Provably Secure NTRUEncrypt over More General Cyclotomic Rings

Yang Yu[1], Guangwu Xu[2], and Xiaoyun Wang[3,4⋆]

[1] Department of Computer Science and Technology, Tsinghua University, P.R.China
y-y13@mails.tsinghua.edu.cn
[2] Department of Electrical Engineering and Computer Science, University of Wisconsin-Milwaukee, USA
gxu4uwm@uwm.edu
[3] Institute for Advanced Study, Tsinghua University, P.R.China
[4] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, P.R.China
xiaoyunwang@mail.tsinghua.edu.cn

Abstract. NTRUEncrypt is a fast and standardized lattice-based public key encryption scheme, but it lacks a proof of security. Stehlé and Steinfeld (EUROCRYPT 2011) first gave a variant of NTRUEncrypt, denoted by pNE, over power-of-2 cyclotomic rings. The pNE scheme is provably secure assuming the hardness of worst-case problems over ideal lattices. Recently, Yu, Xu and Wang (PKC 2017) proposed a pNE variant over prime cyclotomic rings, but it requires the parameters to be of rather larger sizes. In this paper, working with canonical embedding, we modify the key generation algorithm of pNE scheme to make it applicable to general cyclotomic rings. Through an improved analysis, we provide tighter parameters of pNE over prime power cyclotomic rings. To be more specific, even for the general case, our parameters are as good as that obtained by Stehlé and Steinfeld for the case of power-of-2; compared to that of Yu, Xu and Wang (PKC 2017), the sizes of our parameters get significantly reduced. Thus our result not only applies to a larger class of rings but also enjoys greater efficiency. In proving our results, we have developed some technical tools which may be of general interest. Some remarks on further extension of the work (e.g., for more general polynomial rings) have also been made.

1 Introduction

NTRU, introduced by Hoffstein, Pipher and Silverman in [25], is a celebrated public key cryptosystem standardized by IEEE. Its encryption scheme, NTRUEncrypt, is one of the fastest known lattice-based encryption schemes. Due to its excellent performance and potential resistance to quantum computers, NTRUEncrypt is considered as not only a desirable alternative to classical schemes based on integer factorisation or discrete logarithms but also a promising post-quantum

⋆ Corresponding Author.

encryption scheme. Based on the underlying problem of NTRU, various cryptographic primitives are designed, including digital signature [24, 15], identity-based encryption [17], fully homomorphic encryption [31, 7] and multilinear maps [20, 30]. In the last 20 years, a batch of cryptanalysis works [12, 27, 21, 36, 19, 26, 18, 3, 9, 28] were proposed aiming at NTRU family, and NTRUEncrypt is generally believed to be secure in practice. However, classical NTRU lacks a solid security guarantee, which may weaken our confidence in this scheme.

Over the past decade, many provably secure lattice-based schemes have been established based on well-studied lattice problems. A very important problem is the *Learning With Errors* problem (LWE), introduced by Regev [39]. The average-case LWE is shown to be as hard as certain worst-case lattice problems, which is a main attraction of LWE. To obtain better compactness and efficiency, several algebraic variants of LWE were proposed, such as Ring-LWE [32] (RLWE) and Module-LWE [29]. The hardness of these variants is based on some worst-case problems over structured lattices. Some practical applications [4, 16, 6] have been designed based on LWE variants.

In 2011, Stehlé and Steinfeld first proposed a provably secure variant of NTRUEncrypt [40] that we denote by pNE, and gave a reduction from RLWE to the IND-CPA security (*indistinguishability under chosen-plaintext attack*) of pNE. This provides the first theoretical grounding for the security of NTRU in the asymptotic sense. Then, a variant of pNE against chosen-ciphertext attacks [42] and a provably secure NTRU signature scheme [41] were proposed successively. These modified NTRU schemes are restricted to power-of-2 cyclotomic rings, *i.e.* $\mathbb{Z}[X]/(X^{2^k}+1)$, that are scarce. Recently, Yu, Xu and Wang modified pNE to make it work over prime cyclotomic rings, *i.e.* $\mathbb{Z}[X]/(X^{n-1}+\cdots+1)$ with n a prime, in [44], which allows more flexibility of parameter selections. However, due to different ring structures and the possibly rough parameter estimation, the parameters of pNE over prime cyclotomic rings are much larger than that of pNE over power-of-2 cyclotomic rings.

Compared with classical NTRU, provably secure NTRU keeps the same asymptotic efficiency but enjoys a firm theoretical security as well. While pNE is much less practical [8], it shows an important connection between NTRU and RLWE, and between problems over NTRU lattices and worst-case problems over ideal lattices. With the recent calls for post-quantum cryptography by NIST, a better understanding of these problems is necessary and thus the study of pNE would be of theoretical value. An essential issue to be addressed is the choice of the underlying ring for pNE, which is the main motivation of our paper.

Contribution In this paper, we study a new variant of pNE over cyclotomic rings and show that, given appropriate parameters, provably secure NTRU can hold over prime power cyclotomic rings and even more general rings. The key generation algorithm of our pNE is modified and relies on Gaussian sampling with respect to canonical embedding instead of coefficient embedding. We show that the public key, *i.e.* the ratio of two secret polynomials, will be almost uniformly distributed, if the secret polynomials are sampled from certain Gaussians. This is a remarkable property of pNE originally proposed by Stehlé and Steinfeld in [40].

It is worth noting that the "uniformity" of public key holds not only for the case of prime power, but also for general cyclotomic rings.

For a tighter parameter estimation, we develop some new tools. On the one hand, we propose a new discrete Gaussian tail inequality measuring the Euclidean norm of f where f follows a Gaussian with respect to canonical embedding. A main technique is to consider all singular values of the canonical embedding transformation matrix that profile the geometry of the underlying ring. A similar idea was exploited in the tail inequality given in [2], but its tail bound only involves the smallest singular value. Hence our tail bound can be tighter than that in [2] for certain cases as it will be shown in later discussion. On the other hand, we show a series of general results on cyclotomic rings and some special properties of prime power cyclotomic rings. Even though similar results on power-of-2 and prime cyclotomic rings have been established in [40, 44], in this paper we mainly consider these results with respect to canonical embedding rather than coefficient embedding. Thus many technical differences still need to be treated carefully. Exploiting all of these tools, we provide asymptotical parameters of pNE over prime power cyclotomic rings. The parameters of our scheme are improved (see Table 1) in that they have essentially the same sizes as that in the power-of-2 case from [40]. This also means that our parameter sizes are significantly reduced compared with that in [44]. Therefore, our result further enriches the provably secure NTRU family and allows more flexible and compact parameters. Our result also suggests that cryptographic applications over prime power cyclotomic rings are likely to achieve similar efficiency to that over power-of-2 cyclotomic rings.

Table 1. Parameters of provably secure NTRU.

