通信情報保護學會論文誌
第 1 卷, 第 1 號, 1991. 12

이원 이차형과 암호론

최 영 주*

Binary Quadratic Forms and Cryptography

Young-Ju Choie

요 약

리듀스드 이원이차형을 사용한 키 교환법이 소개되었다. 이는 실이차체의 클래스군 위에서의 이산대수문제의 어려움을 이용한 것이다.

Abstract

The key exchange idea by using a reduced binary indefinite quadratic form has been introduced. This is based on the difficulty of solving the discrete logarithm problem on the class group of a real quadratic field.

1. Introduction

Secret messages have been sent and used in military affairs and diplomacy for a long time. Furthermore, nowadays, because of the widespread usage of electronic communication such as electronic banking or electronic mail by computer, secrecy has become an important issue. Hence, there is a tremendous deal of interest in the techniques of making messages meaningless to everyone except the intended receiver.

Cryptograpy is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message, while *cryptanalysis* is aimed at breaking these systems. The message we want to send is called the *plaintext* and the disguised message is called the *ciphertext*. A *cipher* is a method for changing a plaintext into ciphertext using transformation f. The process of altering a plaintext to

* 포항공과대학 수학과

a ciphertext by using enciphering transformation is called *enciphering* or *encryption* and one needs a enciphering key k_E. the reverse process is called *deciphering* or *decryption*. In order to decipher, compute f^{-1}, one needs the deciphering key k_D. With a conventional cryptosystem anyone who knew enough to encipher a message could, with little effort, determine the deciphering key.

However, W. Diffie and M. Hellman[6] discovered an entirely different type of cryptosystem and invented *public key cryptography*. A public key cryptosystem has the property that someone who knows only how to encipher cannot use the enciphering key to find the deciphering key without a prohibitively lengthy computation. In other words the enciphering function f is easy to compute once the enciphering key k_E is known, but is is very hard in practice to compute the inverse function f^{-1} without the deciphering key k_D, from the standpoint of realistic computability. Such a function is called an *one-way trapdoor function*. The most important public cryptographic problems are those of *privacy* and *authentication*. A privacy system is preventing a unauthorized extraction of information from communications over an insecure channel. An authentication system prevents a unauthorized injection of messages into a public channel, assuring the receiver of a message of the legitimacy of its sender.

It has been known that number theory plays a very important role in public key cryptography. The most famous applications of number theroy to cryptography are in the RSA system[7] and Diffie and Hellmans's cryptosystem[6]. The RSA system used the difficulty of prime factorization of a large number and Diffie and Hellmans's cryptosystem used the difficulty of solving a discrete logarithm problem on a finite field. The purpose of this paper is to introduce the key exchange idea by using a reduced binary indefinite quadratic form. This is based on the difficulty of solving the discrete logarithm problem on the class group of a real quadratic field.

2. Real quadratic field and Indefinite binary quadratic forms

Let F_i be the ith Fibonacci number, *i.e*, $F_0=0$, $F_1=1$, and $F_{m+1}=F_m+F_{m-1}$, where $m \in$ N. Let $K=Q(\sqrt{F_{2m}^2+1})$ be the quadratic field formed by adjoining $\sqrt{F_{2m}^2+1}$ to the rational Q. We first review some of the properties of K. The discriminant of a field K is given by

$$\Delta = \begin{cases} 4(F_{2m}^2+1) & \text{if } m \equiv 0 \pmod 3 \\ F_{2m}^2+1 & \text{if } m \equiv 0 \pmod 3 \end{cases}$$

Also, if α, $\beta \in$ K, we use $\bar{\alpha}$ to denote the conjugate of α in K, $S(\alpha)=\alpha+\bar{\alpha}$ is the trace of α, $N(\alpha)=\alpha\bar{\alpha}$ the norm of α.

