Analysis of the Extended Search Space for the Shortest Vector in Lattice

Masaharu Fukase
Department of General Systems Studies, The University of Tokyo
Meguro-ku, Tokyo 153-8902, Japan

and

Kazunori Yamaguchi
Department of General Systems Studies, The University of Tokyo
Meguro-ku, Tokyo 153-8902, Japan

Abstract

Lattice reduction algorithms have been used for cryptanalysis of many public key cryptosystems. Several lattice reduction algorithms have been proposed in the literature while the most popular among them is the BKZ algorithm. When BKZ fails to find a shortest vector, typically it returns a much longer vector than the shortest. We proposed the extended search space to find a shortest vector in such a case in our previous paper and confirmed the effectiveness of it experimentally. In this paper, we justify the effectiveness of the extended search space by additional analysis. For that, we analyzed coefficients of the shortest vector in a lattice based on some heuristic assumptions. Moreover, we examined the distribution of the coefficients that highly affect the inclusion probability in the extended search space. We showed that the inclusion probability can be estimated based on the distribution, and the estimated probability reflected the experimental results in our privious paper.

Keywords: Lattice, Shortest Vector, Extended Search Space

1 INTRODUCTION

A lattice L is the set of all linear combinations with integer coefficients of a set of linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$. The integer n is called the dimension of the lattice L, and $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is called a basis of the lattice L. A lattice has infinitely many bases when $n \geq 2$. The aim of lattice reduction is to compute bases consisting of very short vectors or shortest vectors.

Lattice reduction algorithms have been used for cryptanalysis of many public key cryptosystems. On the other hand, some public key cryptosystems were suggested that are closely related to lattice problems over the previous decade. Among them, the GGH cryptosystem [5] and the NTRU cryptosystem [6] are well known. Although four of the five challenges of the GGH cryptosystem were broken [10], the GGH cryptosystem was improved by the HNF technique [9]. The NTRU cryptosystem was subject to no significant attacks so far.

Many lattice reduction algorithms have been proposed, and some of them have been applied to cryptanalysis of these cryptosystems. The LLL algorithm [7] was the major breakthrough in the lattice reduction. It generates a reduced basis of proven quality in polynomial time. The BKZ algorithm [11] combines the LLL algorithm with exhaustive search in low dimensional sublattices. Although there is no guaranteed run time bound for the BKZ algorithm, the BKZ algorithm works better than the LLL algorithm in practice. The Random Sampling Reduction algorithm (RSR) [12] combines the BKZ algorithm with the Sampling Algorithm (SA) that samples a lattice vector from a search space.

In every iteration of RSR, a lattice vector which is shorter than $\mathbf{b}_1$ at least by the factor $\sqrt{0.99}$ is searched by SA. While the search succeeds, BKZ is called after the search. If the factor $\sqrt{0.99}$ can be decreased, the number of iterations can be decreased. For this, the search space must contain a very short vector such that it is shorter than $\mathbf{b}_1$ by a factor smaller than $\sqrt{0.99}$. In this paper, we show that such chances can be much increased by extending the search space.

In our previous paper [3], we proposed the extended search space, which is determined by the smalle number of parameters. Moreover, we experimentally confirmed that the extended search space includes a shortest vector with considerably high probability. But, we did not present theoretical analysis in [3].

In this paper, we justify the effectiveness of the extended search space by additional analysis. For that, we analyze coefficients of the shortest vector in a lattice based on some heuristic assumptions. Moreover, we examine the distribution of the coefficients that highly affect the inclusion probability in the extended search space. This paper is a revised version of [2].

2 PRELIMINARIES

2.1 Lattice

Definition 1 *Given a set of n linearly independent vectors $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in \mathbb{Z}^{m\times n}$, the* integer lattice *$L \subset \mathbb{Z}^m$ spanned by B is defined as the set*

$$L(B) = \{B\mathbf{x} \mid \mathbf{x} \in \mathbb{Z}^n\}$$

of all integral combinations of $\mathbf{b}_i$'s.

The integer n is called the *dimension* of L. When $n = m$, we say that L is *full-dimensional*. In the rest of this paper we concentrate on full-dimensional integer lattices. The ordered set of vectors $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in \mathbb{Z}^{m\times n}$ is called a *basis* of L.

Every lattice has infinitely many bases when $n \geq 2$. The relation of bases that generate the same lattice can be algebraically characterized as follows.

