하면 $I = (l, b)$는 $\log_2 N(I) < k$인 기약이데알이 된다.

6. 키 생성과정과 복잡도

norm 이 $\sqrt{|D_f|/4}$ 보다 작은 이데알 $J\in O_K$를 선택하여 $P = \phi^{-1}(JO_K)$를 계산하면 $P\in Ker_\phi$가 된다. 암호화는 이진 지수이므로 $O((\log\sqrt{|D_f|})^3)$ 비트 연산이 필요하며, 복호화는 이차적인 두 개의 알고리즘을 포함하므로 $O((\log\sqrt{|D_f|})^2)$ 비트 연산이 필요하게 된다.

결론적으로, 제안하는 IQ_NMO 암호계에서의 암호화과정과 복호화과정은 이차적 또는 3차적이기 때문에 H/W실행 시간은 짧게 된다.

3.3. IQ_NMO 암호계의 안전성

3.3.1. 비밀키의 크기

IQ_NMO 암호계는 판별식 D_f의 소인수분해가 어렵다는 덫에 기초를 두고 있다. 만일 D_f가 완전하게 소인수분해가 된다면 우리의 암호계는 완전하게 파괴되고 만다. 이 점을 고려하여 비밀키인 판별식 D와 conductor f의 크기를 충분히 크게 한다.

3.3.2. 사상 ϕ의 안전성

공격자는 O_f의 어떤 이데알 I에 대하여 $\phi(I)\in O_K$를 계산할 수도 있다. 그런데 $\phi(I)$를 계산하는 일은 D_f를 계산하는 것만큼 intractible하다.

3.3.3. 류반군 $Cls(D_f)$ 위에서의 암호계의 안전성

이산대수문제(DLP)에 대해서는, 류군 $Cl(D)$위에서의 암호계보다 류반군 $Cls(D_f)$위에서의 암호계는 다음과 같은 이유에서 훨씬 더 안전하다. $Pic(O_f)$에서의 이산대수문제를 류 반군 $Cls(D_f)$에서의 DLP로 바꾸는 데에는 $\log|D_f|$의 준지수적(subexponential) 실

행시간이 필요하다[11]. 또한 $Cls(D_f)$에서의 DLP의 계산과정은 ϕ의 원상인 가역이데알을 찾는 것이고, 그 원상은 항상 $h(D_f)/h(D)$개 씩 나타나게 된다. 따라서 그러한 ϕ의 원상들 중에서 DLP를 만족하는 가역이데알을 찾는 방법은 무작위적일 수밖에 없다. 즉, 원상 중에서 이데알을 무작위로 선택하여 DLP의 충족여부를 조사하는 반복적인 과정을 거쳐야 하기 때문에, 여기에 필요한 실행시간 역시 준지수적이다. 따라서 비밀키를 크게 선택하여 소인수분해가 불가능하다면 IQ_NMO 암호계는 매우 안전하다.

3.3.4. 류반군 $Cls(D_f)$의 비가역이데알

최대 order O_K의 류군 $C(O_K)$의 모든 이데알은 소 이데알(prime ideal)의 곱으로 유일하게 인수분해 되지만, 비최대 order O의 류반군 $Cls(O)$의 비가역 이데알은 소 이데알의 곱으로 유일인수분해가 되지 않는다.[6].

3.4. $f=q$, q는 솟수, 인 암호계

이 장에서는 IQ_NMO 암호계의 구체적인 작동과정을 설명하기 위해서 conductor f가 솟수 q인 간단한 경우를 예로 제시한다 .

3.4.1. 사상(map) $Cls(D_q) \rightarrow Cl(D)$

만일 conductor인 f가 솟수 q인 때에는 $\sqrt{|D|/3} < q$ 이다. 그러면 O_K의 모든 기약 이데알은 conductor q와 서로 소가 되므로[7] 사상 ϕ에 의하여 류 반군 $Cls(D_q)$와 $Cl(D)$ 사이에 다음과 같은 사상이 주어지게 된다.

ψ_q : $Cls(D_q) \rightarrow Cl(D)$

$I \mapsto IO_K$,

단, I, IO_K는 모두 기약 이데알이다.

ψ_q의 계산은 다음과 같다.

Algorithm 3

Input : $Cls(O_q)$의 기약이데알 I, $Cls(D_q)$의 판별식 D_q, $Cl(D)$의 판별식 D, conductor q.

Output : $J=\psi_q(I)$.

1. A← a
2. $b_O \leftarrow D \bmod 2$
3. Solve $1=\mu q+\nu a$ for $\mu,\nu\in\mathbb{Z}$ using extended Euclidean algorithm
4. B ← $b\mu+ab_O\ \nu \mod 2a$
5. ideal (A,B) ← Red_{O_K}(A,B)
6. RETURN (A,B)

또한 f가 솟수 q인 경우에 ${\psi_q}^{-1}$의 계산 방법은 다음과 같다.

