Lower bounds of shortest vector lengths in random knapsack lattices and random NTRU lattices

Jingguo Bi[1] and Qi Cheng[2]

[1] Lab of Cryptographic Technology and Information Security
School of Mathematics
Shandong University
Jinan, 250100, P.R. China.
Email: jguobi@mail.sdu.edu.cn
[2] Computer Science School
University of Oklahoma
Norman, OK 73019, USA
Email: qcheng@cs.ou.edu

Abstract. Finding the shortest vector of a lattice is one of the most important problems in computational lattice theory. For a random lattice, one can estimate the length of the shortest vector using the Gaussian heuristic. However, no rigorous proof can be provided for some classes of lattices, as the Gaussian heuristic may not hold for them. In the paper we study two types of random lattices in cryptography: the knapsack lattices and the NTRU lattices. For random knapsack lattices, we prove lower bounds of shortest vector lengths, which are very close to lengths predicted by the Gaussian heuristic. For a random NTRU lattice, we prove that with a overwhelming probability, the ratio between the length of the shortest vector and the length of the target vector, which corresponds to the secret key, is at least a constant, independent of the dimension of the lattice. The main technique we use is the incompressibility method from the theory of Kolmogorov complexity.

Key words: Shortest vector problem , Kolmogorov complexity , Knapsack lattice, NTRU lattice

1 Introduction

A lattice is a set of points in an Euclidean space with periodic structure. Given n linearly independent vectors $\mathbf{b_1}, \ldots, \mathbf{b_n} \in \mathbb{R}^m$ $(n \leq m)$, the lattice generated by them is the set of vectors

$$L(\mathbf{b_1}, \ldots, \mathbf{b_n}) = \{\sum_{i=1}^{n} x_i \mathbf{b_i} : x_i \in \mathbb{Z}\}$$

The vectors $\mathbf{b_1}, \ldots, \mathbf{b_n}$ form a basis of the lattice.

The most famous computational problem on lattices is the shortest vector problem(SVP): Given a basis of a lattice L, find a vector $\mathbf{u} \in L$, such that $\parallel \mathbf{v} \parallel \geq \parallel \mathbf{u} \parallel$ for any vector $\mathbf{v} \in L \setminus \mathbf{0}$. For the hardness of SVP, Ajtai first proved that SVP is NP-hard under a randomized reduction [1] and his result was strengthened in [12][4][3][9][7]. The upper bound for the length of the shortest vector is given in the famous Minkowski Convex Body Theorem. Nevertheless, there is no known efficient algorithm which can always find a vector within the Minkowski bound.

The study of random lattices has a long history, dated back from [18]. It turns out that one can define a measure on the set of all n-dimensional lattices of a fixed determinant, and have a precise estimation of the expected length of the shortest vector [2]. One way to achieve it is to use the so-called Gaussian heuristic. Given a n-dimensional lattice L with determinant $det(L)$, the Gaussian heuristic predicts that there are about $vol(C)/det(L)$ many lattice points in a measurable subset C of $\mathbb{R}^n$ of volume $vol(C)$. It can be made precise, for example, when C is convex and symmetric around the original point O, and $vol(C)$ is much bigger than $det(L)$. If we take C to be an n-sphere centered at O, for C to contain a few points, $vol(C)$ is about $det(L)$. In the other words, the length of the shortest vector can be approximated by the radius of a sphere whose volume is $det(L)$, which is about $\sqrt{n/2e\pi}det(L)^{1/n}$. As an interesting comparison, the Minkowski Convex Body Theorem asserts that if the volume of sphere C is greater than $2^n det(L)$, then it must contain a nonzero lattice point. This gives an upper bound of the shortest vector length at about $\sqrt{2n/e\pi}det(L)^{1/n}$, which is only twice as large as the prediction made from the Gaussian heuristic.

