Efficient provable-secure NTRUEncrypt over any cyclotomic field

Yang Wang, Mingqiang Wang*

School of Mathematics, Shandong University

wyang1114@mail.sdu.edu.cn, wangmingqiang@sdu.edu.cn

Abstract

NTRUEncrypt is a fast lattice-based cryptosystem and a probable alternative of the existing public key schemes. The existing provable-secure NTRUEncrypts are limited by the cyclotomic field it works on - the prime-power cyclotomic field. This is worth worrying, due to the subfield attack methods proposed in 2016. Also, the module used in computation and security parameters rely heavily on the choice of plaintext space. These disadvantages restrict the applications of NTRUEncrypt.

In this paper, we give a new provable secure NTRUEncrypt in standard model under canonical embedding over any cyclotomic field. We give an reduction from a simple variant of RLWE - an error distribution discretized version of RLWE, hence from worst-case ideal lattice problems, to our NTRUEncrypt. In particular, we get a union bound for reduction parameters and module for all choices of plaintext space, so that our NTRUEncrypt can send more encrypted bits in one encrypt process with higher efficiency and stronger security. Furthermore, our scheme's decryption algorithm succeeds with probability $1 - n^{\omega(\sqrt{n \log n})}$ comparing with the previous works' $1 - n^{-\omega(1)}$, making our scheme more practical in theory.

Keywords: NTRU, Ideal lattice, Canonical embedding, Cyclotomic fields, RLWE

1 Introduction

The NTRU encryption scheme, devised by Hoffstein, Pipher and Silverman in [19], was first presented in Crypto'96. It is one of the fastest known lattice-based cryptosystems as testified by its inclusion in the IEEE P1363 standard and regarded as an alternative to RSA and ECC due to its potential of countering attacks by quantum computer. Based

*Corresponding author

on the underlying problem of NTRU, various cryptographic primitives are designed, such as ideuntity-based encryption [11], fully homomorphic encryption [4, 26], digital signatures [10, 18] and multi-linear maps [14]. Meanwhile, a batch of cryptanalysis works were proposed aiming at NTRU family [1, 6, 7, 12, 13, 15, 17, 20, 22, 34]. Althought its description (early version) relies on arithmetic over polynomial ring for small parameters, it is generally believed that NTRU problem is hard and NTRUEncrypt is secure in practice.

However, the security of the first NTRUEncrypt in [19] is heuristic and lack of solid mathematical proof. This leads to a break-and-repair development history of NTRUEncrypt. The first provable secure NTRUEncrypt variant is proposed by Stehlé and Steinfeld in [35]. They gave a reduction from RLWE problem to the IND-CPA security of their NTRUEncrypt. But the modified scheme is restricted to power-of-2 cyclotomic rings. Although Stehlé and Steinfeld's scheme maybe less practical compared with classical NTRUEncrypt [8], it showed an important connection between NTRUEncrypt and RLWE, hence between problems over NTRUEncrypt and worst-case problems over ideal lattices. Recently, Yu, Xu and Wang modified Stehlé and Steinfeld's scheme to make it work over prime cyclotomic rings in [38]. Though the results of Yu allows more flexibility of parameter selections, the size requirements for parameters are more limited, making Yu's scheme less efficiency. Both of the above works are based on coefficient embedding. The first NTRUEncrypt scheme using canonical embedding is discussed in [39] which shows that given approximate parameters, provably secure NTRUEncrypt can work on prime-power cyclotomic rings. Yu's two papers gave a reduction from a variant of RLWE problem proposed in [9] to their NTRUEncrypts.

With the recent calls of post-quantum cryptography by NIST (Dec. 2016), a better understanding of these problems is necessary and the study of NTRUEncrypt is of theoretical value as stated in [39]. Considering the subfield attack proposed in [1, 6, 22], designing practical NTRUEncrypt with more flexible choices of parameters over more general rings (algebraic fields) is worth to do and this is also the main motivation of our paper. Moveover, different choices of the plaintext spaces influence the efficiency of the previous NTRUEncrypts greatly. That is to say, in order to reach the best efficiency in applications, the existing NTRUEncrypts' plaintext space are all limited - only encrypt one bit in each encrypt process. Try to improve the efficiency of NTRU scheme is also a big motivation of our research.

1.1 Our Contributions

In this paper, we give a IND-CPA secure NTRUEncrypt by using canonical embedding over any cyclotomic field and give a reduction from a variant of RLWE problem discussed in [24] to our NTRUEncrypt. Thanks to the RLWE problem we used and the powerful basis and decoding basis discussed in [24], the reduction parameters are much tighter than all the previous results. Moreover, our scheme allows a more flexible choice of parameters. Also, our scheme's decryption algorithm succeeds with probability $1 - n^{\omega(\sqrt{n \log n})}$ comparing with the previous works' $1 - n^{-\omega(1)}$, making our scheme more practical in theory. Our results enrich the provably secure NTRU family. We also give an improved regularity result for

all cyclotomic rings by-products. We exploit some ideals shown in [36, 38, 39], and many technical differences need to be treated carefully.

Our main contributions are summarized as follows.

We design a new variant of NTRUEncrypt by using canonical embedding over any cyclotomic field. We put our scheme to work on the fractional ideal $R^\vee$, the codefferent ideal of any cyclotomic field while the previous works are restricted in prime-power cyclotomic rings.

The RLWE problems we used is a simple variant of the original RLWE problem proposed in [23] - an error distribution discretized version of RLWE. Comparing with the RLWE in polynomial rings, the version we used has less reduction loss and tighter reduction parameters.

We observe that the decryption process is not necessary to consider the so-called coefficient embedding. We only need to consider the coefficients of element represented under the basis of $R^\vee$, and different basis effects the results heavily. So we consider a kind of basis-coefficient embedding and drop the traditional coefficient embedding completely.

We use decoding basis of $R^\vee$ proposed in [24] and subgaussian distribution to analysis the error distribution, which give us a looser bound for estimating the decryption algorithm. These mathematical tools also make our decryption algorithm succeed with an exception of a negligible probability $n^{-\omega(\sqrt{n\log n})}$, much better than the previous works' $n^{-\omega(1)}$ in applications.

Our main result is as following:

Theorem 1.1. *Let l be a positive integer, $n=\varphi(l)\geq 6$, $q\geq 8n$, $q=1 \mod l$ be a prime of size poly(n), $K=\mathbb{Q}(\zeta_l)$ be a cyclotomic field and R be the ring of algebraic integers of K. Assume that $\alpha=\alpha(n)\geq 2$ satisfies $\alpha q\geq\omega(\sqrt{\log n})$. Let $\xi=\alpha\cdot(\frac{nk}{\log(nk)})^{\frac{1}{4}}$ with $k=O(1)$, $\varepsilon\in(0,\frac{1}{2})$ and $p\in R_q^\times$ with $R_q^\times$ the set of invertible elements of $R_q=R/(qR)$. Moreover, let $\sigma\geq n^{\frac{3}{2}}\cdot\sqrt{\ln(8nq)}\cdot q^{\frac{1}{2}+\varepsilon}$ and $\omega(n^{\frac{3}{2}}\sqrt{\log n\log\log n}\cdot\alpha^2\cdot q^2)\cdot\sigma\cdot||p||_\infty^2<q$. Then if there exists an IND-CPA attack against NTRUEncrypt(n,q,p,σ,ξ) proposed in Section 5 that runs in time poly(n) and has success probability $\frac{1}{2}+\frac{1}{poly(n)}$, there exists a poly$(n)-$time algorithm solving $\gamma-$Ideal-SIVP on any ideal lattice of K with $\gamma=\tilde{O}(\frac{\sqrt{n}}{\alpha})$. Moreover, the decryption algorithm succeeds with probability $1-n^{-\omega(\sqrt{n\log n})}$ over the choice of the encryption randomness.*

To have a overview, we take $\sigma=n^{\frac{3}{2}}\cdot\sqrt{\ln(8nq)}\cdot q^{\frac{1}{2}+\varepsilon}$, $\alpha\cdot q=\omega(\sqrt{\log n})$, then $q^{\frac{1}{2}-\varepsilon}=\omega(n^3\log^2 n\cdot||p||_\infty^2)$. Although when p is a "constant" in R, i.e. $p\in\mathbb{Z}$, our result is not as good as [35, 39], when p is a "non-constant polynomial", our results maybe better. In particular, when p is an element whose coefficients are all non-zero with respect to the usual power basis of R, our result is even better than [35], the case of cyclotomic field $K=\mathbb{Q}(\zeta_{2^k})$ - the most commonly used cyclotomic fields. More precisely, in this case, the magnitude of q in [35] becomes $\tilde{\omega}(n^{11})$, in [38] becomes $\tilde{\omega}(n^{11.5})$ and in [39] becomes $\tilde{\omega}(n^{8.5})$, while ours is $\tilde{\omega}(n^6)$. Moreover, in applications, our construction gets rid of the restriction of cyclotomic fields and has potentialities to send more encrypted bits in one encrypt process - about

$O(n)$ times more than [35, 38, 39] when their schemes set p to be a small "polynomial" to approximate the best bound of q and γ. Further, our decryption algorithm succeeds with a probability of $1 - n^{-\omega(\sqrt{n \log n})}$ comparing with the previous work's $1 - n^{-\omega(1)}$. More details are discussed in Section 6.

1.2 Technique Overview

In this section, we give a technique overview about our constructions. Although the main thoughts of our NTRUEncrypt constructions follow Stehlé and Steinfeld's route, many differences exist.

We design our modified NTRUEncrypt in any cyclotomic field by using canonical embedding and give a reduction from a simple variant of RLWE problem proposed in [24] to our scheme. This is quite different from the existing provable-secure NTRUEncrypts, which work in the ring of algebraic integers (or equivalently the cyclotomic polynomial ring) in theory.

The error distribution of the modified RLWE proposed in [24] is a discretization of a gaussian distribution on K to $R^\vee$. It is a kind of subgaussian distribution as discussed in [28]. The properties of subgaussian distribution, together with a simple computation (Lemma 5.1) give us a nice estimation of the infinite norm of elements represented by decoding basis in $R^\vee$. These technical treatment, with the addition of savings by using the simple variant of RLWE problem, can tighten up the bound of q and make our scheme more efficient in theory.

We regard the element as an usual algebraic number and put all computations in cyclotomic fields. More preciously, our scheme is not restricted in the domain R (or equivalent, the polynomial ring) - the ring of algebraic integers of a cyclotomic field. We put it to work on the fractional ideal $R^\vee$, the codefferent ideal of cyclotomic field. Hence, we can get a union bound for module q and security parameter γ, making our schemes have potentialities to send more encrypted bits in each encrypt process with higher efficiency and stronger security.

The key generation algorithm is as follows:

$Input:$ $n, q \in \mathbb{Z},\ p \in\ R_q^\times,\ \sigma \in \mathbb{R}$.

$Output:$ $A\ key\ pair\ (sk,\ pk) \in\ R_q^\times \times R_q^\times$.

1. $Sample\ f^{'}\ from\ D_{R,\sigma};\ let\ f = p \cdot f^{'} + 1;\ if\ (f \mod qR) \notin R_q^\times,\ resample.$

2. $Sample\ g\ from\ D_{R,\sigma};\ if\ (g \mod qR) \notin R_q^\times,\ resample.$

3. $Return\ secret\ key\ sk = f\ and\ public\ key\ pk = h = pg/f \in R_q^\times.$

This is almost the same comparing with the previous works. We use standard method to prove that the algorithm would terminate in expected time. Furthermore, the Gaussian distribution ensures that the secret key is 'short'. The analysis of public key distribution needs to deal with some kinds of q-ary lattices, defined in Section 3.1. By accurate analysis

of the relationship between different fractional ideals, also inspired by [39] as we remarked in Section 3.2, we give a lower bound of λ_1 with respect to l_∞ norm in a kind of q-ary lattice. In this section, we consider the problem absolutely in K, hence get a better result comparing with [39]. We also get an improved regularity result, which is discussed by Micciancio in [27], for any cyclotomic ring by-products.

The NTRUEncrypt is as following:

Key generation : *Use the algorithm describe above, return* $sk = f \in R_q^\times$ *with* $f = 1 \ mod \ pR^\vee$, *and* $pk = h = pg \cdot f^{-1} \in R_q^\times$.

Encryption : *Given message* $m \in \mathcal{P}$, *set* $s, e \hookleftarrow \chi$ *and return* $c = hs + pe + m \in R_q^\vee$.

Decryption : *Given ciphertext* c *and secret key* f, *compute* $c_1 = fc$. *Then return* $m = (c_1 \mod qR^\vee) \mod pR^\vee$.

The plaintext of our scheme is $R^\vee/(pR^\vee)$ with p an invertible element in $R_q = R/(qR)$. Our computations are in $R^\vee$, not restricted in R. By using the decoding basis of $R^\vee$ and basis-coefficient embedding of element in $R^\vee$, we give a tight connection between canonical norms and basis-coefficient norms, which is helpful for us to analyze the decryption algorithm. These operations also enable us to get rid of the limitations of cyclotomic fields in theory. Therefore, we get an uniform result for all cyclotomic field. Moveover, by using Lemma 5.1, we also prove that the failure probability of our decryption process is negligible - $n^{-\omega(\sqrt{n \log n})}$ comparing with the existing schemes' $n^{-\omega(1)}$. Furthermore, as we remark in Remark 5.3, we can put all computations and storages in an integral ideal of R. Hence, in applications, our constructions maybe more practical.

To sum up, though the best bounds of q in [36] is about $n^{1.5}$ times smaller than ours, the biggest advantage of our scheme is that our constructions do not limited by the choice of plaintext space and the cyclotomic fields they work on in theory. Hence, our NTRUEncrypt can send more encrypted bits in one encrypt process with higher efficiency and stronger security. Further, our decryption algorithm succeeds with a probability of $1 - n^{-\omega(\sqrt{n \log n})}$ comparing with the previous work's $1 - n^{-\omega(1)}$. Therefore, we believe, in applications, our scheme would have more advantages.

2 Preliminaries

In this section, we introduce some background results and notations.

2.1 Notations

Throughout this paper, l, n are positive integers. $\hat{l} = l$ when l is odd and $\hat{l} = \frac{l}{2}$ when l is even. Functions $\varphi(n)$ and $\mu(n)$ stand for the Euler function and the Möbius function. We use

$[n]$ to denote the set $\{1, 2, \cdots, n\}$. For $p = 1, 2, \cdots, \infty$, we use $||x||_p$ to represent it's l_p norm corresponding to the canonical embedding. When $p = 2$, we usually use $||x||$ to represent it's l_2 norm. For any matrix $M \in \mathbb{C}^{k\times k}$, we use $\lambda_i(M)$ stand for it's eigenvalues and $s_i(M)$ stand for it's singular values for $i \in [n]$. We arrange eigenvalues and singular values by their magnitude, i.e. $\lambda_1(M) \geq \cdots \geq \lambda_n(M)$ and $s_1(M) \geq \cdots \geq s_n(M)$. For two random variables X, Y, $\Delta(X, Y)$ stands for their statistic distance. Function rad represent the radical of a positive integer n, i.e. for $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ with different primes p_i, $rad(n) = \prod_{i=1}^{k} p_i$.