Lemma 1 *Two lattice bases B, B' generate the same lattice L if and only if there is a unimodular matrix $U \in \mathbb{Z}^{n\times n}$(i.e., $\det U = \pm 1$) such that $B' = BU$.*

Definition 2 *The* determinant *of a lattice $L = L(B)$, denoted by $\det(L)$, is defined as the volume of the parallelepiped spanned by the columns of B, i.e., $\det(L) = \mathrm{Vol}(\{B\mathbf{x} \mid \mathbf{x} \in [0,\ 1)^n\})$.*

The determinant is a lattice invariant. That is, it does not depend on any particular basis.

Definition 3 *For a lattice basis $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$, the corresponding* Gram-Schmidt orthogonalized vectors *$\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ are defined by*

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j}\mathbf{b}_j^* \quad \textit{with} \quad \mu_{i,j} = \langle \mathbf{b}_i, \mathbf{b}_j^* \rangle / \langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle \tag{1}$$

where $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^n x_i y_i$ is the inner product in $\mathbb{R}^n$. We call $\mu_{i,j}$ the Gram-Schmidt coefficients.

For every i, $\mathbf{b}_i^*$ is the component of $\mathbf{b}_i$ that is orthogonal to $\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}$. In particular, vectors $\mathbf{b}_i^*$ and $\mathbf{b}_j^*(j \neq i)$ are orthogonal. We can compute the determinant of the lattice by the product of the lengths of the orthogonalized vectors

$$\det(L(B)) = \prod_{i=1}^n \|\mathbf{b}_i^*\| \tag{2}$$

where $\|\mathbf{x}\| = \sqrt{\sum_{i=1}^n x_i^2}$ is the *Euclidean norm*. Let $\lambda_1(L)$ denote the Euclidean norm of the shortest nonzero lattice vector in the lattice L.

Let $\mathbf{v} = B\mathbf{x}$ with $\mathbf{x} \in \mathbb{Z}^n$ be a vector in the lattice generated by the basis B. From Eq. (1), we can represent $\mathbf{v}$ with the Gram-Schmidt orthogonalized vectors $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ and the Gram-Schmidt coefficients $\mu_{i,j}$ of B. That is, $\mathbf{v} = \sum_{j=1}^n \nu_j \mathbf{b}_j^*$ with $\boldsymbol{\nu} \in \mathbb{R}^n$ such that $\nu_j = \sum_{i=1}^n x_i \mu_{i,j}$. As $\mathbf{b}_j^*$ are pairwise orthogonal,

$$\|\mathbf{v}\|^2 = \sum_{j=1}^n \nu_j^2 \|\mathbf{b}_j^*\|^2. \tag{3}$$

Eq. (3) means that for a lattice vector $\mathbf{v} = \sum_{j=1}^n \nu_j \mathbf{b}_j^*$ to be short, $|\nu_j|$ need to be small.

In the following, we call ν_j *the Gram-Schmidt coefficients* of $\mathbf{v}$. Notice that we defined the Gram-Schmidt coefficients both in Definition 3 and here. We defined them as coefficients $\mu_{i,j}$ obtained during the Gram-Schmidt orothogonalization in Definition 3, and here we defined them as coefficients ν_j of the Gram-Schmidt orothogonalized vectors in a vector. What they mean is essentially the same because $\mu_{i,j} = \langle \mathbf{b}_i, \mathbf{b}_j^* \rangle / \langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle$ and $\nu_j = \langle \mathbf{v}, \mathbf{b}_j^* \rangle / \langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle$. But in order to avoid confusion, we use the symbol μ for the former and ν for the latter.

2.2 Lattice Basis Reduction Algorithms

Several lattice basis reduction algorithms have been proposed.

The BKZ algorithm [11] computes a (δ, β)-BKZ reduced basis for $\delta \in (1/4, 1]$ and an integer β such that $2 \leq \beta < n$. Let $\pi_i : \mathbb{R}^n \to \mathrm{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})^\perp$ be the orthogonal projection. Also, let L_i denote the orthogonal projection of L in span$(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})^\perp$. A (δ, β)-BKZ reduced basis B satisfies

1. $|\mu_{i,j}| \leq \frac{1}{2}$ for all $i > j$, where $\mu_{i,j}$ are the Gram-Schmidt coefficients,
2. $\delta\|b_i^*\|^2 \leq \lambda_1(L_i(\mathbf{b}_1, \ldots, \mathbf{b}_{\min(i+\beta-1,n)}))^2$ for all i.