Most of lattices appearing in cryptanalysis are random in some sense, but some of them are not random according to the above measure. See discussion in [15]. The length of the shortest vector may be much shorter than the prediction made from the Gaussian heuristic. In this paper, we consider two classes of random lattices appeared frequently in cryptography: knapsack lattices and NTRU lattices. Knapsack lattices are closely related to the Lagarias-Odlyzko lattices [10], which was first introduced to solve the knapsack problem. A knapsack lattice is spanned by $\mathbf{b_1}, \ldots, \mathbf{b_n}$ below:

$$\begin{aligned}
\mathbf{b_1} &= (a_1, 1, 0, \ldots, 0)\\
\mathbf{b_2} &= (a_2, 0, 1, \ldots, 0)\\
&\vdots\\
\mathbf{b_n} &= (a_n, 0, 0, \ldots, 1),
\end{aligned}$$

where $a_1, a_2, \cdots, a_n$ are integers. We call the lattice *random*, if $a_1, a_2, \cdots, a_n$ are selected uniformly and independently from r-bit integers, namely, the integers between 0 and $2^r - 1$. Random knapsack lattices were used by Nguyen and Stehle [15] to assess the performance of LLL algorithm. We prove that with probability at least $1 - \frac{1}{nr}$, the length of the shortest vector in the knapsack lattice $L_{a_1,a_2,\cdots,a_n}$ is greater than $\sqrt{\frac{n+1}{2\pi e}} \cdot 2^{\frac{r}{n+1}}(1 + O(\frac{\log(nr)}{n}))$, which is not far away from the Gaussian heuristic.

The NTRU cryptosystem was first introduced at the rump section of Crypto 96 by [6]. It operates in the ring of truncated polynomials given by $\mathbf{Z}[X]/(X^N - 1)$. Define $T(d_1, d_2)$ be the set of polynomials of degree $N-1$ with d_1 coefficients 1, d_2 coefficients -1 and rest coefficients 0. Let β be a positive constant $\leq 1/2$ and let $d = \lfloor \beta N \rfloor$. The security of the NTRU cryptosystem is based on the difficulty of finding short vectors in an NTRU lattice:

$$L^{NTRU} = \begin{pmatrix} 1 & 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_{N-1} \\ 0 & 1 & \cdots & 0 & h_{N-1} & h_0 & \cdots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & h_1 & h_2 & \cdots & h_0 \\ 0 & 0 & \cdots & 0 & q & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & q \end{pmatrix} \tag{1}$$

where q is a positive integer, $(h_0, h_1, \cdots, h_{N-1})$ is the coefficient vector of a polynomial $h(x) = \sum_{i=0}^{N-1} h_i x^i$ and there exist polynomials $f(x) = \sum_{i=0}^{N-1} f_i x^i \in T(d+1, d)$ and $g(x) = \sum_{i=0}^{N-1} g_i x^i \in T(d, d)$ such that

$$h(x)f(x) = g(x) \pmod{q, x^N - 1}.$$

We call an NTRU lattice *random* if $f(x)$ is selected uniformly from the invertible elements (in the ring $(\mathbf{Z}/q\mathbf{Z})[x]/(x^N - 1)$) in $T(d+1, d)$, and $g(x)$ is selected uniformly from $T(d, d)$.

Remark 1. A random NTRU lattice can *not* be obtained by selecting $(h_0, h_1, h_2, \cdots, h_{N-1})$ in (1) randomly from $(\mathbf{Z}/q\mathbf{Z})^N$. If fact, a lattice obtained in that manner is most likely not an NTRU lattice.

Interestingly Gaussian heuristic clearly does not hold for random NTRU lattices. According to the Gaussian heuristic, the shortest vector length is about $\sqrt{Nq/2e\pi}$, but the vector

$$(f_0, f_1, \cdots, f_{N-1}, g_0, g_1, \cdots, g_{N-1}),$$

which will be called the target vector, is in the lattice and has length $O(\sqrt{N})$. Many conjecture that the target vector is indeed the shortest vector in the lattice in most of cases. However, no formal proof has been provided. It is important to bound the length of the shortest vector from below, since if the shortest vector is significantly shorter than the target vector, say that it has length $o(\sqrt{N})$, then it can be recovered by an exhaustive search in time $2^{o(N)}$, and can be used in breaking NTRU cryptosystems [5]. In this paper, we prove that with a overwhelming probability, the ratio between the length of the shortest vector and length of the target vector is at least a constant. In the other word, we prove that most likely, the target vector is as long as the shortest vector up to a constant factor. In particular, if $d = \lfloor N/3 \rfloor$, as it is commonly set, then with a overwhelming probability, the shortest vector in a random NTRU lattice is longer than $\sqrt{0.28N}$.