2.2 Cyclotomic Number Fields, Space H and Geometry

Through out this paper, we consider the cyclotomic number fields. Let $K = Q(\zeta)$ for $\zeta = \zeta_l$ be the l-th primitive unit root, which has minimal polynomial $\Phi_l(x) = \prod_{i|l}(x^i - 1)^{\mu(\frac{l}{i})}$ of degree $n = \varphi(l)$. Hence $[K : Q] = n = \varphi(l)$, and $K \cong \mathbb{Q}[x]/\Phi_l(x)$. We set $R = \mathcal{O}_K = \mathbb{Z}[\zeta]$ be K's ring of integers. Let $q \in \mathbb{Z}$ be a prime, then the factorization of the ideal $\langle q\rangle = qR$ is as follows. Let $d \geq 0$ be the largest integer such that q^d divides l, let $e = \varphi(q^d)$ and let $f \geq 1$ be the multiplicative order of q modulo l/q^d. Then $\langle q\rangle = \prod_{i=1}^{g} \mathfrak{q}_i^e$ where $\mathfrak{q}_i$ are $n/(ef)$ different prime ideals, each of norm q^f.

In particular, for an integer prime $q = 1 \mod l$, we have $e = f = 1$, the ideal $\langle q\rangle$ splits into n distinct prime ideals as $\langle q\rangle = \prod_{i\in\mathbb{Z}_l^*} \mathfrak{q}_i$ with $\mathfrak{q}_i = \left\langle q, \zeta - \omega^i\right\rangle$, where ω is a primitive root in $\mathbb{Z}_q$. The norm of $\mathfrak{q}_i$ is q. We have $\Phi_l(x) = \prod_{i\in\mathbb{Z}_l^*}(x - \omega^i) \mod q$. Note that $R_q = \mathbb{Z}_q[x]/\Phi_l(x)$, the Chinese Remainder Theorem gives us a isomorphism $R_q \cong \prod_{i\in\mathbb{Z}_l^*} \mathbb{Z}_q[x]/(x - \omega^i)$, where the $\prod$ represents the direct product. We will use this property frequently, so from now on, we assume q is a prime such that $q = 1 \mod l$.

Since K/Q is a Galois extension and $[K : Q] = n = 2s$, $s \in \mathbb{Z}^+$, there are n embeddings from K to $\mathbb{C}$. In fact, they are automorphisms of K, all of them are complex embeddings and form K's Galois group. We set $\mathrm{Gal}(K/Q) = \{\sigma_i : \ i = 1, \cdots, n\}$ and use the canonical embedding σ on K, who maps $x \in K$ to $(\sigma_1(x), \cdots, \sigma_n(x)) \in H$, where H is a kind of Minkowski space in algebraic number theory. Here we identity $\sigma_i(\zeta) = \zeta^{l_i}$ with l_i the $l-$th element of $\mathbb{Z}_l^*$, order the σ_i and define $H = \{(x_1, \cdots, x_n) \in \mathbb{C}^n : \ x_{n+1-i} = \overline{x_i}, \ \forall i \in [s]\}$, H is isomorphic to $\mathbb{R}^n$ as an inner product space via the orthonormal basis $\boldsymbol{h}_{i\in[n]}$ defined as follows: assume $\boldsymbol{e}_j \in \mathbb{C}^n$ be the vector with 1 in its j-th coordinate and 0 elsewhere, $\boldsymbol{i}$ be the complex unit, we set $\boldsymbol{h}_j = \frac{1}{\sqrt{2}}(\boldsymbol{e}_j + \boldsymbol{e}_{n+1-j})$ and $\boldsymbol{h}_{n+1-j} = \frac{\boldsymbol{i}}{\sqrt{2}}(\boldsymbol{e}_j - \boldsymbol{e}_{n+1-j})$ for $1 \leq j \leq s$. Moveover, $\sigma(K) \subseteq H \cong K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$.

For any element $x \in K$, we can define the ℓ_p norm of x by $||x||_p = ||\sigma(x)||_p$ for $p < \infty$ and $||x||_\infty = \max_{i\in[n]} |\sigma_i(x)|$. Because multiplication of embedded elements is component-wise, for any $x, y \in K$, we have $||x \cdot y||_p \leq ||a||_\infty \cdot ||y||_p$ for $p \in \{1, \cdots, \infty\}$. The Trace and Norm of $x \in K$ is defined as usual, i.e. $\mathrm{Tr}(x) := \mathrm{Tr}_{K/\mathbb{Q}}(x) = \sum_{i=1}^{n} \sigma_i(x)$ and $\mathrm{N}(x) := \mathrm{N}_{K/\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x)$. The Norm is multiplicative: $\mathrm{N}(x \cdot y) = \mathrm{N}(x) \cdot \mathrm{N}(y)$. The Trace is $\mathbb{Q}-$linear: $\mathrm{Tr}(x + y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$ and $\mathrm{Tr}(c \cdot x) = c \cdot \mathrm{Tr}(x)$ for all $x, y \in K$ and $c \in \mathbb{Q}$. Also note that $\mathrm{Tr}(x \cdot y) = \sum_{i=1}^{n} \sigma_i(x)\sigma_i(y) =< \sigma(x), \overline{\sigma(y)} >$, so $\mathrm{Tr}(x \cdot y)$ is a symmetric bilinear form akin to the inner product of embeddings of x and y.

The absolute discriminant Δ_K of K is a measure of the geometry sparsity of its ring of integers. Let $\alpha_1, \cdots, \alpha_n$ represent the $\mathbb{Z}$ basis of R, then we can define $\Delta_K = |(\sigma_i(\alpha_j))_{1 \le i,j \le n}|^2$, where $|\cdot|$ represents the determinant of matrix. The discriminant of the $l-$th cyclotomic number field is

$$\Delta_K = \left(\frac{l}{\prod_{prime\ p|l} p^{\frac{1}{p-1}}} \right)^n \le n^n.$$

An integral ideal $I \subseteq R$ is the usual ideal defined in a ring and a fractional ideal $J \subseteq K$ is a set such that $dJ \subseteq R$ is a integral ideal for some $d \in R$. It is well known that both I and J admit $\mathbb{Z}$-basis and we can require $d \in \mathbb{Z}$. The norm of an integral ideal is its index as an additive subgroup of R and the norm of a fractional ideal J is defined as $\mathrm{N}(I) = \frac{\mathrm{N}(dI)}{\mathrm{N}(<d>)} = \frac{\mathrm{N}(dI)}{|\mathrm{N}(d)|}$ where $d \in R$ such that $dI \subseteq R$. One can regard integral ideal as a special fractional ideal. For any two fractional ideals I and J, the sum $I + J$ is the set of all $a + b$ for $a \in I$ and $b \in J$, and the product ideal $I \cdot J$ is the set of all finite sums of terms ab for $a \in I$ and $b \in J$. Multiplication extends to fractional ideals in the obvious way and the set of fractional ideals forms a group under multiplication. Every fractional ideal can be represented as the quotient of two integral ideals and has an inverse ideal, written I^{-1}, such that $I \cdot I^{-1} = R$.

2.3 Lattice and Discretization

We define a lattice as a discrete additive subgroup of H and we only deal with full-rank lattices. Assume $B = \{\boldsymbol{b_1}, \cdots, \boldsymbol{b_n}\}$ is the set of basis of a lattice Λ, we have $\Lambda = \mathcal{L}(B) = \{\sum_{i=1}^n z_i \boldsymbol{b_i} \ : \ z_i \in \mathbb{Z}\}$. The determinant of a lattice $\mathcal{L}(B)$ is defined as $|\det(B)|$, which is independent of the choice of basis B. The minimum distance $\lambda_1(\Lambda)$ of a lattice is the length of a shortest nonzero lattice vector. We usually use the l_2 norm, hence $\lambda_1(\Lambda) = \min_{0 \neq \boldsymbol{x} \in \Lambda} ||\boldsymbol{x}||$. The dual lattice of $\Lambda \subseteq H$ is defined as $\Lambda^\vee = \{\boldsymbol{y} \in H : \forall\ \boldsymbol{x} \in \Lambda, < \boldsymbol{x}, \overline{\boldsymbol{y}} >= \sum_{i=1}^n x_i y_i \in \mathbb{Z}\}$. This is actually the complex conjugate of the dual lattice as usually defined in $\mathbb{C}^n$. All of the properties of the dual lattice that we use also hold for the conjugate dual. It is easy to see that $(\Lambda^\vee)^\vee = \Lambda$. If $B = \{\boldsymbol{b_i}\} \subseteq H$ is a set of independent vector of a lattice, its dual basis $D = \{d_j\}$ is characterized by $< \boldsymbol{b_i}, \overline{\boldsymbol{d_j}} >= \delta_{ij}$, where δ_{ij} is the Kronecker delta. It is obvious that $\mathcal{L}(D) = \mathcal{L}(B)^\vee$.

For any fractional ideal I of K, we can represent I as $\mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n$ for some $\beta_i \in K$, $i = 1, \cdots, n$. Then $\sigma(I)$ is a lattice of H, and we call $\sigma(I)$ an ideal lattice and identify I with this lattice and associate with I all the usual lattice quantities. We have $\Delta_K = \det(\sigma(R))^2$, the squared determinant of the lattice $\sigma(R)$. For any fractional norm I, we also have $\det(\sigma(I)) = \mathrm{N}(I) \cdot \sqrt{\Delta_k}$. The following lemma from [23] gives upper and lower bounds on the minimum distance of an ideal lattice in l_2 norm.

Lemma 2.1. *For any fractional ideal I in a number field K of degree n,*

$$\sqrt{n} \cdot \mathrm{N}^{\frac{1}{n}}(I) \le \lambda_1(I) \le \sqrt{n} \cdot \mathrm{N}^{\frac{1}{n}}(I) \cdot \Delta_K^{\frac{1}{2n}}.$$

For any fractional ideal I in K, its dual is defined as $I^\vee = \{a \in K : \ Tr(aI) \subseteq \mathbb{Z}\}$. It is easy to verify $(I^\vee)^\vee = I$, $I^\vee$ is a fractional ideal and $I^\vee$ embeds under σ as the dual lattice

of I as defined before. For any fractional ideal $J \in K$ with $J = \mathbb{Z}\beta_1 + \cdots \mathbb{Z}\beta_n$ for $\beta_i \in J$, the dual of J can be represented as $J^\vee = \mathbb{Z}\beta_1^\vee + \cdots \mathbb{Z}\beta_n^\vee$ where $\mathrm{Tr}(\beta_i\beta_j^\vee) = \delta_{ij}$. In fact, an ideal of K and its inverse are related by multiplication with the dual ideal $R^\vee$: $I^\vee = I^{-1} \cdot R^\vee$. The factor $R^\vee$ is often called the codifferent, and its inverse $(R^\vee)^{-1}$ the different, which is in fact an ideal in R. For more details, one can refer to [5].

We now consider the discretization. As in [24] and [25], the goal is to convert a continuous Gaussian into a Gaussian-like distribution. Given a lattice $\Lambda = \mathcal{L}(B)$, a point $\boldsymbol{x} \in H$ and a point $\boldsymbol{c} \in H$ representing a lattice coset $\Lambda + \boldsymbol{c}$, the goal is to discretize $\boldsymbol{x}$ to a point $\boldsymbol{y} \in \Lambda + \boldsymbol{c}$, written $\boldsymbol{y} = \lfloor \boldsymbol{x} \rceil_{\Lambda+\boldsymbol{c}}$. We want to make the length of $\boldsymbol{y} - \boldsymbol{x}$ is not too large. To do this, we can sample a relatively short vector $\boldsymbol{f}$ from $\Lambda + (\boldsymbol{c} - \boldsymbol{x})$, and output $\boldsymbol{y} = \boldsymbol{f} + \boldsymbol{x}$. We require the method used to choose $\boldsymbol{f}$ be efficient and depend only on the desired coset $\Lambda + (\boldsymbol{c} - \boldsymbol{x})$. We call such a procedure valid.

Three easy methods are described in [24]. We describe the formal definition as in [28], a modified version of [24].

Definition 2.2. *If Bern denotes the Bernoulli distribution, then the univariate Reduction distribution* $Red(a) = Bern(\lceil a \rceil - a) - (\lceil a \rceil - a)$ *is the discrete probability distribution defined for parameter* $a \in \mathbb{R}$ *as taking the values*
1. $1 + a - \lceil a \rceil$ *with probability* $\lceil a \rceil - a$,
2. $a - \lceil a \rceil$ *with probability* $1 - (\lceil a \rceil - a)$.
A random variable $\boldsymbol{R} = (R_1, \cdots, R_n) \in \mathbb{R}^n$ *has a multivariate Reduction distribution* $R \sim Red(\boldsymbol{a})$ *on* $\mathbb{R}^n$ *for parameter* $\boldsymbol{a} = (a_1, \cdots, a_n)$ *if its components* $R_j \sim Red(a_j)$ *for* $j = 1, \cdots, n$ *are independent univariate Reduction random variables.*

Some useful lemmas are stated in [28], we only state the results.

Lemma 2.3. *(1) If* $R_0 \sim Red(a)$ *is a univariate Reduction random variable for parameter* $a \in \mathbb{R}$*, then* R_0 *satisfies* (i) $|R_0| \leq 1$*,* (ii) $E(R_0) = 0$*,* (iii) $Var(R_0) \leq \frac{1}{4}$ *and* (iv) $a - R_0 \in \{\lfloor a \rfloor, \lceil a \rceil\} \subseteq \mathbb{Z}$.
(2) Suppose that the lattice Λ *has (column) basis matrix* B *with* $s_1(B)$ *and* $\boldsymbol{R}$ *is a Reduction random variable of approximate dimension, then* $||B\boldsymbol{R}||^2 \leq n \cdot s_1^2(B)$ *and* $E(||B\boldsymbol{R}||^2) \leq \frac{1}{4} n \cdot s_1^2(B)$.

We now describe the coordinate-wise rounding discretisation which is easy to use for our application. One can check the following definition defines a valid discretisation, more details are in [28].

Definition 2.4. *Suppose* $\Lambda = \mathcal{L}(B)$ *is a* $n-$*dimensional lattice in* $\mathbb{R}^n$*. For* $\boldsymbol{c} \in \mathbb{R}^n$*, the coordinate-wise randomized rounding discretisation* $\lfloor \boldsymbol{x} \rceil^B_{\Lambda+\boldsymbol{c}}$ *of the point* $\boldsymbol{x} \in \mathbb{R}^n$ *to the lattice coset* $\Lambda + \boldsymbol{c}$ *with respect to the basis* B *can then be defined in terms of the multivariate Reduction random variable* $Q_{\boldsymbol{x},\boldsymbol{c}}$ *by the random variable*

$$\lfloor \boldsymbol{x} \rceil^B_{\Lambda+\boldsymbol{c}} = \boldsymbol{x} + BQ_{\boldsymbol{x},\boldsymbol{c}}, \qquad \text{where } Q_{\boldsymbol{x},\boldsymbol{c}} \sim Red(B^{-1}(\boldsymbol{c} - \boldsymbol{x})).$$

The coordinate-wise randomized rounding $\lfloor \boldsymbol{x} \rceil^B_{\Lambda+\boldsymbol{c}}$ of the point $\boldsymbol{x} \in \mathbb{R}^n$ has the properties $E(\lfloor \boldsymbol{x} \rceil^B_{\Lambda+\boldsymbol{c}}) = \boldsymbol{x}$ and $E(||\lfloor \boldsymbol{x} \rceil^B_{\Lambda+\boldsymbol{c}} - \boldsymbol{x}||^2) \leq n \cdot s_1(B)^2$. Also, by Lemma 2.3, it follows that $||\lfloor \boldsymbol{x} \rceil^B_{\Lambda+\boldsymbol{c}}|| \leq ||x|| + \sqrt{n} \cdot s_1(B)$. For lattices in space H, the definition of discretisation is similar.

