Provably Secure NTRUEncrypt over Any Cyclotomic Field

Yang Wang and Mingqiang Wang(✉)

School of Mathematics, Shandong University, Jinan 250100, Shandong, China
wyang1114@mail.sdu.edu.cn, wangmingqiang@sdu.edu.cn

Abstract. NTRUEncrypt is generally recognized as one of candidate encryption schemes for post quantum cryptography, due to its moderate key sizes, remarkable performance and potential capacity of resistance to quantum computers. However, the previous provably secure NTRUEncrypts are only based on prime-power cyclotomic rings. Whether there are provably secure NTRUEncrypt schemes over more general algebraic number fields is still an open problem. In this paper, we answer this question and present a new provably IND-CPA secure NTRUEncrypt over any cyclotomic field. The security of our scheme is reduced to a variant of learning with errors problem over rings (Ring-LWE). More precisely, the security of our scheme is based on the worst-case approximate shortest independent vectors problem (SIVP_γ) over ideal lattices. We prove that, once the field is fixed, the bounds of the reduction parameter γ and the modulus q in our scheme are less dependent on the choices of plaintext spaces. This leads to that our scheme provides more flexibility for the choices of plaintext spaces with higher efficiency under stronger security assumption. Furthermore, the probability that the decryption algorithm of our scheme fails to get the correct plaintext is much smaller than that of the previous works.

Keywords: NTRU · Ideal lattices · Canonical embedding
Cyclotomic fields · Ring-LWE

1 Introduction

The NTRU encryption scheme was devised by Hoffstein, Pipher and Silverman in [15]. 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 resisting attacks by quantum computers. Based on the underlying problem of NTRU, various cryptographic primitives were designed, such as identity-based encryption [8], fully homomorphic encryption [2,20], digital signatures [7,14] and multi-linear maps [11]. Meanwhile, a batch of cryptanalysis works were proposed aiming at NTRU family [1,4,5,9,10,12,16–18].

The security of the first NTRUEncrypt in [15] is heuristic and lacks a solid mathematical proof. This leads to a break-and-repair development history of

C. Cid and M. J. Jacobson, Jr. (Eds.): SAC 2018, LNCS 11349, pp. 391–417, 2019.
https://doi.org/10.1007/978-3-030-10970-7_18

NTRUEncrypt. Stehlé and Steinfeld [29] provided the first provably IND-CPA secure NTRUEncrypt over power of 2 cyclotomic rings. They used the coefficient embedding of polynomial rings and the security of their scheme was based on the corresponding Ring-LWE problem. Although the construction of Stehlé and Steinfeld may be less practical compared with classical NTRUEncrypts [3], their work revealed an important connection between NTRUEncrypt and Ring-LWE, hence between problems over NTRU lattices and worst-case problems (SIVP_γ) over ideal lattices. An open problem proposed by Stehlé and Steinfeld is whether their construction can be improved to more general rings. Recently, Yu, Xu and Wang [31] modified the scheme in [29] to make it work over cyclotomic rings of the forms $\mathbb{Z}[\zeta_p]$ for prime integer p. The modified scheme in [31] allowed more flexibility choices of cyclotomic rings, but the size requirements for parameters were more limited, making the modified schemes less efficiency. The first NTRUEncrypt scheme using canonical embedding was discussed in [32] which showed that given appropriate parameters, provably secure NTRUEncrypt could work over prime-power cyclotomic rings. The security of the schemes proposed in [31,32] relied on a variant of Ring-LWE problems over cyclotomic rings proposed in [6].

With the calls of post-quantum cryptography by NIST, a better understanding of these problems is necessary and the study of NTRUEncrypt is theoretically valuable as stated in [32]. To our knowledge, till now, provably secure NTRUEncrypts were all constructed over prime-power cyclotomic rings by using the coefficient embedding. Also, the security parameter γ and the modulus q rely heavily on the choice of plaintext space. That is to say, in order to reach better efficiency in applications, the plaintext space of the existing NTRUEncrypts were all limited to $\{0,1\}^n$-only embed one bit in each coefficient of polynomials in each encrypt process. If we want to embed more bits in each coefficient of polynomials in each encryption process, the lower bounds of γ and q would become pretty bad. These disadvantages restrict the applications of the existing provably secure NTRUEncrypts. Therefore, eliminating the limitation of choices of cyclotomic fields to solve the open problem proposed in [29] and improving the efficiency of the existing provably secure NTRUEncrypts are worth doing. These are also the main motivations of our research.

1.1 Our Contributions

NTRUEncrypt schemes in the standard model by using the canonical embedding over any cyclotomic field. For any fixed cyclotomic field, we design our scheme in the fractional ideal $R^\vee$, i.e. the codifferent ideal of the ring of integers R. In applications, our scheme can also be converted to work in an integral ideal of R.

Once we fix a cyclotomic field, we get an almost uniform bounds for the reduction parameter γ and the modulus q, which are less dependent on the choices of plaintext spaces. Hence, our scheme provides more flexibility for the choices of plaintext spaces and has potential to send more encrypted bits in one encryption process with higher efficiency under stronger hardness assumption.

We use the subgaussian distribution, the decoding basis and the basis-embedding norm to estimate the decryption error. These tools enable us to get tighter lower bounds of q and γ, they also bring us a smaller decryption error. More precisely, our decryption algorithm succeeds in recovering the correct message with an exception of a negligible probability $n^{-\omega(\sqrt{n \log n})}$, much better than the previous $n^{-\omega(1)}$.

We also get a regularity result (a kind of ring-based leftover hash lemma) for all cyclotomic fields, which is useful to design many cryptographic primitives. Set $R_q^\times$ be the set of invertible elements of $R_q = R/(qR)$, the regularity is about how to construct a tuple $(a_1, \cdots, a_m; \sum_{i=1}^m a_i t_i) \approx U((R_q^\times)^m \times R_q))$, where $a_i \hookleftarrow U(R_q^\times)$ are chosen independently and $\boldsymbol{t}$ subjects to some distributions. Our results enrich the choices of the distributions of $\boldsymbol{t}$.

1.2 Technique Overview

Although the main ideas of our NTRUEncrypt follow Stehlé and Steinfeld's route, many differences exist.

In the previous constructions, analysis of decryption error is the uppermost difficulty which constrains the form of cyclotomic fields. The traditional coefficient embedding decides that this process depends heavily on the form of polynomials f of the corresponding ring $R = \mathbb{Z}[x]/(f(x))$. To overcome this problem, we have a very important observation that the decryption is only relevant to the coefficients corresponding to the basis we choose, and different bases affect the results heavily. The natural choice of coefficient embedding over polynomial rings may mislead us. So we use the decoding basis of $R^\vee$ and define the basis-coefficient embedding to bound the decryption error. These modifications enable us to control the decryption error for all cyclotomic fields in the same way. Then, if we want to enjoy the high computation speed over polynomial rings, it is easy for us to convert our schemes to work in the ring R in theory.

Benefits brought by those tools and our observation are more than these. If we want to reach the highest efficiency, traditional coefficient embedding may limit the number of encrypted bits in each encryption process, i.e. in order to get the highest efficiency, the existing NTRUEncrypts all limited their plaintext space to $\{0,1\}^n$. This is caused by the coefficient embedding and the perspective that we regard the elements as polynomials in the ring R. If we regard constant polynomials and non-constant polynomials as usual algebraic integers, then the tools we use give us an almost uniform bound for the reduction parameter γ and the modulus q, which is less dependent on the choices of plaintext spaces. Meanwhile, the decryption error is much smaller than that of the existing schemes.

The reason why we design our scheme in $R^\vee$ is that we want to use the hardness results about Ring-LWE showed in [22], other than those proposed in [6]. This is a natural choice when we want to use the canonical embedding and to get rid of the troubles caused by different polynomials. By using the recent hardness results about primal-Ring-LWE (i.e. the secret $s \hookleftarrow U(R_q)$) proved in [28], we can also directly design NTRUEncrypt in R (For more details, see Remark 2). The high level construction outline of our scheme is as follows.

The key generation algorithm is essentially the same as the previous works.

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

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

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'. Provable security needs the public key to distribute statistically close to uniformity, and the analysis of the public key distribution needs to deal with some kinds of q-ary lattices, in order to bound the corresponding smooth parameters. By an accurate analysis of the relationship between different fractional ideals, we give a lower bound of λ_1 with respect to l_∞ norm of these q-ary lattices. In this section, we consider these problems absolutely in K, hence get a better result compared with [32] in theory.

Our NTRUEncrypt is as following:

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

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

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

Here, χ is the error distribution of the Ring-LWE problem proposed in [22]. The plaintext space of our scheme is $\mathcal{P} = R^\vee/(pR^\vee)$, where p is an invertible element in R_q. By using the decoding basis of $R^\vee$ and the basis-coefficient embedding of elements in $R^\vee$, we get a tight connection between the canonical norms and the basis-coefficient norms. Moreover, by using subgaussian distributions, we also prove that the decryption error is negligible - $n^{-\omega(\sqrt{n \log n})}$, which is better than the existing $n^{-\omega(1)}$. Furthermore, as we remark in Remark 1, we can put all computations and storages in an integral ideal of R and this modification may enjoy the high computation speed over polynomial rings in theory.

Till now, the magnitude of the modulus q is far away from practicality, and this is the common shortcoming of the provably secure NTRUEncrypts. How to reduce the sizes of parameters is an intriguing open problem.