Scheme	Type of n	Ring density	Modulus q	Euclidean length of key
SS11 [40]	power-of-2	$\Theta(\frac{\log N}{N})$	$\widetilde{\Omega}(n^{4.5})$	$\widetilde{O}(n^{1.5}q^{0.5})$
YXW17 [44]	prime	$\Theta(\frac{1}{\log N})$	$\widetilde{\Omega}(n^{7.5})$	$\widetilde{O}(n^{2.5}q^{0.5})$
This work	prime power	$\Theta(\frac{1}{\log N})$	$\widetilde{\Omega}(n^{4.5})$	$\widetilde{O}(n^{1.5}q^{0.5})$

Furthermore, a generalization of the above discussion to other rings is considered. With certain polynomial $P(X)$ and certain prime number q, a similar regularity result can be proved and thus we may construct pNE over $\mathbb{Z}[X]/(P(X))$. We also point out several attributes of $P(X)$ concerning parameter selections. Even though some factors may not be taken into account, our discussion can still be helpful to choose a suitable ring for cryptosystems.

Organization In Sect. 2, we introduce some notations and basic results that will be used in our discussion. In Sect. 3, we present two discrete Gaussian tail inequalities. In Sect. 4, we show a series of relevant results over general cyclotomic rings and several special properties of prime power cyclotomic rings. Then, we

describe our pNE variant over prime power cyclotomic rings and demonstrate parameter requirements in Sect. 5. Finally, we further discuss a generalization to some other rings in Sect. 6.

2 Preliminaries

Embeddings and Norms Let $P(X) \in \mathbb{Z}[X]$ be a monic irreducible polynomial of degree n and $K = \mathbb{Q}[X]/(P(X))$. For any $t = \sum_{i=0}^{n-1} t_i X^i \in K$, the vector $(t_0, \cdots, t_{n-1}) \in \mathbb{Q}^n$ is called the coefficient vector of t. The *coefficient embedding* maps any element of K to its coefficient vector. We denote by $\|t\|$ (resp. $\|t\|_\infty$) the Euclidean (resp. ℓ_∞) norm of the coefficient vector of t. For $\mathbf{t} = (t^{(1)}, \cdots, t^{(m)}) \in K^m$, its Euclidean norm (under coefficient embedding) is $\|\mathbf{t}\| = \sqrt{\sum_i \|t^{(i)}\|^2}$ and its ℓ_∞ norm is $\|\mathbf{t}\|_\infty = \max_i \|t^{(i)}\|_\infty$. Note that, for $\mathbf{a} = (a_1, \cdots, a_n) \in \mathbb{C}^n$, we also denote by $\|\mathbf{a}\| = \sqrt{\sum_i |a_i|^2}$ its Euclidean norm and by $\|\mathbf{a}\|_\infty = \max_i |a_i|$ its ℓ_∞ norm.

Besides coefficient embedding, *canonical embedding* is also very important, especially in the context of RLWE [32, 33]. Assume that $P(X)$ has s_1 real roots denoted by $\omega_1, \cdots, \omega_{s_1}$, and $2s_2$ complex conjugate roots denoted by $\omega_{s_1+1}, \cdots, \omega_{s_1+2s_2}$ where $\omega_{s_1+k} = \overline{\omega_{s_1+k+s_2}}$ for $k \in \{1, \cdots, s_2\}$. The field K has exactly n embeddings into $\mathbb{C}$ denoted by $\sigma_i : K \to \mathbb{C}$ where $\sigma_i(t) = t(\omega_i)$ for any $t \in K$. Then the canonical embedding $\sigma : K \to \mathbb{C}^n$ is defined as $\sigma(t) = (\sigma_1(t), \cdots, \sigma_n(t))$. Viewing t as its coefficient vector, we have $\sigma(t) = t \cdot \mathbf{V}$ where $\mathbf{V} = (\omega_j^{i-1})_{1 \le i,j \le n}$ and is called the *canonical embedding transformation*. In fact, the canonical embedding maps into the space $H = \{(x_1, \cdots, x_n) \mid x_1, \cdots, x_{s_1} \in \mathbb{R}, x_{s_1+k} = \overline{x_{s_1+k+s_2}}, 1 \le k \le s_2\}$ isomorphic to $\mathbb{R}^n$ as an inner product space, and the inner product $\langle \sigma(s), \overline{\sigma(t)} \rangle$ equals $\sum_i \sigma_i(s)\sigma_i(t) = \mathrm{Tr}(st)$, *i.e.* the *trace* of st over $\mathbb{Q}$. The T_2-*norm* of t is $\mathrm{T}_2(t) = \|\sigma(t)\| = \sqrt{\sum_i |\sigma_i(t)|^2}$, the T_∞-*norm* of t is $\mathrm{T}_\infty(t) = \|\sigma(t)\|_\infty$ and the *algebraic norm* is $\mathrm{N}(t) = \prod_i |\sigma_i(t)|$. For $\mathbf{t} = (t_1, \cdots, t_m) \in K^m$, the T_2-norm of $\mathbf{t}$ is $\mathrm{T}_2(\mathbf{t}) = \sqrt{\sum_i \mathrm{T}_2(t_i)^2}$ and the T_∞-norm of $\mathbf{t}$ is $\mathrm{T}_\infty(\mathbf{t}) = \max_i \mathrm{T}_\infty(t_i)$.

Lattice A full-rank lattice is the set of all integer linear combinations of linearly independent vectors $\mathbf{b}_1, \cdots, \mathbf{b}_n$ in an n-dimensional inner product space V[5]. We call $(\mathbf{b}_1, \cdots, \mathbf{b}_n)$ a basis and n the dimension of the lattice. Let $\mathbf{B}$ be a basis of a lattice $\mathcal{L}$, then the volume of $\mathcal{L}$ is $\mathrm{vol}(\mathcal{L}) = \sqrt{\det(G(\mathbf{B}))}$ where $G(\mathbf{B})$ is the Gram matrix of $\mathbf{B}$. The dual lattice of $\mathcal{L}$ is the lattice $\widehat{\mathcal{L}} = \{\mathbf{c} \in V \mid \forall i, \langle \mathbf{c}, \overline{\mathbf{b}_i} \rangle \in \mathbb{Z}\}$[6]. The first minimum $\lambda_1(\mathcal{L})$ (resp. $\lambda_1^\infty(\mathcal{L})$) is the minimum of Euclidean (resp. ℓ_∞) norm of all non-zero vectors of $\mathcal{L}$. More generally, for $k \le n$, the k-th minimum

[5] For coefficient embedding and canonical embedding, the space V corresponds to $\mathbb{R}^n$ and H respectively.

[6] Actually, the dual lattice that we define is the complex conjugate of that as usually defined in $\mathbb{C}^n$, but all properties of the dual lattice used in this paper hold for the conjugate dual as well.

$\lambda_k(\mathcal{L})$ is the smallest r such that there are at least k linearly independent vectors of $\mathcal{L}$ whose norms are not greater than r.

Let $\mathcal{R}$ be the ring of integers of a field K with an additive isomorphism θ[7] mapping $\mathcal{R}$ to the lattice $\theta(\mathcal{R})$. Let I be an ideal of $\mathcal{R}$, then $\theta(I)$ is an *ideal lattice*. The norm of an ideal I is $\mathrm{N}(I) = |\mathcal{R}/I|$. For any $t \in \mathcal{R}$, we have $\mathrm{N}(\langle t \rangle) = \mathrm{N}(t)$ where $\langle t \rangle = t\mathcal{R}$.

