JSIAM Letters Vol.2 (2010) pp.81–84 ©2010 Japan Society for Industrial and Applied Mathematics

On a knapsack based cryptosystem using real quadratic and cubic fields

Keiichiro Nishimoto[1] and Ken Nakamula[1]

[1] Mathematics and Information Sciences, Graduate School of Science and Engineering, Tokyo Metropolitan University, 1-1 Minami-Osawa, Hachioji, Tokyo 192-0397, Japan

E-mail *nishimoto-keiichiro@ed.tmu.ac.jp*

Received December 21, 2009, Accepted March 20, 2010

Abstract

In [1], a knapsack based cryptosystem is proposed using number fields as a scheme of quantum public key cryptosystems. We studied on key generation of this scheme in the case of imaginary quadratic fields [2]. In this paper, we study the cases of real quadratic fields and cubic fields. We first give some propositions for practical key generation. We then estimate various densities of the generated knapsack problems for these cases and for the imaginary quadratic case. We further generate explicit public keys and knapsack problems for several special cases and test the resistance against low-density attacks.

Research Activity Group Algorithmic Number Theory and Its Applications

1. Introduction

Shor proved that the integer factoring problem and the discrete logarithm problem (DLP) could be solved in polynomial time by using the quantum turing machine (QTM) in [3]. Therefore, public-key cryptosystems based on these problems are not secure when a QTM is realized. A concept of quantum public-key cryptosystem (QPKC) with a concrete scheme (OTU2000) in [1] gives the first answer to this problem. OTU2000, a knapsack based cryptosystem, seems to be secure even against QTM adversaries. We need QTMs only to solve the DLP in number fields for generating public keys from private keys. We are interested in generating keys without QTMs and estimating its security. We gave practical key generation algorithms for imaginary quadratic fields in [2].

The purpose of this paper is to give some propositions and to report the results for OTU2000 over real quadratic and cubic fields. As a consequence, we can efficiently generate explicit public keys such that low-density attacks almost always fail at the stage of solving the shortest vector problem.

In Section 2, we generalize the practical key generation algorithm for imaginary quadratic fields in [2] to arbitrary fields. In Section 3, we give important propositions to implement OTU2000 over real quadratic fields and cubic fields. In Section 4, we show experimental results about various densities of the generated knapsack problem and study the resistance against low-density attacks. In Section 5, we discuss conclusions and future problems.

2. Key generation of OTU2000

First, we generalize the key generation algorithm in [2]. Let K be a number field defined by a monic irreducible polynomial $f \in \mathbb{Z}[x]$ of degree r, $\mathcal{O}_K$ the ring of integers of K, and $\omega_1 := 1, \omega_2, \ldots, \omega_r$ form an integral basis of K. We also define a subset A_t of $\mathcal{O}_K$ by

$$A_t := \left\{ z_1\omega_1 + \cdots + z_r\omega_r \;\middle|\; z_i \in \mathbb{Z},\ -\frac{t}{2} \le z_i \le \frac{t}{2} \right\}. \quad (1)$$

Algorithm 1 Given (n, k, f), this algorithm outputs a private key (f, g, e, p, S) and a public key (n, k, b).

1. Choose $\ell \in \mathbb{Z}$ suitably, and let P be the set of prime elements of K in $A_{2\ell}$.
2. Randomly take a subset $S = \{S_1, \cdots, S_n\}$ of n non-associate elements of P.
3. Choose a rational odd prime number p so that $p\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$ satisfying the following condition (2), and randomly choose $g \in \mathcal{O}_K$ such that $\langle g \pmod{p\mathcal{O}_K} \rangle = (\mathcal{O}_K/p\mathcal{O}_K)^\times$.

$$\prod_{j=1}^{k} S_{i_j} \in A_p \quad \text{for} \quad \forall \{S_{i_1}, \cdots, S_{i_k}\} \subset S. \quad (2)$$

4. Randomly choose $e \in \mathbb{Z}$ with $0 \le e \le p^r - 2$. For each i from 1 to n, compute a_i such that $g^{a_i} \equiv S_i \pmod{p\mathcal{O}_K}$ and compute $b_i \equiv a_i + e \pmod{p^r - 1}$. Set $b := (b_1, \cdots, b_n)$. Then output the private key (f, g, e, p, S) and the public key (n, k, b).