1.3 Organization

In Sect. 2, we introduce some notations and basic results that will be used in our discussion. In Sect. 3, we give a new series of relevant results about some kinds of q-ary lattices. These are important for us to analyze the key generation algorithm of our NTRUEncrypt in Sect. 4. In Sect. 5, we construct the NTRUEncrypt and give a secure reduction from basic lattice problem to the CPA-security of our NTRUEncrypt.

2 Preliminaries

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

2.1 Notations

We set $\hat{l} = l$ 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 $||\cdot||_p$ to represent the l_p norm corresponding to the canonical embedding. When $p = 2$, we usually use $||\cdot||$ to represent the l_2 norm. For any matrix $M \in \mathbb{C}^{n\times n}$, we use $\lambda_i(M)$ stand for its eigenvalues and $s_i(M)$ stand for its singular values for $i \in [n]$. We arrange eigenvalues and singular values by their magnitudes, 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 and Y, $\Delta(X, Y)$ stands for their statistic distance. As usual, $E(X)$ and $Var(X)$ stand for the expectation and the variance of a random variable X. When we write $X \hookleftarrow \xi$, we mean that the random variable X obeys to a distribution ξ. Function rad represents 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, $rad(n) = \prod_{i=1}^{k} p_i$. If S is a finite set, then $|S|$ is its cardinality and $U(S)$ is the uniform distribution over S. Symbols $\mathbb{Z}^+$ and $\mathbb{R}^+$ stand for the sets of positive integers and positive reals. Symbol $\log x$ represents $\log_2 x$ for $x \in \mathbb{R}^+$. For a positive integer a, $\mathbb{Z}_a^\times$ represents the reduced residue system mod a.

2.2 Cyclotomic Fields, Space H and Geometry

Through out this paper, we consider cyclotomic fields. Let $K = \mathbb{Q}(\zeta)$, where $\zeta = \zeta_l$ is a primitive l-th root of unity, which has minimal polynomial $\Phi_l(x) = \prod_{i|l}(x^i - 1)^{\mu(\frac{l}{i})}$ of degree $n = \varphi(l)$. Then $[K : \mathbb{Q}] = n = \varphi(l)$ and $K \cong \mathbb{Q}[x]/\Phi_l(x)$. We set $R = \mathcal{O}_K = \mathbb{Z}[\zeta]$ be the ring of integers of K.

We set $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_i : \ i = 1, \cdots, n\}$ 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 i-th element of $\mathbb{Z}_l^\times$, order the σ_i and define $H = \{(x_1, \cdots, x_n) \in \mathbb{C}^n : x_{n+1-i} = \overline{x_i}, \ \forall i \in [r]\}$. 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 imaginary number such that $\boldsymbol{i}^2 = -1$. We then 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 $1 \leq j \leq r$.

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 $||x \cdot y||_p \leq ||x||_\infty \cdot ||y||_p$ for $p \in \{1, \cdots, \infty\}$. The Trace and Norm of $x \in K$ are 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 discriminant Δ_K of K, the integral and fractional ideals are defined as usual.

Integral ideals can be regarded as special cases of fractional ideals. Recall that, the discriminant of the l-th cyclotomic number field is

$$\Delta_K = (-1)^{\frac{n}{2}} \cdot \left(\frac{l}{\prod_{p|l} p^{\frac{1}{p-1}}} \right)^n \leq n^n,$$

where p runs over all prime factors of l.

Let $q \in \mathbb{Z}$ be a prime, then the factorization of the ideal $(q) = qR$ 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 $(q) = \prod_{i=1}^{g} \mathfrak{q}_i^e$, where $\mathfrak{q}_i$ are $g = n/(ef)$ different prime ideals each of norm q^f. In particular, for a prime $q = 1 \bmod l$, we have $e = f = 1$, the ideal (q) splits into n distinct prime ideals as $(q) = \prod_{i \in \mathbb{Z}_l^\times} \mathfrak{q}_i$ with $\mathfrak{q}_i = \langle q, \zeta - \omega^i \rangle$, where ω is a primitive l-th root of unity in $\mathbb{Z}_q^\times$. The norm of $\mathfrak{q}_i$ is q. We have $\Phi_l(x) = \prod_{i \in \mathbb{Z}_l^\times} (x - \omega^i) \bmod q$.

2.3 Lattice and Discretization

We define a lattice as a discrete additive subgroup of H and we only deal with full-rank lattices. 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, i.e. $\lambda_1(\Lambda) = \min_{0 \neq \boldsymbol{x} \in \Lambda} ||\boldsymbol{x}||$. 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. 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 ideal I, we also have $\det(\sigma(I)) = \mathrm{N}(I) \cdot \sqrt{|\Delta_k|}$. The following lemma from [26] gives upper and lower bounds on the minimum distance of an ideal lattice in l_2 norm.

Lemma 1. *For any fractional ideal I in a number field K of degree n,*

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

For any fractional ideal I in K, its dual is defined as $I^\vee = \{a \in K : \ \mathrm{Tr}(aI) \subseteq \mathbb{Z}\}$. 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. In fact, an ideal of K and its inverse are related by multiplication with the dual ideal $R^\vee$: $I^\vee = I^{-1} \cdot R^\vee$.

One of the most famous lattice problems is SVP. Given a lattice basis B, try to find a shortest vector in $\Lambda \backslash \{0\}$, where $\Lambda = \mathfrak{L}(B)$. The relaxed problem SVP_γ is asking for a nonzero lattice vector that is no longer than γ times the length of a solution of SVP. By restricting SVP to the ideal lattice, we obtain Ideal-SVP. No polynomial quantum algorithm is known to solve the worst-case SVP_γ problem for $\gamma \leq \mathrm{poly}(n)$ and also no algorithm is known to perform non-negligibly better for ideal lattices than classic lattices. The (Ideal-SIVP_γ) SIVP_γ

problem is that given a basis of a lattice Λ of dimension n, try to find n linear independent vectors $x_1, \cdots, x_n \in \Lambda$ such that $\max_{1 \le i \le n} ||x_i|| \le \gamma \cdot \lambda_n(\Lambda)$.

We now consider the discretization. We describe the formal definition as in [24], a modified version of [22]. Define $\lceil x \rceil$ to be the smallest integer that is bigger than or equal to x for any $x \in \mathbb{R}$.

Definition 1. *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*

- $1 + a - \lceil a \rceil$ *with probability* $\lceil a \rceil - a$,
- $a - \lceil a \rceil$ *with probability* $1 - (\lceil a \rceil - a)$.

A random variable $\boldsymbol{R} = (R_1, \cdots, R_n)^T \in \mathbb{R}^n$ *has a multivariate Reduction distribution* $R \sim Red(\boldsymbol{a})$ *on* $\mathbb{R}^n$ *for parameter* $\boldsymbol{a} = (a_1, \cdots, a_n)^T$ *if its components* $R_j \sim Red(a_j)$ *for* $j = 1, \cdots, n$ *are independent univariate Reduction random variables.*

We now describe the coordinate-wise rounding discretisation which is easy to use for our applications.

Definition 2. *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*

$$(\lfloor \boldsymbol{X} \rceil^B_{\Lambda + \boldsymbol{c}} | \boldsymbol{X} = \boldsymbol{x}) = \lfloor \boldsymbol{x} \rceil^B_{\Lambda + \boldsymbol{c}} = \boldsymbol{x} + BQ_{\boldsymbol{x}, \boldsymbol{c}},$$

where $Q_{\boldsymbol{x}, \boldsymbol{c}} \sim Red(B^{-1}(\boldsymbol{c} - \boldsymbol{x}))$.

2.4 Gaussian and Subgaussian Random Variables

For $s > 0$, $\boldsymbol{c} \in H$, define the Gaussian function $\rho_{s, \boldsymbol{c}} : H \to (0, 1]$ as $\rho_{s, \boldsymbol{c}}(\boldsymbol{x}) = e^{-\pi \frac{||\boldsymbol{x} - \boldsymbol{c}||^2}{s^2}}$. By normalizing this function, we obtain the continuous Gaussian probability distribution $D_{s, \boldsymbol{c}}$ of parameter s, whose density is given by $s^{-n} \cdot \rho_{s, \boldsymbol{c}}(\boldsymbol{x})$. We usually omit the subscript $\boldsymbol{c}$ when it is $\boldsymbol{0}$. Let $\boldsymbol{r} = (r_1, \cdots, r_n) \in (\mathbb{R}^+)^n$ be a vector such that $r_j = r_{n+1-j}$ for $j \in \{1, \cdots, \frac{n}{2}\}$, we can define the elliptical Gaussian distributions in the basis $\{\boldsymbol{h}_i\}_{i \le n}$ 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 a 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 $\mathbb{R}^n$.

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 $D_{\Lambda, \sigma, \boldsymbol{c}}(\boldsymbol{x}) = \frac{\rho_{\sigma, \boldsymbol{c}}(\boldsymbol{x})}{\rho_{\sigma, \boldsymbol{c}}(\Lambda)}$ for any $\boldsymbol{x} \in \Lambda$. For $\delta > 0$, we define the smoothing parameter $\eta_\delta(\Lambda)$ as the smallest $\sigma > 0$ such that $\rho_{\frac{1}{\sigma}}(\Lambda^\vee \setminus \boldsymbol{0}) \le \delta$. The following theorem comes from [26]. Here we use $\tilde{B}$ to represent the Gram-Schmidt orthogonalization of B and regard the columns of B as a set of vectors. For $B = (b_1, \cdots, b_n)$, define $||B|| = \max_i ||b_i||$.