The integers of K are those elements α of K such that both $S(\alpha)$ and $N(\alpha)$ in Z; We denote the set of these integers by Θ_K. It is well known that $\Theta_K=[1, w]=Z+wZ$, where

$$w = \begin{cases} \sqrt{(F_{2m}^2+1)} & \text{if } m \not\equiv 0 \pmod 3 \\ \dfrac{1+\sqrt{F_{2m}^2+1}}{2} & \text{if } m \equiv 0 \pmod 3 \end{cases}$$

Let us denote an indefinite binary quadratic form with discriminant $D=b^2-4ac>0$ as follows;

$$f(x, y)=ax^2+bxy+cy^2=f=[a, b, c]$$

Definition 2. 1 (1) *$f=[a, b, c]$ is said to be a reduced form if $a>0$, $c>0$, $b>a+c$, where a, b, c are rational integers. Furthermore, if $gcd(a, b, c)=1$, we call $f=[a, b, c]$ a* primitive *reduced from.*
(2) *Let $f(x, y)=ax^2+bxy+cy^2$ with discriminant D not a perfect square. If there exist integral p, q, r, s such that $ps-qr=1$ with the following property:*

$$x=px^*+qy^*,\ y=rx^*+sy^*,$$

then $f(x, y)=f^*(x^*, y^*)$. Then we say f is equivalent to f^*, and write $f\approx f^*$: or we say f and f^* are in the same *Γ-equivalence class.*

Let us state some well known theorems without proof.

Theorem 2. 1 (1) *There are only finitely many reduced quadratic forms of discriminant D, and each Γ-equivalence class* E *of forms of discriminant D contains at least one reduced form.*
(2) *Let us assume that the form $f=[a, b, c]$ in a Γ-equivalence class* E *is a reduced form.*
(Note. *$f=[a, b, c]$ is a reduced form, $D=b^2-4ac$,*

iff $w=\dfrac{b+\sqrt{D}}{2}>1$ *and* $0<\bar{w}<1$.)

The reduced forms in E *form a cycle $f_0=f$, f_1, f_2, $\cdots$, $f_l=f_0$, where each f_j is related to its prodecessor by $f_j=f_{j-1}\circ M_j$ with $M_j=\begin{pmatrix} n_j & -1 \\ 1 & 0 \end{pmatrix}$ for some integer $n_j\geq 2$, and $f\circ M$ is defined by $f\circ M=f(\alpha x+\beta y, \gamma x+\delta y)$, for $M=\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ and the $M_j=\begin{pmatrix} n_j & -1 \\ 1 & 0 \end{pmatrix}$ are determined by the minus continued fraction expansion of*

$$w=\frac{b+\sqrt{D}}{2}=n_1-\cfrac{1}{n_2-\cfrac{1}{n_3-\cfrac{1}{\cdots-\cfrac{1}{n_l-\cfrac{1}{\cdots}}}}}$$
$$=(n_1, n_2, n_3, .., n_l).$$

which is purely periodic, i.e, *$n_j=n_{j+l}$, becauses f is reduced. Therefore, each reduced form f_0, f_1, f_2, $\cdots$, $f_l=f_0$ in* E *corresponds to a cycle*

$$(n_1, n_2, n_3, \cdots, n_l),\ (n_2, n_3, \cdots, n_1),$$
$$(n_3, n_4, \cdots, n_1, n_2),\ \cdots$$

(Proof) See[4], for instance.

Definition 2.2 (1) *Let us give a dictionary order relation on the cycles in*

$$\{(n_1, n_2, n_3, \cdots, n_l),\ (n_2, n_3, \cdots, n_1),$$
$$(n_3, n_4, \cdots, n_1, n_2),\ \cdots\}.$$

In other words,

$$(n_1, n_2, n_3, \cdots, n_l) > (m_1, m_1, m_3, \cdots, m_l)$$

by defining $n_j>m_j$, or if *$n_j=m_j$ and $n_{j+1}>m_j+1$, where $1\leq j\leq l$. And let each reduced form in* E *corresponds to each cycle*

$$(n_1, n_2, n_3, \cdots, n_l),\ (n_2, n_3, \cdots, n_1),$$
$$(n_3, n_4, \cdots, n_1, n_2),\ \cdots,\ (n_l, n_1, \cdots, n_{l-2}, n_{l-1}),$$

and let $f_l=f_0$. We call the reduced form f the largest reduced form *if f corresponds to the largest cycle among all the cycles which correspond to all the reduced forms in Γ-equivalence class.*
(2) If two forms with discriminant equal to a field discriminant, f_1 *and* f_2, *then a* form f_3 *with the same discrimiant,*

$$f_3(x_3, y_3)=f_1(x_1, y_1)\ f_2(x_2, y_2)$$

(ordinary multiplication) is defined by special bilinear expressions with integral coefficients A_i *and* B_i:

$$x_3 = A_1x_1x_2 + A_2x_1y_2 + A_3x_2y_1 + A_4x_2y_2,$$
$$y_3 = B_1x_1x_2 + B_2x_1y_2 + B_3x_2y_1 + B_4x_2y_2.$$