Definition 2.5. *Suppose $\Lambda = \mathcal{L}(B)$ is a $n-$dimensional lattice in space H. For $\boldsymbol{c} \in H$, the coordinate-wise randomized rounding discretisation $\lfloor \boldsymbol{X} \rceil^B_{\Lambda+\boldsymbol{c}}$ of random variable $\boldsymbol{X}$ to the lattice coset $\Lambda + \boldsymbol{c}$ with respect to the basis B is then defined by the conditional random variable*

$$(\lfloor \boldsymbol{X} \rceil^B_{\Lambda+\boldsymbol{c}} | \boldsymbol{X} = \boldsymbol{x}) = \lfloor \boldsymbol{x} \rceil^B_{\Lambda+\boldsymbol{c}} = \boldsymbol{x} + BQ_{\boldsymbol{x},\boldsymbol{c}}, \qquad \text{where } Q_{\boldsymbol{x},\boldsymbol{c}} \sim Red(B^{-1}(\boldsymbol{c} - \boldsymbol{x})).$$

For a vector $\boldsymbol{x} \in H$, we also have $||\lfloor \boldsymbol{x} \rceil^B_{\Lambda+\boldsymbol{c}}|| \leq ||\boldsymbol{x}|| + \sqrt{n} \cdot s_1(B)$, just as the case defined in $\mathbb{R}^n$.

2.4 Tensors and Basis for R and $R^\vee$

Let K and L be two field extensions of $\mathbb{Q}$, the field tensor product $K \otimes_{\mathbb{Q}} L$ is defined as the set of all $\mathbb{Q}-$linear combinations of pure tensors $a \otimes b$ for $a \in K$ and $b \in L$, where $\otimes$ is $\mathbb{Q}-$bilinear and satisfies the mixed-product property, i.e. for all $e \in \mathbb{Q}$, one have $(a_1 \otimes b) + (a_2 \otimes b) = (a_1 + a_2) \otimes b$, $(a \otimes b_1) + (a \otimes b_2) = (a \otimes (b_1 + b_2))$, $e(a \otimes b) = (ea) \otimes b = a \otimes (eb)$ and $(a_1 \otimes b_1)(a_2 \otimes b_2) = (a_1 a_2) \otimes (b_1 b_2)$. These properties define addition and multiplication in $K \otimes_{\mathbb{Q}} L$, and though the result is not always a field, it will always be one whenever we take the tensor product of two cyclotomic fields in this work. A key fact from algebraic number theory is the following.

Proposition 2.6. *Let l have prime-power factorization $l = \prod l_k = \prod p_k^{\alpha_k}$, i.e. l_k are powers of distinct primes. Then $K = \mathbb{Q}(\zeta_l)$ is isomorphic to the tensor product $\otimes_k K_k$ of the field $K_k = \mathbb{Q}(\zeta_{l_k})$, via the correspondence $\prod_k a_k \to (\otimes_k a_k)$, where on the left we implicitly embed each $a_k \in K_k$ into K.*

When taking $K \cong \otimes_k K_k$, it follows directly from the definitions that the canonical embedding σ of K is the tensor product of the canonical embeddings σ^k of K_k, i.e. $\sigma(\otimes_k a_k) = \otimes_k \sigma^k(a_k)$. This decomposition of σ in turn implies that the trace decomposes as $\mathrm{Tr}_{K/\mathbb{Q}}(\otimes_k a_k) = \prod_k \mathrm{Tr}_{K_k/\mathbb{Q}}(a_k)$.

In our application, we hope that the matrices whose columns are consisted of the basis of R and $R^\vee$ has smaller s_1 and larger s_n. So, we introduce the powerful basis and decoding basis as in [25]. We set τ be the automorphism of K that maps ζ_l to $\zeta_l^{-1} = \zeta_l^{l-1}$, under the canonical embedding it corresponds to complex conjugation $\sigma(\tau(a)) = \overline{\sigma(a)}$. Note that for any l' dividing l, τ also maps $\zeta_{l'} = \zeta_l^{\frac{l}{l'}}$ to $\zeta_{l'}^{-1} = \zeta_l^{-\frac{l}{l'}}$.

Definition 2.7. *The Powerful basis $\vec{p}$ of $K = \mathbb{Q}(\zeta_l)$ and $R = \mathbb{Z}[\zeta_l]$ is defined as follows:*
(1) *For a prime power l, define $\vec{p}$ to be the power basis $(\zeta_l^j)_{(j\in\{0,1,\cdots,n-1\})}$, treated as a vector over $R \subseteq K$.*
(2) *For l having prime-power factorization $l = \prod l_k = \prod p_k^{\alpha_k}$, define $\vec{p} = \otimes_k \vec{p_k}$, the tensor product of the power bases $\vec{p_k}$ of each $K_k = \mathbb{Q}(\zeta_{l_k})$.*
The Decoding basis of $R^\vee$ is $\vec{d} = \tau(\vec{p})^\vee$, the dual of the conjugate of the powerful basis $\vec{p}$.

Also note that $\tau(\vec{p})$ is a $\mathbb{Z}-$basis of R. Different basis of R (or $R^\vee$) are connected by unimodular matrix, hence the spectral norm (i.e. the s_1) may have different magnitude. The following lemma comes from [25], which shows the estimate of $s_1(\sigma(\vec{p}))$ and $s_n(\sigma(\vec{p}))$. We remark that more details one can refer to [24, 25].

Lemma 2.8. *We have $s_1(\sigma(\vec{p})) = \sqrt{\hat{l}}$, $s_n(\sigma(\vec{p})) = \sqrt{\frac{l}{rad(l)}}$.*

We also need the estimate of $s_1(\sigma(\vec{d}))$ and $s_n(\sigma(\vec{d}))$. Assume that $\sigma(\vec{p}) = T$, the lemma shows that $s_1(T) = \sqrt{\hat{l}}$ and $s_n(T) = \sqrt{\frac{l}{rad(l)}}$. By the definition of $\vec{d}$ and dual ideal, through an easy computation, one have $\sigma(\vec{d}) = (T^*)^{-1}$. Hence we have $s_n(\sigma(\vec{d})) = \frac{1}{\sqrt{\hat{l}}}$, $s_1(\sigma(\vec{d})) = \sqrt{\frac{rad(l)}{l}}$. Moreover, one can similarly deduce that $||\sigma(\vec{d})_i|| \leq \sqrt{\frac{rad(l)}{l}}$ for all $i = 1, 2, \cdots, n$.

We define the symbol $||\cdot||_B^c$ the basis-coefficient embedding norm. Given a basis B of a fractional ideal J, for any $x \in J$, written $x = x_1 b_1 + \cdots + x_n b_n$, then the $B-$coefficient embedding of x is the vector $(x_1, \cdots, x_n)$ and the $B-$cofficient embedding norm of x is defined as $||x||_B^c = (\sum_{i=1}^n x_i^2)^{\frac{1}{2}}$. Hence, if we represent $x \in R$ (or $R^\vee$) with respect to the powerful basis (decoding basis), we have

$$\sqrt{\frac{l}{rad(l)}}||x||_{\sigma(\vec{p})}^c \leq ||\sigma(x)|| \leq \sqrt{\hat{l}}||x||_{\sigma(\vec{p})}^c \qquad for\ x \in\ R, \tag{1}$$

and

$$\frac{1}{\sqrt{\hat{l}}}||x||_{\sigma(\vec{d})}^c \leq ||\sigma(x)|| \leq \sqrt{\frac{rad(l)}{l}}||x||_{\sigma(\vec{d})}^c \qquad for\ x \in\ R^\vee. \tag{2}$$

When we write $x \mod qR^\vee$, we use the representative element of the coset $x + qR^\vee$ by $\sum_{i=1}^n x_i \vec{d_i}$ with $x_i \in [-\frac{q}{2}, \frac{q}{2})$ for computation. Similarly, for element $x \in R$, we write $x \mod qR$, we use the representative element of the coset $x+qR$ by $\sum_{i=1}^n x_i \vec{p_i}$ with $x_i \in [-\frac{q}{2}, \frac{q}{2})$. For our applications, we need to do computations in $R^\vee$. Notice that $R \subseteq R^\vee$, any element of R can also be represented as a $\mathbb{Z}-$linear combination of the decoding basis. From now on, we only use the decoding basis of $R^\vee$ and the powerful basis of R. We will omit the subscribe $\sigma(\vec{d})$ when we use the $\sigma(\vec{d})-$cofficient embedding of elements in $R^\vee$.

2.5 Gaussian and Subgaussian Random Variables

For $s > 0$, define the Gaussian function $\rho_s : H \to (0, 1]$ as $\rho_s(\boldsymbol{x}) = e^{-\pi \frac{||x||^2}{s^2}}$. By normalizing this function we obtain the continuous Gaussian probability distribution D_s of

parameter s, whose density is given by $s^{-n} \cdot \rho_s(\boldsymbol{x})$. Let $\boldsymbol{r} = (r_1, \cdots, r_n) \in (\mathbb{R}^+)^n$ be a vector such that $r_j = r_{n+1-j}$ for $j \in [s]$, we can define the elliptical Gaussian distributions in the basis $\{\boldsymbol{h}_i\}_{i \leq n}$ as follows: a sample from $D_{\boldsymbol{r}}$ is given by $\sum_{i \in [n]} x_i \boldsymbol{h}_i$, where x_i are chosen independently from the Gaussian distribution D_{r_i} over $\mathbb{R}$. Note that, if we define map $\varphi : H \to \mathbb{R}^n$ by $\varphi(\sum_{i \in [n]} x_i \boldsymbol{h}_i) = (x_1, \cdots, x_n)$, then $D_{\boldsymbol{r}}$ is also a (elliptical) Gaussian distribution over $\mathbb{R}^n$. The map $\varphi \circ \sigma$ builds a relation of Gaussian distribution between H and $\mathbb{R}^n$.

For a lattice $\Lambda \subseteq H$, $\sigma > 0$ and $\boldsymbol{c} \in H$, we define the lattice Gaussian distribution of support Λ, deviation σ and center $\boldsymbol{c}$ by $D_{\Lambda,\sigma,\boldsymbol{c}}(\boldsymbol{b}) = \frac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{b})}{\rho_{\sigma,\boldsymbol{c}}(\Lambda)}$, for any $\boldsymbol{b} \in \mathbb{R}^n$. We usually omit the subscript $\boldsymbol{c}$ when it is $\boldsymbol{0}$. For $\delta > 0$, we define the smoothing parameter $\eta_\delta(\Lambda)$ as the smallest $\sigma > 0$ such that $\rho_{\frac{1}{\sigma}}(\Lambda^\vee \setminus \boldsymbol{0}) \leq \delta$. It quantifies how large σ needs to be for $D_{L,\sigma,\boldsymbol{c}}$ to behave like a continuous Gaussian. We will use following lemmas from [29], [31], [3] and [16].

Lemma 2.9. *For any full-rank lattice Λ and positive real $\varepsilon > 0$, we have $\eta_\varepsilon(\Lambda) \leq \sqrt{\frac{\ln(2n(1+\frac{1}{\varepsilon}))}{\pi}} \cdot \lambda_n(\Lambda)$.*

Lemma 2.10. *For any full-rank lattice Λ, $\boldsymbol{c} \in H$, $\varepsilon \in (0,1)$ and $\sigma \geq \eta_\varepsilon(L)$, we have $\Pr_{\boldsymbol{b} \hookleftarrow D_{\Lambda,\sigma,\boldsymbol{c}}}[||\boldsymbol{b} - \boldsymbol{c}|| \geq \sigma\sqrt{n}] \leq \frac{1+\varepsilon}{1-\varepsilon} \cdot 2^{-n}$.*

Lemma 2.11. *For any full-rank lattice Λ and any positive real $\varepsilon > 0$, we have $\eta_\varepsilon(\Lambda) \leq \sqrt{\frac{\ln(2n(1+\frac{1}{\varepsilon}))}{\pi}} \cdot \frac{1}{\lambda_1^\infty(\Lambda^\vee)}$.*

Lemma 2.12. *Let B_n denote the Euclidean unit ball. Then for any lattice Λ and any $\sigma > 0$, $\rho_\sigma(\Lambda/(\sqrt{n}\sigma B_n)) < 2^{-2n} \cdot \rho_r(\lambda)$, where $\Lambda/(\sqrt{n}\sigma B_n)$ is the set of lattice points of norm greater than $\sqrt{n}\sigma$. Hence, $\Pr_{\boldsymbol{x} \hookleftarrow D_{\Lambda,\sigma}}(||\boldsymbol{x}|| > \sqrt{n}\sigma) < 2^{-2n}$.*

Lemma 2.13. *Let $\Lambda' \subseteq \Lambda$ be full-rank lattices. For any $\boldsymbol{c} \in H$, $\varepsilon \in (0, 1/2)$ and $\sigma \geq \eta_\varepsilon(\Lambda')$, we have $\Delta(D_{\Lambda,\sigma,\boldsymbol{c}} \mod \Lambda', U(\Lambda/\Lambda')) \leq 2\varepsilon$.*

It is convenient for us to use the notion of subguassian random variables in our application. We only introduce the definition and some lemmas we need, more details can be found in [24], [28], [30] and [37]. We describe the definitions as in [28].

Definition 2.14. *For $\delta \geq 0$, a real-valued random variable X is $\delta-$subgaussian with standard parameter $b \geq 0$ if*

$$E(e^{tX}) \leq e^{\delta} e^{\frac{1}{2}b^2t^2} \qquad for\ all\ t \in \mathbb{R}.$$

A real-valued random variable X is $\delta-$subgaussian random variable with scaled parameter $s \geq 0$ if

$$E(e^{2\pi tX}) \leq e^{\delta} e^{\pi s^2 t^2} \qquad for\ all\ t \in \mathbb{R}.$$

Notice that if $X \sim N(0, b^2)$, then X is a $\delta-$subgaussian random variable with standard parameter b, the $e^{\frac{1}{2}b^2t^2}$ term is exactly the moment-generating function of the one-dimension Gaussian distribution of parameter b over $\mathbb{R}$. A real-valued random variable is $\delta-$subgaussian with standard parameter b if and only if it is $\delta-$subgaussian with scaled parameter $\sqrt{2\pi}b$. One can extend the definitions to $\mathbb{R}^n$ or space H.

Definition 2.15. *For any $\delta \geq 0$, a multivariate random variable $\boldsymbol{X}$ on $\mathbb{R}^n$ is $\delta-$subgaussian with standard parameter $b \geq 0$ if*

$$E(e^{<\boldsymbol{t},\boldsymbol{X}>}) \leq e^{\delta}e^{\frac{1}{2}b^2||\boldsymbol{t}||^2} \qquad for\ all\ \boldsymbol{t} \in \mathbb{R}^n.$$

A multivariate random variable $\boldsymbol{Z}$ on H is a $\delta-$subgaussian with standard parameter $b \geq 0$ if

$$E(e^{<\boldsymbol{t},\boldsymbol{Z}>}) \leq e^{\delta}e^{\frac{1}{2}b^2||\boldsymbol{t}||^2} \qquad for\ all\ \boldsymbol{t} \in H.$$

This definition is equivalent to say that a random vector $\boldsymbol{X}$ or its distribution is $\delta-$subgaus sian with standard parameter b if for all unit vector $\boldsymbol{t} \in \mathbb{R}^n$, the random variable $< \boldsymbol{X}, \boldsymbol{t} >$ is $\delta-$subgaussian with standard parameter b. Using the inequality $\cosh(x) \leq e^{\frac{x^2}{2}}$, it can be shown that any $B-$bounded centered univariate random variable X (i.e. $E[X] = 0$ and $|X| \leq B$) is $0-$subguassian with standard parameter B ($0-$subgaussian with scaled parameter $B\sqrt{2\pi}$).