$Cls(D_q)$의 모든 기약이데알의 norm은 $\sqrt{|D|/3}$ 보다 작으며, 우리의 가정에 의해서 norm이 $\sqrt{|D|/3}<q$ 인 $Cl(D)$의 모든 기약이데알은 q와 서로 소이기 때문에, $Cl(D)$의 임의의 기약이데알 J에 대하여 $I=\phi^{-1}(J)=J\cap O_K$는 원시(primitive) 가역 이데알이고 $N(J)=N(I)$이다. 이때 만일 $Cls(D_q)$의 가역 이데알 I의 norm $N(I)<\sqrt{|D|/4}$ 이면 I,J 모두 기약이데알이 된다. 그러므로 $Cls(D_q)$의 모든 가역 이데알 I의 norm $N(I)<\sqrt{|D|/4}$ 으로 한정하면, $\psi_q(I)\cap O_K$는 기약이데알이 되므로 사상 ψ_q의 유일한 역상을 계산할 수 있게 된다. 이렇게 조건이 제한된 역사상 ψ_q^{-1}의 계산 알고리즘은 다음과 같다.

Algorithm 4

Input : 기약이데알 J=(A,B)$\in Cl(D)$, 단 $N(I)<\sqrt{|D|/4}$, q는 conductor

Output : 기약이데알 $I\in Cls(D_q)$,

단 $\psi_q^{-1}(J)=I$=(a,b).

1. a ← A
2. b ←B$q \mod 2a$
3. RETURN (a,b)

따라서 $f=q$, q는 솟수, 인 경우의 암호계는 3.2. 절에서 제안된 암호계에서 위에서$f=q$, q는 솟수로 치환한 암호계이며, 그의 계산 복잡도는 다음과 같다.

3.4.2. 사상 ϕ의 안전성

만일 공격자가 conductor q를 아는 경우에는 사상

ψ_q를 계산할 수 있고 따라서 모든 메시지 이데알을 복원할 수 있게 된다. 사상 ψ_q는 $\psi_q = Red_{O_K} \circ \phi$로 구성되어 있기 때문에, 임의의 이데알 $I \in Cls(D_f)$의 O_K에서의 상 $\phi(I)$를 계산할 수 있다면 메시지를 복원할 수 있게 된다. 따라서 이 암호계에서는 conductor q가 알려지지 않도록 해야 한다. 따라서 이 암호계의 안전성은 conductor q가 충분히 크고 보관이 잘 된다면 3.3절에 언급한 IQ_NMO 암호계의 안전성에 의하여 대단히 안전하다.

3.4.3. 암호계의 비밀키의 크기

우선 이변수 함수 $L_n[s,c]$를 다음과 같이 정의하자. $L_n[s,c] = \exp((c+o(1))\log^s n \log\log^{1-s} n))$

그러면 $|D_q|$를 소인수분해하는 데에 소요되는 실행시간은 $L_{|D_f|}[1/3, (64/9)^{1/3}]$이다[12]. 만일 D_q를 768 비트 이상으로 정하면 수체 선별법(number field sieve)으로서는 인수분해가 불가능해 진다. 또한 타원곡선법을 이용하면, 예상되는 실행시간은 $L_q[1/2, 2^{1/2}]$이고, q의 크기를 256 비트 이상으로 정하면 타원곡선법 역시 인수분해가 불가능 해진다.

IV. 결 론

현재에는 IQC의 여러 가지 성질들을 이용하여 ECC 또는 RSA를 공격하는 방안들이 연구되고 있다. 예를 들면 잘 알려진 동형 $E(GF(p)) \simeq O_f/(\pi-1)O_f$, $\pi \notin \mathbb{Z}$,를 이용하여 ECC를 분석하거나, $Cls(O_f)$의 구조를 연구하여 RSA를 분석하려는 노력이 계속되고 있기 때문에 IQC에 기반한 암호계의 연구가 더욱 중요하게 되었다. 본 논문에서는 IQC에 기반한 암호화와 복호화가 빠른 새로운 IQ_NMO 암호계를 제안하여 비밀키와 공개키의 생성과정을 설명하였으며 암호계의 복잡도와 안정성을 분석하였다. 본 논문의 내용중의 일부를 이용하여 ECC에 기반하여 발전해온 DLP, ElGamal 암호계, RSA 등의 공격에 응용 할 수 있다.

감사의 글

본 논문은 광주교육대학교 2012년도 학술진흥장학재단의 후원으로 수행되었음.

참고 문헌

[1] J. Buchmann, H. C. Williams “A key-exchange system based on imaginary quadratic fields”, Journal of Cryptology 1,3 pp.107-118, 1988.

[2] N. Koblitz, “Elliptic curve cryptosystems”, Math. Comp., 48, pp.203-209, 1987.

[3] D. Hühnlein, “ Efficient implementation of cryptosystem based on non-maximal imaginary quadratic orders, Proc. of SAC’99, Springer, LNCS 1758, pp.150-167, 2000.

[4] 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.

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

[6] 김용태, 복소이차 류 반군위에서의 암호계의 안전성에 관한 소고, 한국전자통신학회논문지, 6권, 1호, pp. 90-96, 2011.

[7] D. Cox, Primes of the form $x^2 + ny^2$, John Wiley & Son, New York, 1989.

[8] http://www.math.edu/users/villegas/gpbook

[9] http://pari.math.u-bordeau.fr/

[10] 김용태, “Efficient Serial Gaussian Normal Basis Multiplier over Binary Extension Fields, 한국전자통신학회논문지, 4권, 3호, pp. 197-203, 2009.

[11] 김용태, “복소 이차체위에서 공개키 암호계에 관한 소고, 한국전자통신학회논문지, 4권, 4호, pp. 90-96, 2009.

[12] D. Hühnlein, “Cryptosystems based on quadratic orders, PhD-thesis, TU-Darmstadt, Germany, 2000.

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