By restricting SVP(*Shortest Vector Problem*) and γ-SVP(*Approximate Shortest Vector Problem with approximation factor* γ) to ideal lattices, we get Ideal-SVP and γ-Ideal-SVP. These ideal lattice problems do not seem to be substantially easier than the versions for general lattice (perhaps, except for very large γ [13]). Currently, it is believed that the worst-case hardness of γ-Ideal-SVP is against subexponential quantum attacks, for any $\gamma \leq \mathrm{poly}(n)$.

Probability and Statistics For a distribution D over a domain E, we write $z \hookleftarrow D$ when the random variable z is sampled from D, and denote by $D(x)$ the probability of $z = x$. If the domain E is a finite set, we use $U(E)$ to denote the uniform distribution over E. For two distributions D_1, D_2 over the same discrete domain E, their statistical distance is $\Delta(D_1; D_2) = \frac{1}{2}\sum_{x\in E} |D_1(x) - D_2(x)|$. If $\Delta(D_1; D_2) = o(n^{-c})$ for any constant $c > 0$, then we call D_1, D_2 statistically close with respect to n.

Cyclotomic Ring Let ξ_n be a primitive n-th root of unity. The n-th cyclotomic polynomial, denoted by $\Phi_n(X)$, is the minimal polynomial of ξ_n. It is known that $\Phi_n(X) = \prod_{i\in\mathbb{Z}_n^*}(X - \xi_n^i) \in \mathbb{Z}[X]$. Each cyclotomic polynomial $\Phi_n(X)$ corresponds to a binomial $\Theta_n(X)$ defined as $X^n - 1$ if n is odd and $X^{n/2} + 1$ if n is even, and $\Theta_n(X)$ is a multiple of $\Phi_n(X)$. A cyclotomic ring is a quotient ring of the form $\mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X))$. For some special n, the form of $\Phi_n(X)$ is regular and simple. If n is a prime, we have $\Phi_n(X) = X^{n-1} + X^{n-2} + \cdots + 1$. More generally, if $n = d^\nu$ is a power of prime d, we have $\Phi_n(X) = \Phi_d(X^{d^{\nu-1}})$ and call it a *prime power cyclotomic ring*.

If a prime q satisfies $q = 1 \bmod n$, then $\Phi_n(X)$ splits completely into distinct linear factors modulo q. Given n, according to Dirichlet's theorem on arithmetic progressions, there exist infinitely many primes congruent to 1 modulo n. Furthermore, Linnik's theorem asserts that the smallest such q is of size $\mathrm{poly}(n)$ (a concrete bound is $O(n^{5.2})$, see [43]).

Gaussian Measures Let $\rho_{r,\mathbf{c}}(\mathbf{x}) = \exp\left(-\pi\|\mathbf{x} - \mathbf{c}\|^2/r^2\right)$ be the n-dimensional Gaussian function with center $\mathbf{c} \in V$ and width r. When $\mathbf{c} = \mathbf{0}$, the Gaussian function is written as $\rho_r(\mathbf{x})$. We denote by ψ_r the (continuous) Gaussian distribution over $\mathbb{R}$ with mean 0 and width r whose probability density function is $\rho_r(x)/r$. Let ψ_r^n be the *spherical Gaussian distribution* over $\mathbb{R}^n$ of the vector $(v_1, \cdots, v_n)$ where all v_i's follow ψ_r independently. We can restrict ψ_r over $\mathbb{Q}$ so that $\psi_r^{n'}$ can be viewed as a distribution over $\mathbb{Q}[X]/(\Theta_n(X))$ where $n' = \deg(\Theta_n(X))$, which only leads to a negligible impact on our results, as

[7] Both coefficient embedding and canonical embedding are additive isomorphisms.

explained in [14]. For $S \subseteq V$, the sum $\sum_{\mathbf{x}\in S} \rho_{r,\mathbf{c}}(\mathbf{x})$ (resp. $\sum_{\mathbf{x}\in S} \rho_r(\mathbf{x})$) is denoted as $\rho_{r,\mathbf{c}}(S)$ (resp. $\rho_r(S)$). The *discrete Gaussian distribution* over a lattice $\mathcal{L}$ with center $\mathbf{c}$ and width r is defined by $D_{\mathcal{L},r,\mathbf{c}}(\mathbf{x}) = \rho_{r,\mathbf{c}}(\mathbf{x})/\rho_{r,\mathbf{c}}(\mathcal{L})$, for any $\mathbf{x} \in \mathcal{L}$. In later discussion, we will use discrete Gaussians with respect to the canonical embedding σ of the ring $\mathcal{R}$. Viewing $\mathbb{Z}^n$ as $\mathcal{R}$ by coefficient embedding, we denote by $\widetilde{\rho}_{r,\mathbf{c}}(\mathbf{x}) = \exp\left(-\pi \mathrm{T}_2(\mathbf{x}-\mathbf{c})^2/r^2\right)$ the Gaussian function evaluated by T_2-norm, and by $\widetilde{D}_{\mathbb{Z}^n,r,\mathbf{c}}$ the corresponding discrete Gaussian distribution. Similarly, the subscript $\mathbf{c}$ is omitted when $\mathbf{c} = \mathbf{0}$. Sampling from $\widetilde{D}_{\mathbb{Z}^n,r,\mathbf{c}}$ is in fact to sample from $D_{\sigma(\mathbb{Z}^n),r,\sigma(\mathbf{c})}$ and then map to $\mathbb{Z}^n$ via σ^{-1}. Thus the results for discrete Gaussians also hold for $\widetilde{D}_{\mathbb{Z}^n,r,\mathbf{c}}$ by replacing Euclidean norm and inner product with T_2-norm and corresponding inner product. For $\delta > 0$, we denote the *smoothing parameter* by $\eta_\delta(\mathcal{L}) = \min\{r : \rho_{1/r}(\widehat{\mathcal{L}}) \leq 1+\delta\}$. We now recall some results which will be used later.