Remark 2 *Actually, we implemented and experimented under the following settings. We set ℓ to be the smallest so that $A_{2\ell}$ has at least n non-associate prime elements of K. If q is the smallest p satisfying (2), we take p in the step 3 randomly between q and $2q$. Then S is almost determined by ω_i and n, but it does not cause a problem since K and p are still hidden.*

3. Real quadratic fields and cubic fields

We first give important propositions to implement OTU2000 over real quadratic fields and cubic fields. Different from the imaginary quadratic case, there are two difficulties in Algorithm 1 when we take S and p. One is how to judge associate in P. It is easy to judge associate in imaginary quadratic fields since the group of units is finite and simple. In order to judge associate in other fields, there are so many $\alpha, \beta \in A_{2\ell}$ with the same norm, and it is necessary to compute and see whether $\alpha/\beta \in \mathcal{O}_{\mathcal{K}}$ for each such pair, since the group of units is infinite. Hence, we change the step 1 as follows:

1. Let $P = \emptyset$. Repeat the following by increasing ℓ until P has at least n element. For each $\pi \in A_{2\ell}$, if π is a prime element with norm coprime to any element of P, then replace P by $P \cup \{\pi\}$. For each $\pi \in P$, if π' is a non-associate conjugate of π which belongs to $A_{2\ell}$, then replace P by $P \cup \{\pi'\}$.

Then P does not have associate elements.

Next is how to verify the condition (2). There is a simple sufficient condition of (2) for imaginary quadratic fields using norms [1,2]. Then, to choose p, we may compute norms n times instead of computing multiplications $\binom{n}{k}$ times. There is, however, no such sufficient condition for real quadratic fields and cubic fields. Therefore, we propose several sufficient conditions in the following.

3.1 The case of real quadratic fields

Proposition 3 *Let $K = \mathbb{Q}(\sqrt{\theta})$ be a real quadratic field and $\mathcal{O}_K = \mathbb{Z}[\omega]$ be the ring of integers of K, where θ is a square-free positive integer, $\omega = (1+\sqrt{\theta})/2$ if $\theta \equiv 1 \pmod 4$ and $\omega = \sqrt{\theta}$ otherwise. For $z_{ij} \in \mathbb{Z}$ and $z_i \in \mathbb{Z}_{>0}$, write $\prod_{j=1}^{k}(z_{1j} + z_{2j}\omega) = X_1 + X_2\omega$ and $(z_1 + z_2\omega)^k = X_1{}' + X_2{}'\omega$ with $X_i, X_i{}' \in \mathbb{Z}$. Assume $|z_{ij}| \le z_i$ $(i = 1, 2, j = 1, \dots, k)$. Then $|X_i| \le X_i{}'(i = 1, 2)$.*

Proposition 3 means that the product of k integers in $A_{2\ell}$ always belongs to A_p if the condition

$$(\ell + \ell\omega)^k \in A_p \tag{3}$$

holds. Namely, (3) is a sufficient condition of (2). Therefore, we can choose p by one power computation. The size of p, however, grows big as θ grows big in general. So we propose the following proposition to make the size of p as small as possible.

Proposition 4 *Let $K, \mathcal{O}_K$ and ω be as above. Write $(c + \omega/c)^k = X_{1,c} + X_{2,c}\omega$, where c is a positive integer. Put $c_m := \lfloor \sqrt{\omega} + 0.5 \rfloor$. Then the minimum $X_{i,c}$ is X_{i,c_m} if $\omega = \sqrt{\theta}$ and is X_{i,c_m} or $X_{i,c_m \pm 1}$ otherwise $(i = 1, 2)$.*

By Proposition 4, if we let P be a subset of the set $\{z_1 + z_2\omega \,|\, z_i \in \mathbb{Z}, |z_1| \le \ell c, |z_2| \le \lfloor \ell/c \rfloor\}$ instead of the set $A_{2\ell}$ in the step 1, then the condition

$$\left(\ell c + \left\lfloor \frac{\ell}{c} \right\rfloor \omega\right)^k \in A_p \quad (c = \lfloor \sqrt{\omega} + 0.5 \rfloor) \tag{4}$$

is a sufficient condition of (2). Similar type of refinement is possible for imaginary quadratic fields, too.