Theorem 1. *There is a probabilistic polynomial time algorithm that, given a basis B of an n-dimensional lattice $\Lambda = \mathcal{L}(B)$, a standard deviation $\sigma \geq ||\tilde{B}|| \cdot \sqrt{\log n}$, and a $\boldsymbol{c} \in H$, outputs a sample whose distribution is $D_{\Lambda,\sigma,\boldsymbol{c}}$.*

We will also use the following lemmas from [23], [25] and [13].

Lemma 2. *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 3. *For any full-rank lattice Λ, $\boldsymbol{c} \in H$, $\varepsilon \in (0,1)$ and $\sigma \geq \eta_\varepsilon(\Lambda)$, 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 4. *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 5. *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 $\Delta(D_{\Lambda,\sigma,\boldsymbol{c}} \bmod \Lambda', U(\Lambda/\Lambda')) \leq 2\varepsilon$.*

It is convenient for us to use the notion of subguassian random variables in our application. We describe the definitions as in [24].

Definition 3. *For $\delta \geq 0$, a real-valued random variable X is δ-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 δ-subgaussian random variable with scaled parameter $s \geq 0$ if

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

A real-valued random variable is δ-subgaussian with standard parameter b if and only if it is δ-subgaussian with scaled parameter $\sqrt{2\pi}b$. One can extend the definitions to $\mathbb{R}^n$ or space H.

Definition 4. *For any $\delta \geq 0$, a multivariate random variable $\boldsymbol{X}$ on $\mathbb{R}^n$ is δ-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 δ-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 δ-subgaussian with standard parameter b if for all unit vector $\boldsymbol{t}$, the random variable $<\boldsymbol{X}, \boldsymbol{t}>$ is δ-subgaussian with standard parameter b.

Definition 5. *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 subgaussian random variable. Moreover, we have the following useful lemma which is proposed in [24].

Lemma 6. *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* $(d^2_{\boldsymbol{Z}} + (\frac{1}{2})^2 s_1(B)^2)^{\frac{1}{2}}$*.*

2.5 Basis for R and $R^\vee$, Ring-LWE problem

In our application, we hope that the matrices whose columns are consisted of the basis of R or $R^\vee$ have smaller s_1 and larger s_n. So, we introduce the powerful basis and the decoding basis as in [22]. 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 $\sigma(\tau(a)) = \overline{\sigma(a)}$.

Definition 6. *The Powerful basis* $\overrightarrow{p}$ *of* $K = \mathbb{Q}(\zeta_l)$ *and* $R = \mathbb{Z}[\zeta_l]$ *is defined as follows:*

- *For a prime power* l*, define* $\overrightarrow{p}$ *to be the power basis* $(\zeta_l^j)_{(j\in\{0,1,\cdots,n-1\})}$*, treated as a vector over* $R \subseteq K$*.*
- *For* l *having prime-power factorization* $l = \prod l_k = \prod p_k^{\alpha_k}$*, define* $\overrightarrow{p} = \otimes_k \overrightarrow{p_k}$*, the tensor product of the power basis* $\overrightarrow{p_k}$ *of each* $K_k = \mathbb{Q}(\zeta_{l_k})$*.*

The Decoding basis of $R^\vee$ *is* $\overrightarrow{d} = \tau(\overrightarrow{p})^\vee$*, the dual of the conjugate of the powerful basis* $\overrightarrow{p}$*.*

Different bases of R (or $R^\vee$) are connected by some unimodular matric, hence the spectral norm (i.e. the s_1) may have different magnitudes. The following lemma comes from [22], which shows the estimates of $s_1(\sigma(\overrightarrow{p}))$ and $s_n(\sigma(\overrightarrow{p}))$.

Lemma 7. *We have* $s_1(\sigma(\overrightarrow{p})) = \sqrt{\hat{l}}$*,* $s_n(\sigma(\overrightarrow{p})) = \sqrt{\frac{l}{rad(l)}}$ *and* $||\sigma(\overrightarrow{p})_i|| = \sqrt{n}$ *for all* $i = 1, \cdots, n$*.*

We also need the estimates of $s_1(\sigma(\overrightarrow{d}))$ and $s_n(\sigma(\overrightarrow{d}))$. Assume that $\sigma(\overrightarrow{p}) = T$, Lemma 7 shows that $s_1(T) = \sqrt{\hat{l}}$ and $s_n(T) = \sqrt{\frac{l}{rad(l)}}$. By the definitions of $\overrightarrow{d}$ and the dual ideal, an easy computation shows that $\sigma(\overrightarrow{d}) = (T^*)^{-1}$. Hence we have $s_n(\sigma(\overrightarrow{d})) = \frac{1}{\sqrt{\hat{l}}}$, $s_1(\sigma(\overrightarrow{d})) = \sqrt{\frac{rad(l)}{l}}$. Moreover, one can similarly deduce

that $||\sigma(\overrightarrow{d})_i|| \leq \sqrt{\frac{rad(l)}{l}}$ for all $i = 1, 2, \cdots, n$. The following definition is also useful.

Definition 7. *Given a basis B of a fractional ideal J, for any $x \in J$ with $x = x_1 b_1 + \cdots + x_n b_n$, the B-coefficient embedding of x is defined as the vector $(x_1, \cdots, x_n)$ and the B-coefficient embedding norm of x is defined as $||x||_B^c = (\sum_{i=1}^n x_i^2)^{\frac{1}{2}}$.*

If we represent $x \in R$ (or $R^\vee$) with respect to the powerful basis (or decoding basis), we have

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

and

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

We will omit the subscript $\sigma(\overrightarrow{d})$ of $||\cdot||^c_{\sigma(\overrightarrow{d})}$ in the following applications. When we write $x \bmod qR^\vee$, we use the representative element of the coset $x + qR^\vee$ as $\sum_{i=1}^n x_i \overrightarrow{d}_i$ with $x_i \in [-\frac{q}{2}, \frac{q}{2})$. From now on, we only use the decoding basis of $R^\vee$ and the powerful basis of R.

The Ring-LWE distribution and Ring-LWE problem are defined as those in [22]. Define $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$.

Definition 8. *For a distribution ψ over $K_{\mathbb{R}}$ and a secret $s \hookleftarrow \lfloor \psi \rceil_{R^\vee} \in R_q^\vee$, a sample from* Ring-LWE *distribution $A^\times_{s,\psi}$ over $R_q^\times \times R_q^\vee$ is generated by choosing $a \hookleftarrow U(R_q^\times)$, $e \hookleftarrow \lfloor \psi \rceil_{R^\vee}$ and outputting $(a, b = a \cdot s + e \bmod qR^\vee)$. The average-case decision version of the* Ring-LWE *problem, denoted by* R-DLWE$^\times_{q,\psi}$*, is to distinguish with non-negligible advantage between independent samples from $A^\times_{s,\psi}$, and the same number of uniformly random and independent samples from $R_q^\times \times R_q^\vee$.*

Theorem 2. *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 $q = q(n) \geq 2$, $q = 1 \bmod l$ 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$^\times_{q,\psi}$ *given only k samples, where ψ is the Gaussian distribution $D_{\xi \cdot q}$ with $\xi = \alpha \cdot (\frac{nk}{\log(nk)})^{\frac{1}{4}}$.*

3 Some New Results on q-Ary Lattices

In this section, we shall prove some useful results which will be used in Sect. 4.

3.1 q-Ary Lattices

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 $\phi_i = \omega^{l_i}$, where l_i is the i-th element in $\mathbb{Z}_l^\times$, then $\Phi_l(x) = \prod_{i=1}^n (x-\phi_i) = \prod_{i=1}^n (x-\phi_i^{-1}) \bmod q$. 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 non-empty $S \subseteq \{1, 2, \cdots, n\}$. Since any monomials of the form $x - \alpha$ with $\alpha \neq \phi_i$ for $i = 1, 2, \cdots, n$ is an invertible element in R_q, any principal ideal of R_q is of the form described above. We will use I_S to represent the ideal $\prod_{i\in S}(x-\phi_i)R_q$ of R_q.

Let I be a proper ideal of R_q, there is a unique ideal J of R such that $qR \subseteq J \subseteq R$ and $I = J/qR$. In fact, if we set $I = f(x)R_q$, then $J = (f(x), q)R$. 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 an R module inclusion relations

$$qR^\vee \subseteq qJ^\vee \subseteq R^\vee \subseteq J^\vee. \tag{3}$$

Moreover, $R^\vee/qJ^\vee$ is an R submodule of $J^\vee/qJ^\vee$. Let $\boldsymbol{a} \in (R_q)^m$, the definitions of the q-ary lattices are as followings:

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

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

Here, $R^\vee \cdot \boldsymbol{a} = \{t \cdot \boldsymbol{a} = (ta_1, \cdots, ta_m) : t \in R^\vee\}$. We also define $\boldsymbol{a}^\perp$ and $L(\boldsymbol{a})$ as $\boldsymbol{a}^\perp(R_q)$ and $L(\boldsymbol{a}, R_q)$. The dual $M^\vee$ of a lattice $M \subseteq K^m$ is defined as the set of all $\boldsymbol{x} \in K^m$ such that $\mathrm{Tr}(\boldsymbol{x} \cdot \boldsymbol{v}) := \sum_{j=1}^m \mathrm{Tr}(x_j \cdot v_j) \in \mathbb{Z}$ for all $\boldsymbol{v} \in M$. The following lemma shows the dual relations between $\boldsymbol{a}^\perp(I)$ and $L(\boldsymbol{a}, I)$.