Definition 2.16. *A random variable $\boldsymbol{Z}$ on $\mathbb{R}^n$ or H is a noncentral subgaussian random variable with noncentrality parameter $||E(\boldsymbol{Z})|| \geq 0$ and deviation parameter $d \geq 0$ if the centered random variable $\boldsymbol{Z}_0 = \boldsymbol{Z} - E(\boldsymbol{Z})$ is a $0-$subgaussian random variable with standard parameter d.*

We regard a central subgaussian random variable as a special case of a noncentral sub-gaussian random variable. A fact showed in [28] Theorem 3 states that the coordinate-wise randomized rounding discretisation of $\boldsymbol{z}$ to $\lfloor \boldsymbol{z} \rceil^B_{\Lambda+\boldsymbol{c}}$ for $\Lambda = \mathcal{L}(B) \subseteq H$ and $\boldsymbol{c} \in H$ is a noncentral subgaussian random variable with noncentrality parameter $||\boldsymbol{z}||$ and deviation parameter $\frac{1}{2}s_1(\sigma(B))$. Moveover, [28] proposed the following useful lemma.

Lemma 2.17. *Suppose that B is a column basis matrix for a lattice in H with largest singular value $s_1(B)$ and $\boldsymbol{Z}$ is an independent noncentral subgaussian random variable with deviation parameter $d_{\boldsymbol{Z}}$. The coordinate-wise randomized rounding discretisation of $\boldsymbol{Z}$ to $\lfloor \boldsymbol{Z} \rceil^B_{\Lambda+\boldsymbol{c}}$ is a noncentral subgaussian random variable with noncentrality parameter $||E(\boldsymbol{Z})||$ and deviation parameter $(d^2_{\boldsymbol{Z}} + (\frac{1}{2})^2 s_1(B)^2)^{\frac{1}{2}}$.*

2.6 RLWE Problem

We first state a definition of RLWE with a slight different comparing with [23] by scaling the b component by a factor of q and describe the worst-case result shown in [23].

Definition 2.18. *For a secret $s \in R_q^\vee$ and a distribution ψ over $K_\mathbb{R}$, a sample from RLWE distribution $A_{s,\psi}$ over $R_q \times (K_\mathbb{R}/(qR^\vee))$ is generated by choosing $a \hookleftarrow U(R_q)$, choosing $e \hookleftarrow \psi$, and outputting $(a, b = a \cdot s + e \mod qR^\vee)$.*

Definition 2.19. *The average-case decision version of the RLWE problem, denoted $R-DLWE_{q,\psi}$, is to distinguish with non-negligible advantage between independent samples from $A_{s,\psi}$ where $s \hookleftarrow U(R_q^\vee)$, and the same number of uniformly random and independent samples from $R_q \times (K_\mathbb{R}/(qR^\vee))$.*

Theorem 2.20. *Let K be the l-th cyclotomic number field having dimension $n = \varphi(l)$ and $R = \mathcal{O}_K$ be its ring of integers. Let $\alpha = \alpha(n) > 0$, and let $q = q(n) \geq 2$, $q = 1 \mod l$ be a poly(n)-bounded prime such that $\alpha q \geq \omega(\sqrt{\log n})$. Then there is a polynomial-time quantum reduction from $\tilde{O}(\frac{\sqrt{n}}{\alpha})$-approximate SIVP on ideal lattices in K to the problem of solving $R-DLWE_{q,\psi}$ given only k samples, where ψ is the Gaussian distribution $D_{\xi \cdot q}$ with $\xi = \alpha \cdot (\frac{nk}{\log(nk)})^{\frac{1}{4}}$.*

We will use a variant of RLWE whose support set is $R_q \times R_q^\vee$, which is discussed in [24]. Let χ be a discrete error distribution over $R^\vee$, we modify Definition 2.19 by letting $R-DLWE_{q,\chi}$ be the problem of distinguishing between $A_{s,\chi}$ and uniform samples from $R_q \times R_q^\vee$. The following lemma shows that for a wide family of discrete error distributions, the hardness of the discrete version follows from that of the continuous one.

Lemma 2.21. *Let p and q be positive coprime integers, and $\lfloor \cdot \rceil$ be a valid discretization to cosets of $pR^\vee$. There exists an efficient transformation that on input $\omega \in R_p^\vee$ and a pair $(a', b') \in R_q \times (K_\mathbb{R}/(qR^\vee))$, outputs a pair $(a = pa', b) \in R_q \times R_q^\vee$ with the following guarantees: if the input pair is uniformly distributed then so is the output pair; and if the input pair is distributed according to the RLWE distribution $A_{s,\psi}$ for some $s \in R^\vee$ and distribution ψ over $K_\mathbb{R}$, then the output pair is distributed according to $A_{s,\chi}$ where $\chi = \lfloor p \cdot \psi \rceil_{\omega + pR^\vee}$.*

The distribution of s above is uniform distribution over $R^\vee$, we need to change it to error distribution. This modification makes the secret short, which is very useful in some applications. The following lemma shows this variant of RLWE is as hard as the original one by using the technique proposed in [2].

Lemma 2.22. *Let p and q be positive coprime integers, $\lfloor \cdot \rceil$ be a valid discretization to cosets of $pR^\vee$, and ω be an arbitrary element in $R_p^\vee$. If $R-DLWE_{q,\chi}$ is hard given some k samples then so is the variant of $R-DLWE_{q,\chi}$ in which the secret is sampled from $\chi := \lfloor p \cdot \psi \rceil_{\omega + pR^\vee}$, given $k-1$ sapmles.*

In our applications, we will set $p = 1$, $\omega = 0$ and $\chi = \lfloor D_{\xi \cdot q} \rceil_{R^\vee}$. Here we use the coordinate-wise randomized discretisation $\lfloor \cdot \rceil_\Lambda^B$ with $\Lambda = \sigma(R^\vee)$ and B the decoding basis for $R^\vee$. Hence, a vector $\boldsymbol{x}$ sampled from χ is a noncentral subgaussian random variable with

noncentrality parameter $||\boldsymbol{x}||$ and deviation parameter $\frac{1}{2}s_1(\sigma(B))$ and has the property

$$||\boldsymbol{x}|| \leq \sqrt{n}s_1(\sigma(B)) + \sqrt{n}q\xi \leq \sqrt{n}q\xi + \sqrt{n} \cdot \sqrt{\frac{rad(l)}{l}} \tag{3}$$

with overwhelming probability.

In fact, we can give a elaborate estimate by using Lemma 2.17. One can see the elaborate estimate in Section 5. One should also note that when we restrict a to $R_q^\times$, the problem remains hard as stated in [35]. From now on we denote $A_{s,\psi}^\times$ the distribution on $R_q^\times \times R_q^\vee$ and denote $R - DLWE_{q,\psi}^\times$ the problem of distinguishing distributions of $U(R_q^\times \times R_q^\vee)$ and $A_{s,\psi}^\times$.

3 Some New Results on q-Ary Lattices

We first describe an isomorphism theorem which is helpful for us to analyse the q-ary lattices we need. In some textbooks, it is called the fourth isomorphism theorem or lattice isomorphism theorem. We only describe it's ring's version. When come to groups or modules, the results are almost the same.

Proposition 3.1. *Let R be a ring, and B an ideal of R. Then every subring of R/B is of the form A/B, for some subring A of R such that $B \subseteq A \subseteq R$, the corresponding relation is $1-1$. In particular, every ideal of R/B is of the form A/B, for some ideal A of R such that $B \subseteq A \subseteq R$.*

We know that $R_q = \mathbb{Z}_q[x]/\Phi_l(x)$ and $\mathbb{Z}_q[x]$ is a principal ideal domain, hence R_q is a principal ideal ring. If we set $\phi_i = \omega^i$, where i is the i-th element in $\mathbb{Z}_l^*$ as in Section 2.2, then $\Phi_l(x) = \prod_{i=1}^n (x - \phi_i) = \prod_{i=1}^n (x - \phi_i^{-1}) \mod q$. For any proper ideal $I \in R_q$, we can write $I = \langle f(x) \rangle R_q$, where $f(x)$ contains at least one monomials of $x - \phi_i$, i.e. $f(x) = \prod_{i \in S}(x - \phi_i)$ for some $S \subseteq \{1, 2, \cdots, n\}$. We will use I_S represents the ideal $\prod_{i \in S}(x - \phi_i)R_q$ of R_q.

Let $\boldsymbol{a} \in (R_q)^m$, I ba an proper ideal of R_q, we know there is an ideal J of R such that $qR \subseteq J \subseteq R$ and $I = J/qR$. In fact, if we set $I = \langle f(x) \rangle R_q$, then $J = \langle f(x), q \rangle R$. Considering the relation $qJ \subseteq qR \subseteq J \subseteq R$, We get $R^\vee \subseteq J^\vee \subseteq (qR)^\vee \subseteq (qJ)^\vee$, which implies $R^\vee \subseteq J^\vee \subseteq \frac{1}{q}(R)^\vee \subseteq \frac{1}{q}(J)^\vee$. Thus we get the R module inclusion relations $qR^\vee \subseteq qJ^\vee \subseteq R^\vee \subseteq J^\vee$. Moveover, $R^\vee/qJ^\vee$ is a R submodule of $J^\vee/qJ^\vee$.

3.1 q-Ary Lattices

With the relations describe above in mind, we define the q-ary lattice we need for our analysis of public key distribution in Section 4. The definitions are as followings:

$$\boldsymbol{a}^\perp(I) = \{(t_1, \cdots, t_m) \in R^m : \forall\, i,\ (t_i \mod qR) \in I \ \ and \ \ \sum_{i=1}^m t_i a_i = 0 \mod qR\},$$

$$L(\boldsymbol{a}, I) = \{(t_1, \cdots, t_m) \in (J^\vee)^m : \exists\ s \in R^\vee,\ \forall i,\ t_i = a_i \cdot s \mod qJ^\vee\}.$$

In fact, $\boldsymbol{a}^\perp(I) = \{(t_1, \cdots, t_m) \in J^m : \sum_{i=1}^m t_i a_i = 0 \mod qR\}$ and $L(\boldsymbol{a}, I) = \{(t_1, \cdots, t_m) \in (R^\vee)^m : \exists\ s \in R^\vee,\ \forall i,\ t_i = a_i \cdot s \mod qJ^\vee\}$, since $qJ^\vee \subseteq R^\vee$ and $a_i \cdot s \in R^\vee$. It is easy to see that both $\boldsymbol{a}^\perp(I)$ and $L(\boldsymbol{a}, I)$ are well-defined and are q modules, hence the value s can take over all elements in $R^\vee$. We also define $\boldsymbol{a}^\perp$ and $L(\boldsymbol{a})$ as $\boldsymbol{a}^\perp(R_q)$ and $L(\boldsymbol{a}, R_q)$. The following lemma shows the dual relations between $\boldsymbol{a}^\perp(I)$ and $L(\boldsymbol{a}, I)$.

Lemma 3.2. *Let $\boldsymbol{a}^\perp(I)$ and $L(\boldsymbol{a}, I)$ be defined above, then we have $\boldsymbol{a}^\perp(I) = q(L(\boldsymbol{a}, I))^\vee$ and $L(\boldsymbol{a}, I) = q(\boldsymbol{a}^\perp(I))^\vee$.*

Proof. We first show $\boldsymbol{a}^\perp(I) \subseteq q(L(\boldsymbol{a}, I))^\vee$ and $L(\boldsymbol{a}, I) \subseteq q(\boldsymbol{a}^\perp(I))^\vee$. $\forall\ \boldsymbol{t} \in \boldsymbol{a}^\perp(I)$ and $\boldsymbol{z} \in L(\boldsymbol{a}, I)$, we only need to show $\sum_{i=1}^m \mathrm{Tr}(t_i \cdot z_i) = 0 \mod q\mathbb{Z}$. Note that $z_i = a_i \cdot s + q \cdot z_i^{'}$ for some $z_i^{'} \in J^\vee$, we have

$$\sum_{i=1}^m \mathrm{Tr}(t_i \cdot z_i) = \mathrm{Tr}(s \cdot \sum_{i=1}^m t_i \cdot a_i) + q \cdot \sum_{i=1}^m \mathrm{Tr}(t_i \cdot z_i^{'}).$$

By the definition, $\sum_{i=1}^m t_i \cdot a_i = q \cdot r$ for some $r \in R$. Thus $\sum_{i=1}^m \mathrm{Tr}(t_i \cdot z_i) \in q\mathbb{Z}$.

To complete the proof, we will show $q(L(\boldsymbol{a}, I))^\vee \subseteq \boldsymbol{a}^\perp(I)$. $\forall\ \boldsymbol{x} \in (L(\boldsymbol{a}, I))^\vee$, we need to show $q \cdot x_i \in J$ for all $i \in [m]$ and $\sum_{i=1}^m q x_i \cdot a_i \in qR$. Note that $q(J^\vee)^m \subseteq L(\boldsymbol{a}, I)$, we can take $\boldsymbol{v^{(i)}}$ be the vectors in $L(\boldsymbol{a}, I)$ such that the i-th coordinate is $q \cdot s^{'}$ with $s^{'} \in J^\vee$ and 0 elsewhere. We have $\mathrm{Tr}(\boldsymbol{x} \cdot \boldsymbol{v^{(i)}}) = \mathrm{Tr}(x_i \cdot q \cdot s^{'}) \in \mathbb{Z}$, hence $q \cdot x_i \in J$, since $s^{'}$ can take over all elements of $J^\vee$.

$\forall\ \boldsymbol{t} \in L(\boldsymbol{a}, I)$, $\sum_{i=1}^m \mathrm{Tr}(x_i \cdot t_i) \in \mathbb{Z}$. We write t_i as $a_i \cdot s + q \cdot t_i^{'}$ with $t_i^{'} \in J^\vee$, then

$$\sum_{i=1}^m \mathrm{Tr}(x_i \cdot t_i) = \mathrm{Tr}(s \cdot \sum_{i=1}^m a_i \cdot x_i) + \sum_{i=1}^m \mathrm{Tr}(q x_i \cdot t_i^{'}),$$

the latter sum is in $\mathbb{Z}$, hence $\mathrm{Tr}(s \cdot \sum_{i=1}^m a_i \cdot x_i) \in \mathbb{Z}$ and we get $\sum_{i=1}^m a_i \cdot x_i \in R$. Therefore we have proved $\boldsymbol{a}^\perp(I) = q(L(\boldsymbol{a}, I))^\vee$, by taking dual in both side, we finish the proof. □

3.2 Lower Bound of λ_1^∞ in $L(a, I)$

Let $I_S = \prod_{i \in S}(x - \phi_i)R_q \subseteq R_q$ and $J_S = \langle f_S(x), q\rangle\, R \in R$ where $f_S(x) = \prod_{i \in S}(x - \phi_i)$. We have $qR \subseteq J_S \subseteq R$ and $I_S = J_S/qR$. The factorization of ideal $\langle q\rangle\, R$ is $\prod_{i=1}^n \mathfrak{q}_i$ with $\mathfrak{q}_i = \langle q, x - \phi_i\rangle$, here we still use i to represent the i-th element in $\mathbb{Z}_l^*$. Since R is a Dedekind domain, each $\mathfrak{q_i}$ is a maximal ideal, hence $\mathfrak{q_i}$ and $\mathfrak{q_j}$ is coprime for any $i, j \in [n]$, $\mathfrak{q_i} \cdot \mathfrak{q_j} = \mathfrak{q_i} \cap \mathfrak{q_j} = \langle q, (x - \phi_i)(x - \phi_j)\rangle$. Therefore, $J_S = \prod_{i \in S} \mathfrak{q}_i$, $J_S^{-1} = \prod_{i \in S} \mathfrak{q}_i^{-1}$. Further, we have $J_S^\vee = \prod_{i \in S} \mathfrak{q}_i^{-1} R^\vee$. The following lemma is an analogue of Chinese Remainder Theorem.