Lemma 1 ([35], Lemma 3.3). *Let $\mathcal{L}$ be an n-dimensional full-rank lattice and $\delta \in (0,1)$. Then $\eta_\delta(\mathcal{L}) \leq \sqrt{\ln(2n(1+1/\delta))/\pi} \cdot \lambda_n(\mathcal{L})$.*

Lemma 2 ([37], Lemma 3.5). *Let $\mathcal{L}$ be an n-dimensional full-rank lattice and $\delta \in (0,1)$. Then $\eta_\delta(\mathcal{L}) \leq \sqrt{\ln(2n(1+1/\delta))/\pi}/\lambda_1^\infty\left(\widehat{\mathcal{L}}\right)$.*

Lemma 3 ([35], Lemma 4.4). *Let $\mathcal{L} \subseteq V$ be an n-dimensional full-rank lattice and $\delta \in (0,1)$. Then $\Pr_{\mathbf{b}\hookleftarrow D_{\mathcal{L},r,\mathbf{c}}}(\|\mathbf{b}-\mathbf{c}\| \geq r\sqrt{n}) \leq \frac{1+\delta}{1-\delta}2^{-n}$ for $\mathbf{c} \in V$ and $r \geq \eta_\delta(\mathcal{L})$.*

Lemma 4 ([1], Lemma 2.9 [8].). *Let $\mathcal{L} \subseteq V$ be an n-dimensional full-rank lattice. Then $\Pr_{\mathbf{b}\hookleftarrow D_{\mathcal{L},r}}(|\langle \mathbf{b}, \mathbf{v}\rangle| \geq rt) \leq 2\exp(-\pi t^2)$ for $r > 0$, $t > 0$ and any unit vector $\mathbf{v} \in V$.*

Lemma 5 ([23], Corollary 2.8). *Let $\mathcal{L}' \subseteq \mathcal{L} \subseteq V$ be full-rank lattices and $\delta \in (0, 1/2)$. For $\mathbf{c} \in V$ and $r \geq \eta_\delta(\mathcal{L}')$, we have $\Delta(D_{\mathcal{L},r,\mathbf{c}} \bmod \mathcal{L}'; U(\mathcal{L}/\mathcal{L}')) \leq 2\delta$.*

Lemma 6 ([23], Theorem 4.1). *There exists a polynomial-time algorithm that, given a basis $(\mathbf{b}_1, \cdots, \mathbf{b}_n)$ of a lattice $\mathcal{L}$, a parameter $r = \omega(\sqrt{\log n}) \max \|\mathbf{b}_i\|$ and a center $\mathbf{c}$, outputs samples from a distribution statistically close to $D_{\mathcal{L},r,\mathbf{c}}$ with respect to n.*

Hardness of RLWE The Ring Learning With Errors problem (RLWE) was first proposed in [32] and shown hard for specific settings. In [14], Ducas and Durmus gave an "easy-to-use" setting for RLWE and instantiated RLWE over general cyclotomic rings. In this paper, we follow the setting of [14].

Definition 1 (RLWE error distribution in [14]). *Let $\mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X))$. Given ψ a distribution over $\mathbb{Q}[X]/(\Theta_n(X))$, we define $\overline{\psi}$ as the distribution over $\mathcal{R}$ obtained by $e = \lfloor e' \bmod \Phi_n(X) \rceil \in \mathcal{R}$ with $e' \hookleftarrow \psi$. Here we denote by $\lfloor f \rceil$ the polynomial whose coefficients are derived by rounding coefficients of f to the nearest integers.*

[8] A clear proof was given in [28], Lemma 6

Definition 2 (RLWE **distribution in [14]**). *Let* $\mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X))$ *and* $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. *For* $s \in \mathcal{R}_q$ *and* ψ *a distribution over* $\mathbb{Q}[X]/(\Theta_n(X))$, *we define* $A_{s,\psi}$ *as the distribution over* $\mathcal{R}_q \times \mathcal{R}_q$ *obtained by sampling the pair* $(a, as + e)$ *where* $a \hookleftarrow U(\mathcal{R}_q)$ *and* $e \hookleftarrow \overline{\psi}$.

Definition 3 ($\mathsf{RLWE}_{q,\psi,k}$). *Let* $\mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X))$ *and* $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. *The problem* $\mathsf{RLWE}_{q,\psi,k}$ *in the ring* $\mathcal{R}$ *is defined as follows. Given* k *samples drawn from* $A_{s,\psi}$ *where* $s \hookleftarrow U(\mathcal{R}_q)$ *and* k *samples from* $U(\mathcal{R}_q \times \mathcal{R}_q)$, *distinguish them with an advantage* $1/\operatorname{poly}(n)$.

For certain error distributions, RLWE can be reduced from γ-Ideal-SVP. Note that γ-Ideal-SVP discussed here is for the ring $\mathcal{R}$ and with respect to canonical embedding.

Theorem 1 ([14], Theorem 2). *Let* n *be an integer and* $n' = \frac{3+(-1)^{n-1}}{4} n$. *Choose* q *to be a prime congruent to* 1 *modulo* n. *Assume that* $\alpha \in (0,1)$ *is a real number such that* $\alpha q > \omega(\sqrt{\log n})$. *Then for* $\gamma = \tilde{O}\left(\sqrt{n}/\alpha\right)$ *and* $t = \sqrt{n'}\alpha q \left(\frac{\varphi(n)k}{\log(\varphi(n)k)}\right)^{1/4}$, *there exists a randomized quantum reduction from* γ-*Ideal-*SVP *on ideal lattices in* $\mathbb{Z}[X]/(\Phi_n(X))$ *to* $\mathsf{RLWE}_{q,\psi_t^{n'},k}$ *that runs in time* $O(q \cdot \operatorname{poly}(n))$.

Let $\mathcal{R}_q^\times$ be the set of all invertible elements of $\mathcal{R}_q$. As explained in [40], one can restrict $A_{s,\psi}$ to $\mathcal{R}_q^\times \times \mathcal{R}_q$ and sample s from ψ, which leads to a variant of RLWE (to distinguish $A_{s,\psi}$ and $U(\mathcal{R}_q^\times \times \mathcal{R}_q)$) with same hardness.

3 Discrete Gaussian Tail Inequalities

In our scheme, secret polynomials are drawn from discrete Gaussians with respect to canonical embedding, while most arithmetic operations over the ring are still with respect to coefficient embedding. In this section, we will give two tail inequalities of Euclidean norm for a discrete Gaussian using T_2-norm.

Let $P(X) \in \mathbb{Z}[X]$ be a monic irreducible polynomial of degree n and $\mathcal{R} = \mathbb{Z}[X]/(P(X))$. Let $\mathbf{V}$ be the canonical embedding transformation of $\mathcal{R}$ and $\mathbf{U} = \mathbf{V}\mathbf{V}^*$ where $\mathbf{V}^*$ is the conjugate transpose of $\mathbf{V}$. Notice that $\mathrm{T}_2(f)^2 = \|\sigma(f)\|^2 = f\mathbf{U}f^t$, hence $\mathrm{T}_2(f) \geq s_1(\mathbf{V})\|f\|$ where $s_1(\mathbf{V})$ is the smallest singular value of $\mathbf{V}$. By Lemma 3, we get immediately the following tail inequality.

Lemma 7. *Let* $P(X) \in \mathbb{Z}[X]$ *be a monic irreducible polynomial of degree* n *and* $\mathcal{R} = \mathbb{Z}[X]/(P(X))$. *Let* $\mathbf{V}$ *be the canonical embedding transformation of* $\mathcal{R}$ *and* $s_1(\mathbf{V})$ *be the smallest singular value of* $\mathbf{V}$. *For* $\delta \in (0,1)$ *and* $r \geq \eta_\delta(\sigma(\mathbb{Z}^n))$ *where* σ *is the canonical embedding, then*

$$\Pr_{f \hookleftarrow \tilde{D}_{\mathbb{Z}^n,r}} \left(\|f\| \geq \frac{r\sqrt{n}}{s_1(\mathbf{V})} \right) \leq \frac{1+\delta}{1-\delta} 2^{-n}.$$

Lemma 7 coincides with Lemma 3 in [2], and the tail bound only depends on the smallest singular value $s_1(\mathbf{V})$. Next we are to present a new tail inequality involving all singular values of $\mathbf{V}$.