Lemma 8. *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 only need to prove $\boldsymbol{a}^\perp(I) = q(L(\boldsymbol{a}, I))^\vee$, since the other equality can be easily deduced by taking dual in both side of $\boldsymbol{a}^\perp(I) = q(L(\boldsymbol{a}, I))^\vee$.

We start with showing that $\boldsymbol{a}^\perp(I) \subseteq q(L(\boldsymbol{a}, I))^\vee$. For any $\boldsymbol{t} \in \boldsymbol{a}^\perp(I)$ and $\boldsymbol{z} \in L(\boldsymbol{a}, I)$, we only need to show $\sum_{i=1}^m \mathrm{Tr}(t_i \cdot z_i) = 0 \bmod q\mathbb{Z}$. 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 $q(L(\boldsymbol{a}, I))^\vee \subseteq \boldsymbol{a}^\perp(I)$. For any $\boldsymbol{x} \in (L(\boldsymbol{a}, I))^\vee$, 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 $q \cdot x_i \in J$. Note that $\forall\, \boldsymbol{t} \in L(\boldsymbol{a}, I)$, $\sum_{i=1}^{m} \mathrm{Tr}(x_i \cdot t_i) \in \mathbb{Z}$. 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 $\boldsymbol{a}^\perp(I) = q(L(\boldsymbol{a}, I))^\vee$. We finish the proof.

3.2 Lower Bound of λ_1^∞ in $L(\boldsymbol{a}, I)$

In this section, we shall give an estimate of the lower bound of λ_1^∞ for $L(\boldsymbol{a}, I)$ with $\boldsymbol{a} \hookleftarrow U((R_q^\times)^m)$, where λ_1^∞ is the length of a shortest vector (corresponding to the l_∞ norm) in the lattice $L(\boldsymbol{a}, I)$. The proof mainly follows the thoughts of [29]. Let $I_S = \prod_{i \in S}(x - \phi_i)R_q \subseteq R_q$ and $J_S = (f_S(x), q)R \subseteq R$, where $f_S(x) = \prod_{i \in S}(x - \phi_i)$ for $S \subseteq \{1, 2, \cdots, n\}$. The factorization of ideal $(q)R$ is $\prod_{i=1}^{n} \mathfrak{q}_i$ with $\mathfrak{q}_i = (q, x - \phi_i)R$. Since R is a Dedekind domain, each $\mathfrak{q}_\mathfrak{i}$ is a maximal ideal, hence $\mathfrak{q}_\mathfrak{i}$ and $\mathfrak{q}_\mathfrak{j}$ is coprime for any $i \neq j \in [n]$, $\mathfrak{q}_\mathfrak{i} \cdot \mathfrak{q}_\mathfrak{j} = \mathfrak{q}_\mathfrak{i} \cap \mathfrak{q}_\mathfrak{j} = (q, (x - \phi_i)(x - \phi_j))R$. Therefore, $J_S = \prod_{i \in S} \mathfrak{q}_i$, $J_S^{-1} = \prod_{i \in S} \mathfrak{q}_i^{-1}$. Further, we have $J_S^\vee = \prod_{i \in S} \mathfrak{q}_i^{-1} R^\vee$.

Lemma 9. *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 $p \leq 2^{(3m+1)n} q^{-\varepsilon m n}$ 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 $< B = \frac{q^\beta}{n}$. Recall that, $\boldsymbol{t} \in L(\boldsymbol{a}, I_S)$ if and only if there is an $s \in R^\vee$ such that $t_i = a_i \cdot s \bmod qJ_S^\vee$ for all $i \in [m]$. Meanwhile, for any $s \in R^\vee$, all the elements of the coset $s + qJ_S^\vee$ satisfy the equation $t_i = a_i \cdot s \bmod qJ_S^\vee$ for the same t_i. We give an upper bound of p by the union bound, summing the probabilities $p(\boldsymbol{t}, s) = \Pr_{\boldsymbol{a}}[\, t_i = a_i \cdot s \bmod qJ_S^\vee,\ \forall i \in [m]]$ over all possible values of $\boldsymbol{t}$ of infinity norm $< B$ and $s \in R^\vee/(qJ_S^\vee)$. Since the $\{a_i\}_{i=1}^m$ are independent, we have $p(\boldsymbol{t}, s) = \prod_{i \leq m} p_i(t_i, s)$, where $p_i(t_i, s) = \Pr_{a_i}[t_i = a_i \cdot s \bmod qJ_S^\vee]$. So, we have

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

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 $S' = [n] \setminus S$. We have an isomorphism 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 $i_j \in S'$ for $j = 1, \cdots, |S'|$. 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 for the case $p_i(a_i, s) \neq 0$, 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 $s = 0 \bmod \mathfrak{q}_j R^\vee$ and $t_i \neq 0 \bmod \mathfrak{q}_j R^\vee$, or $s \neq 0 \bmod \mathfrak{q}_j R^\vee$ and $t_i = 0 \bmod \mathfrak{q}_j R^\vee$. In both cases, we have $p_i(a_i, s) = 0$, since $a_i \in R_q^\times$. Then, for $j \in S''$, we have $t_i = a_i \cdot s = 0 \bmod \mathfrak{q}_j R^\vee$, regardless of the value of $a_i \in R_q^\times$. For any $j \in S' \setminus S''$, we have $t_i = a_i \cdot s \neq 0 \bmod \mathfrak{q}_j R^\vee$, the value of a_i is unique, since $s \neq 0 \bmod \mathfrak{q}_j R^\vee$ 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 that there are $(q-1)^{n+d-|S'|}$ different a_i in $R_q^\times$ satisfy $t_i = a_i \cdot s \bmod qJ_S^\vee$, i.e. $p_i(t_i, s) = (q-1)^{d-|S'|}$. Therefore, we can rewrite the sum's conditions by

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

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

Case 1: Suppose that $d \geq \beta \cdot n$. Since $t \in \mathfrak{h} = \prod_{i\in S''} \mathfrak{q}_i R^\vee$, and $\mathfrak{h}$ is a fractional ideal of K, we have $(t) = tR^\vee \subseteq \mathfrak{h}$ and (t) is a full-rank R-submodule of $\mathfrak{h}$. Hence,

$$|\mathrm{N}(t)| = \mathrm{N}((t)) \geq \mathrm{N}(\mathfrak{h}) \geq \mathrm{N}(\prod_{i\in S''} \mathfrak{q}_i \cdot R^\vee) = (\prod_{i\in S''} \mathrm{N}(\mathfrak{q}_i))\mathrm{N}(R^\vee) = q^d \cdot |\Delta_K|^{-1}.$$

Note that $|\Delta_K| \leq n^n$, we have $|\mathrm{N}(t)| \geq \frac{q^d}{n^n}$ and conclude that

$$||t||_\infty \geq \frac{1}{\sqrt{n}}||t|| \geq |\mathrm{N}^{\frac{1}{n}}(t)| \geq \frac{q^{\frac{d}{n}}}{n} \geq \frac{q^\beta}{n} = B. \tag{4}$$

Case 2: 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 different 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,

$$N(B, d) \leq \frac{vol(\mathfrak{B}(B + \lambda, 0))}{vol(\mathfrak{B}(\lambda, 0))} = (\frac{B}{\lambda} + 1)^n \leq (2q^{\beta - \frac{d}{n}} + 1)^n \leq 2^{2n} q^{n\beta - d},$$

where we have used the fact that $\lambda_1^\infty(\mathfrak{h}) \geq \frac{q^{\frac{d}{n}}}{n}$ from (4).

We claim that the number of $s \in R^\vee/(qJ_S^\vee)$ and $s \in \mathfrak{h}$ is $q^{|S'|-d}$. In fact, if s satisfies the above conditions, $s \in \mathfrak{h}/(qJ_S^\vee)$. Using a kind of isomorphism relation

(Lemma 2.14 in [21]) which states that for any fractional ideals $\mathfrak{a}$, $\mathfrak{b}$ and integral ideal $\mathfrak{c}$ with $\mathfrak{b} \subseteq \mathfrak{a}$, $\mathfrak{ac}/\mathfrak{bc} \cong \mathfrak{a}/\mathfrak{b}$, we have

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

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

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

We finish the proof.

Remark: The estimate of $N(B,d)$ in the case $d < \beta\cdot n$ is originally inspired by [32], it may be standard. This lemma and the following regularity theorem can be regarded as a special case of Lemma 5.2 and Theorem 5.3 in [28].

3.3 Improved Results on Regularity

In this subsection, we discuss the regularity results of any cyclotomic ring. The following result is a direct consequence of Lemmata 4, 5, 8 and 9. By Lemmas 9 and 8, we have $\lambda_1^\infty((\boldsymbol{a}^\perp(I_S))^\vee) = \frac{1}{q}\lambda_1^\infty(L(\boldsymbol{a}, I_S)) \ge \frac{1}{n} q^{\frac{|S|}{mn}-\frac{|S|}{n}-\frac{1}{m}-\varepsilon}$, except with a fraction of $2^{(3m+1)n} q^{-\varepsilon mn}$ of $\boldsymbol{a} \in (R_q^\times)^m$ for $S \subseteq [n]$ and $m \ge 2$. Then Lemma 4 tells us that $\eta_\delta((a^\perp(I_S))^\vee) \le n\sqrt{\frac{\ln(2mn(1+\frac{1}{\delta}))}{\pi}} \cdot q^{\frac{|S|}{n}+\frac{1}{m}-\frac{|S|}{mn}+\varepsilon}$ for any $\delta > 0$. Therefore, Lemma 5 gives us the following lemma.