3.2 The case of cubic fields

We can generalize Proposition 3 for cubic fields as follows:

Proposition 5 *Let $K = \mathbb{Q}(\omega)$ be a cubic field such that the ring of integers of K is $\mathcal{O}_K = \langle 1, \omega, \omega^2 \rangle$, where ω is a root of $f(x) = x^3 + a_2x^2 + a_1x + a_0$ with $a_0, a_1, a_2 \le 0$ irreducible over $\mathbb{Q}$. For $z_{ij} \in \mathbb{Z}$ and $z_i \in \mathbb{Z}_{>0}$, write $\prod_{i=1}^{k}(z_{1j} + z_{2j}\omega + z_{3j}\omega^2) = X_1 + X_2\omega + X_3\omega^2$ and $(z_1 + z_2\omega + z_3\omega^2)^k = X_1{}' + X_2{}'\omega + X_3{}'\omega^2$ with $X_i, X_i{}' \in \mathbb{Z}$. Assume $|z_{ij}| \le z_i$ $(i = 1, 2, 3, j = 1, \dots, k)$. Then $|X_i| \le X_i{}'$ $(i = 1, 2, 3)$.*

Proposition 5 is not so practical since $\mathcal{O}_K$ must have a power basis with another condition. Therefore we propose a proposition applicable to any cubic fields.

Proposition 6 *Let K be a cubic field such that the ring of integers of K is $\mathcal{O}_K = \langle 1, \omega_2, \omega_3 \rangle$. For $z_{ij} \in \mathbb{Z}$ and $s, t, u \in \mathbb{Z}_{\ge 0}$, write $\prod_{j=1}^{k}(z_{1j} + z_{2j}\omega_2 + z_{3j}\omega_3) = X_1 + X_2\omega_2 + X_3\omega_3$, $\omega_2{}^t\omega_3{}^u = z_1{}^{(tu)} + z_2{}^{(tu)}\omega_2 + z_3{}^{(tu)}\omega_3$ and $\sum_{s+t+u=k}\{|z_1{}^{(tu)}| + |z_2{}^{(tu)}|\omega_2 + |z_3{}^{(tu)}|\omega_3\}\binom{k}{s}\binom{k-s}{t} = M_1 + M_2\omega_2 + M_3\omega_3$, where $X_i, z_i{}^{(tu)}, M_i \in \mathbb{Z}$. If $M = \max|z_{ij}|$ and $C = \max|M_i|$, then $|X_i| \le M^kC$.*

By Proposition 6, the coefficients of the product of k integers in $A_{2\ell}$ is bounded by $C\ell^k$. Therefore, the condition

$$\ell^k C \le 2p \tag{5}$$

is a sufficient condition of (2). In order to evaluate C, we may compute $\omega_2{}^t\omega_3{}^u$ for about $k^2/2$ pairs (t, u). Then we can choose p by condition (5) for arbitrary cubic fields. In such a way, we can generate keys efficiently. Whether it is effective or not, this kind of discussion is possible for general number fields.

4. Experimental results

We now give the results of our experiment using MAGMA [4]. Our environment is as follows:

CPU: AMD Opteron 246x2 2GHz(Dual),
Software: MAGMA V2.15-14.

4.1 Bit size of p and various densities

In computational experiments, we generated 10 private keys for each given input parameter $(n, k, \theta \,\text{or}\, f)$ with $k = \lfloor \sqrt{n} \rfloor$ and compared the average of bit size of p, various densities d, κ [5] and D [6]. Because $\max_i b_i \approx p^r$, we regard $n/\log_2 p^r = d$, $k \log_2 n / \log p^r = \kappa$ and $dH(k/n) = D$, where $H(x) := -x\log_2 x - (1-x)\log_2(1-x)$ is an entropy function. In Fig. 1, θ means the quadratic field $K = \mathbb{Q}(\sqrt{\theta})$, f means the cubic field $K = \mathbb{Q}[x]/(f[1]x^3 + f[2]x^2 + f[3]x + f[4])$ and h means the class number of the given field.