Lemma 3.3. *Let J be a fractional ideal of K and $J_i = I_i \cdot R^\vee \subseteq J$ for $i \in [n]$, where $I_i \subseteq R$ ba ideals and are pairwise coprime. Then we have a isomorphism between $J/\prod_{i\in[n]} J_i$ and the direct sum $J/J_1 \oplus \cdots \oplus J/J_n$.*

Proof. We define the map $\varphi : J \longrightarrow J/J_1 \oplus \cdots \oplus J/J_n$ by mapping $x \in \mathcal{J}$ to $(x \mod J_1, \cdots, x \mod J_n)$. Note that $J_i \cap J_j = I_i I_j R^\vee = J_i \cdot J_j$ for any $i, j \in [n]$, we have the kernel of φ is $\prod_{i\in[n]} J_i$. So we only need to prove φ is a surjective.

Set $M_i = \prod_{j=1, j\neq i}^{n} J_j$, we have $M_i \subseteq J_j$ for $j \neq i$ and $M_1 + M_2 = (J_2 + J_1)J_3 \cdots J_n = J_3 \cdots J_n$, since $J_i + J_j = (I_i + I_j)R^\vee = R \cdot R^\vee = R^\vee$. Hence $M_1 + M_2 + \cdots + M_n = R^\vee$. We can take $e_i \in M_i$ such that $e_1 + e_2 + \cdots + e_n = 1 \in R \subseteq R^\vee$. These $\{e_i\}$ satisfy $e_i = 0 \mod J_j$ for $j \neq i$ and $e_i = 1 \mod J_i$. $\forall\ (x_1, \cdots, x_n) \in J/J_1 \oplus \cdots \oplus J/J_n$, $x_i \in J$ for $i \in [n]$. If we take $x = e_1 x_1 + \cdots + e_n x_n \in J$, we have $x \mod J_i = x_i$, i.e. $\varphi(x) = (x_1, \cdots, x_n)$. We have finished the proof. □

Now we can give a lemma which shows that for $\boldsymbol{a} \hookleftarrow U((R_q^\times)^m)$, the lattice $L(\boldsymbol{a}, I_S)$ is extremely unlikely to contain unusually short vectors for the infinity norm.

Lemma 3.4. *For any $S \subseteq [n]$, $m \geq 2$ and $\varepsilon > 0$, we have $\lambda_1^\infty(L(\boldsymbol{a}, I_S)) \geq B$, with $B = \frac{q^\beta}{n}$, where $\beta = (1 - \frac{1}{m})(1 - \frac{|S|}{n}) - \varepsilon$, except with probability $p \leq 2^{(3m+1)n} q^{-\varepsilon mn}$ over the uniformly random choice of $\boldsymbol{a} \in (R_q^\times)^m$.*

Proof. Let p denote the probability, over the randomness of $\boldsymbol{a}$, that $L(\boldsymbol{a}, I_S)$ contains a non-zero vector $\boldsymbol{t}$ of infinity norm $\leq B = \frac{q^\beta}{n}$. We upper bound p by the union bound, summing the probabilities $p(\boldsymbol{t}, s) = \Pr_{\boldsymbol{a}}[\forall i,\ t_i = a_i \cdot s \mod q J_S^\vee]$. Since the a_i's are independent, we have $p(\boldsymbol{t}, s) = \prod_{i\leq m} p_i(t_i, s)$, where $p_i(t_i, s) = \Pr_{a_i}[t_i = a_i \cdot s \mod q J_S^\vee]$. In other words, we have

$$p \leq \sum_{\substack{\boldsymbol{t} \in (J^\vee)^m \\ \forall i,\ 0 < ||t_i||_\infty < B}} \sum_{s \in R^\vee / qJ^\vee} \prod_{i=1}^{m} \Pr_{a_i}[t_i = a_i \cdot s \mod q J_S^\vee].$$

Note that $qJ_S^\vee = q \prod_{i\in S} \mathfrak{q}_i^{-1} R^\vee = q \cdot \prod_{i\in S} \mathfrak{q}_i^{-1} \cdot R \cdot R^\vee = \prod_{i\in S'} \mathfrak{q}_i \cdot R^\vee$, where $S' = [n] \setminus S$. Using Lemma 3.3, we get an isomorphisms between $J_S^\vee / qJ_S^\vee$ and $J_S^\vee/(\mathfrak{q}_{i_1} R^\vee) \oplus \cdots \oplus J_S^\vee/(\mathfrak{q}_{i_{S'}} R^\vee)$, where $i_j \in S'$. Also we have $R^\vee/qJ_S^\vee \cong R^\vee/(\mathfrak{q}_{i_1} R^\vee) \oplus \cdots \oplus R^\vee/(\mathfrak{q}_{i_{S'}} R^\vee)$.

We claim that there must be a set $S'' \subseteq S'$ such that $s, t_i \in \prod_{i\in S''} \mathfrak{q}_i R^\vee$ and $s, t_i \notin \mathfrak{q}_j R^\vee$ for all $j \in S' \setminus S''$. Otherwise, there are some $j \in S'$ such that either $s = 0 \mod \mathfrak{q}_j R^\vee$ and $t_i \neq 0 \mod \mathfrak{q}_j R^\vee$, or $s \neq 0 \mod \mathfrak{q}_j R^\vee$ and $t_i = 0 \mod \mathfrak{q}_j R^\vee$. In both cases, we have $p_{t_i}(a_i, s) = 0$, since $a_i \in R_q^\times$. Therefore, for $j \in S''$, we have $t_i = a_i \cdot s = 0 \mod \mathfrak{q}_j R^\vee$ regardless of the value of $a_i \in R_q^\times$. For any $j \in S' \setminus S''$, we have $t_i = a_i \cdot s \neq 0 \mod \mathfrak{q}_j R^\vee$, the value of a_i is unique, since $s \neq 0 \mod \mathfrak{q}_j R^\vee$ and $a_i \in R_q^\times$. For $j \in [n] \setminus S'$, the value of a_i can be arbitrary. Hence, overall, if we set $|S''| = d$, we get $p_i(t_i, s) = (q-1)^{d - |S'|}$. By noting that for any $s \in R_q$, all the element of the coset $s + qJ^\vee$ satisfy the equation $t_i = a_i \cdot s \mod qJ^\vee$ for the same t, we can rewrite the sum's conditions by

$$p \leq \sum_{0\leq d\leq |S'|} \sum_{\substack{S'' \subseteq S' \\ |S''|=d \\ \mathfrak{h}=\prod_{i\in S''}\mathfrak{q}_i R^\vee}} \sum_{\substack{s\in R^\vee/(qJ^\vee) \\ s\in\mathfrak{h}}} \sum_{\substack{\boldsymbol{t}\in (J^\vee)^m \\ \forall i,\ 0<||t_i||_\infty<B \\ t_i\in\mathfrak{h}}} \prod_{i=1}^{m}(q-1)^{d-|S'|}.$$

Set $\mathfrak{h}=\prod_{i\in S''}\mathfrak{q}_i R^\vee$, with $S''\in S'$ and $|S''|=d$. Let $N(B,d)$ denote the number of $t\in J^\vee$ such that $||t||_\infty<B$ and $t\in\mathfrak{h}$. We consider two cases for $N(B,d)$ depending on d.

Suppose that $d\geq\beta\cdot n$. Since $t\in\mathfrak{h}=\prod_{i\in S''}\mathfrak{q}_i R^\vee$, $\mathfrak{h}$ is fraction ideal, we have $\langle t\rangle = tR^\vee\subseteq\mathfrak{h}$ and $\langle t\rangle$ is a full-rank R-submodule of $\mathfrak{h}$. Hence, $\mathrm{N}(t)=\mathrm{N}(\langle t\rangle)\geq\mathrm{N}(\mathfrak{h})\geq\mathrm{N}(\prod_{i\in S''}\mathfrak{q}_i\cdot R^\vee)=(\prod_{i\in S''}\mathrm{N}(\mathfrak{q}_i))\mathrm{N}(R^\vee)=q^d\cdot\Delta_K^{-1}$. Thus $\mathrm{N}(t)\geq\frac{q^d}{n^n}$. We conclude that $||t||_\infty\geq\frac{1}{\sqrt{n}}||t||\geq\mathrm{N}^{\frac{1}{n}}(t)\geq\frac{q^{\frac{d}{n}}}{n}\geq\frac{q^\beta}{n}=B$.

Suppose now that $d<\beta\cdot n$. Define $\mathfrak{B}(l,\boldsymbol{c})=\{\boldsymbol{x}\in H:\ ||\boldsymbol{x}-\boldsymbol{c}||_\infty<l\}$. Note that $\sigma(\mathfrak{h})$ is a lattice of H, we get $N(B,d)$ is at most the number of points of $\sigma(\mathfrak{h})$ in the region $\mathfrak{B}(B,0)$. Let $\lambda=\frac{\lambda_1^\infty(\mathfrak{h})}{2}$, then for any two elements $\boldsymbol{v_1}$ and $\boldsymbol{v_2}\in\mathfrak{h}$, we have $\mathfrak{B}(\lambda,\boldsymbol{v_1})\cap\mathfrak{B}(\lambda,\boldsymbol{v_2})=\phi$. For any $\boldsymbol{v}\in\mathfrak{B}(B,0)$, we also have $\mathfrak{B}(\lambda,\boldsymbol{v})\subseteq\mathfrak{B}(B+\lambda,0)$. Therefore, $N(B,d)\leq\frac{vol(\mathfrak{B}(B+\lambda,0))}{vol(\mathfrak{B}(\lambda,0))}=(\frac{B}{\lambda}+1)^n\leq(2q^{\beta-\frac{d}{n}}+1)^n\leq 2^{2n}q^{n\beta-d}$.

We claim that the number of $s\in R^\vee/(qJ^\vee)$ and $s\in\mathfrak{h}$ is $q^{|S'|-d}$. In fact, if s satisfies the above conditions, $s\in\mathfrak{h}/(qJ^\vee)$. Using a kind of isomorphism theorem which states that for any fractional ideals $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{c}$ with $\mathfrak{a}\subseteq\mathfrak{b}$, $\mathfrak{ac}/\mathfrak{bc}\cong\mathfrak{a}/\mathfrak{b}$, we have

$$\mathfrak{h}/(qJ^\vee)\cong\prod_{i\in S''}\mathfrak{q}_i R^\vee/(\prod_{i\in S'}\mathfrak{q}_i R^\vee)\cong\prod_{i\in S''}\mathfrak{q}_i/(\prod_{i\in S'}\mathfrak{q}_i)\cong R/(\prod_{i\in(S'\setminus S'')}\mathfrak{q}_i).$$

Hence, we have $|\mathfrak{h}/(qJ^\vee)|=|R/(\prod_{i\in(S'\setminus S'')}\mathfrak{q}_i)|=q^{|S'|-d}$. Using the above B-bound and the fact that the number of subsets of S' of cardinality d is $\leq 2^d$, setting $\mathfrak{P}=\prod_{i=1}^m(q-1)^{d-|S'|}$, we can rewrite the inequality of p as

$$\begin{aligned}
p &\leq \left(\sum_{0\leq d<\beta\cdot n}+\sum_{\beta\cdot n\leq d\leq|S'|}\right)\sum_{\substack{S''\subseteq S' \\ |S''|=d \\ \mathfrak{h}=\prod_{i\in S''}\mathfrak{q}_i R^\vee}}\sum_{\substack{s\in R^\vee/(qJ^\vee) \\ s\in\mathfrak{h}}}\sum_{\substack{\boldsymbol{t}\in(J^\vee)^m \\ \forall i,\ 0<||t_i||_\infty<B \\ t_i\in\mathfrak{h}}}\mathfrak{P} \\
&\leq \sum_{0\leq d<\beta\cdot n}\sum_{\substack{S''\subseteq S' \\ |S''|=d \\ \mathfrak{h}=\prod_{i\in S''}\mathfrak{q}_i R^\vee}}\sum_{\substack{s\in R^\vee/(qJ^\vee) \\ s\in\mathfrak{h}}}\sum_{\substack{\boldsymbol{t}\in(J^\vee)^m \\ \forall i,\ 0<||t_i||_\infty<B \\ t_i\in\mathfrak{h}}}\mathfrak{P} \\
&\leq 2^{|S'|}\max_{d<\beta\cdot n}\frac{q^{|S'|-d}N^m(B,d)}{(q-1)^{m(|S'|-d)}} \\
&= 2^{|S'|}\max_{d<\beta\cdot n}(1+\frac{1}{q-1})^{m(|S'|-d)}\frac{N^m(B,d)}{(q-1)^{(m-1)(|S'|-d)}} \\
&\leq \max_{d<\beta\cdot n}2^{|S'|+2mn}(1+\frac{1}{q-1})^{m(|S'|-d)}q^{mn\beta+|S'|-m|S'|-d} \\
&\leq 2^{|S'|(1+m)+2mn}\cdot q^{mn\beta+|S'|-m|S'|}\leq 2^{n(1+3m)}\cdot q^{-\varepsilon mn}.
\end{aligned}$$

We finish the proof. □

Remark: The estimate of $N(B,d)$ in the case $d < \beta \cdot n$ is inspired by [39].

3.3 Improved Results on Regularity

The following result is a direct consequence of Lemmata 2.10, 2.13, 3.2 and 3.4.

Lemma 3.5. *Let $q = 1 \mod l$ be a prime, $m \geq 2$, $\delta \in (0, \frac{1}{2})$, $\varepsilon > 0$, $S \subseteq [n]$, $\boldsymbol{c} \in R^m$ and $\boldsymbol{t} \hookleftarrow D_{R^m,\sigma,\boldsymbol{c}}$, where $\sigma \geq n\sqrt{\frac{\ln(2mn(1+\frac{1}{\delta}))}{\pi}} \cdot q^{\frac{|S|}{n}+\frac{1}{m}-\frac{|S|}{mn}+\varepsilon}$. Then for all exception a fraction of $2^{(3m+1)n}q^{-\varepsilon mn}$ of $a \in (R_q^\times)^m$, we have*

$$\Delta\left(\boldsymbol{t} \mod \boldsymbol{a}^\perp(I_S); U(R^m/\boldsymbol{a}^\perp(I_S))\right) \leq 2\delta.$$

Let χ be a distribution over R_q and denote $\mathbb{D}_\chi$ the distribution of such tuple $(a_1, \cdots, a_m, \sum_{i=1}^m t_i a_i) \in (R_q^\times)^m \times R_q$ where $a_i \hookleftarrow U(R_q^\times)$ and $t_i \hookleftarrow \chi$ for all $i = 1, 2, \cdots, m$. The regularity of the generalized knapsack function $(t_1, \cdots, t_m) \to \sum_{i=1}^m t_i a_i$ is the statistical distance between $\mathbb{D}_\chi$ and $U((R_q^\times)^m \times R_q)$. In [27], Micciancio discussed the regularity over general rings and used it to design one-way functions. Some improved regularity results are given in [35], [38] and [39]. Here, we can also give an improved result of regularity, by taking $S = \phi$ and $\boldsymbol{c} = 0$ in Lemma 3.5.