Lemma 10. *Let $q = 1 \bmod l$ be a prime, $K = \mathbb{Q}(\zeta_l)$, $R = \mathcal{O}_K$, $m \ge 2$, $\delta \in (0, \frac{1}{2})$, $\varepsilon > 0$, $S \subseteq [n]$, $\boldsymbol{c} \in R^m$ and $\boldsymbol{t} \hookleftarrow D_{R^m,\sigma,\boldsymbol{c}}$, where $\sigma \ge n\sqrt{\frac{\ln(2mn(1+\frac{1}{\delta}))}{\pi}} \cdot q^{\frac{|S|}{n}+\frac{1}{m}-\frac{|S|}{mn}+\varepsilon}$. Then for all except a fraction of $2^{(3m+1)n} q^{-\varepsilon mn}$ of $\boldsymbol{a} \in (R_q^\times)^m$, we have*

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

Let $\mathbb{D}_\chi$ be 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 $a_i \hookleftarrow U(R_q^\times)$ are chosen independently and $\boldsymbol{t} \hookleftarrow D_{R^m,\sigma}$. 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 $U((R_q^\times)^m \times R_q)$. Note that for each $\boldsymbol{a} \hookleftarrow U((R_q^\times)^m)$, the map $\boldsymbol{t} \mapsto \sum_{i=1}^m a_i t_i$ induces an isomorphism from the quotient $R^m/\boldsymbol{a}^\perp$ to its range. The latter is R_q, thanks to the invertibility of a_i's. By taking $S = \phi$ and $\boldsymbol{c} = 0$ in Lemma 10, we deduce the following result.

Theorem 3. *Let $q = 1 \bmod l$ be a prime, $K = \mathbb{Q}(\zeta_l)$, $R = \mathcal{O}_K$, $m \geq 2$, $\delta \in (0, \frac{1}{2})$, $\varepsilon > 0$ and $a_i \hookleftarrow U(R_q^\times)$ for all $i \in [m]$. 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 Sect. 3, we can derive a key generation algorithm for NTRUEncrypt as in [29]. Further, by choosing appropriate parameters, we can show that the key generation algorithm terminates in expected time and the public key distribution is very closed to the uniform distribution.

The key generation algorithm is as follows:

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

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

Notice that for powerful basis $\overrightarrow{p}$ of R, we have $||\overrightarrow{p}|| = \sqrt{n}$. Hence, as long as $\sigma \geq \sqrt{n} \cdot \sqrt{\log n}$, we can sample an element in polynomial time to obey the distribution $D_{R,\sigma}$ by using Theorem 1. The following lemma shows that the key generation algorithm can terminate with high probability by executing only several times. Proofs in this section are standard and are put in Appendix A.

Lemma 11. *Let l be a positive integer, $n = \varphi(l)$ and q be a prime such that $q = 1 \bmod l$. Assume $\sigma \geq n \cdot \sqrt{\frac{\ln(2n(1+\frac{1}{\varepsilon}))}{\pi}} \cdot q^{\frac{1}{n}}$, for an arbitrary $\varepsilon \in (0, \frac{1}{2})$. Let $a \in R$ and $p \in R_q^\times$. Then*

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

Next, we show that the generated secret key by the key generation algorithm is short. This lemma is very useful for us to analyze the decryption error in Sect. 5.

Lemma 12. *Let $n \geq 5$, $q \geq 8n$, $q = 1 \bmod l$ be a prime and $\sigma \geq \sqrt{\frac{2\ln(6n)}{\pi}} \cdot n \cdot q^{\frac{1}{n}}$. Then with probability at least $1 - 2^{3-n}$, the secret key f, g satisfy $||f|| \leq 2\sqrt{n}\sigma||p||_\infty$ and $||g|| \leq \sqrt{n}\sigma$.*

The last lemma of this section estimates the statistic distance between the distribution of public key and the uniform distribution over $R_q^\times$. The proof is essentially the same as Theorem 3 in [29]. We denote by $D_{\sigma,z}^\times$ the discrete Gaussian $D_{R,\sigma}$ restricted to $R_q^\times + z$.

Lemma 13. *Let $\varepsilon > 0$, $n \geq 5$, $q \geq 8n$ 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 $z_i = -y_i p^{-1} \bmod qR$ for $i \in \{1, 2\}$. Then*

$$\Delta\left[\frac{y_1 + p \cdot D_{\sigma,z_1}^\times}{y_2 + p \cdot D_{\sigma,z_2}^\times} \bmod qR,\ U(R_q^\times)\right] \leq \frac{2^{9n}}{q^{\lfloor \varepsilon n \rfloor}}.$$

5 NTRUEncrypt Scheme and Security Analysis

In this section, we give our modified NTRUEncrypt. Meanwhile, we shall analyze the decryption error and give an elementary reduction from R-DLWE$_{q,D_{q\xi}}^\times$ to the CPA-security of our scheme.

The plaintext space of our scheme is $\mathcal{P} = R^\vee/pR^\vee$ with $p \in R_q^\times$. Denote $\chi = \lfloor D_{\xi \cdot q} \rceil_{R^\vee}$ with $\xi = \alpha \cdot (\frac{nk}{\log(nk)})^{\frac{1}{4}}$, where $k = O(1)$ is a positive integer. We will use the decoding basis for element $x \in R \subseteq R^\vee$. One should note that $f = 1 \bmod pR$ implies $f = 1 \bmod pR^\vee$.

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

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

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

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

Lemma 14. *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 of $R^\vee$, 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 6. Therefore, by the Definition 5, 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 $\frac{1}{2}\cdot\left(\frac{q^2\xi^2}{2\pi}+\frac{1}{4}s_1^2(B)\right)\cdot||\boldsymbol{t}||^2 = \Omega(\alpha^2\cdot q^2\cdot\sqrt{n}\log^{-\frac{1}{2}} n\cdot||\boldsymbol{t}||^2)$. Therefore,

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

We finish the proof.

By using Lemma 14, we can get an estimate for $||\boldsymbol{x}||_\infty$ with $\boldsymbol{x} \hookleftarrow \chi = \lfloor D_{q\cdot\xi} \rceil$. Choosing $\boldsymbol{t} = (\frac{1}{\sqrt{2}}, 0, \cdots, 0, \frac{1}{\sqrt{2}})$ and $\boldsymbol{t} = (\frac{\boldsymbol{i}}{\sqrt{2}}, 0, \cdots, 0, -\frac{\boldsymbol{i}}{\sqrt{2}})$, where $\boldsymbol{i}$ is the imaginary number such that $\boldsymbol{i}^2 = -1$, 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 $\Pr_{\boldsymbol{x}\hookleftarrow\chi}(|\sigma_1(x)| > \omega(\sqrt{n\log n}\alpha^2q^2)) \leq 2n^{-\omega(\sqrt{n\log n})}$. Similarly, one can also prove that $\Pr_{\boldsymbol{x}\hookleftarrow\chi}(|\sigma_k(x)| > \omega(\sqrt{n\log n}\alpha^2q^2)) \leq 2n^{-\omega(\sqrt{n\log n})}$ for any $k = 1, 2\cdots, \frac{n}{2}$. Therefore, we conclude that

$$\Pr_{\boldsymbol{x}\hookleftarrow\chi}(||\sigma(x)||_\infty > \omega(\sqrt{n\log n}\cdot\alpha^2\cdot q^2)) \leq n\cdot n^{-\omega(\sqrt{n\log n})} \leq n^{-\omega'(\sqrt{n\log n})}. \tag{5}$$

In order to show that the decryption algorithm succeeds in recovering the correct message with high probability, we need the parameters C_1 and C_2 such that $C_1||x||^c \leq ||x|| \leq C_2||x||^c$.

Lemma 15. *Let $n \geq 5$, $q \geq 8n$, $q = 1 \bmod l$, $\sigma \geq \sqrt{\frac{2\ln(6n)}{\pi}}\cdot n\cdot q^{\frac{1}{n}}$, $C_1 = \sqrt{\hat{l}}$ and $C_2 = \sqrt{\frac{rad(l)}{l}}$. If $\omega(n^{\frac{3}{2}}\sqrt{\log n\log\log n})\cdot\alpha^2\cdot q^2\cdot\sigma\cdot||p||_\infty^2 < \frac{q}{2}$, then with probability $1-n^{-\omega(\sqrt{n\log n})}$, the decryption algorithm of* NTRUEncrtpt *recovers m.*

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

Note that $||fc||_\infty^c \leq ||fc||^c \leq C_1||fc|| = C_1||pgs+pfe+fm|| \leq C_1(||pgs|| + ||pfe|| + ||fm||)$. By the choice of σ and Lemma 12, with probability greater than

$1-2^{3-n}$, $||f|| \leq 2\sqrt{n}\sigma||p||_\infty$ and $||g|| \leq \sqrt{n}\sigma$. Hence, combining with (5), we get

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

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

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

where we have used that

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

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

$$\begin{aligned} ||fc||_\infty^c &\leq C_1(\omega(n\sqrt{\log n} \cdot \alpha^2 \cdot q^2) \cdot \sigma \cdot ||p||_\infty^2 + n \cdot \sigma \cdot ||p||_\infty^2 \cdot C_2) \\ &\leq \omega(n^{\frac{3}{2}}\sqrt{\log n \log\log n} \cdot \alpha^2 \cdot q^2) \cdot \sigma \cdot ||p||_\infty^2 \end{aligned}$$

with probability $1-n^{-\omega(\sqrt{sn\log n})}$, where we have used the fact that $C_2 \leq 1$ and $C_1 = O(\sqrt{n\log\log n})$. We conclude the results we need.