Remark 2. There are other variants of NTRU cryptosystems, which correspond to lattices of slightly different forms. We will not discuss them due to the space limitation. Nevertheless similar results can be obtained by our techniques.

Since it is known that approximating the shortest vector by any constant factor is NP-hard [9] for general lattices, this result provides a strong evidence for the security of the NTRU cryptosystem against the lattice reduction attack.

We regard the main contribution of this paper is to use Kolmogorov complexity to study the expected length of a random lattice in certain class, which is powerful yet conceptually simple. The rest of the paper is organized as follows. In Section 2, we will review some backgrounds about lattices and Kolmogorov complexity. The lower bound for the shortest vector length of the random knapsack lattice will be studied in Section 3. In Section 4 we prove the lower bound of the length of the shortest vector for a random NTRU lattice. The proof in Section 3 is simpler, which can be considered as a warm-up for Section 4. We conclude this paper in Section 5. In this paper, we use log to denote the logarithm base 2 and use ln to denote the natural logarithm.

2 Preliminaries

2.1 Lattices

Let $\mathbb{R}^m$ be the m-dimensional Euclidean space. A lattice in $\mathbb{R}^m$ is the set

$$L(\mathbf{b_1}, \ldots, \mathbf{b_n}) = \{\sum_{i=1}^{n} x_i \mathbf{b_i} : x_i \in \mathbb{Z}\}$$

of all integral combinations of n linearly independent (column) vector $\mathbf{b_1}, \ldots, \mathbf{b_n} \in \mathbb{R}^m$. The integer n and m are called the rank and dimension of the lattice. A lattice can be conveniently represented by a matrix $\mathbf{B}$, where $\mathbf{b_1}, \ldots, \mathbf{b_n}$ are the row vectors. The determinant of the lattice L is defined as

$$\det(L(\mathbf{B})) = \sqrt{\det(\mathbf{B}\mathbf{B}^T)} \tag{2}$$

The most famous computational problem on lattices is the shortest vector problem(SVP): Given a basis of a lattice L, find a vector $\mathbf{u} \in L$, such that $\| \mathbf{v} \| \geq \| \mathbf{u} \|$ for any vector $\mathbf{v} \in L \setminus \mathbf{0}$. The following is a well-known theorem on the upper bound of the shortest vector length in lattice L.

Theorem 1 *(Minkowski) Any lattice L of rank n contains a non-zero vector $\mathbf{v}$ with*

$$||\mathbf{v}|| \leq (1 + o(1))\sqrt{2n/e\pi}\det(L)^{\frac{1}{n}}$$

In many literatures, the theorem is presented with a weaker bound $\sqrt{n}\det(L)^{\frac{1}{n}}$.

2.2 Number of integral points in a sphere

To obtain our results, it is important to have an accurate estimation of the number of integral points inside of n-sphere centered at the origin of radius R. Denote the number by $W(n, R)$. In general, one can approximate $W(n, R)$ by the volume of the sphere, denoted by $V(n, R)$. However, if the radius of the sphere is small, compared to the square root of the dimension, then the volume estimate is not very accurate. More precisely, if the radius of the sphere $R \geq n^{1/2+\epsilon}$, the number of integral points in the sphere is equal to the volume

$$V(n, R) = (\sqrt{\pi n} + O(1))^{-1}(\sqrt{\frac{2\pi e}{n}}R)^n$$

with a small additive error. If r is $\sqrt{\alpha n}$ for some small constant α, then the estimation using volume is not so precise. To see this, note that when

$\alpha < \frac{1}{2\pi e}$, the volume of the sphere is exponentially small, yet it still contains many integral points. We should use the result found in [14] to estimate $W(n, R)$ for $R = O(\sqrt{n})$:

Proposition 1. *Let α be a constant. Then there exists a constant δ, depending only on α, such that $W(n, \sqrt{\alpha n}) \geq e^{\delta n}$ for n large enough. Moreover, as α gets larger, δ is approaching $\ln(\sqrt{2\pi e\alpha})$.*

