Regular paper

Journal of the KIECS. pp. 737-744, vol. 13, no. 4, Aug. 31 2018, t. 90, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2018.13.4.737

RSA 암호계에 대한 결정적 공격법에 관한 연구

김용태*

On a Deterministic Attack Against The RSA Cryptosystem

Yong-Tae Kim*

요 약

RSA 암호계는 가장 널리 쓰이는 공개키 암호계로서, 암호화뿐만 아니라 전자서명이 가능한 최초의 알고리즘으로 알려져 있다. RSA 암호계의 안정성은 큰 수를 소인수 분해하는 것이 어렵다는 것에 기반을 두고 있다. 이러한 이유로 큰 정수의 소인수분해 방법에 많은 연구가 진행되고 있으나, 지금까지 알려진 연구 결과는 모두 실험적이거나 확률적이다. 본 논문에서는, 복소 이차체의 order의 류 반군의 구조와 비 가역 이데알의 성질을 이용하여 인수분해를 하지 않으면서 큰 정수의 소인수를 구하는 알고리즘을 구성한 다음, RSA 암호계에 대한 결정적 공격법을 제안하기로 한다.

ABSTRACT

The RSA cryptosystem is a one of the first public-key cryptosystems and is widely used for secure data transmission and electric signature. The security of the RSA cryptosystem is based on the difficulty of factoring large numbers.. Though many studies on finding methods for factoring large numbers are going on, the results of that are all experimental or probabilistic. We, in this paper, construct an algorithm for finding large prime factors of integers without factoring integers using properties of the structure of semigroup of imaginary quadratic order and non-invertible ideal, then propose our methods foe deterministic attack against RSA cryptosystem.

키워드

RSA Cryptosystem, Deterministic Attack, Class Semigroup, Non-Invertible Ideal
RSA 암호계, 결정적 공격, 류 반군, 비가역 이데알

Ⅰ. 서 론

RSA 암호계는 1978년에 MIT 교수이던 Rivest, Shamir와 Adleman의 연구[1]에 의해 체계화되었으며, RSA 암호계는 공개키 암호시스템의 하나로, 암호화뿐만 아니라 전자서명이 가능한 최초의 알고리즘으로 알려져 있다. RSA 암호계가 갖는 전자서명 기능은 인증을 요구하는 전자 상거래 등에 RSA 암호계의 광범위한 활용을 가능하게 하였다. RSA 암호계의 안정성은 큰 수를 소인수 분해하는 것이 어렵다는 것에 기반을 두고 있다. 이러한 관점에 초점을 맞추어 지난 40년 동안 RSA 암호계를 공격하기 위한 많은 연구가 진행되고 있다. 그러나 지금까지 어떤 양의 실수 k에 대해서 b-bit 정수를 다항식 시간(polynomial time) 즉, $O(b^k)$안에 소인수분해 할 수 있는 알고리즘이 알려지지 않고 있다. 양자 컴퓨터를 이용하지 않는다는

* 교신저자: 광주교육대학교 수학교육과
• 접 수 일 : 2018. 06. 01
• 수정완료일 : 2018. 07. 08
• 게재확정일 : 2018. 08. 15
• Received : Jun. 01, 2018, Revised : Jul. 08, 2018, Accepted : Aug. 15, 2018
• Corresponding Author : Yong-Tae Kim
Dept. of Mathematics Education, Gwangju National University of Education
Email : ytkim@gnue.ac.kr

전제하에서, 100자리 이상의 큰 정수 N을 소인수분해 하는 지금까지 알려진 가장 빠른 알고리즘은 일반 수체 체(general number field sieve, GNFS)알고리즘이며, 몇 가지 실험을 통하여 얻은 정수 $n(\lfloor \log_2 n \rfloor +1)$ 비트의 소인수분해 복잡도는 $\exp((\sqrt[3]{\frac{64}{9}}+o(1))(\ln n)^{\frac{1}{3}}(\ln\ln n)^{\frac{2}{3}}) = L_n[\frac{1}{3}, \sqrt[3]{\frac{64}{9}}]$이다.