Remark 1. We remark that we can put all computations in an integral ideal $I = \hat{l} \cdot R^\vee \subseteq R$ by multiplying an integer $\hat{l}$(in this case, the corresponding q is $\hat{l}$ times bigger than the q in Lemma 15). 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 $f = 1 \bmod pR^\vee$, we have $\hat{l} \cdot f = \hat{l} \bmod pI$. Therefore, $\hat{m} = \hat{l}^{-1}(\hat{l}((f \cdot \hat{c} \bmod qI) \bmod pI) \bmod pI)$ with $\hat{m} \in I/(pI)$ and $gcd(p, \hat{l}) = 1$. Since the corresponding 'decoding basis' of I is connected with the usual power basis of R by an invertible matrix $M \in \mathbb{Z}^{n\times n}$, this modification may enjoy the high computation speed over polynomial rings.

Remark 2. By using the recent hardness results about primal-Ring-LWE (i.e. the secret $s \hookleftarrow U(R_q)$) proved in [28], we can directly design NTRUEncrypt in R. If we set $\mathcal{P} = R/pR$ and choose $s, e \hookleftarrow \lfloor D_{\xi \cdot q} \rceil_R$ (techniques used in [22, Lemma 2.23] can be modified to R), then the same encryption and decryption process also work. In this case, we use the powerful basis of R. Correspondingly, if we set $\alpha \cdot q = \omega(\sqrt{\log n})$, magnitudes of $||s||_\infty$ and $||e||_\infty$ are $\tilde{O}(n)$. Then, we can estimate that $q = \tilde{O}(\sqrt{\frac{rad(l)}{l}} \cdot n^{\frac{3}{2}} \cdot \sigma)$ is sufficient to decrypt correctly with probability greater than $1-n^{-\tilde{O}(n)}$. Therefore, we have $q = \tilde{O}(n^6 \cdot \sqrt{\frac{rad(l)}{l}}) \in (\tilde{O}(n^5), \tilde{O}(n^6)]$. But, the reduction parameter $\gamma \leq \tilde{O}(n^{12.5})$, due to the reduction loss of primal-Ring-LWE problem, see [28]. In this situation, we can have high efficiency with weaker hardness guarantee, so, an assessment from the view of actual attacks need be done as in [8].

Remark 3. The reason why we constrain our NTRUEncrypt schemes in cyclotomic fields is that we want to use the decoding basis of $R^\vee$. If a general number field has such a good basis, we can also design NTRUEncrypt over general fields by using our techniques, together with the hardness results showed in [27]. More details are discussed in [30].

Remark 4. By using similar techniques, we can also give a module version of NTRUEncrypt. The security reduction of this modified version of NTRUEncrypt can be reduced to the corresponding Module-LWE problems. More details are put in Appendix B.

The security of our 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 $p \in R_q$. We put the proof in Appendix C.

Lemma 16. *Let* $n \geq 5$, $q \geq 8n$, $q = 1 \bmod l$, $\sigma \geq \sqrt{\ln(8nq)} \cdot n^{\frac{3}{2}} \cdot q^{\frac{1}{2}+\varepsilon}$, $\delta > 0$ *and* $\varepsilon \in (0, \frac{1}{2})$. *If there exists an IND-CPA attack against* NTRUEncrypt *that runs in time* T *with advantage* δ, *then there exists an algorithm solving* R-DLWE$^{\times}$ *with parameters* q *and* $q\xi$ *that runs in time* $T' = T + O(n)$ *with advantage* $\delta' = \delta - q^{-\Omega(n)}$.

In a summary, we have the following result.

Theorem 4. *Let* l *be a positive integer,* $n = \varphi(l) \geq 5$, $q \geq 8n$, $q = 1 \bmod l$ *be a prime of size* $poly(n)$ *and* $K = \mathbb{Q}(\zeta_l)$. *Assume that* $\alpha \in (0, 1)$ *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* $poly(n)$ *with advantage* $\frac{1}{poly(n)}$, *there exists a* $poly(n)$*-time algorithm solving* Ideal-SIVP$_\gamma$ *on any ideal lattice of* K *with* $\gamma = \tilde{O}(\frac{\sqrt{n}}{\alpha})$. *Moreover, the decryption algorithm succeeds in regaining the correct message with probability* $1 - n^{-\omega(\sqrt{n \log n})}$ *over the choice of the encryption randomness.*

To sum up, though the magnitude of q is little far away from practicality, the biggest advantage of our scheme is that it is less dependent on the choice of p and is not limited by the cyclotomic fields it bases on. Hence, our schemes provide more flexibility for the choices of plaintext spaces and get rid of the dependence of the cyclotomic fields, 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 in recovering the correct message with a probability of $1 - n^{-\omega(\sqrt{n \log n})}$, while the previous works were $1 - n^{-\omega(1)}$. Therefore, we believe, our scheme may have more advantages in theory.

Acknowledgement. We would like to express our gratitude to Bin Guan and Yang Yu for helpful discussions. We also thank the anonymous SAC'18 reviewers for their

valuable comments and suggestions. The authors are supported by National Cryptography Development Fund (Grant No. MMJJ20180210), NSFC Grant 61832012, NSFC Grant 61672019 and the Fundamental Research Funds of Shandong University (Grant No. 2016JC029).

A Missing Proofs in Sect. 4

Proof of Lemma 11: 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 $i \le n$. By Lemma 1 and the properties of cyclotomic ring, we have $\lambda_1(\mathfrak{q}_i) = \lambda_n(\mathfrak{q}_i) \le \sqrt{n} N(\mathfrak{q}_i)^{\frac{1}{n}} (\sqrt{|\Delta_K|})^{\frac{1}{n}} \le n q^{\frac{1}{n}}$. By Lemmas 2 and 5, we know that $f' \bmod \mathfrak{q}_i$ is within distance 2ε to uniformity on $R/\mathfrak{q}_i$, so we have $f' = -a/p \bmod \mathfrak{q}_i$ with probability less than $\frac{1}{q} + 2\varepsilon$ as we need.

Proof of Lemma 12: Set $\varepsilon = \frac{1}{3n-1}$. Note that $\lambda_n(R) = \lambda_1(R) \le \sqrt{n} \cdot (\sqrt{|\Delta_K|})^{\frac{1}{n}} \le n$. By Lemma 2, we have $\eta_\varepsilon(R) \le \sqrt{\frac{2\ln(6n)}{\pi}} \cdot n$. Hence, $\Pr_{x \hookleftarrow D_{R,\sigma,c}}(||x|| \ge \sqrt{n}\sigma) \le \frac{3n}{3n-2} 2^{-n}$. Meanwhile, σ satisfies the condition in Lemma 11, so we get

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

Therefore, we have $||f'||,\ ||g|| \le \sqrt{n}\sigma$ with probability no less than $1 - 2^{3-n}$. Moreover we can estimate $||f|| \le 1 + ||p||_\infty \cdot ||f'|| \le 2\sqrt{n}\sigma ||p||_\infty$.

Proof of Lemma 13: 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 $|\Pr_a - (q-1)^{-n}| \le 2^{2n+5} q^{-\lfloor \varepsilon n \rfloor} \cdot (q-1)^{-n} =: \varepsilon'$ except a fraction $\le 2^{8n} q^{-2n\varepsilon}$ of $a \in R_q^\times$. Note that $a_1 f_1 + a_2 f_2 = a_1 z_1 + a_2 z_2$ is equivalent to $(y_1 + pf_1)/(y_2 + pf_2) = -a_2/a_1$ in $R_q^\times$ and $-a_2/a_1 \hookleftarrow U(R_q^\times)$ when $\boldsymbol{a} \hookleftarrow U(R_q^\times)^2$, we get $\Pr_{\boldsymbol{a}} := \Pr_{f_1,f_2}[a_1 f_1 + a_2 f_2 = a_1 z_1 + a_2 z_2] = \Pr_{-a_2/a_1}$ 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 $a_1 f_1 + a_2 f_2 = a_1 z_1 + a_2 z_2 \bmod qR$ 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 $\boldsymbol{a}^{\perp\times} = \boldsymbol{a}^\perp \setminus (\cup_{I \subseteq R_q} \boldsymbol{a}^\perp(I)) =$

$\boldsymbol{a}^{\perp}\backslash(\cup_{S\subseteq[n],S\neq\phi}\boldsymbol{a}^{\perp}(I_S))$. Similarly, we have $R_q^{\times}+qR = R\backslash(\cup_{S\subseteq[n],S\neq\phi}(I_S+qR))$. Using the inclusion-exclusion principal, we get

$$D_{R^2,\sigma}(\boldsymbol{z}+\boldsymbol{a}^{\perp\times}) = \sum_{S\subseteq[n]}(-1)^{|S|}\cdot D_{R^2,\sigma}(\boldsymbol{z}+\boldsymbol{a}^{\perp}(I_S)), \tag{6}$$

$$D_{R,\sigma}(z_i+R_q^{\times}+qR) = \sum_{S\subseteq[n]}(-1)^{|S|}\cdot D_{R,\sigma}(z_i+I_S+qR), \quad \forall\, i\in\{1,\ 2\}. \tag{7}$$