Theorem 3.6. *Let $q = 1 \mod l$ be a prime, $m \geq 2$, $\delta \in (0, \frac{1}{2})$, $\varepsilon > 0$ and $a_i \hookleftarrow U(R_q^\times)$ for all $i \in [n]$. Assume $\boldsymbol{t} \hookleftarrow D_{R^m,\sigma}$, where $\sigma \geq n\sqrt{\frac{\ln(2mn(1+\frac{1}{\delta}))}{\pi}} \cdot q^{\frac{1}{m}+\varepsilon}$. Then we have*

$$\Delta\left((a_1, \cdots, a_m, \sum_{i=1}^m t_i a_i); U((R_q^\times)^m \times R_q)\right) \leq 2\delta + 2^{(3m+1)n}q^{-\varepsilon mn}.$$

4 Analysis of Key Generation Algorithm

With the results in Section 3, we can derive a key generation algorithm for NTRUEncrypt as in [35]. Further, by choosing appropriate parameters, we can show that the key generation algorithm terminates in limited time and the key distributions are very closed to the uniform distribution.

The key generation algorithm is as follows:

Input : $n, q \in \mathbb{Z}$, $p \in R_q^\times$, $\sigma \in \mathbb{R}$.

Output : *A key pair* $(sk, pk) \in R_q^\times \times R_q^\times$.

1. *Sample* $f^{'}$ *from* $D_{R,\sigma}$; *let* $f = p \cdot f^{'} + 1$; *if* $(f \mod qR) \notin R_q^\times$, *resample.*
2. *Sample* g *from* $D_{R,\sigma}$; *if* $(g \mod qR) \notin R_q^\times$, *resample.*
3. *Return secret key* $sk = f$ *and public key* $pk = h = pg/f \in R_q^\times$.

The following lemma shows that the key generation algorithm can terminate with executing only several times.

Lemma 4.1. *Let l be a positive integer and q be a prime such that $q = 1 \mod l$. Let $\sigma > n \cdot \sqrt{\frac{\ln(2n(1+\frac{1}{\varepsilon}))}{\pi}} \cdot q^{\frac{1}{n}}$, for an arbitrary $\varepsilon \in (0, \frac{1}{2})$. Let $a \in R$ and $p \in R_q^\times$. Then*

$$\Pr_{f' \hookleftarrow D_{R,\sigma}}[(p \cdot f + a \mod qR) \notin R_q^\times] \leq n(\frac{1}{q} + 2\varepsilon).$$

Proof. Thanks to the Chinese Remainder Theorem, we only need to bound the probability that $p \cdot f^{'} + a \in \mathfrak{q}_i$ is no more than $\frac{1}{q} + 2\varepsilon$, for any $i \leq n$. Here we set i to represent the i-th element in $\mathbb{Z}_m^*$. By Lemma 2.1, we have $\lambda_1(\mathfrak{q}_i) = \lambda_n(\mathfrak{q}_i) \leq \sqrt{n} N(\mathfrak{q}_i)^{\frac{1}{n}} (\sqrt{\Delta_K})^{\frac{1}{n}} \leq n q^{\frac{1}{n}}$. By Lemma 2.9 and 2.13, we know that $p \cdot f^{'} \mod \mathfrak{q}_i$ is within distance 2ε to uniformity on $R/\mathfrak{q}_i$, so we have $f^{'} = -a/p \mod \mathfrak{q}_i$ with probability $\leq \frac{1}{q} + 2\varepsilon$, as we need. □

Next, we show that the generated secret key by the key generation algorithm is small. This lemma is very useful for us to analyze the probability of success in the decryption algorithm in Section 5.

Lemma 4.2. *Let $n \geq 6$, $q \geq 8n$, $q = 1 \mod l$ be a prime and $\sigma \geq \sqrt{\frac{2\ln(6n)}{\pi}} \cdot n \cdot q^{\frac{1}{n}}$. Then with probability $\geq 1 - 2^{3-n}$, the secret key f, g satisfy $||f|| \leq 2\sqrt{n}\sigma ||p||_\infty$ and $||g|| \leq \sqrt{n}\sigma$.*

Proof. Set $\varepsilon = \frac{1}{3n-1}$. Note that $\lambda_n(R) = \lambda_1(R) \leq \sqrt{n} \cdot (\sqrt{\Delta_K})^{\frac{1}{n}} = n$. By Lemma 2.9, we have $\eta_\varepsilon(R) \leq \sqrt{\frac{2\ln(6n)}{\pi}} \cdot n$. Hence, $\Pr_{x \hookleftarrow D_{R,\sigma,\mathbf{c}}}(||x|| \geq \sqrt{n}\sigma) \leq \frac{3n}{3n-2} 2^{-n}$. Meanwhile, σ satisfies the condition in Lemma 4.1, so we get

$$\begin{aligned}
\Pr_{g \hookleftarrow D_{R,\sigma}}(||g|| \geq \sqrt{n}\sigma \mid g \in R_q^\times) &= \frac{\Pr_{g \hookleftarrow D_{R,\sigma}}(||g|| \geq \sqrt{n}\sigma \text{ and } g \in R_q^\times)}{\Pr_{g \hookleftarrow D_{R,\sigma}}(g \in R_q^\times)} \\
&\leq \frac{\Pr_{g \hookleftarrow D_{R,\sigma}}(||g|| \geq \sqrt{n}\sigma)}{\Pr_{g \hookleftarrow D_{R,\sigma}}(g \in R_q^\times)} \\
&\leq \frac{3n}{3n-2} \cdot 2^{-n} \cdot \frac{1}{1 - n(\frac{1}{q} + 2\varepsilon)} \leq 2^{3-n}.
\end{aligned}$$

Hence, we have $||f^{'}||$, $||g|| \leq \sqrt{n}\sigma$ with probability $\geq 1 - 2^{3-n}$. Then we can estimate $||f|| \leq 1 + ||p||_\infty \cdot ||f^{'}|| \leq 2\sqrt{n}\sigma ||p||_\infty$.

□

The last lemma of this section estimates the statistic distance between the distribution of public key and the uniform distribution on $R_q^\times$. The proof is almost the same with [35, Thm 3] or [38, Thm 2]. We denote by $D_{\sigma,z}^\times$ the discrete Gaussian $D_{R,\sigma}$ restricted to $R_q^\times + z$.

Lemma 4.3. *Let* $0 < \varepsilon < \frac{1}{2}$ *and* $\sigma \geq n^{\frac{3}{2}}\sqrt{\ln(8nq)} \cdot q^{\frac{1}{2}+2\varepsilon}$. *Let* $p \in R_q^\times$, $y_i \in R_q$ *and* $z_i = -y_i p^{-1} \mod qR$ *for* $i \in \{1,2\}$. *Then*

$$\Delta\left[\frac{y_1 + p \cdot D^\times_{\sigma,z_1}}{y_2 + p \cdot D^\times_{\sigma,z_2}} \mod q, U(R_q^\times)\right] \leq \frac{2^{5n}}{q^{\lfloor \varepsilon n \rfloor}}.$$

Proof. For $a \in R_q^\times$, we define $\Pr_a = \Pr_{f_1,f_2}[(y_1 + pf_1)/(y_2 + pf_2) = a]$, where $f_i \hookleftarrow D^\times_{\sigma,z_i}$. It is suffice to show that $|\Pr_a - (q-1)^{-n}| \leq 2^{2n+5}q^{-\lfloor \varepsilon n \rfloor} \cdot (q-1)^{-n} =: \varepsilon'$ except a fraction $\leq 2^{7n}q^{-2n\varepsilon}$ of $a \in R_q^\times$. Note that $a_1f_1 + a_2f_2 = a_1z_1 + a_2z_2$ is equivalent to $(y_1 + pf_1)/(y_2 + pf_2) = -a_2/a_1$ in $R_q^\times$ and $-a_2/a_1 \hookleftarrow R_q^\times$ when $\boldsymbol{a} \hookleftarrow (R_q^\times)^2$, we get $\Pr_{\boldsymbol{a}} := \Pr_{f_1,f_2}[a_1f_1 + a_2f_2 = a_1z_1 + a_2z_2] = \Pr_{-a_2/a_1}$ for $\boldsymbol{a} \in (R_q^\times)^2$.

The set of solutions $(f_1, f_2) \in R^2$, $f_i \hookleftarrow D^\times_{\sigma,z_i}$, to the equation $a_1f_1 + a_2f_2 = a_1z_1 + a_2z_2 \mod qR$ is $\boldsymbol{z} + \boldsymbol{a}^{\perp\times}$, where $\boldsymbol{z} = (z_1, z_2)$ and $\boldsymbol{a}^{\perp\times} = \boldsymbol{a}^\perp \cap (R_q^\times + qR)^2$. Therefore

$$\Pr_{\boldsymbol{a}} = \frac{D_{R^2,\sigma}(\boldsymbol{z} + \boldsymbol{a}^{\perp\times})}{D_{R,\sigma}(z_1 + R_q^\times + qR) \cdot D_{R,\sigma}(z_2 + R_q^\times + qR)}.$$

Note that $\boldsymbol{a} \in (R_q^\times)^2$, we know for any $\boldsymbol{t} \in \boldsymbol{a}^\perp$, $t_2 = -t_1\frac{a_1}{a_2}$, so t_1 and t_2 are in the same ideal I of R_q. It follows that $\boldsymbol{a}^{\perp\times} = \boldsymbol{a}^\perp \setminus (\cup_{I \subseteq R_q} \boldsymbol{a^\perp(I)}) = \boldsymbol{a}^\perp \setminus (\cup_{S \subseteq [n], S \neq \phi} \boldsymbol{a^\perp(I_S)})$. Similarly, we have $R_q^\times + qR = R \setminus (\cup_{S \subseteq [n], S \neq \phi}(I_S + qR))$. Using the inclusion-exclusion principal, we get

$$D_{R^2,\sigma}(\boldsymbol{z} + \boldsymbol{a}^{\perp\times}) = \sum_{S \subseteq [n]} (-1)^{|S|} \cdot D_{R^2,\sigma}(\boldsymbol{z} + \boldsymbol{a}^\perp(I_S)), \tag{4}$$

$$\forall\ i \in \{1,\ 2\}, \quad D_{R,\sigma}(z_i + R_q^\times + qR) = \sum_{S \subseteq [n]} (-1)^{|S|} \cdot D_{R,\sigma}(z_i + I_S + qR). \tag{5}$$

In the rest of the proof, we show that, except for a fraction $\leq 2^{7n}q^{-2n\varepsilon}$ of $\boldsymbol{a} \in (R_q^\times)^2$:

$$D_{R^2,\sigma}(\boldsymbol{z} + \boldsymbol{a}^{\perp\times}) = (1 + \delta_0) \cdot \frac{(q-1)^n}{q^{2n}},$$

$$\forall\ i \in \{1,\ 2\}, \quad D_{R,\sigma}(z_i + R_q^\times + qR) = (1 + \delta_i) \cdot \frac{(q-1)^n}{q^n},$$

where $|\delta_i| \leq 2^{2n+2}q^{-\lfloor \varepsilon n \rfloor}$ for $i \in \{0,1,2\}$. These imply that $|Pr_a - (q-1)^{-n}| \leq \varepsilon'$.
Handling (4): When $|S| \leq \varepsilon n$, we apply Lemma 3.5 with $m = 2$ and $\delta = q^{-n-\lfloor \varepsilon n \rfloor}$. Note that $qR^2 \subseteq \boldsymbol{a}^\perp(I_S) \subseteq R^2$, we have $|R^2/\boldsymbol{a}^\perp(I_S)| = \frac{|R^2/(qR^2)|}{|\boldsymbol{a}^\perp(I_S)/(qR^2)|}$. Meanwhile, $|R^2/(qR^2)| = q^{2n}$ and $|\boldsymbol{a}^\perp(I_S)/(qR^2)| = |I_S| = q^{n-|S|}$, since $|R_q|/|I_S| = |R_q/I_S| = q^{|S|}$. Therefore for all except a fraction $\leq \frac{2^{7n}}{q^{2n\varepsilon}}$ of $\boldsymbol{a} \in (R_q^\times)^2$,

$$\left|D_{R^2,\sigma}(\boldsymbol{z} + \boldsymbol{a}^\perp(I_S)) - q^{-n-|S|}\right| = |D_{R^2,\sigma,-\boldsymbol{z}}(\boldsymbol{a}^\perp(I_S)) - q^{-n-|S|}| \leq 2\delta.$$

When $|S| > \varepsilon n$, we can choose $S' \subseteq S$ with $|S'| = \lfloor \varepsilon n \rfloor$. Then we have $\boldsymbol{a}^\perp(I_S) \subseteq \boldsymbol{a}^\perp(I_{S'})$ and hence $D_{R^2,\sigma,-\boldsymbol{z}}(\boldsymbol{a}^\perp(I_S)) \leq D_{R^2,\sigma,-\boldsymbol{z}}(\boldsymbol{a}^\perp(I_{S'}))$. Using the result proven before,

we conclude that $D_{R^2,\sigma,-\boldsymbol{z}}(\boldsymbol{a}^{\perp}(I_S)) \leq 2\delta + q^{-n-\lfloor \varepsilon n \rfloor}$. Overall, we get

$$\begin{aligned}\left| D_{R^2,\sigma}(\boldsymbol{z}+\boldsymbol{a}^{\perp\times}) - \frac{(q-1)^n}{q^{2n}} \right| &= \left| D_{R^2,\sigma}(\boldsymbol{z}+\boldsymbol{a}^{\perp\times}) - \sum_{k=0}^{n}(-1)^k \tbinom{n}{k} q^{-n-k} \right| \\ &\leq 2^{n+1}\delta + 2\sum_{k=\lceil \varepsilon n \rceil}^{n} \tbinom{n}{k} q^{-n-\lfloor \varepsilon n \rfloor} \\ &\leq 2^{n+1}(\delta + q^{-n-\lfloor \varepsilon n \rfloor})\end{aligned}$$

for all except a fraction $\leq \frac{2^{7n}}{q^{2n\varepsilon}}$ of $\boldsymbol{a} \in (R_q^{\times})^2$, since the are 2^n choices of S. The δ_0 satisfies $|\delta_0| \leq \frac{q^{2n}}{(q-1)^n} 2^{n+1}(\delta + q^{-n-\lfloor \varepsilon n \rfloor}) = (\frac{q}{q-1})^n \cdot 2^{n+2} \cdot q^{\lfloor -\varepsilon n \rfloor} \leq 2^{2n+2} q^{\lfloor -\varepsilon n \rfloor}$ as required.