In Fig. 1, we see that the bit size of p grows big as the discriminant and the class number of the field grow big for imaginary quadratic fields. For real quadratic fields and cubic fields, we can guess that there are many fields with small p because there are many fields with class number 1. We, however, could not make p small when the discriminant is big.

In Fig. 2, we see that each density for real quadratic fields is almost the same as that density for imaginary quadratic fields. On the other hand, it is slightly low for cubic fields. Furthermore, we can make density d enough high with an appropriate choice of the parameters. But, we can not make densities κ and D enough high because $k \ll n$. Therefore, it seems that there is an efficient reduction from the generated knapsack problem to the

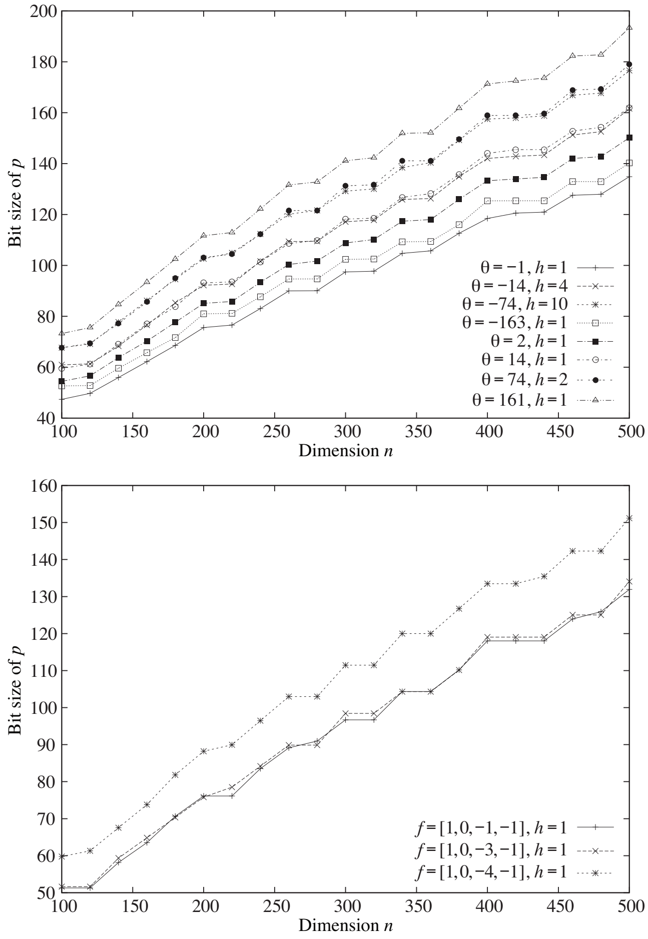

Fig. 1. Comparison of the bit size of p.

lattice shortest vector problem [5,6]. In the next subsection, we discuss about this in detail.

4.2 *Resistance against low-density attack*

A Knapsack problem generated by OTU2000 is as follows: Given a set $\{b_1, b_2, \cdots, b_n\}$ of public key and a cipher text $c = \sum_{i=1}^{n} m_i b_i$ ($m_i \in \{0,1\}$), find the m_i's.

The reduced lattice problem from a knapsack problem is as follows: Given a lattice L spanned by $v_1, v_2, \ldots, v_{n+1}$, find the shortest vector of L, where λ is an integer larger than $\sqrt{n}$ and

$$\begin{aligned} v_1 &= (1, 0, \cdots, 0, \lambda b_1), \\ v_2 &= (0, 1, \cdots, 0, \lambda b_2), \\ &\vdots \\ v_n &= (0, 0, \cdots, 1, \lambda b_n), \\ v_{n+1} &= (0, 0, \cdots, 0, \lambda c). \end{aligned} \tag{6}$$

The idea of the low-density attack is that if we can find the shortest vector of the lattice L, it may be the solution of the knapsack problem, i.e. $(m_1, \cdots, m_n, 0)$ may be the shortest vector of L with high probability. Here we use the type of lattice proposed by Lagarias and Odlyzko [7] because $k \ll n$.