이 방법은 유리수 체(rational sieve) 또는 이차 체(quadratic sieve)를 개선한 것으로, 이 방법을 이용하여 큰 정수 n을 소인수분해 할 때에는 n-smooth number 만을 찾으면 된다는 장점이 있다. 또한 20~25 자리의 수(64.~83 비트)정도의 소인수를 찾아내는 가장 빠른 알고리즘은 1985년에 Lenstra가 제안한 유한체 위에서의 타원곡선법이다. 타원곡선법을 이용하여 현재까지 찾아낸 가장 큰 약수는 2013년에 R. Propper가 찾아낸 83자리 수이다. 그러나 그의 방법은 타원곡선의 개수를 충분히 크게 하여 그 중에서 우연히 약수를 얻는 확률적인 방법으로, 약수의 자릿수가 증가함에 따라 필요한 타원곡선의 개수가 비선형적(non-linear)으로 증가하기 때문에 일반화하기에는 적절하지 않은 방법으로 간주되고 있다. 결과적으로 큰 정수를 소인수분해하는 가장 효과적인 두 방법은 모두 실험적이거나 확률적이다[2]. 한편, 복소 이차체 위에서의 암호계를 처음으로 고안한 사람은 Buchmann 과 Williams[3]이다. 그들은 Gauss의 저서 정수론[4]의 복소 이차체와 이데알의 이론을 이용하여 기존의 키 분배(key-exchange) 체계와 그의 안전성을 새로운 방향으로 정립하였으며 그의 제자들[5]에 의해서 후속연구가 진행되고 있다. 그 후, Zanardo와 Zannier의 연구[6]를 시작으로 수체에서 order의 류 반군의 구조와 이데알의 성질을 밝히는 연구가 계속되고 있다. 본 논문에서는 복소 이차체의 류 반군, 이데알 등의 대수적 구조와 이진수열의 성질 등에 관한 연구[7-8]를 이용하여, 큰 수(10^{400} 이상)를 소인수분해를 하지 않으면서 소인수를 구하는 알고리즘을 구성하고, 이를 이용한 RSA 암호계에 대한 결정적 공격법을 제안하고자 한다.

II. RSA 암호계의 개요와 알려진 공격법

이 장에서 사용하는 용어와 기호는 대부분 [1-2]를 참조하였다.

2.1 RSA 암호계의 개요

RSA 암호계는 두 개의 키를 사용한다. 여기서 키란 메시지를 열고 잠그는 상수(constant)를 의미한다. 일반적으로 많은 공개키 알고리즘의 공개키(public key)는 모두에게 알려져 있으며 메시지를 암호화(encrypt)하는데 쓰이며, 암호화된 메시지는 개인키(private key)를 가진 자만이 복호화(decrypt)하여 열어볼 수 있다. 하지만 RSA 공개키 알고리즘은 이러한 제약조건이 없다. 즉 개인키로 암호화하여 공개키로 복호화할 수도 있다.

A라는 사람(Alice)이 B라는 사람(Bob)에게 메시지 M을 전하고자 할 때 A는 B의 열린 자물쇠를 들고와 그의 메시지 M을 봉인(공개키 암호화 과정에 해당)하고, 그런 다음 B에게 전해 주면, 자물쇠의 열쇠(개인키에 해당)를 가지고 있는 B가 그 메시지 M을 열어보는(개인키 복호화 과정에 해당) 방법이다. 그렇지만 중간에 그 메시지를 가로채는 사람(eavesdropper)은 그 열쇠를 가지고 있지 않으므로 메시지 M을 열람할 수 없도록 만든 암호계이다.

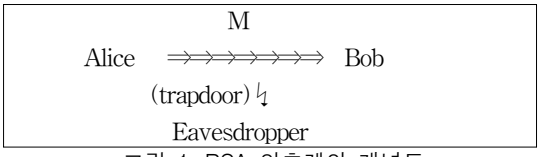

그림 1. RSA 암호계의 개념도
Fig. 1 The concept of RSA cryptosystem

즉, Alice 와 Bob 이 유무선으로 주고받는 메시지 M은 언제든지 도청을 당하고 있다는 가정 하에서, 주고 받는 내용을 도청 또는 해킹을 통하여 메시지 M을 알아내는 경우에도 그 내용이 무엇인지를 알아 볼 수 없도록 덫(trapdoor)을 설치해서, 비밀키를 알고 있는Alice 와 Bob만이 알 수 있고 도청자(eavesdropper)는 알 수 없도록 만든 암호계이다.