To find δ from α, one defines $\theta(z) = 1 + 2\sum_{i=1}^{\infty} z^{i^2}$. Set $\delta(\alpha, x) = \alpha x + \ln\theta(e^{-x})$. We can compute $\delta = \min_{x\geq 0} \delta(\alpha, x)$. As a comparison, $W(n, \sqrt{0.1n}) \approx e^{0.394415n}$, and $V(n, \sqrt{0.1n}) \approx e^{0.267645n}$. $W(n, \sqrt{0.5n}) \approx e^{1.07246n}$, and $V(n, \sqrt{0.5n}) \approx e^{1.07236n}$. For $\alpha > 0.5$, the difference between $\log V(n, \sqrt{\alpha n})/n$ and $\log W(n, \sqrt{\alpha n})/n$ is less than 0.0001. See Table 1 in [14]. We also have

Proposition 2. *Let δ be a constant. Then there exists a constant α such that if a n-sphere centered at the origin contains more than $e^{\delta n}$ many integral points, the radius of the sphere must be greater than $\sqrt{\alpha n}$ for n large enough. As δ gets larger, α is approaching $e^{2\delta}/2\pi e$.*

2.3 Kolmogorov complexity

The Kolmogorov complexity of a binary string x, conditional to y, is defined to be the length of the shortest program that given the input y, prints the string x, and is denoted by $K(x|y)$. We define $K(x)$ to be $K(x|\epsilon)$, where ϵ is the empty string. It turns out that if one switches from one programming language to another, the Kolmogorov complexity is invariant, up to an additive constant, as long as both of the programming languages are Turing Universal. The book [11] gave an excellent introduction to the theory of Kolmogorov complexity.

One can show that for any positive integer s, $K(s) \leq \log s + O(1)$. If $s = 1^n$, the binary string of length n consisting of only 1, then $K(s) \leq \log n + O(1)$. Similarly if s is the first n binary digits of the number π after the decimal point, then $K(s) \leq \log n + O(1)$. From the examples, one can see that the Kolmogorov complexity is a good measure of randomness in the string.

For each constant c, a positive integer x is c-incompressible if $K(x) \geq \log(x) - c$. By the counting argument, one can show

Proposition 3. *For any y, a finite set A of cardinality m has at least $m(1 - 2^{-c}) + 1$ elements x with $K(x|y) \geq \log m - c$.*

This observation yields a simple yet powerful proof technique — the incompressibility method.

3 Lower bound for the length of shortest vector of knapsack lattice

Knapsack lattices are closely related to the lattices introduced by Lagarias and Odlyzko [10] to solve the knapsack problem: Given positive integers $a_1, a_2, \ldots, a_n$ and s, whether there is a subset of the a_i that sums to s. That is equivalent to determine whether $s = \sum_{i=1}^{n} m_i a_i$ is solvable under the conditions $m_i \in \{0, 1\}, 1 \leq i \leq n$. For more details about the knapsack cryptosystem, please refer to [13][17][10][16] .

To solve the knapsack problem, one usually studies the lattice spanned by $\mathbf{b_1}, \ldots, \mathbf{b_n}$ below.

$$\begin{aligned} \mathbf{b_1} &= (a_1, 1, 0, \ldots, 0) \\ \mathbf{b_2} &= (a_2, 0, 1, \ldots, 0) \\ &\vdots \\ \mathbf{b_n} &= (a_n, 0, 0, \ldots, 1) \end{aligned}$$

We denote the lattice by $L_{a_1, a_2, \cdots, a_n}$.

From the equation (2), we can compute that $\det(L) = \sqrt{\sum_i^n a_i^2 + 1}$. From Theorem 1, we can get that the length of the shortest vector is smaller than $\sqrt{\frac{2n}{e\pi}} (\sum_i^n a_i^2 + 1)^{\frac{1}{2n}} \approx \sqrt{\frac{2n}{e\pi}} \cdot 2^{\frac{r}{n}}$. For the lower bound of the shortest vector's length, we prove a theorem below.

Theorem 1. *Let β be a constant. Let n be a positive integer and $r = \lfloor \beta n \rfloor$. Let $S = s_1 s_2 \cdots s_{nr}$ be a binary string with length nr and*

$$K(S|n, r) > nr - \log(nr).$$

For $1 \leq i \leq n$, let a_i be the integer whose binary representation is

$$s_{1+(i-1)r} s_{2+(i-1)r} \cdots s_{r+(i-1)r}.$$

Then there exists a constant α, depending only on β, such that for the knapsack lattice $L_{a_1, a_2, \cdots, a_n}$, the shortest vector's length is greater than $\sqrt{\alpha n}$. Moreover, as β gets larger, α is approaching $2^{2\beta}/2\pi e$.