Lemma 8. *Let $P(X) \in \mathbb{Z}[X]$ be a monic irreducible polynomial of degree n and $\mathcal{R} = \mathbb{Z}[X]/(P(X))$. Let $\mathbf{V}$ be the canonical embedding transformation of $\mathcal{R}$ and $s_1(\mathbf{V}), \cdots, s_n(\mathbf{V})$ be all singular values of $\mathbf{V}$. For $r > 0, t > 0$, then*

$$\Pr_{f \hookleftarrow \tilde{D}_{\mathbb{Z}^n, r}} \left(\|f\| \geq rt \cdot \sqrt{\sum_{i=1}^{n} \frac{1}{s_i(\mathbf{V})^2}} \right) \leq 2n \cdot \exp(-\pi t^2).$$

In particular, for $t = \omega\left(\sqrt{\ln n}\right)$, the above probability is $n^{-\omega(1)}$.

Proof. Let $\mathbf{U} = \mathbf{V}\mathbf{V}^*$, then it is known that $\mathbf{U}$ is a real symmetric matrix. Thus there exist $\mathbf{u}_1, \cdots, \mathbf{u}_n \in \mathbb{R}^n$ satisfying (1) each $\mathbf{u}_i$ is an eigenvector of $\mathbf{U}$ corresponding to the eigenvalue $s_i(\mathbf{V})^2$; (2) all these $\mathbf{u}_i$'s are unit vectors and orthogonal to each other. Let $\pi_i(\cdot)$ be the projection to $\mathbf{u}_i$, then $f = \sum_{i=1}^{n} \pi_i(f)$ and all $\pi_i(f)$'s are orthogonal to each other.

For a better illustration, we denote by $\langle a, b \rangle_M$ the inner product of $a, b \in \mathcal{R}$ under canonical embedding, *i.e.* $\langle a, b \rangle_M = \langle \sigma(a), \sigma(b) \rangle = a\mathbf{V}(b\mathbf{V})^* = a\mathbf{U}b^t$. Then we have

$$\pi_i(f) = \langle f, \mathbf{u}_i \rangle \mathbf{u}_i = (f\mathbf{u}_i^t)\mathbf{u}_i = \langle f, \mathbf{u}_i\mathbf{U}^{-1} \rangle_M \mathbf{u}_i.$$

Let $\mathbf{u}_i' = \mathbf{u}_i\mathbf{U}^{-1} = \mathbf{u}_i / s_i(\mathbf{V})^2$, then

$$\mathrm{T}_2(\mathbf{u}_i') = \|\sigma(\mathbf{u}_i')\| = \sqrt{\mathbf{u}_i'\mathbf{U}\mathbf{u}_i'^t} = \sqrt{\mathbf{u}_i\mathbf{U}^{-1}\mathbf{u}_i^t} = \frac{1}{s_i(\mathbf{V})}.$$

Note that we have applied T_2 and σ to $\mathbb{R}^n$. This is a natural extension, e.g., by $\sigma(\mathbf{u}) = \mathbf{u}\mathbf{V}$.

By the union bound, we have

$$\begin{aligned}
\Pr_{f \hookleftarrow \tilde{D}_{\mathbb{Z}^n, r}} \left(\|f\| \geq rt \cdot \sqrt{\sum_{i=1}^{n} \frac{1}{s_i(\mathbf{V})^2}} \right) &= \Pr_{f \hookleftarrow \tilde{D}_{\mathbb{Z}^n, r}} \left(\sum_{i=1}^{n} \|\pi_i(f)\|^2 \geq \sum_{i=1}^{n} \frac{r^2t^2}{s_i(\mathbf{V})^2} \right) \\
&\leq \sum_{i=1}^{n} \Pr_{f \hookleftarrow \tilde{D}_{\mathbb{Z}^n, r}} \left(\|\pi_i(f)\|^2 \geq \frac{r^2t^2}{s_i(\mathbf{V})^2} \right) \\
&= \sum_{i=1}^{n} \Pr_{f \hookleftarrow \tilde{D}_{\mathbb{Z}^n, r}} \left(|\langle f, \mathbf{u}_i' \rangle_M| \geq rt \cdot \mathrm{T}_2(\mathbf{u}_i') \right)
\end{aligned}$$

By Lemma 4, the following inequality holds

$$\Pr_{f \hookleftarrow \tilde{D}_{\mathbb{Z}^n, r}} \left(|\langle f, \mathbf{u}_i' \rangle_M| \geq rt \cdot \mathrm{T}_2(\mathbf{u}_i') \right) \leq 2\exp(-\pi t^2).$$

We now complete the proof. □

Remark Let $W_1 = \frac{\sqrt{n}}{s_1(\mathbf{V})}$ and $W_2 = \sqrt{\sum_{i=1}^{n} \frac{1}{s_i(\mathbf{V})^2}} \cdot \omega\left(\sqrt{\ln n}\right)$ corresponding to the tail bound parameters in Lemmata 7 and 8 respectively. In general W_2 can be much smaller than W_1 and the tail probability is still negligible in n, which will be discussed later. Furthermore, following a similar proof of Lemma 8, we can also prove new tail inequalities for the so-called ellipsoid Gaussian that is a natural generalization of the discrete Gaussian we focused in this paper. We include this part in Appendix A for interested readers.

4 New Results on General Cyclotomic Rings

In this section, we will develop a series of results on general cyclotomic rings and give several special properties of prime power cyclotomic rings. While similar results restricted to power-of-2 and prime cyclotomic rings have been discussed in [40, 44], our results are a wider extension and some of them are with respect to canonical embedding instead of coefficient embedding.

4.1 Duality Results for Module Lattices

Let $K = \mathbb{Q}[X]/(\Phi_n(X)) \cong \mathbb{Q}(\xi_n)$ and $\mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X)) \cong \mathbb{Z}[\xi_n]$ be the ring of integers of K. Let $q = 1 \bmod n$ be a prime and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. We know that $\Phi_n(X)$ splits completely into distinct linear factors modulo q. Let $\{\phi_i\}_{i=1,\cdots,\varphi(n)}$ be the set of all roots of $\Phi_n(X)$ modulo q, then each ideal of $\mathcal{R}_q$ is of the form $\prod_{i\in S}(X-\phi_i)\cdot\mathcal{R}_q$ with $S \subseteq \{1,\cdots,\varphi(n)\}$ and denoted by I_S. We also denote by J_S the ideal $\{t \in \mathcal{R} \mid t \bmod q \in I_S\}$ and by $\bar{S}$ the set $\{1,\cdots,\varphi(n)\} \setminus S$.