• RSA 암호계의 덫은 자연수의 소인수분해가 어렵다는 사실이다.

2.2 키의 생성

A와 B가 보안이 보장되어 있지 않은 환경에서 서로 비밀 메시지를 주고받고 싶다고 가정하자. A가 B에게 메시지를 전달하기 위해서는 B의 공개키가 필요하다. B는 아래와 같은 과정으로 그만의 공개키와 개인키를 제작한다.

1) 두 개의 서로 다른 큰(10^{200}이상) 소수(prime number) p 와 q 를 선택한다.
2) 두 수의 곱 $N=pq$를 계산한다.
3) $\phi(N)=(p-1)(q-1)$을 계산한다. 단, ϕ는 Eulerd의 totient 함수이다.
4) $1<e<\phi(N), \gcd(e,\phi(N))=1$ 인 정수 e 를 찾는다.
5) 확장된 유클리드 호제법을 이용하여 $de\equiv 1 \bmod \phi(N)$인 정수 d를 구한다.
6) B의 공개키는 $<N,e>$, 개인키는 $<N,d>$ 이다. B는 $<N,e>$만을 A에게 공개하고, A는 이 공개키를 사용하여 자신의 메시지를 암호화하게 된다.

2.3 암호화

A가 M이란 메시지를 B에게 보내고 싶다고 하자. 일단 A는 이 M을 N보다 작은 수 m으로 변환한다. 이 변환법(padding scheme)은 B에게도 미리 알려져 있어야 한다. 예를 들면, 메시지를 토막내어 하나의 메시지가 일정 수의 비트를 넘지 않게 하는 방법이 있다. 하지만 실제로는 이중보안을 위해 더욱 복잡한 변환법이 사용된다. 그리고 A는 B의 공개키 $<N,e>$를 획득하고, 다음과 같이 c를 계산한다.

$$m^e \equiv c \bmod N. \quad (1)$$

그리고 이 c를 B에게 보낸다.

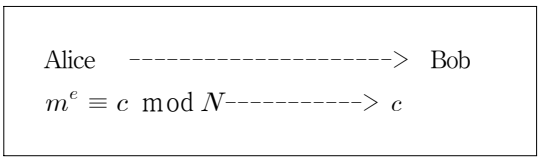

그림 2. 암호문의 전송
Fig. 2 The transmission of encrypted message

2.4 복호화

B는 A에게서 받은 암호화된 메시지 c에서 N,d를 이용하여. 다음과 같이 m을 복원한다.

$$c^d \equiv (m^e)^d \equiv m^{1+\phi(N)t} \quad (2)$$
$$\equiv m(m^{\phi(n)})^t \equiv m\times 1^t \equiv m \bmod N$$

왜냐하면 $de\equiv 1 \bmod \phi(N)$ 이므로 $de=1+\phi(N)t$이기 때문이다.

2.5 RSA 암호계의 안전성

N을 공개하지만 도청자가 $N=pq$ (400자리정도)의 소인수 p 와 q를 알지 못하면

$$\phi(N)=\phi(pq)=\phi(p)\phi(q)=(p-1)(q-1) \quad (3)$$

의 값을 구하기는 현재의 컴퓨터로서는 거의 불가능하다. 따라서 일차합동식$de\equiv 1 \bmod \phi(N)$을 만족하는 비밀키 d의 값을 알 수가 없기 때문에 는 것이다.

2.6 RSA 암호계에 대한 알려진 공격법

이절에서는 지금까지 알려진 RSA 암호계에 대한 공격법 중에서 [9]를 참조하여 중요한 이론 몇 가지를 요약하기로 한다.