Theorem 2. 2 (1) *To compound* $f=[a, b, c]$ *with itself, let* $n=gcd(a, b)$, *and solve* $by/n \equiv 1$ (mod a/n) *for* y. *Then* $[a, b, c] \circ [a, b, c] \approx [a^2/n^2, b-2acy/n, *]$ *with the third coefficient computed from the discriminant formula.*

(2) *To compound* $f_1=[a_1, b_1, c_1]$ *and* $f_2=[a_2, b_2, c_2]$, *let* $\beta=(b_1+b_2)/2$. *Let* $m=gcd(a_1, \beta)$, *and* $n=gcd(m, a_2)$. *Solve* $a_1x+\beta y=m$ *for* x *and* y *and*

$$mz/n \equiv x\left(\frac{b_2-b_1}{2}\right)-c_1y \ (mod\ a_2/n)\ for\ z.$$

The form compounded of f_1 *and* f_2 *is then*

$$[a_1a_2/n^2, b_1+2a_1z/n, *],$$

with the third coefficient being computed from the discriminant formula.

(*Proof*) See page 64-65[1].

Remark (1) For a given form f and integer x, f^x can be computed by using the repeated squaring method, *i, e.*, change x into a binary digit number and find the composition form f^x by using *Theorem 2. 2*. It involves only Euclidean algorithm and, therefore, takes a polynomial number of bit operations to compute f^x.

(2) The largest reduce form can be found by using the (minus) continued fraction. Once we find one cycle which corresponds to a reduced form, it is easy to find the largest reduced form in one Γ-equivalence class by sorting all the reduced cycles in the class.

3. A key exchange system

In this section we describe a public key exchange system: a scheme by which two individuals A and B, who never meet, can still develop a secret key for communication over a public channel. The basic idea is due to that of Diffie and Hellman by using the *discrete logarithm* problem: Let A and B agree on some finite group G and some element g in G, both of which can be made public. A selects some positive integer $a(<ord(G))$ at random, keeps it secret and transmits $x=g^a$ to B. B selects some positive integer $b(<ord(G))$ at random, keeps it secret and transmits $y=g^b$ to A. A determines $K=y^a$ and B determines $K=x^b$; K is used as the secret communication key. If one could determine a or b from knowing x, y, g and G, one could compute K. The problem of determining a, given G, g and x, is called *the discrete logarithm* problem in G. In this section we will present a key exchange system when G is the class group of a real quadratic field $Q(\sqrt{F_{2m}^2+1})$, where F_{2m} is the $2m^{th}$ Fibonacci number. This scheme is based on those of [2] and [6].

The real quadratic field $Q(\sqrt{F_{2m}^2+1})$ and a binary indfinite quadratic form $f=[a, b, c]$ whose discriminant is the same as the field discriminant (see[4]) are publically known. The following steps are performed to exchange a secret key between two users A and B:

(1) A selects at random a large integer m and d and computes the largest reduced form f_1 such that $f_1 \approx f^d$ by using repeated squaring method and

an algorithm given in *Theorem 2. 2.* (m, f_1) is sent to B.

(2) B selects t at random and computes the largest reduced form f_2 such that $f_2 \approx f$ by using the repeated squaring method and an algorithm given in Theorem 2. 2 and sends f_2 to A.

(3) A computes the largest reduced form $f^* \approx f_2^d$. B computes the largest reduced form $f^{**} \approx f_1^t$. Since $f^* \approx f_2^d \approx (f^t)^d = (f^d)^t \approx f_1^t \approx f^{**}$, we have the largest reduced form $f^* = f^{**} = [a, b, c]$; this number $[a, b, c]$ can be used as the secret key between A and B.

Remark we note that this key exchange system prevents a cryptanalyst from attacking all files simultaneously, by using a different m for each user. Even though an attacker has solved the discrete logarithm in the field $Q(\sqrt{F_{2m}^2+1})$ for a certain m, this does not solve it for other m.