Proof. Suppose vector $\mathbf{v} = (v_1, \ldots, v_{n+1})$ be the shortest vector of the lattice L, then $\mathbf{v}$ should be the linear combination of $\mathbf{b_1}, \ldots, \mathbf{b_n}$,

$$\mathbf{v} = \sum_{i=1}^{n} t_i \mathbf{b_i}$$

where $t_i \in \mathbb{Z}$ and t_i are not all zero. So we have

$$v_1 = t_1a_1 + t_2a_2 + \ldots + t_na_n \tag{3}$$

$$v_i = t_{i-1}, 2 \leq i \leq n+1 \tag{4}$$

From equation(3)(4), we have $v_1 = \sum_{i=2}^{n} v_ia_i$, where the coefficients v_i for $2 \leq i \leq n+1$ are not all zero. Let k be the smallest integer greater than 2 such that $v_k \neq 0$. Then we can get

$$a_k = \frac{v_1 - \sum_{i=2,i\neq k}^{n+1} v_ia_i}{v_k} \tag{5}$$

From equation (5), we see that there exists a program that will print S, given $(a_1, a_2, \cdots, a_{k-1}, a_{k+1}, \cdots, a_n)$ and $\mathbf{v}$. The length of such a program (not including the input) is $O(1)$. Suppose that the length of the vector $\mathbf{v}$ is R. To describe $\mathbf{v}$, we note that it is an integral point in the $(n+1)$-hypersphere of radius R centered at the origin. So we only need to use $\log W(n+1, R)$ bits. That is

$$K(S|n,r) < (n-1)r + \log W(n+1, R) + O(1)$$

On the other hand, we have $K(S|n,r) > nr - \log(nr)$. So $\log W(n+1, R) \geq \beta n + O(\log n)$. It follows from Proposition 2 that R is large than $\sqrt{\alpha n}$ for some constant α.

Corollary 1. *Let β be a constant. Let n be a positive integer and $r = \lfloor \beta n \rfloor$. If $a_1, a_2, \cdots, a_n$ are selected randomly and independently from integers between 0 and $2^r - 1$, then with probability at least $1 - \frac{1}{nr}$, the length of the shortest vector in the lattice $L_{a_1,a_2,\cdots,a_n}$ is greater than $\sqrt{\alpha n}$. Moreover, as β gets larger, α is approaching $2^{2\beta}/2\pi e$.*

Proof. If $a_1, a_2, \cdots, a_n$ are selected uniformly and independently from integers between 0 and $2^r - 1$, then if we write them as binary strings of length r, and concatenate them together to form a binary string S of length nr, then with probability $1 - \frac{1}{nr}$, $K(s|n, s) > nr - \log(nr)$.

A similar result can be achieved if r grows super-linearly in n.

Corollary 2. *Let $r = n^{1+\epsilon}$. If $a_1, a_2, \cdots, a_n$ are selected randomly and independently from integers between 0 and $2^r - 1$, then with probability at least $1 - \frac{1}{nr}$, the length of the shortest vector in the lattice $L_{a_1,a_2,\cdots,a_n}$ is greater than $\sqrt{\frac{n+1}{2\pi e}} \cdot 2^{\frac{r}{n+1}}(1 + O(\frac{\log(nr)}{n}))$.*

4 Lower bound for the length of shortest vector of NTRU lattice

The NTRU algorithm was first introduced by [6] at the rump section of Crypto 96. It operates in the ring of truncated polynomials given by $\mathbf{Z}[X]/(X^N - 1)$. The security of the NTRU cryptosystem is based on the difficulty of finding short vectors in NTRU lattices.