- Coppersmith의 공격법
  Coppersmith[10]의 정리를 적용하여, 공격자(attacker)는 공개키를 이용하여 평문을 암호화하여 RSA 암호계에 대한 선택적 평문 공격을 완료한 다음, 도청한 암호문과의 동등성을 검증하는 공격법이다.
- 중국인의 나머지 정리(Chinese Remainder Theorem) 공격법
  Open SSL, Java, NET 등의 다양한 암호화 저장함수에 대하여 중국인의 나머지정리를 기반으로 하는 서명과 복호법을 이용하여 공격하는 방법이다.
- 인수분해 공격법
  RSA암호계의 덫인 공개키 $N=pq$을 두 소인수 p 와 q로 인수분해하는 공격법으로, 성공한다면 RSA 암호계를 완전하게 깨트리는 가장 결정적인 공격법이다. 따라서 정수를 소인수분해하는 다양한 수학적인 방법이 연구되고 있으며 거꾸로 이 공격법을 방어하기 위한 수의 임의생성 기법[11]이 다양하게 연구되고 있다.

- 부채널 분석(side-channel analysis) 공격법
  자료처리기(processor) 에서는 프로그램의 지시 흐름에서 조건부 가지(branch)의 선택여부를 결정하는 가지 예상자(branch predictor)를 결정한다. 이러한 가지 예상자 등을 이용하여 부분적으로 암호계를 분석하는 공격법이다[12].

이 중에서 Coppersmith의 공격법, 중국인의 나머지 정리 공격법, 부채널 분석 공격법 등은 부분적 또는 확률적 공격법이고 인수분해 공격법은 결정적 공격법이다. 인수분해 공격법은 기존(classical)의 컴퓨터상에서 기존의 알고리즘을 사용한다면 400자리 정수를 200자리의 두 소수로 인수분해 하는데 걸리는 시간은 400만년 이상 걸리게 된다고 알려져 있다[2]. 그런데 현재 개발 중인 양자(quantum)컴퓨터상에서 그에 맞도록 개발된 알고리즘을 사용한다면 기대이상으로 빠른 시간에 정수의 소인수분해가 이루어진다고 보고 있으나 양자컴퓨터를 완전하게 상용화하는 데에는 앞으로 30년 후에나 가능할 것으로 예견되고 있다[13].

III. 복소 이차체 류 반군의 구조

이 장에서는 복소 이차체 류 반군에 기반하는 새로운 인수분해 공격법을 제안하고자 한다.

3.1 복소 이차체 비-최대 류반군의 구축

복소 이차체 order의 기호는 [14]를 따르고 최대 order와 비최대 order의 관계는 [15]를 참고하기로 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 이차체가 되며 K의 최대 order를 O라고 하자. 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, 또한 K안에서 $w=(D+\sqrt{D})$로 놓으면, 판별식이 $D_f=f^2D$인 order는 $O_f=[1, fw]$이고 이때 $f=[O:O_f]$이며 f를 O_f의 conductor라부며, $f>1$이면 order $O_f=[1, fw]$를 비최대 order이라고 부른다. 비 최대 order O_f의 임의의 이데알은 $A=[a,b+c\gamma]$, $\gamma=fw$, $a,b,c\in\mathbb{Z}$, $a>0,c>0,c|a,c|b$ 이고 $ac|N(b+c\gamma)$이다. 또한 O_f의 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. $I(O_f)$를 O_f의 0이 아닌 분수 이데알, $P(O_f)$를 O_f의 0이 아닌 주이데알(principal ideal)이라 할 때, $Cls(O_f)=I(O_f)/P(O_f)$를 복소 이차체 K 또는 비최대 order O_f의 류 반군(class semigroup)이라고 정의한다.

3.2 류 반군 $Cls(O_f)$의 구조

Zanard 등[6]은 수체의 한 order의 류 반군의 구조를 설명하였다. 특히, order가 이차인 경우에는 류 반군 $Cls(O_f)$는 Clifford 반군이 되므로, 다음과 같은 대수적 구조에 대한 다음의 동치 명제가 성립한다는 사실을 보였다.

(C1) Clifford 반군 $Cls(O_f)$에 속하는 모든 원소 x는 $Cls(O_f)$의 한 군 G_k에 속한다.

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

(C3) $Cls(O_f)$ 는 군 G_k들의 semilattice이다.

위의 동치명제 중에서 우리 논문에 중요한 내용은 (C3)의 $Cls(O_f)$는 군 G_k들의 semilattice라는 사실이다. 그러면 $Cls(O_f)$는 다음과 같은 성질을 갖게 된다.