There is no proven polynomial time bound for the BKZ algorithm, but the algorithm behaves well in practice. Although the quality of a (δ, β)-BKZ reduced basis is better for larger β, the computational cost increases for larger β. For $\delta \in [1/3, 1]$, a δ-LLL reduced basis [7] coincides with a $(\delta, 2)$-BKZ reduced basis.

Schnorr proposed Random Sampling Reduction (RSR) [12]. Recall that for a lattice vector $\mathbf{v} = \sum_{j=1}^n \nu_j \mathbf{b}_j^*$ to be short, $|\nu_j|$ need to be small. It is well known that the initial vectors $\mathbf{b}_1^*, \ldots, \mathbf{b}_k^*$ are usually longer than subsequent vectors $\mathbf{b}_j^*$ for $j > k$ if B is reduced by BKZ. So Gram-Schmidt coefficients $\nu_1, \ldots, \nu_k$ have a larger impact on the overall length of $\mathbf{v}$ than ν_j for $j > k$. Then, it is reasonable to assume that a vector $\mathbf{v} = \sum_{j=1}^n \nu_j \mathbf{b}_j^*$ such that

$$|\nu_j| \leq \begin{cases} \frac{1}{2} & \text{for } j < n-u \\ 1 & \text{for } n-u \leq j < n \end{cases}, \quad \nu_n = 1 \tag{4}$$

for some $1 \leq u \leq n$ is likely to be short. There are at least 2^u distinct lattice vectors of this form. Sampling Algorithm (SA) generates a single vector $\mathbf{v}$ satisfying (4). Let $S_{u,B}$ be the set of vectors satisfying (4) for the specified u. We call $S_{u,B}$ the *SA search space*.

Sampling Algorithm (SA)

```
Input: lattice basis $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ with $\mu_{i,j}$ and an integer $u$ such that $1 \leq u < n$.
Output: $\mathbf{v}$ satisfying (4).
$\mathbf{v} := \mathbf{b}_n$
for $j = 1, \ldots, n-1$  $\mu_j := \mu_{n,j}$
for $i = n-1, \ldots, 1$
Select $y \in \mathbb{Z}$ randomly such that $|\mu_i - y| \leq \begin{cases} 1/2 & \text{if } i < n-u \\ 1 & \text{if } i \geq n-u \end{cases}$
$\mathbf{v} := \mathbf{v} - y\mathbf{b}_i$
for $j = 1, \ldots, n-1$  $\mu_j := \mu_j - y\mu_{i,j}$
```

Given a lattice basis $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$, RSR samples by SA up to 2^u distinct lattice vectors $\mathbf{v} = \sum_{j=1}^{n} \nu_j \mathbf{b}_j^*$ satisfying (4) until a vector $\mathbf{v}$ such that $\|\mathbf{v}\|^2 < 0.99\|\mathbf{b}_1\|^2$ is found. Subsequently RSR inserts the vector found by SA into the basis, and BKZ is used to reduce the new basis. This random sampling by SA and BKZ process are iterated several times.

2.3 Extended Search Space

In [3], we proposed an extended search space bounded by a function $f(x) = ka^{n-x}$. The extended search space $W_{k,a,j_0,B}$ is defined formally as follows.

Definition 4 *Let B be a lattice basis, and let $k, a \in \mathbb{R}^+$, $j_0 \in \mathbb{Z}_n^+$. Then the extended search space $W_{k,a,j_0,B}$ is the set of all lattice vectors $\mathbf{v} = \sum_{j=1}^{n} \nu_j \mathbf{b}_j^*$ subject to*

$$\nu_j \in \begin{cases} (-\lceil 2ka^{n-j} \rceil/2, \lceil 2ka^{n-j} \rceil/2] & \text{for } 1 \leq j < j_0, \\ \{1, \ldots, \lceil ka^{n-j} \rfloor\} & \text{for } j = j_0, \\ \{0\} & \text{for } j_0 < j \leq n, \end{cases} \tag{5}$$

for $j = 1, \ldots, n$.

For the search in $W_{k,a,j_0,B}$, we can use GenSample which was proposed as one of variants of SA in [8]. The random coin toss in SA is replaced by the binary digits of the integer argument x in GenSample. In [8], it is proved that GenSample generates a different vector for a different index x.

3 ANALYSIS OF THE EXTENDED SEARCH SPACE

In the following, we estimate the probability with which the shortest vector is included in the extended search space.