Handling (5): Note that for any $S \in [n]$, $det|I_S + qR| = |R/J_S| = q^{|S|}$, where J_S is the ideal of R such that $J_S/(qR) = I_S$. By Minkowski's Theorem, we have $\lambda_1(I_S + qR) = \lambda_n(I_S + qR) \leq \sqrt{n} \cdot q^{\frac{|S|}{n}}$. Lemma 2.9 gives that $\sigma > \eta_\delta(I_S + qR)$ for any $|S| \leq \frac{n}{2}$ with $\delta = q^{-\frac{n}{2}}$. Therefore, Lemma 2.13 shows that $|D_{R,\sigma,-z_i}(I_S + qR) - q^{-|S|}| \leq 2\delta$. For the case $|S| > \frac{n}{2}$, we can choose $S^{'} \subseteq S$ with $|S| \leq \frac{n}{2}$. Using the same argument above, we get $D_{R,\sigma,-z_i}(I_S^{'} + qR) \leq D_{R,\sigma,-z_i}(I_S + qR) \leq 2\delta + q^{-\frac{n}{2}}$. Therefore,

$$\begin{aligned}\left| D_{R,\sigma}(z_i + R_q^{\times} + qR) - \frac{(q-1)^n}{q^n} \right| &= \left| D_{R,\sigma}(z_i + R_q^{\times} + qR) - \sum_{k=0}^{n}(-1)^k \tbinom{n}{k} q^{-k} \right| \\ &\leq 2^{n+1}\delta + 2\sum_{k=\frac{n}{2}}^{n} \tbinom{n}{k} q^{-k} \\ &\leq 2^{n+1}(\delta + q^{-\frac{n}{2}})\end{aligned}$$

which leads to the desired bound on δ_i, $i = 1,\ 2$. □

5 NTRUEncrypt Scheme and Security Analysis

In this section, we describe the NTRUEncrypt. We set the plaintext message space $\mathcal{P} = R^{\vee}/pR^{\vee}$. Denote $\chi = \lfloor D_{\xi \cdot q} \rceil_{R^{\vee}}$ with $\xi = \alpha \cdot (\frac{nk}{\log(nk)})^{\frac{1}{4}}$ where k is a positive integer. We will use decoding basis for element $x \in R \subseteq R^{\vee}$. One should note that $f = 1 \mod pR$ implies $f = 1 \mod pR^{\vee}$.

Key generation : *Use the algorithm describe in Section* 4, *return* $sk = f \in R_q^{\times}$ *with* $f = 1 \ mod\ pR^{\vee}$, *and* $pk = h = pg \cdot f^{-1} \in R_q^{\times}$.

Encryption : *Given message* $m \in \mathcal{P}$, *set* $s, e \hookleftarrow \chi$ *and return* $c = hs + pe + m \in R_q^{\vee}$.

Decryption : *Given ciphertext* c *and secret key* f, *compute* $c_1 = fc$. *Then return* $m = (c_1 \mod qR^{\vee}) \mod pR^{\vee}$.

We first give an accurate estimate of the infinite norm of elements sampled from the discertisation of a Gaussian distribution.

Lemma 5.1. *Assume that* $\xi = \alpha\left(\frac{nk}{\log nk}\right)^{\frac{1}{4}}$, $\chi = \lfloor D_{\xi\cdot q}\rceil_{R^\vee}$, $\alpha\cdot q \geq \omega(\sqrt{\log n})$ *and* $k = O(1)$. *Set* $\delta = \omega(\sqrt{n\log n}\cdot\alpha^2\cdot q^2)$ *and* B *the decoding basis for* $R^\vee$, *then for any* $\boldsymbol{t}\in H$, *we have* $\Pr_{\boldsymbol{x}\hookleftarrow\chi}(|(\boldsymbol{t},\boldsymbol{x})| > \delta||\boldsymbol{t}||^2) \leq n^{-\omega(\sqrt{n\log n})\cdot||\boldsymbol{t}||^2}$.

Proof. Note that a gaussian random variable $\boldsymbol{x}\hookleftarrow D_{q\cdot\xi}$ has mean $\mathbf{0}$ and deviation $\frac{q\cdot\xi}{\sqrt{2\pi}}$, the discretisation $\lfloor\boldsymbol{x}\rceil$ is a noncentral subgaussian random variable with noncentrality parameter 0 and deviation parameter $(\frac{q^2\xi^2}{2\pi}+\frac{1}{4}s_1(B)^2)^{\frac{1}{2}}$, by Lemma 2.17. Hence, we have

$$E(e^{(\boldsymbol{t},\lfloor\boldsymbol{x}\rceil)}) \leq e^{\frac{1}{2}\cdot\left(\frac{q^2\xi^2}{2\pi}+\frac{1}{4}s_1(B)^2\right)\cdot||\boldsymbol{t}||^2}.$$

For any $\boldsymbol{x}\hookleftarrow D_{q\cdot\xi}$, by taking the Chernoff bound, we get

$$\begin{aligned}\Pr(|(\boldsymbol{t},\lfloor\boldsymbol{x}\rceil)| > \delta\cdot||\boldsymbol{t}||^2) &= \Pr(e^{|(\boldsymbol{t},\lfloor\boldsymbol{x}\rceil)|} > e^{\delta\cdot||\boldsymbol{t}||^2})\\ &\leq 2\cdot e^{\frac{1}{2}\cdot\left(\frac{q^2\xi^2}{2\pi}+\frac{1}{4}s_1^2(B)\right)\cdot||\boldsymbol{t}||^2-\delta\cdot||\boldsymbol{t}||^2}.\end{aligned}$$

Now, we estimate the value of $\frac{1}{2}\cdot\left(\frac{q^2\xi^2}{2\pi}+\frac{1}{4}s_1^2(B)\right)\cdot||\boldsymbol{t}||^2$. Since $s_1(B)=\sqrt{\frac{rad(l)}{l}}\leq 1$, we have $\frac{1}{2}\cdot\left(\frac{q^2\xi^2}{2\pi}+\frac{1}{4}s_1^2(B)\right)\cdot||\boldsymbol{t}||^2 = \frac{1}{2}\cdot\left(\frac{q^2\alpha^2}{2\pi}\left(\frac{nk}{\log(nk)}\right)^{\frac{1}{2}}+\frac{1}{4}\frac{rad(l)}{l}\right)\cdot||\boldsymbol{t}||^2 = \Omega(\alpha^2\cdot q^2\cdot\sqrt{n}\log^{-\frac{1}{2}}n\cdot||\boldsymbol{t}||^2)$. Therefore,

$$\Pr(|(\boldsymbol{t},\lfloor\boldsymbol{x}\rceil)| > \delta\cdot||\boldsymbol{t}||^2) \leq e^{-||\boldsymbol{t}||^2\cdot(\log n-1)\cdot\omega(\alpha^2q^2\sqrt{\frac{n}{\log n}})} \leq n^{-\omega(\sqrt{n\log n})\cdot||\boldsymbol{t}||^2}.$$

□

By using Lemma 5.1, we can get a useful estimate for $||\boldsymbol{x}||_\infty$ with $\boldsymbol{x}\hookleftarrow\chi=\lfloor D_{q\cdot\xi}\rceil$. Choose $\boldsymbol{t}=(\frac{1}{2},0,\cdots,0,\frac{1}{2})$ and $\boldsymbol{t}=(\frac{i}{2},0,\cdots,0,-\frac{i}{2})$, we get

$$\Pr_{\boldsymbol{x}\hookleftarrow\chi}(|\mathrm{Re}(\sigma_1(\boldsymbol{x}))| > \frac{1}{\sqrt{2}}\omega(\sqrt{n\log n}\cdot\alpha^2\cdot q^2) \leq n^{-\omega(\sqrt{n\log n})}$$

and

$$\Pr_{\boldsymbol{x}\hookleftarrow\chi}(|\mathrm{Im}(\sigma_1(\boldsymbol{x}))| > \frac{1}{\sqrt{2}}\omega(\sqrt{n\log n}\cdot\alpha^2\cdot q^2) \leq n^{-\omega(\sqrt{n\log n})}.$$

Hence we have $\Pr_{\boldsymbol{x}\hookleftarrow\chi}(|\sigma_1(x)| > \omega(\sqrt{n\log n}\alpha^2q^2)) \leq n^{-\omega(n\log n)}$. Similarly, one can prove that $\Pr_{\boldsymbol{x}\hookleftarrow\chi}(|\sigma_k(x)| > \omega(\sqrt{n\log n}\alpha^2q^2)) \leq n^{-\omega(n\log n)}$ for any $k=1,2\cdots,n$. Therefore, we conclude

$$\Pr_{\boldsymbol{x}\hookleftarrow\chi}(||\sigma(x)||_\infty > \omega(\sqrt{n\log n}\cdot\alpha^2\cdot q^2)) \leq n\cdot n^{-\omega(\sqrt{n\log n})} \leq n^{-\omega(\sqrt{n\log n})}. \tag{6}$$

In order to show that the decryption algorithm succeeds with high probability, we need some relations between $||x|$ and $||x||^c$ for any $x\in K$, i.e. we need the parameters C_1 and C_2 such that $C_1||x||^c \leq ||x|| \leq C_2||X||^c$. Recall that for decoding basis, we have $C_1=\frac{1}{\sqrt{l}}$ and $C_2=\sqrt{\frac{rad(l)}{l}}$.

Lemma 5.2. *Let $n \geq 6$, $q \geq 8n$, $q = 1 \mod l$, $\sigma \geq \sqrt{\frac{2\ln(6n)}{\pi}} \cdot n \cdot q^{\frac{1}{n}}$, $C = \sqrt{\hat{l}}$ and $C_2 = \sqrt{\frac{rad(l)}{l}}$. If $\omega(n^{\frac{3}{2}}\sqrt{\log n \log\log n}) \cdot \alpha^2 \cdot q^2 \cdot \sigma \cdot ||p||_\infty^2 < q$, then with probability $1 - n^{-\omega(\sqrt{n\log n})}$, the decryption algorithm of NTRUEncrtpt recovers m.*

Proof. Notice that $f \cdot h \cdot s = p \cdot g \cdot s \mod qR^\vee$, we have $fc = pgs + pfe + fm \mod qR^\vee \in R^\vee$. If $||pgs + pfe + fm||_\infty^c < \frac{q}{2}$, then we have fc has the representation $pgs + pfe + fm$ when compute mod $qR^\vee$. Hence, we have $m = (fc \mod qR^\vee) \mod pR^\vee$, since $f = 1 \mod pR = 1 \mod pR^\vee$. It thus suffices to give an upper bound on the probability that $||fc||_\infty^c \geq \frac{q}{2}$.

Note that $||fc||_\infty^c \leq ||fc||^c \leq C||fc|| = C||pgs + pfe + fm|| \leq C(||pgs|| + ||pfe|| + ||fm||)$. By the choice of parameters and Lemma 4.2, with probability $\geq 1 - 2^{3-n}$, $||f|| \leq 2\sqrt{n}\sigma||p||_\infty$ and $||g|| \leq \sqrt{n}\sigma$. Hence, combining with (6), we get

$$\begin{aligned} ||pfe|| + ||pgs|| &\leq 2\sqrt{n}\sigma||p||_\infty^2 \cdot ||s||_\infty + \sqrt{n}\sigma||p||_\infty \cdot ||e||_\infty) \\ &\leq \omega(n\sqrt{\log n} \cdot \alpha^2 \cdot q^2)\sigma||p||_\infty^2 \end{aligned}$$

with probability $1 - n^{-\omega(\sqrt{n\log n})}$. Since $m \in R^\vee/(pR^\vee) \subseteq K$, by reducing modulo the $p\sigma(\vec{d})_i$'s, we can write m into $\sum_{i=1}^n \varepsilon_i p\sigma(\vec{d})_i$ with $\varepsilon_i \in (-\frac{1}{2}, \frac{1}{2}]$. Hence

$$||m|| = ||\sum_{i=1}^n \varepsilon_i p\sigma(\vec{d})_i|| \leq ||p||_\infty ||\sum_{i=1}^n \varepsilon_i \sigma(\vec{d})_i|| \leq \frac{\sqrt{n}}{2}||p||_\infty C_2,$$

by using

$$||\sum_{i=1}^n \varepsilon_i \sigma(\vec{d_i})|| = ||\sum_{i=1}^n (\varepsilon_i \vec{d_i})|| \leq C_2 \cdot ||\sum_{i=1}^n (\varepsilon_i \vec{d_i})||^c \leq C_2 \cdot \frac{\sqrt{n}}{2}.$$

So, we have $||fm|| \leq ||f|| \cdot ||m|| \leq n\sigma||p||_\infty^2 C_2$ with probability $\geq 1 - 2^{3-n}$. Therefore, putting these results together, we have

$$\begin{aligned} ||fc|| &\leq C(\omega(n\sqrt{\log n} \cdot \alpha^2 \cdot q^2) \cdot \sigma \cdot ||p||_\infty^2 + n \cdot \sigma \cdot ||p||_\infty^2 \cdot C_2) \\ &\leq \omega(n^{\frac{3}{2}}\sqrt{\log n \log\log n} \cdot \alpha^2 \cdot q^2) \cdot \sigma \cdot ||p||_\infty^2 \end{aligned}$$

with probability $1 - n^{-\omega(\sqrt{n\log n})}$, where we have used the fact that $C_2 \leq 1$ and $C = O(\sqrt{n \log\log n})$. We get the results we need. □

Remark 5.3. *We remark that we can put all computations in an integral ideal $I = \hat{l} \cdot R^\vee \subseteq R$ by multiplying an integer $\hat{l}$ without changing the conditions on q and α. The only change is a slight modification on the decryption algorithm. We use symbol $\hat{a}$ to represent the corresponding element of $a \in R^\vee$, i.e. $\hat{a} = \hat{l} \cdot a$. Note that $f = 1 \mod pR = 1 \mod pR^\vee$, we have $\hat{l} \cdot f = \hat{l} \mod pI$. Therefore, $\hat{m} = \frac{1}{\hat{l}}(\hat{l}(f \cdot \hat{c} \mod qI) \mod pI)$ with $\hat{m} \in I/(pI)$.*

The security of the scheme follows by an elementary reduction from $R - DLWE^\times_{q,D_{q\xi}}$, exploiting the uniformity of the public key in $R_q^\times$ and the invertibility of $p \in R_q$. It's proof is almost the same as in [35] or [38].

Lemma 5.4. *Let $n \geq 6$, $q \geq 8n$, $q = 1 \mod l$, $\sigma \geq \sqrt{\ln(8nq)} \cdot n^{\frac{3}{2}} \cdot q^{\frac{1}{2}+\varepsilon}$, $\delta > 0$ and $\varepsilon \in (0, \frac{1}{2})$. If there exists an IND-CPA attack against NTRUEncrypt that runs in time T and has success probability $\frac{1}{2} + \delta$, then there exists an algorithm solving R-DLWE$^{\times}$ with parameters q and $q\xi$ that runs in time $T' = T + O(n)$ and has success probability $\delta' = \delta - q^{-\Omega(n)}$.*

Proof. Let $\mathfrak{A}$ be the given IND-CPA attack algorithm, we construct an algorithm $\mathfrak{B}$ against $R-DLWE^{\times}_{q,D_{q\xi}}$ as follows. Given oracle $\mathfrak{O}$ that samples from either $U(R_q^{\times} \times R_q^{\vee})$ or $A^{\times}_{s,D_{q\xi}}$ for some $s \hookleftarrow \chi$, $\mathfrak{B}$ calls $\mathfrak{O}$ to get a sample (h', c') from $R_q^{\times} \times R_q^{\vee}$, then runs $\mathfrak{A}$ with public key $h = p \cdot h' \in R_q^{\times}$. When $\mathfrak{A}$ outputs challenge messages $m_0,\ m_1 \in \mathcal{P}$, $\mathfrak{B}$ picks $b \hookleftarrow U(0,1)$, computes $c = p \cdot c' + m_b \in R_q^{\vee}$ and give it to $\mathfrak{A}$. When $\mathfrak{a}$ returns its guess b', $\mathfrak{B}$ returns 1 when $b' = b$ and 0 otherwise.