In the rest of the proof, we show that, except for a fraction $\leq 2^{8n}q^{-2n\varepsilon}$ of $\boldsymbol{a}\in(R_q^{\times})^2$:

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

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

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 (6): When $|S|\leq\varepsilon n$, we apply Lemma 10 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 above, 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 $\leq\frac{2^{8n}}{q^{2n\varepsilon}}$ 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 (7): Note that for any $S\in[n]$, $\det(I_S+qR) = |R/J_S|\cdot\sqrt{|\Delta_K|} = q^{|S|}\cdot\sqrt{|\Delta_K|}$, where J_S is the ideal of R such that $J_S/(qR) = I_S$. By Minkowski's Theorem, we have $\lambda_1(I_S+qR) = \lambda_n(I_S+qR)\leq n\cdot q^{\frac{|S|}{n}}$. Lemma 2 implies that

$\sigma > \eta_\delta(I_S + qR)$ for any $|S| \leq \frac{n}{2}$ with $\delta = q^{-\frac{n}{2}}$. Therefore, Lemma 5 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 for $i = 1,\ 2$.

B Module NTRUEncrypt

The hardness assumption of Ring-LWE may be possible weaker than the classic LWE: classic LWE is known to be as hard as the standard worst-case problems on Euclidean lattices, whereas Ring-LWE is only known to be as hard as their restrictions to special classes of ideal lattices which are a subset of Euclidean lattices. To 'overcome' this shortcoming, Langlois and Stehlé gave some worst-case to average-case reducitons for module lattices in 2015. In this section, we give a modified version of NTRUEncrypt over modules and a reduction from Module-LWE to the Module-NTRUEncrypt.

B.1 Basic Hard Problems

We first introduce some basic definitions and corresponding results about Module-LWE (MLWE). A subset $M \subseteq K^d$ is an R-module if it is closed under addition and under multiplication by elements of R. It is a finitely generated module if there exists a finite family $\{\boldsymbol{b}_k\}$ of vectors in K^d such that $M = \sum_k R \cdot \boldsymbol{b}_k$. When K is a cyclotomic field as we required, there exists a so-called pseudo-bases for M as stated in [19]: For every module M, there exist $I_{k1 \leq k \leq d}$ with I_k nonzero ideal of R and $\{\boldsymbol{b}\}_{1 \leq k \leq d}$ linearly independent vectors of K^d such that $M = \sum_{1 \leq k \leq d} I_k \cdot \boldsymbol{b}_k$. We call $[\{I_k\}, \{\mathrm{b}_k\}]$ a pseudo-basis of M. We remark that we only deal with the full-rank modules, i.e. the number of ideals and vectors is equal to d.

The canonical embedding can be extend to K^d in the usual way. For any $\boldsymbol{x} \in K^d$ with $\boldsymbol{x} = (x_1, \cdots, x_d)$, we define the map σ by $\sigma(\boldsymbol{x}) = (\sigma(x_1), \cdots, \sigma(x_n))$. Therefore, $\sigma(K^d) \subseteq H^d \cong \mathbb{R}^{nd}$ and any module of K^d is a full-rank lattice in H^d, we regard a module M as a module lattice.

The definitions of Module-LWE distribution and Module-LWE problem are as followings. We define $T_{R^\vee} = K \otimes_{\mathbb{Q}} \mathbb{R}/R^\vee$.

Definition 9. *Let ψ be some distribution on $T_{R^\vee}$ and $\boldsymbol{s} \in (R_q^\vee)^d$ be a vector. The* Module-LWE *distribution $A_{\boldsymbol{s},\psi}^{(M)}$ is a distribution on $(R_q)^d \times T_{R^\vee}$ obtained by choosing a vector $\boldsymbol{a} \in (R_q)^d$ uniformly at random, and $e \hookleftarrow \psi \in T_{R^\vee}$, and returning $(\boldsymbol{a}, \frac{1}{q}\sum_{i=1}^d a_i \cdot s_i + e)$.*

Let $q \geq 2$ and Ψ be a family of distributions on $T_{R^\vee}$.

- The search version of the Module-LWE denoted by $\mathrm{MSLWE}_{q,\Psi}$ is as follows: Let $\boldsymbol{s} \in (R_q^\vee)^d$ be a secret and $\psi \in \Psi$; Given arbitrarily many samples from $A_{\boldsymbol{s},\psi}^{(M)}$, the goal is to find $\boldsymbol{s}$.
- The decision version of the Module-LWE denoted by $\mathrm{MDLWE}_{q,\Psi}$ is as follows: Let $\boldsymbol{s} \in (R_q^\vee)^d$ be uniformly random and $\psi \in \Psi$; The goal is to distinguish between arbitrarily many independent samples from $A_{\boldsymbol{s},\psi}^{(M)}$ and the same number of independent samples from $U((R_q)^d \times T_{R^\vee})$.

In [19], an elementary reduction from Module-SIVP to Module-LWE is given.

Theorem 5. *Let $M \subseteq K^d$, $\varepsilon(N) = N^{-\omega(1)}$ with $N = nd$, $\alpha \in (0,1)$ and $q \geq 2$ be a prime, with $q \leq \mathrm{poly}(N)$ and $q = 1 \bmod l$ such that $\alpha q \geq 2\sqrt{d} \cdot \omega(\sqrt{\log(n)})$. There is a quantum reduction from solving M-SIVP$_{\tilde{\omega}(\frac{\sqrt{Nd}}{\alpha})}$ to solving MDLWE$_{q,D_\xi}$, given only k samples, in polynomial time with non-negligible advantage with $\xi = \alpha(\frac{nk}{\log(nk)})$.*

As in the case of Ring-LWE, we can also modify the distribution of $A_{\boldsymbol{s},\psi}^{(M)}$ to $(R_q^\times)^d \times R_q^\vee$. We scale the b component by a factor of q, so that it is an element of $K_\mathbb{R}/(qR^\vee)$. The corresponding error distribution is $D_{q\xi}$ with $\xi = \alpha \cdot (\frac{nk}{\log(nk)})$ and k the number of samples. Then we discretize the error, by taking $e \hookleftarrow \lfloor D_{q\xi} \rceil$. The decision version of MLWE becomes to distinguish between the modified distribution of $A_{\boldsymbol{s},\lfloor D_{q\xi} \rceil}^{(M)}$ and the uniform samples from $(R_q)^d \times R_q^\vee$. Notice that by using the same method proposed in [24, Lemma 2.24], we can change the secret $\boldsymbol{s}$ to obey the distribution of the errors, i.e. $\boldsymbol{s} = (s_1, \cdots, s_d)$ with $s_i \hookleftarrow \lfloor D_{q\xi} \rceil$. At last, if we restrict $\boldsymbol{a} \in (R_q^\times)^d$, the difficult of this problem does not decrease. We still use symbol $A_{\boldsymbol{s},D_{q\xi}}^{(M)}$ to denote the distribution of $(\boldsymbol{a}, b)$ obtained by choosing $\boldsymbol{a} \hookleftarrow U((R_q^\times)^d)$, $\boldsymbol{s} \hookleftarrow (\lfloor D_{q\xi} \rceil)^d$, $e \hookleftarrow \lfloor D_{q\xi} \rceil$ and $b = \sum_{i=1}^d a_i \cdot s_i + e$. We will use the symbol $\mathrm{MDLWE}_{q,D_{q\xi}}^\times$ to denote the problem of distinguish the samples from $A_{\boldsymbol{s},D_{q\xi}}^{(M)}$ and $U((R_q^\times)^d \times R_q^\vee)$.

B.2 Modified Module NTRUEncrypt

In this subsection, we give a modified version of NTRUEncrypt whose security rely on the corresponding MDLWE problem. 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* $(sk,\ pk) \in\ R_q^\times \times (R_q^\times)^d$.

1. *Sample* $f^{'}$ *from* $D_{R,\sigma}$; *let* $f = p \cdot f^{'} + 1$; *if* $(f \bmod qR) \notin R_q^\times$, *resample.*
2. *For* $i = 1, \cdots, d$, *sample* g_i *from* $D_{R,\sigma}$; *if* $(g_i \bmod qR) \notin R_q^\times$, *resample.*
3. *Return* $sk = f$ *and* $pk = (h_1, \cdots, h_d) = (pg_1/f, \cdots, pd_d/f) \in (R_q^\times)^d$.

By the results of Sect. 4, the statistical distance of the distribution of pk and $U((R_q^\times)^d)$ is less than $d \cdot \frac{9n}{q^{\lfloor \varepsilon n \rfloor}}$. Then algorithm can terminate in expected time and for all $i = 1, \cdots, d$, the l_2 norm of f_i and g_i is small with overwhelming probabilities.