Given $\mathbf{a} \in \mathcal{R}_q^m$, for each i, we choose an $\tilde{a}_i \in \mathcal{R}$ such that $\pi(\tilde{a}_i) = a_i$ where $\pi : \mathcal{R} \to \mathcal{R}_q$ is the canonical homomorphism. Now we define $\mathcal{R}$-modules $\mathbf{a}^{\perp}(J_S)$ and $\mathcal{L}(\mathbf{a}, J_S)$ as follows:

$$\mathbf{a}^{\perp}(J_S) := \left\{(t_1,\cdots,t_m) \in \mathcal{R}^m \mid \sum_{i=1}^{m} t_i\tilde{a}_i = 0 \bmod q\right\} \bigcap J_S^m,$$

$$\mathcal{L}(\mathbf{a}, J_S) := \{(t_1,\cdots,t_m) \in \mathcal{R}^m \mid \exists s \in \mathcal{R}, \forall i, t_i - \tilde{a}_i s \in J_S\}.$$

Here we denote by J_S^m the direct product $J_S \times \cdots \times J_S$. We first comment that the above two modules are well defined as it is trivial to see that they are independent of the choice of $\tilde{a}_i$, since $q\mathcal{R} \subseteq J_S$. Secondly, we note that the $\mathcal{R}$-modules $\mathbf{a}^{\perp}(J_S)$ and $\mathcal{L}(\mathbf{a}, J_S)$ defined above are equivalent to that given in [40].

In this subsection, we view each element of $\mathcal{R}$ as its canonical embedding and work with the inner product space H. Compared with coefficient embedding, this leads to a different duality result. For $t \in \mathcal{R}$, we denote by $\bar{t}$ the polynomial $t(X^{-1})$, where $X^{-1} \in \mathcal{R}$ is the inverse of X. It is easy to check that $\sigma(\bar{t}) = \overline{\sigma(t)}$. By abuse of notation, we also denote by $\langle s, \bar{t}\rangle$ the inner product $\langle \sigma(s), \overline{\sigma(t)}\rangle = \mathrm{Tr}(st)$. Let $\mathcal{R}^{\vee} = \{a \in K \mid \mathrm{Tr}(a\mathcal{R}) \subseteq \mathbb{Z}\}$ be the fractional ideal corresponding to the dual lattice of $\mathcal{R}$. The following lemma gives an explicit expression of the dual lattice $\widehat{\mathbf{a}^{\perp}(J_S)}$.

Lemma 9. *Let $\mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X))$. Let $q = 1 \bmod n$ be a prime and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Given $S \subseteq \{1, \cdots, \varphi(n)\}$ and $\mathbf{a} \in \mathcal{R}_q^m$, viewing each element of $\mathcal{R}$ as its canonical embedding, we have:*

$$\widehat{\mathbf{a}^{\perp}(J_S)} = \frac{1}{q}\left\{(t_1, \cdots, t_m) \in (\mathcal{R}^{\vee})^m \mid \exists s \in \mathcal{R}^{\vee}, \forall i, t_i - \tilde{a}_i s \in J_{\bar{S}}\mathcal{R}^{\vee}\right\}.$$

Proof. Let $\mathcal{L}'(\mathbf{a}, J_{\bar{S}}) = \frac{1}{q}\left\{(t_1, \cdots, t_m) \in (\mathcal{R}^{\vee})^m \mid \exists s \in \mathcal{R}^{\vee}, \forall i, t_i - \tilde{a}_i s \in J_{\bar{S}}\mathcal{R}^{\vee}\right\}$. We first prove that $\mathcal{L}'(\mathbf{a}, J_{\bar{S}}) \subseteq \widehat{\mathbf{a}^{\perp}(J_S)}$. Let $\mathbf{t} = (t_1, \cdots, t_m) \in \mathcal{L}'(\mathbf{a}, J_{\bar{S}})$ and $\mathbf{t}' = (t'_1, \cdots, t'_m) \in \mathbf{a}^{\perp}(J_S)$. We shall prove that $\sum_i \langle t_i, t'_i\rangle = \sum_i \mathrm{Tr}(t_i t'_i) \in \mathbb{Z}$. To this end, we notice that by the definition of $\mathcal{L}'(\mathbf{a}, J_{\bar{S}})$, there exists $s \in \mathcal{R}^{\vee}$ such that $qt_i = \tilde{a}_i s + b_i$ and $b_i \in J_{\bar{S}}\mathcal{R}^{\vee}$. The fact that $J_S J_{\bar{S}} = \langle q\rangle$ implies $\mathrm{Tr}(b_i t'_i) = 0 \bmod q$. Also by definition, $\sum_i \tilde{a}_i t'_i = 0 \bmod q$. Therefore,

$$\sum_i \langle t_i, t'_i\rangle = \frac{1}{q}\sum_i \mathrm{Tr}((\tilde{a}_i s + b_i)t'_i) = \frac{1}{q}\mathrm{Tr}\left(s\sum_i \tilde{a}_i t'_i\right) + \frac{1}{q}\sum_i \mathrm{Tr}\left(b_i t'_i\right)$$

is an integer.

Next we prove $\widehat{\mathcal{L}'(\mathbf{a}, J_{\bar{S}})} \subseteq \mathbf{a}^{\perp}(J_S)$. Let $\mathbf{t} = (t_1, \cdots, t_m) \in \widehat{\mathcal{L}'(\mathbf{a}, J_{\bar{S}})}$. Since $\frac{1}{q}(J_{\bar{S}}\mathcal{R}^{\vee}, 0, \cdots, 0) \subseteq \mathcal{L}'(\mathbf{a}, J_{\bar{S}})$ and $J_{\bar{S}}J_S = \langle q\rangle$, we obtain $t_1 \in J_S$. For the same reason, we have $t_i \in J_S$ for any $i \in \{1, \cdots, m\}$. For any $v \in \mathcal{R}^{\vee}$, from the fact that $\frac{1}{q}(\tilde{a}_1, \cdots, \tilde{a}_m)v \in \mathcal{L}'(\mathbf{a}, J_{\bar{S}})$, we have that $\mathrm{Tr}(v\sum_i \tilde{a}_i t_i) = 0 \bmod q$, which means that $\sum_i \tilde{a}_i t_i = 0 \bmod q$. Thus $\mathbf{t} = (t_1, \cdots, t_m) \in \mathbf{a}^{\perp}(J_S)$ and the proof is completed. □

By scaling a certain factor, we obtain the following duality result between two families of module lattices $\mathbf{a}^{\perp}(J_S)$ and $\mathcal{L}(\mathbf{a}, J_S)$.