To describe the parameters of the NTRU cryptosystem, we begin by choosing an integer $N \geq 1$ and two moduli p, q such that $\gcd(N, p) = \gcd(p, q) = 1$. Let R, R_p, and R_q be the convolution polynomial rings

$$R = \mathbf{Z}[x]/(x^N - 1), R_p = (\mathbf{Z}/p\mathbf{Z})[x]/(x^N - 1), R_q = (\mathbf{Z}/q\mathbf{Z})[x]/(x^N - 1)$$

For any positive integers d_1 and d_2, define the set

$$T(d_1, d_2) = \left\{ a(x) \in R : \begin{array}{l} a(x) \text{ has } \; d_1 \text{ coefficients equal to 1;} \\ d_2 \;\text{ coefficients equal to } -1; \\ \text{has all other coefficients equal to 0} \end{array} \right\}$$

Polynomials in $T(d_1, d_2)$ are called ternary polynomials. The public parameters is (N, p, q, d). The private key consists of two randomly chosen polynomials

$$f(x) \in T(d+1, d) \text{ and } g(x) \in T(d, d)$$

and then computes the inverses

$$F_q(x) = f(x)^{-1} \text{ in } R_q \text{ and } F_p(x) = f(x)^{-1} \text{ in } R_p$$

compute

$$h(x) = F_q(x) * g(x) \text{ in } R_q \tag{6}$$

and the public key is the polynomial $h(x)$. From equation (6) we can obtain relationship

$$f(x) * h(x) \equiv g(x) \text{ in } R_q \tag{7}$$

where $f(x)$ and $g(x)$ have very small coefficients.

Define the NTRU lattice :

$$L^{NTRU} = \begin{pmatrix} \mathbf{b_1} \\ \mathbf{b_2} \\ \vdots \\ \mathbf{b_{2N}} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_{N-1} \\ 0 & 1 & \cdots & 0 & h_{N-1} & h_0 & \cdots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & h_1 & h_2 & \cdots & h_0 \\ 0 & 0 & \cdots & 0 & q & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & q \end{pmatrix} \tag{8}$$

where $(h_0, h_1, \cdots, h_{N-1})$ are coefficients of $h(x)$. Since $g(1) = 0$, so $h(1) = 0 \pmod q$, thus this lattice has a trivial short vector $(1^N, 0^N)$, which can be shorter than the private key. If we adopt Coppersmith and Shamir's approach [5], and use a slightly different lattice of rank $2N-2$:

$$\begin{pmatrix} 1-1/N & -1/N & \cdots & -1/N & h_0 & h_1 & \cdots & h_{N-1} \\ -1/N & 1-1/N & \cdots & -1/N & h_{N-1} & h_0 & \cdots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -1/N & -1/N & \cdots & 1-1/N & h_1 & h_2 & \cdots & h_0 \\ 0 & 0 & \cdots & 0 & q-q/N & -q/N & \cdots & -q/N \\ 0 & 0 & \cdots & 0 & -q/N & q-q/N & \cdots & -q/N \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & -q/N & -q/N & \cdots & q-q/N \end{pmatrix} \tag{9}$$

then the short vector $(1^N, 0^N)$ is eliminated from the lattice. Coppersmith and Shamir proved if one can find a sufficiently short vector in the NTRU lattice, then the short vector gives us an equivalent private key.

Lemma 1. *Assume that $d = \lfloor \beta N \rfloor$ for some constant $1/10 < \beta \leq 1/2$. For any polynomial f, if we randomly select a polynomial g in $T(d,d)$, then with probability at least $1 - 2^{-0.1N}$, we have*

$$K(g|N, f) \geq \gamma N$$

for some constant γ, when N is large enough.

Proof. The cardinality of the set $T(d,d)$ is

$$\binom{N}{d}\binom{N-d}{d} \geq \frac{2^{(-2\beta\log\beta-(1-2\beta)\log(1-2\beta))N}}{N^{O(1)}}.$$

So we may take $\gamma = -2\beta\log\beta - (1-2\beta)\log(1-2\beta) - 0.1$.

In most applications of NTRU cryptosystems, q is set to be a power of two. In the following theorem, we assume that q is a prime for simplicity. The proof for the power of two case is similar but more technical. We will include the proof in the full version of the paper.

Theorem 2. *Let N be an odd prime. Let $q < N^2$ be a prime. Assume that q has order $N-1$ in $(\mathbf{Z}/N\mathbf{Z})^*$. Fix a polynomial f in $T(d+1,d)$,* *which is invertible in R. Suppose that g is a polynomial in $T(d,d)$ such that*

$$K(g|N,f) \geq \gamma N$$

for some constant γ. The length of the shortest vector in L^{NTRU} is greater than $\sqrt{\alpha N}$ for some constant α depending only on γ.