1) $Cls(O_f)$는 군 G_k들의 서로 소인 합집합으로 표현된다. 단, $k\in\mathscr{E}$, $\mathscr{E}$는 semilattice이다.
2) $h,k\in\mathscr{E}$가 $\mathscr{E}$ 안에 주어진 부분 순서관계 $h\le k$가 있으면 bonding 준동형사상(homomorphism) $\phi_{h,k}: G_h\to G_k$ 가 존재한다.

이때, order O_f의 0 아닌 이데알 E 에 대하여, $E^2=\lambda E$, $\lambda\in K^*$ 이 성립하는 이데알 E의 동치류

$\overline{E}$를 idempotent라고 부르거나 이데알 E를 idempotent라고 부르며, semilattice $\mathscr{E}$은 $Cls(O_f)$의 모든 idempotent $\overline{E}$들로 구성된다.

정리 1. ([6], Proposition 13)

$Cls(O_f)$의 모든 idempotent는 $k|f$에 대하여 $E=[k,b_k]$형태인 이데알의 동치류 $\overline{E}$이다.

정리 2.([6], CLAIM 참조) 임의의 이차 order O의 모든 이데알은 $I=h[q,a+\eta]$인 형태로 표현된다. 단, $a,h,q\in\mathbb{Z}^+, q|N(a+\eta), 0\le a<q, hq$는 이데알 I에 포함되는 최소 자연수이다. 또한 부분군 $h<q,a+\eta>$ 가 O-이데알이 될 필요충분조건은 $q|N(a+\eta)$ 이다.

그러면 $\overline{E}$는 f의 유일한 약수 k와 일대일 대응을 하며, $Cls(O_f)$의 idempotent는 부분군 G_k들과 일대일 대응을 하게 된다. 만일 e 가 $Cls(O_f)$의 한 idempotent 원소일 때 대응하는 부분군은 다음과 같다.

$$G_e = \{\ x\in Cls(O_f)\mid xe=x\text{이고}\quad xy=e,\ y\in Cls(O_f)\} \tag{4}$$

따라서 $Cls(O_f)$는 군 G_e들로 분할된다. 그러므로 최대 order O와 $E_k=[k,f\omega]$, 단 $k|f$, 는 idempotent이다. 또한 $Cls(O_f)$의 부분군 G_1은 O_f의 모든 가역 이데알의 집합이므로 Picard 군이며, 나머지 부분군의 원소는 모두 비가역(non-invertible) 이데알의 동치류이다. 지금, 본 논문의 전개의 필요에 따라 임의의 O_f-이데알 $I=[a,b+\gamma]$에 대하여

$$\gcd(I)=\gcd(a, Tr(b+\gamma), N(b+\gamma)) \tag{5}$$

로 정의한다.

이제, $Cls(O_f)$의 특징을 몇 가지 소개하기로 한다. Gauss[4]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 3. 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 dD는 모두 짝수이든지 또는 모두 홀수(same parity)이므로 $k\eta-\gamma\in k\mathbb{Z}$이다. 따라서 $[k,k\eta]=[k,\gamma]$ 이다.

정리 4. 두 O_f-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

$$\gcd(U(x,y))=k=lcm(k_1,k_2) \tag{6}$$

이다.

이러한 사실과 동치조건 (C3)에서, $Cls(O_f)$의 구조는 다음과 같음을 알 수 있다.

정리 5. 류 반군 $Cls(O_f)=\dot{\bigcup_{k|f}} G_k$, 단 G_k, $k|f$, 는 $\gcd(A)=k$인 모든 O_f-이데알 A를 포함하는 집합이고 서로 소이다. 단, $G_k=\{\overline{I}\in Cls(O_f)\mid IE_k\sim I$이고 $\overline{J}\in Cls(O_f)$가 존재하여 $IJ\sim E_k\}$이다.

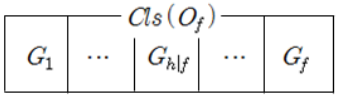

그림 3. 류 반군 $Cls(O_f)$의 구조
Fig. 3 The structure of $Cls(O_f)$

IV. 복소 이차체 류 반군에 기반한 새로운 공격법

이장에서는 RSA 암호계에 대한 결정적 공격법인 복소 이차체 류 반군에 기반하는 새로운 인수분해 공격법을 제안하고자 한다.