Lemma 10. *Let $\mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X))$ and $n' = \deg(\Theta_n(X))$. Let $q = 1 \bmod n$ be a prime and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Let $g = \prod_p (1 - X^{n/p}) \in \mathcal{R}$ where p runs over all odd primes dividing n. Given $S \subseteq \{1, \cdots, \varphi(n)\}$ and $\mathbf{a} \in \mathcal{R}_q^m$, viewing each element of $\mathcal{R}$ as its canonical embedding, we have:*

$$\widehat{\mathbf{a}^{\perp}(J_S)} = \frac{g}{qn'} \cdot \mathcal{L}(\mathbf{a}, J_{\bar{S}}).$$

Proof. According to Corollary 2.18 in [33], we have $R^{\vee} = \langle g/n'\rangle$. By Lemma 9, we get the result immediately. □

Next, we shall show a quantitative relationship between the first minima of $\widehat{\mathbf{a}^{\perp}(J_S)}$ and $\mathcal{L}(\mathbf{a}, J_{\bar{S}})$.

Lemma 11. *Let $\mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X))$ and $n' = \deg(\Theta_n(X))$. Let $q = 1 \bmod n$ be a prime and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Given $S \subseteq \{1, \cdots, \varphi(n)\}$ and $\mathbf{a} \in \mathcal{R}_q^m$, viewing each element of $\mathcal{R}$ as its canonical embedding, we have:*

$$\lambda_1^{\infty}\left(\widehat{\mathbf{a}^{\perp}(J_S)}\right) \geq \frac{\lambda_1^{\infty}(\mathcal{L}(\mathbf{a}, J_{\bar{S}}))}{qn'}.$$

Proof. Let $\mathbf{v} = (v_1, \cdots, v_m) \in \widehat{\mathbf{a}^{\perp}(J_S)}$ such that $\mathrm{T}_\infty(\mathbf{v}) = \lambda_1^\infty\left(\widehat{\mathbf{a}^{\perp}(J_S)}\right)$. By Lemma 10, we have that $(u_1, \cdots, u_m) \in \mathcal{L}(\mathbf{a}, J_{\bar{S}})$ where $u_i = \frac{qn'}{g} \cdot v_i$ for all $i \in \{1, \cdots, m\}$ and g is defined in Lemma 10. Since $g \in \mathcal{R}$, from the definition of $\mathcal{L}(\mathbf{a}, J_{\bar{S}})$, it follows that $\mathbf{u}' = (gu_1, \cdots, gu_m) = qn' \cdot (v_1, \cdots, v_m) \in \mathcal{L}(\mathbf{a}, J_{\bar{S}})$. Thus we conclude that $\lambda_1^\infty\left(\widehat{\mathbf{a}^{\perp}(J_S)}\right) = \mathrm{T}_\infty(\mathbf{v}) = \frac{\mathrm{T}_\infty(\mathbf{u}')}{qn'} \geq \frac{\lambda_1^\infty(\mathcal{L}(\mathbf{a}, J_{\bar{S}}))}{qn'}$. □

4.2 On the Absence of Unusually Short Vector in $\mathcal{L}(\mathbf{a}, J_S)$

Let $\mathcal{R}_q^\times$ be the set of all invertible elements of $\mathcal{R}_q$, *i.e.* $\mathcal{R}_q^\times = \mathcal{R}_q \setminus \bigcup_{i=1}^{\varphi(n)} I_{\{i\}}$. For $\mathbf{a} \hookleftarrow U((\mathcal{R}_q^\times)^m)$, the lattice $\mathcal{L}(\mathbf{a}, J_S)$ is nearly impossible to contain an unusually short vector for the ℓ_∞ norm with respect to canonical embedding.

Lemma 12. *Let $n > 2$ and $\mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X))$. Let $q = 1 \bmod n$ be a prime and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. For any $S \subseteq \{1, \cdots, \varphi(n)\}$, $m \geq 2$ and $\epsilon > 0$, viewing each element of $\mathcal{R}$ as its canonical embedding, we have $\lambda_1^\infty(\mathcal{L}(\mathbf{a}, J_S)) \geq q^{(1-\frac{1}{m})\frac{|S|}{\varphi(n)} - \epsilon}$ with probability $\geq 1 - \frac{2^{(2m+1)\varphi(n)}}{q^{\epsilon m \varphi(n)}}$ over the uniformly random choice of $\mathbf{a}$ in $(\mathcal{R}_q^\times)^m$.*

Proof. Let $\beta = (1 - \frac{1}{m})\frac{|S|}{\varphi(n)} - \epsilon$ and $B = q^\beta$. Let p be the probability over the randomness of $\mathbf{a}$ that $\lambda_1^\infty(\mathcal{L}(\mathbf{a}, J_S)) < B$.

Recall that by the definition, $\mathbf{t} \in \mathcal{L}(\mathbf{a}, J_S)$ is verified by finding an $s \in \mathcal{R}$ such that $\mathbf{t} - s\tilde{\mathbf{a}} \in J_S^m$, where $\tilde{\mathbf{a}} = (\tilde{a}_1, \cdots, \tilde{a}_m)$. It is easy to see that for any $s' \in s + J_S$, $\mathbf{t} - s'\tilde{\mathbf{a}} \in J_S^m$ still holds true. Therefore, we only need to consider a set of representatives of all cosets of J_S, say $\{s_1 \cdots, s_r\}$ with $r = \left|\mathcal{R}/J_S\right| = \left|\mathcal{R}_q/I_S\right|$. Now for a non-zero vector $\mathbf{t} \in \mathcal{R}^m$ with $\mathrm{T}_\infty(\mathbf{t}) < B$ and an s_j, we denote $p(\mathbf{t}, s_j) = \Pr_{\mathbf{a}}(\forall i, t_i - \tilde{a}_i s_j \in J_S)$ and $p_i(t_i, s_j) = \Pr_{a_i}(t_i - \tilde{a}_i s_j \in J_S)$. Then we have $p(\mathbf{t}, s_j) = \prod_i p_i(t_i, s_j)$.

For $f \in \mathcal{R}$, let $S(f) = \{i \in S \mid f(\phi_i) = 0 \bmod q\}$. It suffices to consider such $(\mathbf{t}, s_j)$ pairs that $S(s_j) = S(t_i)$ for all $i \in \{1, \cdots, m\}$; otherwise, we would have $p(\mathbf{t}, s_j) = 0$ due to the invertibility of a_i. For each such pair, we set $d = |S(s_j)|$. Notice that there are $(q-1)^{d+\varphi(n)-|S|}$ distinct a_i's in $\mathcal{R}_q^\times$ such that $t_i - \tilde{a}_i s_j \in J_S$, *i.e.* $p_i(t_i, s_j) = (q-1)^{d-|S|}$, then we have $p(\mathbf{t}, s_j) = \prod_{i=1}^m p_i(t_i, s_j) = (q-1)^{m(d-|S|)}$. Therefore, the probability p is bounded by

$$p \leq \sum_{0 \leq d \leq |S|} \sum_{\substack{S' \subseteq S \\ |S'| = d}} \sum_{\substack{j=1 \\ S(s_j) = S'}}^{r} \sum_{\substack{\mathbf{t} \in \mathcal{R}^m \\ \forall i, 0 < \mathrm{T}_\infty(t_i) < B \\ S(t_i) = S'}} (q-1)^{m(d-|S|)}.$$

For $|S'| = d$, let $N(B, d)$ be the number of $t \in \mathcal{R}$ such that $\mathrm{T}_\infty(t) \in (0, B)$ and $S(t) = S'$. We first show a lower bound of $\lambda_1^\infty(J_{S'})$. For any t such that $S' \subseteq S(t)$, the ideal $\langle t \rangle$ is a full-rank sub-ideal of the ideal $J_{S'}$. Thus, we have $\mathrm{N}(t) = \mathrm{N}(\langle t \rangle) \geq \mathrm{N}(J_{S'}) = q^d$. By equivalence of norms and arithmetic-geometric inequality, we conclude that $\mathrm{T}_\infty(t) \geq \frac{\mathrm{T}_2(t)}{\sqrt{\varphi(n)}} \geq \mathrm{N}(t)^{1/\varphi(n)} \geq q^{d/\varphi(n)}$, which

implies that $\lambda_1^{\infty}(J_{S'}) \geq q^{d/\varphi(n)}$. As a direct result, we get $N(B,d) = 0$ when $d \geq \beta\varphi(n)$.