Proof. First observe that since f is invertible, we have

$$|K(g|N,f) - K(h|N,f)| = O(1).$$

Since q is a primitive root modulo N, we have that

$$(x^N - 1)/(x-1) = x^{N-1} + x^{N-2} + \cdots + 1$$

is an irreducible polynomial over $\mathbf{F}_q$.

Suppose the vector $\mathbf{V} = (v_1, v_2, \ldots, v_{2N}) \in \mathbf{Z}^{2N}$ is the shortest vector of L^{NTRU}. If it is $(1^N, 0^N)$, then its length is $\sqrt{N}$. Otherwise there exists integers $k_1, \ldots, k_N$ such that

$$\mathbf{V} = \sum_{i=1}^{N} v_i \mathbf{b_i} + \sum_{j=1}^{N} k_j \mathbf{b_{N+j}}. \tag{10}$$

From equation(10), we can obtain that

$$\begin{aligned} h_0 v_1 + h_{N-1} v_2 + \ldots + h_1 v_N &\equiv v_{N+1} \pmod{q} \\ h_1 v_1 + h_0 v_2 + \ldots + h_2 v_N &\equiv v_{N+2} \pmod{q} \\ &\vdots \\ h_{N-1} v_1 + h_{N-2} v_2 + \ldots + h_0 v_N &\equiv v_{2N} \pmod{q} \end{aligned}$$

Let ω be the N-primitive root of unit in the algebraic closure of $\mathbf{F}_q$. The ranks of the circulant matrix

$$\begin{pmatrix} v_1 & v_N & \cdots & v_2 \\ v_2 & v_1 & \cdots & v_3 \\ \vdots & \vdots & \ddots & \vdots \\ v_N & v_{N-1} & \cdots & v_1 \end{pmatrix} \tag{11}$$

depends on the roots of the polynomial $v_1 + v_N x + \cdots + v_2 x^{N-1}$. More precisely, if d elements in $\{1, \omega, \omega^2, \omega^{N-1}\}$ are zeros of the polynomial, then the rank is $N - d$ [8]. Since $(v_1, \cdots, v_N)$ can not be all 1, the rank is at least $N-1$. If

$$v_1 + v_N + \cdots + v_2 \neq 0 \pmod{q},$$

then the rank is N, we can recover $(h_0, h_1, \ldots, h_{N-1})$ from $\mathbf{v}$. Otherwise the rank is $N-1$, then $(h_0, h_1, \ldots, h_{N-1})$ is in a 1-dimensional solution space of the linear system, namely, it equals to $B_1 + aB_2$, where $B_1, B_2 \in \mathbf{F}_q^N$ can be uniquely determined by $\mathbf{v}$, and $a \in \mathbf{F}_q$. Suppose that the length of the vector $\mathbf{v}$ is R. To describe $\mathbf{v}$, note that $\mathbf{v}$ is an integral point in the $(2N)$-hypersphere of radius R centered at the origin. So we can use $\log W(2N, R)$ bits. To describe h, we just need $\mathbf{v}$ and a.

$$K(g|N, f) \leq K(h|N, f) + O(1) \leq \log(W(2N, R)) + \log q + O(1)$$

Since $K(g|N, f) \geq \gamma N$, we have

$$W(2N, R) \geq 2^{\gamma N}/N^{O(1)}.$$

Hence $R \geq \sqrt{\alpha N}$ for some constant α by Proposition 2.

The above theorem shows that with a overwhelming probability, the shortest vector in a random NTRU lattice is at least a constant factor away from the target vector. In many practical applications of the NTRU cryptosystem, d is set to be close to $\lfloor N/3 \rfloor$. In this case, we calculate α.

Corollary 3. *If $d = \lfloor N/3 \rfloor$, then with probability greater than $1 - 2^{-0.1N}$, the shortest vector in a random NTRU lattice has length greater than $\sqrt{0.28N}$.*

Proof. By Lemma 1, we can take γ to be 1.48. Then

$$W(2N, R) \geq 2^{1.48N} = e^{0.51*2N}.$$

Hence $R \geq \sqrt{0.14 * 2N} = \sqrt{0.28N}$.