4. Complexity Result

We begin with the following remark.

Remark For given α, β in Θ_K, the ring of integers of K, we say that α divides β and denote this by $\alpha \mid \beta$ if there exists some γ in Θ_K such that $\beta = \alpha\gamma$. If $\eta \mid 1$, η is called a unit of K. It is known that there are infinitely many units in Θ_K; If η is one of them, then η can be written as $\eta = \pm \varepsilon^n$, where n integer and $\varepsilon (>1)$ is the fundamental unit of K.

Lemma 4. 1 *The fundamental unit of* Θ_K *can be found by considering the smallest integer* T *for which*

$$T^2 - DU^2 = \pm 4, \ T>0, \ U>0,$$

in the field $K = Q(\sqrt{D})$. *Then the fundamental unit of* Θ_K *is* $\frac{T+U\sqrt{D}}{2}$ *and most general unit is* $\pm [\frac{T \pm U\sqrt{D}}{2}]^m$.

(*Proof*) See page 101[5].

The regulator $\log \varepsilon = R$ of K determines the number l of reduced forms in any Γ-equivalence class because $l < (R+c)/\gamma$ (where $\gamma = (1+\sqrt{5})/2$) for some constant c, *i.e*, $l = O(R)$.

Theorem 4. 1 *Let* l *be the number of a indefinite binary reduced quadratic form in* Γ *a equivalence class of the field* $Q(\sqrt{F_{2m}^2+1})$. *Then* $l \approx O(2m)$.

(*Proof*) We note that the fundamental unit of $Q(\sqrt{F_{2m}^2+1})$ is $(F_{2m} + \sqrt{F_{2m}^2+1})$. Since we get

$$T^2 - U^2 = -4, \ T = 2F_{2m}^2, \ U = 1,$$

the fundamental unit $\varepsilon = F_{2m} + \sqrt{F_{2m}^2+1}$, from the Lemma 4. 1. So, the regulator $R = \log\varepsilon = \log(F_{2m} + \sqrt{F_{2m}^2+1}) \approx \log 3 F_{2m}$. Since $\log F_{2m} \approx \log(\frac{1+\sqrt{5}}{2})^{2m}$, $l \approx 2m$.

Remark (1) To get the largest reduced form f^* from given form f in the class E of $Q(\sqrt{F_{2m}^2+1})$, we need to compute a cycle whose length is $O(2m)$ which takes a polynomial bit operation of Δ, *i.e*, log Δ. So, it will take a polynomial bit operation for user A and B to get the common public key f^*.

(2) This system would be broken if we could solve the discrete logarithm problem in the class group G of $Q(\sqrt{F_{2m}^2+1})$. This problem can be solved in sub-exponential time by the index calculus me-

thod if the class number h of $Q(\sqrt{F_{2m}^2+1})$ is known. However, the best algorithm known for determining h has the complexity $O((\Delta)^{\frac{1}{5}+o(1)})$, assuming the extended Riemann hypothesis[5].

References

1. D.A.Buell, Binary Quadratic Forms, *Springer-verlag*, 1989.
2. J.Buchmann and H.C.Williams, Quadratic Fields and Cryptography, in Number Theory and Cryptography, *London Math. Soc. Lecture Note Series* 154, pp.9-25.
3. J.Buchmann and H.C.Williams., A key exchange system based on imaginary quadratic fields, *Jour. of Cryptology* No. 1, 107-118, 1988.
4. YJ. Choie, Rational period functions, Class numbers and Diophantine equations, *submitted* 1990.
5. H. Cohen, A Course in Algorithmic Algebraic Number theory, *Lecture notes*.
6. W. Diffie and M.Hellman, New directions in cryptography, *IEEE Trans. Informat. Theory* IT-22, pp. 644-654, 1976.
7. R.Rivest, A.Shamir, and L.Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communicatins of the ACM* Vol. 21, pp.120-126, 1987.

□ 著者紹介

崔 暎 周(正會員)

1982년 2월 이화여자대학교 이학사
1986년 5월 Temple 대학교 이학박사
1986년 5월~1988년 8월 Ohio 주립 대학교 강사
1988년 9월~1990년 1월 Maryland 대학교 조교수(방문)
1989년 9월~1990년 1월 Colorado 대학교 조교수
1990년 2월~현재 포항공과대학 조교수