Note that h' is uniformly random in $R_q^{\times}$, so is the public key h given to $\mathfrak{A}$. Thus, it is within statistical distance $q^{-\Omega(n)}$ of the public key distribution in the genuine attack. Moreover, when $c' = hs + e$ with $s,\ e \hookleftarrow \chi$, the ciphertext c given to $\mathfrak{A}$ has the right distribution as in the IND-CPA attack. Therefore, if $\mathfrak{O}$ outputs samples from $A^{\times}_{s,D_{q\xi}}$, $\mathfrak{A}$ succeeds an $\mathfrak{B}$ returns 1 with probability $\geq \frac{1}{2} + \delta - q^{-\Omega(n)}$.

Now, if $\mathfrak{O}$ outputs samples from $U(R_q^{\times} \times R_q^{\vee})$, then c is uniformly random in R_q and independent of b. Hence, $\mathfrak{B}$ outputs 1 with probability $\frac{1}{2}$. The claimed advantage of $\mathfrak{B}$ follows. □

In a summary, we have the following results.

Theorem 5.5. *Let l be a positive integer, $n = \varphi(l) \geq 6$, $q \geq 8n$, $q = 1 \mod l$ be a prime of size poly(n) and $K = \mathbb{Q}(\zeta_l)$. Assume that $\alpha = \alpha(n) \geq 2$ satisfies $\alpha q \geq \omega(\sqrt{\log n})$. Let $\xi = \alpha \cdot (\frac{nk}{\log(nk)})^{\frac{1}{4}}$ with $k = O(1)$, $\varepsilon \in (0, \frac{1}{2})$ and $p \in R_q^{\times}$. Moreover, let $\sigma \geq n^{\frac{3}{2}} \cdot \sqrt{\ln(8nq)} \cdot q^{\frac{1}{2}+\varepsilon}$ and $\omega(n^{\frac{3}{2}}\sqrt{\log n \log\log n} \cdot \alpha^2 \cdot q^2) \cdot \sigma \cdot ||p||_{\infty}^2 < q$. Then if there exists an IND-CPA attack against NTRUEncrypt(n, q, p, σ, ξ) that runs in time poly(n) and has success probability $\frac{1}{2} + \frac{1}{poly(n)}$, there exists a poly$(n)-$time algorithm solving $\gamma-$Ideal-SIVP on any ideal lattice of K with $\gamma = \tilde{O}(\frac{\sqrt{n}}{\alpha})$. Moreover, the decryption algorithm succeeds with probability $1 - n^{-\omega(\sqrt{n \log n})}$ over the choice of the encryption randomness.*

6 Comparison with Previous Works

In applications, we hope we can take q as small as possible and α (hence γ), as big as possible (as small as possible). In previous works [35, 38, 39], the results of q and γ depend heavily on the choice of p, i.e. p is a 'constant' or p is an 'usual polynomial'. Therefore, in applications, the number of encrypted bit in each encrypt process depends heavily on the choice of p. We can take a comparison for an overview.

(1) p **is a 'constant'.**

In this case, by taking $q\alpha = \Omega(\log^{\frac{3}{4}} n)$, one have the approximate parameter $\gamma = \tilde{O}(\frac{\sqrt{n}}{\log^{0.75} n} \cdot q)$ in [38, 39]. The magnitude of q and γ are $q^{\frac{1}{2}-\varepsilon} = \omega(l^{3.75} \log^{1.5} l \cdot ||p||^2)$

and $\gamma = \tilde{\omega}(l^8 \cdot ||p||^4)$ with l be a prime in [38] and $q^{\frac{1}{2}-\varepsilon} = \omega(d^{0.5} l^{2.25} \log^{1.5} l \cdot ||p||^2)$ and $\gamma = \tilde{\omega}(dl^5 \cdot ||p||^4)$ with $l = d^v$, d is a prime in [39]. In [35], one can set $\alpha \cdot q = \omega(n\sqrt{\log n})$, then $q^{\frac{1}{2}-\varepsilon} = \omega(n^{2.5} \log^2 n \cdot ||p||^2)$ and $\gamma = \tilde{\omega}(n^{5.5} \cdot ||p||^4)$. In [36], they improved the result to $q = \tilde{\omega}(n^{4.5})$.

(2) p **is an 'usual polynomial'.**

In this case, by taking $q\alpha = \Omega(\log^{\frac{3}{4}} n)$, one have the approximate parameter $\gamma = \tilde{O}(\frac{\sqrt{n}}{\log^{0.75} n} \cdot q)$ in [38, 39]. The magnitude of q and γ are $q^{\frac{1}{2}-\varepsilon} = \omega(l^{4.75} \log^{1.5} l \cdot ||p||^2)$ and $\gamma = \tilde{\omega}(l^{10} \cdot ||p||^4)$ with l be a prime in [38] and $q^{\frac{1}{2}-\varepsilon} = \omega(d^{0.5} l^{3.25} \log^{1.5} l \cdot ||p||^2)$ and $\gamma = \tilde{\omega}(dl^7 \cdot ||p||^4)$ with $l = d^v$, d is a prime in [39]. In [35], one can set $\alpha \cdot q = \omega(n\sqrt{\log n})$, then $q^{\frac{1}{2}-\varepsilon} = \omega(n^{3.5} \log^2 n \cdot deg(p) \cdot ||p||^2)$ and $\gamma = \tilde{\omega}(n^{7.5} \cdot deg(p) \cdot ||p||^4)$.

(3) **Our results.**

In our scheme, we regard 'constant', i.e. $p \in \mathbb{Z}$, and 'usual polynomial' as an element of algebraic number in $R^\vee$. In both cases, they have the same status. Hence, our results do not depend on the choice of p. By by taking $q\alpha = \Omega(\log^{\frac{3}{4}} n)$, one have the approximate parameter $\gamma = \tilde{O}(\frac{\sqrt{n}}{\log^{0.75} n} \cdot q)$, as in [38] and [39]. Then, one can take $q^{\frac{1}{2}-\varepsilon} = \omega(n^3 \log^3 n \cdot ||p||_\infty^2)$ and $\gamma = \tilde{\omega}(n^{6.5} \cdot ||p||_\infty^4)$. In particular, our results eliminate the limitation of cyclotomic fields.

In order to reach the best bounds, the previous results must set $p \in \mathbb{Z}$, which limits the number of encrypted bits. The usual case is set $p = 2$ to encrypt one bit each time. If one wants to encrypt n bits each time, which means that every coefficient of the power basis (or monomial) must be used. The bound of q would become very bad, see case (2). Note that when represented under decoding bases, $||p|| \leq \sqrt{\frac{rad(l)}{l}} \cdot ||p||^c$, where $\sqrt{\frac{rad(l)}{l}} = \sqrt{\frac{\prod_p (p-1)}{n}}$. If we want to make the best of the number of encrypted bits, for example, take every coefficient's value in $[0, \cdots, n]$, the results of previous work would become pretty bad, since the previous results also depend on $||p||$ while ours only depend on $||p||_\infty$. More precisely, when we want to encrypt $O(n)$ bits each time, the magnitude of q in [35] becomes $\tilde{\omega}(n^{11})$, in [38] becomes $\tilde{\omega}(n^{11.5})$ and in [39] becomes $\tilde{\omega}(n^{8.5})$ comparing with ours $\tilde{\omega}(n^6)$, when we want to encrypt $O(n \log(n))$ bits each time, the magnitude of q in [35] becomes $\tilde{\omega}(n^{15})$, in [38] becomes $\tilde{\omega}(n^{15})$ and in [39] becomes $\tilde{\omega}(n^{13})$ comparing with ours $\tilde{\omega}(n^{10})$.

That is to say, if we consider to encrypt many bits in each encryption process, one can see our construction has potentialities to do much better than [35, 38, 39], since our scheme has no limits on the choice of p.

7 Conclusion

To sum up, though the best bounds of q is about $n^{1.5}$ times smaller than ours, our scheme do not limited by the choice of p and the cyclotomic fields it works on. Hence, our scheme get rid of the dependence of the plaintext space, so that our NTRUEncrypt has potentialities to send more encrypted bits in each encrypt process with higher efficiency and stronger security. Further, our decryption algorithm succeeds with a probability of $1 - n^{-\omega(\sqrt{n \log n})}$ comparing

with the previous work's $1 - n^{-\omega(1)}$. Therefore, we believe, in applications, our scheme may have more advantages.

Acknowledgement

The authors would like to express their gratitude to Bin Guan and Yang Yu for helpful discussions.

References

[1] M. Albrecht, S. Bai, L. Ducas: *A subfield lattice attack on overstretched NTRU assumptions: Cryptanalysis of some FHE and graded encoding schemes.* CRYPTO 2016, LNCS, vol. 9814, 153-178, (2016).

[2] B. Applebaum, D. Cash, C. Peikert, A. Sahai: *Fast cryptographic primitives and circular secure encryption based on hard learning problems.* CRYPTO 2009, LNCS, vol. 5677, 595-618, (2009).

[3] W. Banaszczyk: *New bounds in some transference theorems in the geometry of numbers.* Math. Ann., **296**(4), 625-635, (1993).

[4] J. W. Bos, K. Lauter, J. Loftus, M. Naehrig: *Improved security for a ring based fully homomorphic encryption scheme.* IMACC 2013, LNCS, vol. 8308, 45-64, (2013).

[5] K. Conrad: *The different ideal.* Available at *Http://www.math.uconn.edu/∼kconrad/blurbs/.*

[6] J. H. Cheon, J. Jeong, C. Lee: *An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low-level encoding of zero.* LMS J. COMPUT. MATH., **19**(A), 255-266, (2016).

[7] D. Coppersmith, A. Shamir: *Lattice attacks on NTRU.* EUROCRYPT 1997, LNCS, vol. 1233, 52-61, (1997).

[8] D. Cabarcas, P. Weiden, J. A. Buchmann: *On the efficiency of provably secure NTRU.* PQCrypto 2014, LNCS, vol. 8772, 22-39, (2014).

[9] L. Ducas, A. Durmus: *Ring-LWE in polynomial rings.* PKC 2012, LNCS, vol. 7293, 34-51, (2012).

[10] L. Ducas, A. Durmus, T. Lepoint, V. Lyubashevsky: *Lattice signatures and bimodal gaussians.* CRYPTO 2013, LNCS, vol. 8042, 40-56, (2013).

[11] L. Ducas, V. Lyubashevsky, T. Prest: *Efficient identity-based encryption over NTRU lattices.* ASIACRYPT 2014, LNCS, vol. 8874, 22-41, (2014).

[12] L. Ducus, P. Q. Nguyen: *Learning a zonotope and more : Cryptanalysis of NTRUSign countermeasures.* ASIACRYPT 2012, LNCS, vol. 7658, 433-450, (2012).

[13] C. Gentry: *Key recovery and message attacks on NTRU-composite.* EUROCRYPT 2001, LNCS, vol. 2045, 182-194, (2001).

[14] S. Garg, C. Gentry, S. Halevi: *Candidate multilinear maps from ideal lattices*. EUROCRYPT 2013, LNCS, vol. 7881, 1-17, (2013).

[15] N. Gama, P. Q. Nguyen: *New chosen-ciphertext attacks on NTRU*. PKC 2007, LNCS, vol. 4450, 89-106, (2007).

[16] C. Gentry, C. Peikert, V. Vaikuntanathan: *Trapdoors for hard lattices and new cryptographic constructions*. Proc. of STOC, ACM, New York, 197-206, (2008).

[17] N. Howgrave-Graham: *A hybird lattice-reduction and meet-in-the-middle attack against NTRU*. CRYPTO 2007, LNCS, vol. 4622, 150-169, (2007).

[18] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. H. Silverman, W. Whyte: *NTRUSign: Digital signatures using the NTRU lattice*. CT-RSA 2003, LNCS, vol. 2612, 122-140, (2003).

[19] J. Hoffstein, J. Pipher, J. H. Silverman: *NTRU: A ring-based public key cryptosystem*. ANTS 1998, LNCS, vol. 1423, 267-288, (1998).

[20] E. Jaulmes, A. Joux: *A chosen-ciphertext attack against NTRU*. CRYPTO 2000, LNCS, vol. 1880, 20-35, (2000).

[21] A. W. Knapp: *Basic algebra*. Birkhãuser Boston, (2006).

[22] P. Kirchner, P. A. Fouque: *Revisting lattice attacks on overstretched NTRU parameters*. EUROCRYPT 2017, LNCS, vol. 10210, 3-26, (2017).

[23] V. Lyubashevsky, C. Peikert, O. Regev: *On ideal lattices and learning with errors over rings*. EUROCRYPT 2010, LNCS, vol. 6110, 1-23, (2010).

[24] V. Lyubashevsky, C. Peikert, O. Regev: *A Toolkit for Ring-LWE Cryptography*. Crypto. ePrint Archive, 2013:293, (2013).

[25] V. Lyubashevsky, C. Peikert, O. Regev: *A Toolkit for Ring-LWE Cryptography*. EUROCRYPT 2013, LNCS, vol. 7881, 35-54, (2013).

[26] A. López-Alt, E. Tromer, V. Vaikuntanathan: *On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption*. Proc. of STOC, ACM, New York, 1219-1234, (2012).

[27] D. Micciancio: *Generalized compact knapsacks, cyclic lattices, and efficient oneway functions*. Comput. Complex. **16**(4), 365-411, (2007).

[28] S. Murphy, R. Player: *Noise Distributions in Homomorphic Ring-LWE*. Crypto. ePrint Archive, 2017:698, (2017).

[29] D. Micciancio, O. Regev: *Worst-case to average-case reductions based on gaussian measures*. SIAM J. Comput., **37**(1), 267-302, (2007).

[30] D. Micciancio and O. Regev: *Trapdoor for lattices: Simpler, tighter, faster, smaller*. EUROCRYPT 2012, LNCS, vol. 7237, 700-718, (2012).

[31] C. Peikert: *Limits on the hardness of lattice problems in ℓ_p nroms*. Comput. Complexity, **2**(17), 300-351, (2008).

[32] C. Perkert: *An efficient and parallel Gaussian sampler for lattices*. CRYPTO 2010, LNCS, vol. 6223, 80-97, (2010).

[33] O. Regev: *On lattices, learning with errors, random linear codes, and cryptography*. J. ACM, **56**(6), 1-40, (2009).

[34] R. Steinfeld, S. Ling, J. Pieprzyk, C. Tartary, H. Wang: *NTRUCCA: how to strengthen NTRUEncrypt to chosen-ciphertext security in the standard model*. PKC 2012, LNCS, vol. 7293, 353-371, (2012).

[35] D. Stehlé, R. Steinfeld: *Making NTRU as secure as worst-case problems over ideal lattices*. EUROCRYPT 2011, LNCS, vol. 6632, 27-47 (2011).

[36] D. Stehlé, R. Steinfeld: *Making NTRUEncrypt and NTRUSign as secure as worst-case problems over ideal lattices*. Crypto. ePrint Archive, 2013:004, (2013).

[37] R. Vershynin: *Introduction to the non-asymptotic analysis of random matrices*. Available at http://www-personal.umich.edu/ romanv/papers/non-asymptotic-rmt-plain.pdf.

[38] Y. Yu, G. W. Xu, X. Y. Wang: *Provably Secure NTRU Instances over Prime Cyclotomic Rings*. PKC 2017, LNCS, vol. 10174, 409-434, (2017).

[39] Y. Yu, G. W. Xu, X. Y. Wang: *Provably Secure NTRUEncrypt over More General Cyclotomic Rings*. Crypto. ePrint Archive, 2017: 304, (2017).