4.1 제안하는 RSA 에 대한 공격법

RSA 암호계에 대한 결정적 공격법은 덫인 $N=pq$를 소인수분해하거나 N의 소인수 p또는 q를 찾는 것이다. 큰 정수의 소인수분해법에 관한 방법은 잘 알려져 있으며 끊임없이 연구가 진행되고 있다. 그러나 우리가 제안하는 공격법은 N을 소인수분해하지 않고 이제 복소 이차에의 류 반군의 구조와 bonding 준동형사상의 성질에 기반하여 직접 N의 소인수 p또는 q를 찾는 방법이다. 이제 제안하는 공격법의 알고리즘에 필요한 몇 가지 정리들을 인용하기로 한다.

먼저, 정리 5에서 제시한 Clifford 반군 $Cls(O_f)$의 서로 소인 부분군 G_k들 사이에서 주어지는 bonding 준동형사상에 의해서 도출되는 Zanardo 등[6]의 정리를 소개하고 부분군 G_k에 속하는 원소(동치류)들 간의 중요한 관계를 인용하기로 한다.

정리 6. ([6], Proposition 16, 17] 참조) k가 conductor f의 약수일 때, $E_k=[k,\gamma]$는 idempotent 이고, I를 $\bar{I}\in G_k$ 인 O_f-이데알이라 하자. 그러면 가역 이데알 $J\in G_1$이 존재하여 $I\sim JE_k$이다.

따라서 정리 6에 의하면 Clifford 반군 $Cls(O_f)$의 모든 bonding 준동형사상은 전사(surjective)이다.

정리 7. ([16], Proposition 2.3) 비최대 order O_f의 두 이데알 $I=[a_1,b_1+\gamma]$와 $J=[a_2,b_2+\gamma]$에 대하여 $\bar{I},\bar{J}\in G_k$일 필요충분조건은

$$\gcd(I)=\gcd(J) \tag{8}$$

이다.

정리 8. conductor 가 f인 order D_f 의 류 반군 $Cls(O_f)$에는 모든 $k|f$에 대하여 $\gcd(E)=k$인 idempotent 이데알 E가 유일하게 존재한다.

(증명) 정리 1과 정리 3에 의해서 자명하다.

따름정리 9. p,q가 소수, conductor $f=pq$ 일 때, $\gcd(E)=p$ 또는 q인 idempotent 이데알 E가 $Cls(O_{pq})$에 존재하며, 부분군 G_p의 임의의 비가역 이데알 J에 대하여 $\gcd(E)=\gcd(J)=p$ 이다.

(증명) 정리 5과 정리 7과 정리 8에서 의해서 자명하다.

그러면 정리 5와 따름정리 9에 의하여 $Cls(O_{pq})$의 구조는 다음과 같다.

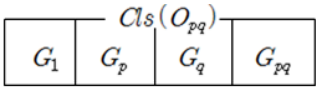

그림 4. 류 반군 $Cls(O_{pq})$의 구조
Fig. 4 The structure of $Cls(O_{pq})$

4.2 결정적 공격 알고리즘

이 절에서는 인수분해 방법을 사용하지 않고, RSA 암호계의 공개키이면서 덫인 $N=pq$의 소인수 p또는 q를 찾는 알고리즘을 제안하기로 한다.

Algorithm

Step 1. 판별식 $D<0$ 가 아주 작은 이차체 $K=\mathbb{Q}(\sqrt{D})$을 선택한다.

Step 2. conductor $f=pq$인 비최대 order $O_{pq}=\mathbb{Z}[\eta]$를 구축한다. 단, $\eta=pq\sqrt{D}$

Step 3. 복소 이차 order O_{pq}의 류 반군 $Cls(O_{pq})$의 구조를 구성한다.

Step 4. $Cls(O_{pq})$의 가역 이데알의 bonding 준동형사상 $\phi_{1,p}$ 또는 $\phi_{1,q}$의 이미지인 G_p 또는 G_q의 비가역 이데알 J를 구한다.

Step 5. $\gcd(J)$를 구한다.

위의 Algorithm의 타당성을 다음 정리에서 증명한다.