In computational experiments, we generated 5 public keys for each given input parameter $(n, k, \theta$ or $f)$ and chose 200 plain texts randomly for each key. After that, we computed cipher texts and created the corresponding lattices as above. Furthermore, we applied LLL reduction algorithm [8] to these lattices. Then OTU2000 is broken if the vector $v = (m_1, \cdots, m_n, 0)$ belongs to the LLL reduced basis. We also take $\lambda = n$ and LLL parameters δ to 0.999 and η to 0.501. Below we show the breaking rate of the attack with 1000 lattices.

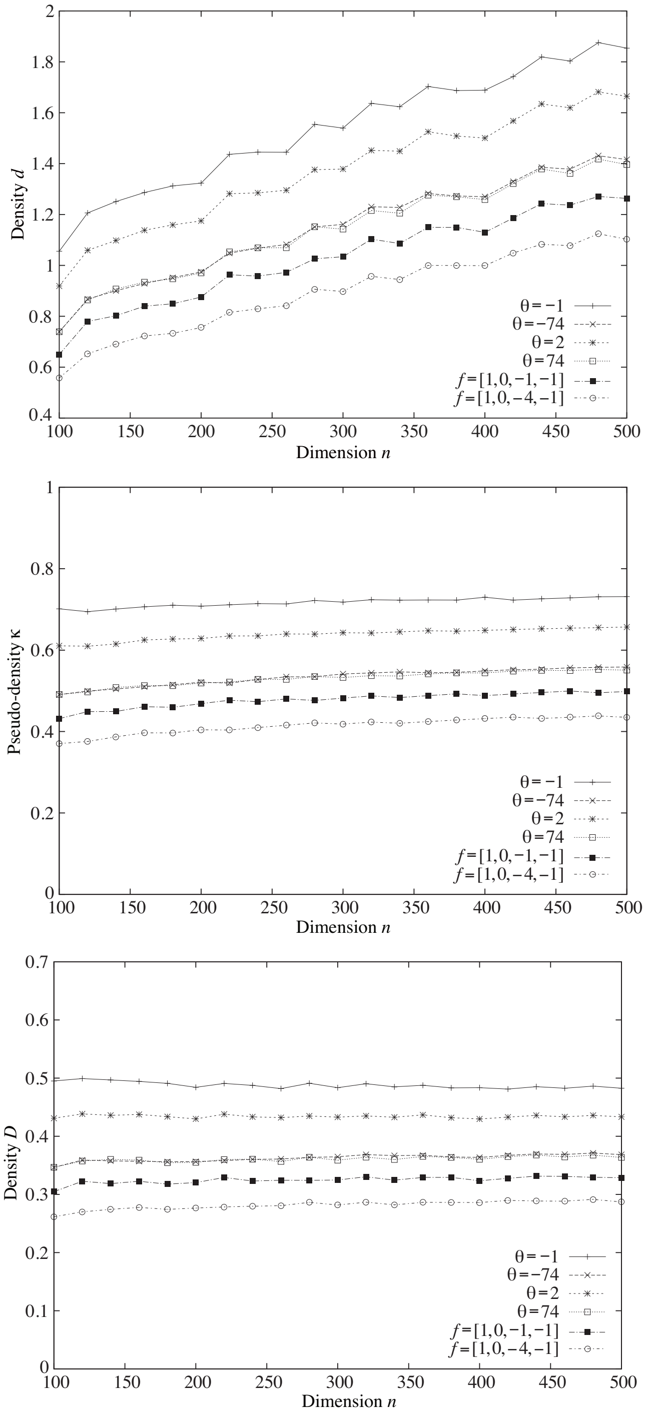

Fig. 2. Comparison of the densities d, κ, D.