Let $\mathbf{v}$ be the shortest vector in the lattice generated by the basis B, and let $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ be the corresponding Gram-Schmidt orthogonalized vectors. Recall that we can represent $\mathbf{v}$ with $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ as $\mathbf{v} = \sum_{j=1}^{n} \nu_j \mathbf{b}_j^*$. Then,

$$\|\mathbf{v}\|^2 = \sum_{j=1}^{n} \nu_j^2 \|\mathbf{b}_j^*\|^2. \tag{6}$$

If $\mathbf{v}$ is the shortest vector, each ν_j must be small. So, each ν_j^2 should cancel the term $\|\mathbf{b}_j^*\|^2$. If ν_j^2 exactly cancels $\|\mathbf{b}_j^*\|^2$,

$$|\nu_j| = t/\|\mathbf{b}_j^*\| \text{ for } j = 1, \ldots, n \tag{7}$$

holds for some constant $t \in \mathbb{R}_+$. For actual data, this does not hold. So, we introduce error terms $t_j \in \mathbb{R}$ for $j = 1, \ldots, n$ into Eq. (7):

Assumption 1

$$|\nu_j| = (t + t_j)/\|\mathbf{b}_j^*\| \textit{ for } j = 1, \ldots, n. \tag{8}$$

Here, t is determined later.

It is well known that if a random lattice basis is reduced by LLL or BKZ, the lengths of the Gram-Schmidt orthogonalized vectors of the basis resemble a geometric sequence $\|\mathbf{b}_j^*\|^2 \approx q^{j-1}\|\mathbf{b}_1\|^2$ for some $q \in [0, 1]$. This observation is crucial for Schnorr's analysis in [12] and supported also in [1] and [4]. In practice, we estimate q by the least mean square method. Here, in order to estimate the similarity, we represent the approximate equation $\|\mathbf{b}_j^*\|^2 \approx q^{j-1}\|\mathbf{b}_1\|^2$ by an equation

$$\|\mathbf{b}_j^*\|^2 = e^{\delta_j} q^{j-1} \|\mathbf{b}_1\|^2 \text{ for } j = 1, \ldots, n, \tag{9}$$

by introducing error terms e^{δ_j} for $j = 1, \ldots, n$. Here, $|\delta_j|$ must be small. Then, from Eq. (8) and Eq. (9),

$$\begin{aligned} |\nu_j| &= (t + t_j)/(e^{\delta_j} q^{j-1} \|\mathbf{b}_1\|^2)^{1/2} \\ &= t/(q^{j-1}\|\mathbf{b}_1\|^2)^{1/2} + ((1 - e^{\delta_j/2})t \\ &\quad + t_j)/(e^{\delta_j} q^{j-1} \|\mathbf{b}_1\|^2)^{1/2} \\ &= (t(q^{1/2})^{1-n}/\|\mathbf{b}_1\|)(q^{1/2})^{n-j} \\ &\quad + ((1 - e^{\delta_j/2})t + t_j)/(e^{\delta_j} q^{j-1} \|\mathbf{b}_1\|^2)^{1/2}. \end{aligned}$$

Let $k = t(q^{1/2})^{1-n}/\|\mathbf{b}_1\|$, $a = q^{1/2}$, and $\epsilon_j = ((1 - e^{\delta_j/2})t + t_j)/(e^{\delta_j} q^{j-1} \|\mathbf{b}_1\|^2)^{1/2}$. Then,

$$|\nu_j| = ka^{n-j} + \epsilon_j. \tag{10}$$

Here, k and a are parameters for the extended search space. From Definition 4, for $\mathbf{v} = \sum_{j=1}^{n} \nu_j \mathbf{b}_j^*$ to be included in the extended search space, ν_j for $j = 1, \ldots, n$ need to satisfy at least the following inequality:

$$|\nu_j| \leq \lceil 2ka^{n-j} \rceil/2. \tag{11}$$

From Eq. (10), for ν_j to satisfy Eq. (11) the following condition needs to be satisfied:

Condition 1

$$\epsilon_j \leq \pi_j \textit{ with } \pi_j = \lceil 2ka^{n-j} \rceil/2 - ka^{n-j}. \tag{12}$$

Note that $\pi_j \leq 0.5$. If Condition 1 is satisfied for all j, then $\mathbf{v} = \sum_{j=1}^{n} \nu_j \mathbf{b}_j^*$ is included in the extended search space.