We also 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 $k = O(1)$ is a positive integer and use decoding basis for element $x \in R \subseteq R^\vee$. The Module-NTRUEncrypt is as follows:

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

Encryption: *Given message* $m \in \mathcal{P}$, *set* $\boldsymbol{s} \hookleftarrow \chi^d$, $e \hookleftarrow \chi$ *and return the cipher*

$$c = \sum_{i=1}^{d} h_i \cdot s_i + pe + m \in R_q^\vee.$$

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

Notice that $c_1 = f \cdot c = p\sum_{i=1}^{d} g_i \cdot s_i + pfe + fm \bmod qR^\vee$, hence under the decoding basis, we have $||c_1||_\infty^c \leq \omega(d \cdot n^{\frac{3}{2}} \cdot \sqrt{\log n \log\log n \cdot \alpha^2 \cdot q^2}) \cdot \sigma \cdot ||p||_\infty^2$ with probability $1 - n^{-\omega(\sqrt{n \log n})}$. Therefore, we get the following lemma.

Lemma 17. *Let* $n \geq 5$, $q \geq 8n$, $q = 1 \bmod l$, $\sigma \geq \sqrt{\frac{2\ln(6n)}{\pi}} \cdot n \cdot q^{\frac{1}{n}}$, $C = \sqrt{\hat{l}}$ *and* $C_2 = \sqrt{\frac{rad(l)}{l}}$. *If* $\omega(d \cdot n^{\frac{3}{2}} \sqrt{\log n \log\log n}) \cdot \alpha^2 \cdot q^2 \cdot \sigma \cdot ||p||_\infty^2 < q$, *then with probability* $1 - n^{-\omega(\sqrt{n \log n})}$, *the decryption algorithm of* Module-NTRUEncrtpt *recovers* m.

The security of the scheme follows by an elementary reduction from $\text{MDLWE}_{q, D_{q\xi}}^\times$, exploiting the uniformity of the public key in $(R_q^\times)^d$ and the invertibility of $p \in R_q$. It's proof is similar to Lemma 16.

Lemma 18. *Let* $n \geq 5$, $q \geq 8n$, $q = 1 \bmod l$, $\sigma \geq \sqrt{\ln(8nq)} \cdot n^{\frac{3}{2}} \cdot q^{\frac{1}{2}+\varepsilon}$, $\delta > 0$ *and* $\varepsilon \in (0, \frac{1}{2})$. *If there exists an IND-CPA attack against* Module-NTRUEncrypt *that runs in time* T *with advantage* δ, *then there exists an algorithm solving* $\text{MDLWE}^\times$ *with parameters* q *and* $q\xi$ *that runs in time* $T^{'} = T + O(n)$ *with advantage* $\delta^{'} = \delta - q^{-\Omega(n)}$.

In a summary, we have the following results.

Theorem 6. *Let l be a positive integer, $n = \varphi(l) \geq 5$, $q \geq 8n$, $q = 1 \bmod l$ be a prime of size poly(n), $K = \mathbb{Q}(\zeta_l)$, $R = \mathcal{O}_k$, $M \subseteq K^d$ with d a positive integer and $N = nd$. Assume that $\alpha \in (0,1)$ satisfies $\alpha q \geq 2\sqrt{d} \cdot \omega(\sqrt{\log n})$. 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 $\omega(d \cdot n^{\frac{3}{2}} \sqrt{\log n \log\log n} \cdot \alpha^2 \cdot q^2) \cdot \sigma \cdot ||p||_\infty^2 < q$. Then, if there exists an IND-CPA attack against* Module-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 γ-*Module-SIVP *with $\gamma = \tilde{\omega}(\frac{\sqrt{Nd}}{\alpha})$. Moreover, the decryption algorithm succeeds with probability $1 - n^{-\omega(\sqrt{n \log n})}$ over the choice of the encryption randomness.*

C Proof of Lemma 16

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 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 and $\mathfrak{B}$ 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.

References

1. Albrecht, M., Bai, S., Ducas, L.: A subfield lattice attack on overstretched NTRU assumptions. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9814, pp. 153–178. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53018-4_6
2. Bos, J.W., Lauter, K., Loftus, J., Naehrig, M.: Improved security for a ring-based fully homomorphic encryption scheme. In: Stam, M. (ed.) IMACC 2013. LNCS, vol. 8308, pp. 45–64. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-45239-0_4
3. Cabarcas, D., Weiden, P., Buchmann, J.: On the efficiency of provably secure NTRU. In: Mosca, M. (ed.) PQCrypto 2014. LNCS, vol. 8772, pp. 22–39. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-11659-4_2
4. Cheon, J.H., Jeong, J., Lee, C.: 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). https://doi.org/10.1112/S1461157016000371

5. Coppersmith, D., Shamir, A.: Lattice attacks on NTRU. In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 52–61. Springer, Heidelberg (1997). https://doi.org/10.1007/3-540-69053-0_5
6. Ducas, L., Durmus, A.: Ring-LWE in polynomial rings. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 34–51. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-30057-8_3
7. Ducas, L., Durmus, A., Lepoint, T., Lyubashevsky, V.: Lattice signatures and bimodal Gaussians. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8042, pp. 40–56. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40041-4_3
8. Ducas, L., Lyubashevsky, V., Prest, T.: Efficient identity-based encryption over NTRU lattices. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8874, pp. 22–41. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45608-8_2
9. Ducas, L., Nguyen, P.Q.: Learning a zonotope and more: cryptanalysis of NTRUSign countermeasures. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 433–450. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34961-4_27
10. Gama, N., Nguyen, P.Q.: New chosen-ciphertext attacks on NTRU. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 89–106. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-71677-8_7
11. Garg, S., Gentry, C., Halevi, S.: Candidate multilinear maps from ideal lattices. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 1–17. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38348-9_1
12. Gentry, C.: Key recovery and message attacks on NTRU-composite. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 182–194. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44987-6_12
13. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing, STOC 2008, pp. 197–206, ACM, New York (2008). https://doi.org/10.1145/1374376.1374407
14. Hoffstein, J., Howgrave-Graham, N., Pipher, J., Silverman, J.H., Whyte, W.: NTRUSign: digital signatures using the NTRU lattice. In: Joye, M. (ed.) CT-RSA 2003. LNCS, vol. 2612, pp. 122–140. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-36563-X_9
15. Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: a ring-based public key cryptosystem. In: Buhler, J.P. (ed.) ANTS 1998. LNCS, vol. 1423, pp. 267–288. Springer, Heidelberg (1998). https://doi.org/10.1007/BFb0054868
16. Howgrave-Graham, N.: A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 150–169. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74143-5_9
17. Jaulmes, É., Joux, A.: A chosen-ciphertext attack against NTRU. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol. 1880, pp. 20–35. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-44598-6_2
18. Kirchner, P., Fouque, P.-A.: Revisiting lattice attacks on overstretched NTRU parameters. In: Coron, J.-S., Nielsen, J.B. (eds.) EUROCRYPT 2017. LNCS, vol. 10210, pp. 3–26. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56620-7_1
19. Langlois, A., Stehlé, D.: Worst-case to average-case reductions for module lattices. Des. Codes Cryptogr. **75**(3), 565–599 (2015). https://doi.org/10.1007/s10623-014-9938-4

20. López-Alt, A., Tromer, E., Vaikuntanathan, V.: On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In: Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing, STOC 2012, pp. 1219–1234. ACM, New York (2012). https://doi.org/10.1145/2213977.2214086
21. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 1–23. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_1
22. Lyubashevsky, V., Peikert, C., Regev, O.: A toolkit for ring-LWE cryptography. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 35–54. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38348-9_3
23. Micciancio, D., Regev, O.: Worst-case to average-case reductions based on Gaussian measures. SIAM J. Comput. **37**(1), 267–302 (2007). https://doi.org/10.1137/S0097539705447360
24. Murphy, S., Player, R.: Noise distributions in homomorphic ring-LWE. Cryptology ePrint Archive, Report 2017/698 (2017). https://eprint.iacr.org/2017/698
25. Peikert, C.: Limits on the hardness of lattice problems in ℓ_p norms. In: Proceedings of the Twenty-Second Annual IEEE Conference on Computational Complexity, CCC 2007, pp. 333–346. IEEE Computer Society, Washington (2007). https://doi.org/10.1109/CCC.2007.12
26. Peikert, C.: An efficient and parallel Gaussian sampler for lattices. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 80–97. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14623-7_5
27. Peikert, C., Regev, O., Stephens-Davidowitz, N.: Pseudorandomness of ring-LWE for any ring and modulus. In: Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, pp. 461–473. ACM, New York (2017). https://doi.org/10.1145/3055399.3055489
28. Rosca, M., Stehlé, D., Wallet, A.: On the ring-LWE and polynomial-LWE problems. Cryptology ePrint Archive, Report 2018/170 (2018). https://eprint.iacr.org/2018/170
29. Stehlé, D., Steinfeld, R.: Making `NTRU` as secure as worst-case problems over ideal lattices. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 27–47. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-20465-4_4
30. Wang, Y., Wang, M.: CRPSF and NTRU signatures over cyclotomic fields. Cryptology ePrint Archive, Report 2018/445 (2018). https://eprint.iacr.org/2018/445
31. Yu, Y., Xu, G., Wang, X.: Provably secure NTRU instances over prime cyclotomic rings. In: Fehr, S. (ed.) PKC 2017. LNCS, vol. 10174, pp. 409–434. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-662-54365-8_17
32. Yu, Y., Xu, G., Wang, X.: Provably secure NTRUEncrypt over more general cyclotomic rings. Cryptology ePrint Archive, Report 2017/304 (2017). https://refeprint.iacr.org/2017/304