정리 10. 위의 Algorithm을 실행하면 $N=pq$의 소인수 p또는 q를 구하게 된다.

(증명) 잘 알려져 있는 바와 같이, 초등 정수론에

의하면 비가역 이데알의 특징은 소(prime) 이데알들의 곱으로 유일하게 인수분해가 되지 않으며, 그러한 비 가역 이데알은 수체에 무한히 많이 있다[14]. 따라서 모든 비 최대 order O_f의 류반군 $Cls(O_f)$에는 무수히 많은 비가역 이데알이 존재한다. 정리 8에 의해서 $\gcd(E)=p$ 또는$\gcd(E)=q$인 $Cls(O_{pq})$의 idempotent 이데알 E가 유일하게 존재한다. Algorithm의 Step 4에서 구한 G_p 또는 G_q의 비 가역 이데알 J는 따름정리 9에 의하여 $J\in G_p$인 경우에는 $\gcd(J)=p$, $J\in G_q$인 경우에는 $\gcd(J)=q$이다. 따라서 어느 경우에든 공개키 N의 소인수인 p 또는 q를 구하게 된다.

4.3 $Cls(O_f)$의 비가역 이데알의 구축 예시

Algorithm과 정리 10에서 알 수 있듯이, 류 반군 $Cls(O_f)$의 비가역 이데알을 찾는 일이 매우 중요하다. 이제, 복소 이차체 $K=\mathbb{Q}[\sqrt{-5}]$에서 류 반군 $Cls(O_f)$의 비가역 이데알을 찾는 구체적인 예를 알아보기로 한다. K의 최대 order는 $O=\mathbb{Z}[\sqrt{-5}]$, conductor p인 비최대 order는 $O_p=\mathbb{Z}[\eta]$, 단, $\eta=p\sqrt{-5}$, p는 10^{20}정도의 소수이다. 그러면 정리 1에 의해서 $Cls(O_p)$의 idempotent는 $\overline{O}$ 와 $\overline{E}$, $E=[p,\eta]$ 2개뿐이므로 정리 5에 의해서 $Cls(O_p)=G_1\cup G_p$ 이다. 이제 $G_p\neq\{\overline{E}\}$임을 보이고자 한다. 다시 말하면, 부분군 G_p는 항등원 $\overline{E}$ 이외의 동치류를 갖는다는 사실을 보이고 또한 bonding 준동형사상 $\phi_{1,p}: G_1\to G_p$ 가 존재하여 $\phi_{1,p}(\overline{I})=\overline{I}\,\overline{E}\neq\overline{E}$ 임을 보이고자 한다. $p>2$이므로 $I=[2,1+\eta]$는 가역(invertible) 이데알이다. 따라서 $\overline{I}\in G_1$이고 $IE\sim E$임을 보이면 된다. 귀류법을 적용하여, 만일 $IE=\lambda E, \lambda\in K$라고 가정해 보자. 그러면

$$(\lambda E)(\lambda E)'=(IE)(IE)'=2pE \tag{9}$$

그러므로

$$2pE=N(\lambda)EE'=N(\lambda)pE. \tag{10}$$

식 (10)에 의해서

$$2E^e=2pO=N(\lambda)E^e=N(\lambda)pO. \tag{11}$$

따라서 $\frac{N(\lambda)}{2}$는 $O\cap\mathbb{Q}$이므로 $N(\lambda)=2$.

따라서 모두는 0이 아닌 정수 $x,y,z\in\mathbb{Z}$가 존재하여 등식 $x^2+5y^2=2z^2$ 이 성립한다. 그러나 이것은 모순이다. 왜냐하면 등식 $x^2+5y^2=2z^2$의 양변에 $\bmod 5$를 취하면 $x^2\equiv 2z^2 \bmod 5$ 가 되지만, 5를 법(modulo)으로 2는 제곱일 수 없기 때문이다. 따라서 idempotent E와 동치가 아닌 비가역 이데알 IE가 존재하며 정리 7에 의해서

$$\gcd(IE)=\gcd(E)=p \tag{12}$$

이므로 원하는 소수 p를 찾게 된다.