4 DISTRIBUTION OF ϵ_j

The analysis in Section 3 explains why the search in the extended search space worked in [3]. From the analysis in Section 3, ν_j can be divided into two part: the exponential part ka^{n-j} and the perturbation part ϵ_j.

Here, we used the bases of the GGH cryptosystem. In the GGH cryptosystem, the private basis R is defined as $R = dI + R'$ where $d = l\lceil 1 + \sqrt{n}\,\rceil$ is a parameter from a given integer bound l(e.g., $l = 4$) and R' is a perturbation matrix with entries chosen independently and uniformly at random from $\{-l, \ldots, +l\}$. R is transformed into a public basis B by applying elementary column operations $2n$ times. At every step we add to a column a random integer combination of the other columns. The coefficients in the integer combination are chosen at random from $\{-1,\, 0,\, +1\}$.

Let R be a GGH private basis and let B be its $(0.99, \beta)$-BKZ reduced public basis. Then the shortest vector $\mathbf{v}$ is included in R. We represent $\mathbf{v}$ by the Gram-Schmidt orthogonalized vectors $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ as $\mathbf{v} = \sum_{j=1}^{n} \nu_j \mathbf{b}_j^*$. We computed ν_j from the unimodular matrix U such that $R = BU$. In our experiments, we used the version 5.5.1 of the NTL software package [13] with some additional programs written in C++. We used the BKZ routine of the NTL with quadratic precision. All programs were run on a 2.33 GHz Intel Core 2 Quad with Linux.

Here, we experimentally find out the distribution of t_j and δ_j. For this, we must first determine t. Here, we replace ν_j in (6) with (7). Because the length of the shortest vector $\mathbf{v}$ is λ_1, we have

$$\lambda_1^2 = \sum_{j=1}^{n}(t^2/\|\mathbf{b}_j^*\|^2)\|\mathbf{b}_j^*\|^2 = nt^2. \tag{13}$$

From this, we have $t = \lambda_1/n^{1/2}$.

We got $t = 4.743, q = 0.943, a = 0.971, k = 0.946$ for a $(0.99, 10)$-BKZ reduced public basis in dimension 160. Figure 1 and Figure 2 show the distribution of t_j and δ_j for the $(0.99, 10)$-BKZ reduced public basis in dimension 160. We found that t_j and δ_j tend to distribute according to the normal distribution.

Next, assuming the distributions of t_j and δ_j are the normal distributions, we estimate the probability with which Condition 1 is satisfied for each j. Recall that $\epsilon_j = ((1 - e^{\delta_j/2})t + t_j)/(e^{\delta_j}q^{j-1}\|\mathbf{b}_1\|^2)^{1/2}$. We computed 10^6 possible values of ϵ_j according to the distribution of t_j and δ_j for each j. Then we computed Pr$[\epsilon_j \leq \pi_j]$ for each j. Figure 3 shows the actual values of π_j. Finally, we got the probability with which Condition 1 is satisfied for all j as 0.000942 by $\prod_{j=1}^{n}$ Pr$[\epsilon_j \leq \pi_j]$. We note that the probability obtained experimentally for $(0.99, 10)$-BKZ reduced public bases in [3] was roughly 10 times higher than the probability 0.000942. So far, we have interpreted the cause of the difference between the probabilities was the errors occurred in assuming the distribution of δ_j and t_j.

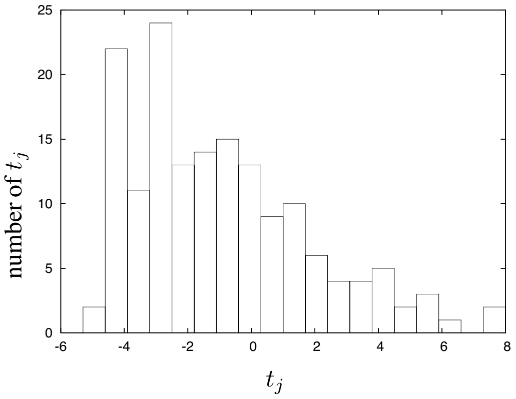

Figure 1: The distribution of t_j. The average of t_j is -0.909, and the variance is 7.846.