From Fig. 3, we saw that the breaking rate decreases as densities grow high when the size n is less than about 150. We have actually generated public keys when the size n is up to 200. For these reduced lattice problems, our experiments showed that LLL reduction can not find the shortest vector if the size n exceeds 150.

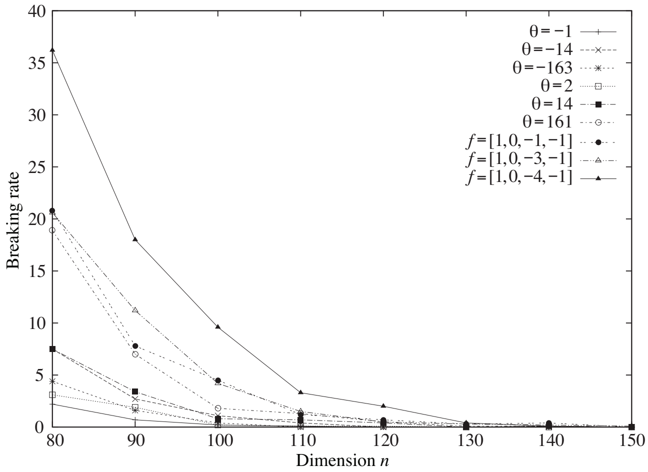

Fig. 3. Comparison of the breaking rate.

5. Conclusions and considerations

We proposed some propositions to implement OTU 2000 over real quadratic fields and cubic fields. Furthermore, we showed experimental results about various densities and estimated the resistance against low-density attack. As a result, we saw that densities grew high when the class number was small and the discriminant was small for real quadratic fields. A similar fact is also observed at least for cubic fields we experimented. These densities are slightly lower than those for imaginary quadratic fields with small class number. But it is worth to use the case of real quadratic and cubic fields with small class number. Because, for imaginary quadratic fields, densities are low when the class number is large, and there are only finitely many fields when the class number is bounded.

In addition, the breaking rate by the low-density attack decreases as densities grow high when the size n is less than about 150. On the other hand, our experiment shows that LLL algorithm can not find the shortest vector if the size n exceeds 150 regardless of the densities. Hence, it seems that we should take a security parameter n more than at least 150 to generate keys which have resistance against low-density attack with LLL reduction.

The lower estimate (5) of p is not so sharp. To improve the estimate is an important future problem. We estimated resistance against low-density attack only using LLL reduction. Therefore, it is an important future problem that we estimate resistance using BKZ reduction and other reductions. It will also be interesting to study the case of number fields of higher degrees.

References

[1] T. Okamoto, K. Tanaka and S. Uchiyama, Quantum public-key cryptosystems, in: Proc. of CRYPTO 2000, B. Mihir ed., Lect. Notes Comput. Sci., Vol. 1880, pp. 147–165, Springer-Verlag, Berlin, 2000.

[2] K. Nishimoto and K. Nakamula, On key generation of OTU 2000 and related problems, Trans. JSIAM, **18** (2008), 185–197.

[3] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in: Proc. of the 35th Annual Symposium on Foundations of Computer Science, pp. 124–134, 1994.

[4] MAGMA Group, MAGMA, http://magma.maths.usyd.edu.au/magma/MagmaInfo.html.

[5] P. Q. Nguyen and J. Stern, Adapting density attacks to low-weight knapsacks, in: Proc. of ASIACRYPT 2005, R. Bimal ed., Lect. Notes Comput. Sci., Vol. 3788, pp. 41–58, Springer-Verlag, Berlin, 2005.

[6] N. Kunihiro, New definition of density on knapsack cryptosystem, in: Proc. of AFRICACRYPT 2008, V. Serge ed., Lect. Notes Comput. Sci., Vol. 5023, pp. 156–173, Springer-Verlag, Berlin, 2008.

[7] J. C. Lagarias and A. M. Odlyzko, Solving low-density subset sum problems, J. ACM, **32** (1985), 229–246.

[8] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász, Factoring polynomials with rational coefficients, Math. Ann., **261** (1982), 515–534.