Note that if the target vector is the shortest vector, then $R = \sqrt{4N/3}$. It is an interesting open problem to close the gap.

5 Conclusion

In this paper, we study the length of shortest vector of random knapsack lattices and random NTRU lattices. Let $a_1, a_2, \cdots, a_n$ be integers selected uniformly and independently from integers between 0 and $2^r - 1$, then with probability at least $1 - \frac{1}{nr}$, the length of the shortest vector in the knapsack lattice $L_{a_1, a_2, \cdots, a_n}$ is greater than $\sqrt{\frac{n+1}{2\pi e}} \cdot 2^{\frac{r}{n+1}}(1 + O(\frac{\log(nr)}{n}))$. For random NTRU lattices, we obtain that with a overwhelming probability, the lower bound of the shortest vector length of NTRU lattice is $\Omega(\sqrt{N})$. The main problem left open by this work is to prove that with a high probability, the target vector is shortest in a random NTRU lattice.

References

1. M. Ajtai. The shortest vector problem in l2 is NP-hard for randomized reductions (extended abstract) 10-19. In Proc. 30th ACM Symp. on Theory of Computing (STOC), pages 10-19. ACM, 1998.
2. M. Ajtai. Random lattices and a conjectured 0-1 law about their polynomial time computable properties. In Proc. of FOCS 2002, pages 13–39, IEEE, 2002.
3. D. Aharonov and O. Regev. Lattice problems in NP intersect coNP. Journal of the ACM, 52(5):749-765, 2005. Preliminary version in FOCS 2004.
4. J.-Y. Cai and A. Nerurkar. Approximating the SVP to within a factor $(1 + 1/\dim)$ is NP-hard under randomized reductions. J. Comput. System Sci., 59(2):221-239, 1999.
5. D. Coppersmith, A. Shamir, Lattice attacks on NTRU, Proceedings of EUROCRYPT 97.
6. J. Hoffstein, J. Pipher, and J. Silverman. NTRU: a ring based public key cryptosystem. In Proc. of ANTS III, volume 1423 of LNCS, pages 267–288. Springer-Verlag, 1998. First presented at the rump session of Crypto 96.
7. I. Haviv and O. Regev. Tensor-based hardness of the shortest vector problem to within almost polynomial factors. In Proc. 39th ACM Symp. on Theory of Computing (STOC), pages 469-477, 2007.
8. A. W. Ingleton. The Rank of Circulant Matrices. J. London Math. Soc. 1956 s1-31: 445-460.
9. S. Khot. Hardness of approximating the shortest vector problem in lattices. In Proc. 45th Annual IEEE Symp. on Foundations of Computer Science (FOCS), pages 126-135, 2004.
10. J.C.Lagarias and A.M.Odlyzko.Solving low-density subset sum problems. Jounal of the Association for Computing Machinery, January 1985.
11. M.Li and P.Vita′nyi,An introduction to Kolmogorov complexity and its applications of Springer-Verlag,1993.
12. D. Micciancio. The shortest vector problem is NP-hard to approximate to within some constant. SIAM J. on Computing, 30(6):2008-2035, Mar. 2001. Preliminary version in FOCS 1998.
13. R.C.Merkle, and M.E.Hellman, Hiding Information and Signatures in Trapdoor Knapsacks.IEEE Trans.inf.Theory vol.24, 1978, 525-530.
14. J. E. Mazo and A. M. Odlyzko, Lattice points in high-dimensional spheres,. Monatsh. Math. 110 (1990), 47-61.
15. Phong Q. Nguyen and Damien Stehle. LLL on the Average. Proceedings of ANTS VII. F. Hess, S. Pauli and M. Pohst (Ed.), vol. 4076 of Lecture Notes in Computer Science, Springer-Verlag, pages 238-256.
16. A.M.Odlyzko, The rise and fall of knapsack cryptosystems. In Cryptology and Computional Number Theory, vol.42 of Symposina in Applied Mathematics, 1990, 75-88
17. A.Shamir, A Polynomial Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem. IEEE Trans.inf.Theory vol.30, 1984, 699-704.
18. C. L. Siegel, A mean Value theorem in geometry of numbers. Annals of Mathematics, 46(2):340-347, 1945.