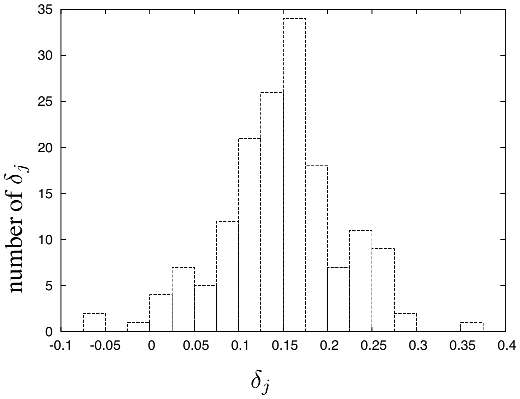

Figure 2: The distribution of δ_j. The average of δ_j is 0.149, and the variance is 0.00464.

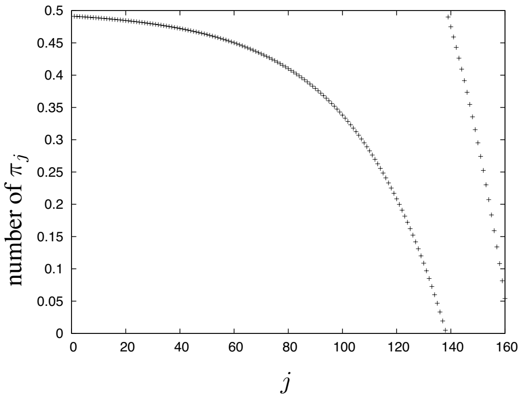

Figure 3: Values of π_j

5 CONCLUSION

We estimated the deviation of a basis from the so-called geometric sequence assumption by introducing error terms δ_j. We showed that error terms δ_j for the geometric sequence assumption distributed according to the normal distribution. In our experiment, the deviation factor e^{δ_j} was less than 1.5 at the maximum. So, it can be said that the deviation tend to be small.

We also examined the actual distribution of t_j on Assumption 1. Because values of t_j was very small compared with values of $\|\mathbf{b}_j^*\|$, it can be said that the deviation of actual bases from Assumption 1 is also small.

Moreover, we showed the method to estimate the probability with which the shortest vector was included in the extended search space by utilizing the distribution of δ_j and t_j.

References

[1] Ajtai, M.: The Worst-Case Behaviour of Schnorr's Algorithm Approximating the Shortest Nonzero Vector in a Lattice. Proceedings of the thirty-fifth annual ACM symposium on Theory of computing, (2002).

[2] Fukase, M., Yamaguchi, K.: The Analysis of ESS for the Shortest Vector in Lattice. Proceedings of SICT 2010, pp. 209-213, (2010).

[3] Fukase, M., Yamaguchi, K.: Exhaustive Search for Finding a Very Short Vector in High-Dimensional Lattices. Proceedings (short papers) of IWSEC 2010, pp. 26-41, (2010).

[4] Gama, N., Nguyen, P.Q.: Predicting Lattice Reduction. EUROCRYPT 2008, vol. 4965 of LNCS, pp. 31-51, (2008).

[5] Goldreich, O., Goldwasser, S., Halevi, S.: Public-Key Cryptosystems from Lattice Reduction Problems. Advances in Cryptology - Crypto'97, vol. 1294 of LNCS, Springer-Verlag, pp. 112-131, (1997).

[6] Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A Ring-Based Public Key Cryptosystem. Proceedings of ANTS III, vol. 1423 of LNCS, Springer-Verlag, pp. 267-288, (1998).

[7] Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring Polynomials with Rational Coefficients. Mathematische Ann., vol. 261, pp. 513-534, (1982).

[8] Ludwig, C.: Practical Lattice Basis Sampling Reduction. PhD thesis, TU Darmstadt, Available at http://elib.tu-darmstadt.de/diss/000640/. (2005).

[9] Micciancio, D.: Improving Lattice Based Cryptosystems Using the Hermite Normal Form. Silverman, pp. 126-145.

[10] Nguyen, P.Q.: Cryptanalysis of the Goldreich-Goldwasser-Halevi Cryptosystem from Crypto'97. Advances in Cryptology - Crypto'99, vol. 1666 of LNCS, Springer-Verlag, pp. 288-304, (1999).

[11] Schnorr, C.P., Euchner, M.: Lattice Basis Reduction: Improved Practical Algorithms and Solving Subset Sum Problems. Math. Programming, vol. 66, pp. 181-199, (1994).

[12] Schnorr, C.P.: Lattice Reduction by Random Sampling and Birthday Methods. STACS 2003, vol. 2607 of LNCS, Springer-Verlag, pp. 145-156, (2003).

[13] Shoup, V.: NTL - A Library for Doing Number Theory. Available at http://www.shoup.net/ntl/index.html.