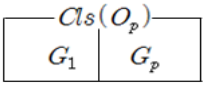

그림 5. 류 반군 $Cls(O_p)$의 구조
Fig. 5 The structure of $Cls(O_p)$

V. 결 론

본 논문에서는 복소 이차체의 비최대 order의 류 반군의 구조를 분석하였다. 그 후, 류 반군에 속하는 비가역 이데알 의 성질을 이용하여 큰 정수를 인수분해를 하지 않고 그의 소인수를 구하는 알고리즘을 구성하였다, 또한 그 알고리즘을 적용하여 RSA 암호계의 덫인 공개키 $N=pq$를 인수분해를 하지 않고 그의 소인수 p 또는 q를 구하는 결정적 공격법을 제안하였으며 공격법의 핵심인 비가역을 구하는 예를 들었다. 개발 중인 양자 컴퓨터가 상용화되어 큰 수의 인수분해 실행 속도가 급격하게 빨라지기 전까지는 RSA 암호계는 계속 사용될 것이다. 제안하는 결정적 공격법에 대한 후속 연구가 지속되기를 기대한다.

감사의 글
본 논문은 2018년도 광주교육대학교 학술연구비 지원에 의한 것임

References

[1] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and

Public-Key Cryptosystems," *Comm. of the Association for Computing Machinery*, vol. 21, no. 2, 1978, pp. 120 - 126.

[2] G. Simmons, *Contemporary Cryptology; The Science of Information Integrity*. New York: IEEE Press, 1992.

[3] J. Buchmann and H. Cilliams, "A key-exchange system based on imaginary quadratic fields," *J. of Cryptology* vol. 1, no. 3, 1988, pp.107-118.

[4] K. Fauss, *Disquisitiones Arithmeticae*. New Haven, USA: Translated by A. C. Clarke, Yale Univ. Press, 1966.

[5] G. Catagnos and F. Laguillaumite, "On the Security of Cryptosystems with Quadratic Decryption; The Nicest Cryptanalysis," In *Proc. of Eurocrypt '09, Köln, Germany, Lecture Notes in Computer Science 5479, Springer-Verlag*, Berlin, Germany, 2009, pp.260-277.

[6] P. Zanardo and U. Zannier, "The class semigroup of orders in number fields", *Mathematical Proc. Philosophy Society*. vol. 115. no.1, London, 1994, pp.379-391.

[7] M. Kwon, S. Cho, J. Kim, and U. Choi, "Rearrangement of Sequences through the Generation Principle," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 13, no. 1, 2018, pp. 133-140.

[8] H. Kim, S. Cho, and U. Choi, "On the Construction of the 90/150 State Transition Matrix Corresponding to the Trinomial $x^{2^n-1}+x+1$," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 13, no. 2, 2018, pp. 383-389.

[9] A. Lone and M. Udd, "Common attacks on RSA and its variants with possible countermeasures," *Int. J. of Emerging Rearch in Management & Technology*, vol. 5, no.5, 2016, pp.65-70.

[10] D. Coppersmith, "Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities," *J. of Cryptology*, vol 10 no. 4, 1997, pp. 233 - 260.

[11] U. Choi, S. Cho, H. Kim, M. Kwon, and S. Kim,"Synthesis of 90/102(170)/150 linear CA using 90/150 linear CA," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 9, 2016, pp. 885-891.

[12] A. Schlösser, "Hot electron Luminescence in silicon structures as photonic side channel." Ph.D. thesis, *Berlin Institute of Technology*, Berlin, 2014.

[13] R. Alvarez, X. Zhou, and J. O'Brien, "Experimental realization of Shor's quantum factoring algorithm using qubit recycling," *Nature Photonics*, vol. 6 no.11, 2012, pp. 773-779.

[14] W. Adams and L. Goldstein, *Introduction to number theory*. New Jersey, USA: Prentice-Hall, 1976.

[15] D. Cox, "*Primes of the form* x^2+ny^2." New York, USA: John Wiley & Sons, 1989.

[16] M. Jacobson, Jr., "The Security of Cryptosystems Based on Class Semigroups of Imaginary Quadratic Non-maximal Orders," *ACISP 2004, Sidney, July, Lecture Notes in Computer Science 3108, Springer-Verlag. Berlin*, 2004, pp.149-156.

저자 소개

김용태(Yong-Tae Kim)

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