We now suppose that $d < \beta\varphi(n)$. For any $\mathbf{c} \in H$ and $l > 0$, let $C(l, \mathbf{c}) = \{\mathbf{v} \in H \mid \|\mathbf{v} - \mathbf{c}\|_{\infty} < l\}$. We notice that $N(B,d)$ is at most the number of points of the lattice $J_{S'}$ in the region $C(B, \mathbf{0})$. For any two different points $\mathbf{v}_1, \mathbf{v}_2 \in J_{S'}$, it can be verified that $C(\lambda, \mathbf{v}_1) \bigcap C(\lambda, \mathbf{v}_2) = \emptyset$ where $\lambda = \lambda_1^{\infty}(J_{S'})/2$. For any $\mathbf{v} \in C(B, \mathbf{0})$, we also have that $C(\lambda, \mathbf{v}) \subseteq C(B + \lambda, \mathbf{0})$. Combining the fact that $\lambda_1^{\infty}(J_{S'}) \geq q^{d/\varphi(n)}$, it follows that $N(B,d) \leq \frac{\mathrm{vol}(C(B+\lambda,\mathbf{0}))}{\mathrm{vol}(C(\lambda,\mathbf{0}))} = (\frac{B}{\lambda} + 1)^{\varphi(n)} \leq 3^{\varphi(n)} q^{\beta\varphi(n)-d}$.

Notice that the number of subsets of S is $2^{|S|}$ and the number of s_j's satisfying $S(s_j) = S'$ is $(q-1)^{|S|-|S'|}$, a straightforward computation yields

$$p \leq 2^{|S|} \max_{d < \beta\varphi(n)} \frac{N(B,d)^m}{(q-1)^{(m-1)(|S|-d)}} \leq 2^{(2m+1)\varphi(n)} q^{-\varphi(n)m\epsilon}.$$

We now complete the proof. □

Remark The above proof makes use of ideas from [41], but we consider the case with respect to canonical embedding instead of coefficient embedding. It is remarked that for coefficient embedding, we can also obtain a similar conclusion for general cyclotomic rings by using the quantitative relationship between Euclidean norm and T_2-norm.

4.3 Improved Results on Regularity

Let χ be a distribution over $\mathcal{R}_q$. We denote by $\mathbb{D}_{\chi}$ the distribution of such tuple $(a_1, \cdots, a_m, \sum_{i=1}^m t_i a_i) \in (\mathcal{R}_q^{\times})^m \times \mathcal{R}_q$ where $a_i \hookleftarrow U(\mathcal{R}_q^{\times})$ and $t_i \hookleftarrow \chi$ for all $i \in \{1, \cdots, m\}$. The *regularity* of the generalized knapsack function $(t_1, \cdots, t_m) \mapsto \sum_{i=1}^m t_i a_i$ is the statistical distance between $\mathbb{D}_{\chi}$ and $U((\mathcal{R}_q^{\times})^m \times \mathcal{R}_q)$.

In [34], Micciancio discussed the regularity over general rings and used it to design one-way functions. Improved regularity results for power-of-2 and prime cyclotomic rings were proposed in [40, 44] respectively. However, the results in [40, 44] only focus on two special classes of cyclotomic rings and are under coefficient embedding. The regularity result with respect to canonical embedding was shown in [33] and applied to general cyclotomic rings, but it has some limitations for certain cryptographic applications.[9] Here, we will give an improved result that applies to general cyclotomic rings and has more flexibility than that in [33]. In particular, we will focus on the case where $m = 2$ for pNE applications.

Since $a_i \in \mathcal{R}_q^{\times}$, there are $q^{(m-1)(\varphi(n)-|S|)}$ elements of $\mathbf{a}^{\perp}(J_S)$ in $[0, q-1]^{m\varphi(n)}$. Thus we have that $|\mathbb{Z}^{m\varphi(n)}/\mathbf{a}^{\perp}(J_S)| = q^{\varphi(n)+(m-1)|S|}$. The following lemma can be proved by combining Lemmata 2, 5, 11 and 12.

Lemma 13. *Let $n > 2, \mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X))$ and $n' = \deg(\Theta_n(X))$. Let $q = 1 \bmod n$ be a prime and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Let $S \subseteq \{1, \cdots, \varphi(n)\}$, $m \geq 2, \epsilon >$*

[9] As discussed in [44], it does not suffice to construct pNE only from the regularity result in [33].

$0, \delta \in (0, \frac{1}{2})$. *Let* $r \geq n'\sqrt{\ln(2m\varphi(n)(1+1/\delta))/\pi} \cdot q^{\frac{1}{m}+(1-\frac{1}{m})\frac{|S|}{\varphi(n)}+\epsilon}$, $\mathbf{c} \in \mathbb{R}^{m\varphi(n)}$ *and* $\mathbf{t} \hookleftarrow \widetilde{D}_{\mathbb{Z}^{m\varphi(n)},r,\mathbf{c}}$. *Then for all except a fraction* $\leq 2^{(2m+1)\varphi(n)}q^{-\epsilon m\varphi(n)}$ *of* $\mathbf{a} \in (\mathcal{R}_q^\times)^m$, *we have*

$$\Delta\left(\mathbf{t} \bmod \mathbf{a}^\perp(J_S); U(\mathbb{Z}^{m\varphi(n)}/\mathbf{a}^\perp(J_S))\right) \leq 2\delta$$

and

$$\left|\widetilde{D}_{\mathbb{Z}^{m\varphi(n)},r,\mathbf{c}}(\mathbf{a}^\perp(J_S)) - q^{-\varphi(n)-(m-1)|S|}\right| \leq 2\delta.$$

Remark Let $\mathbf{t} \in \mathcal{R}^m$ be a Gaussian sample in Lemma 13. Choose $\delta = q^{-cn}$ with $c = O(1)$ and $r = \widetilde{O}(n^{1.5})q^{\frac{1}{m}+\epsilon'}$. From Lemma 15, we will see that $\|\mathbf{t}\| = \widetilde{O}(n^{1.5})\sqrt{m}q^{\frac{1}{m}+\epsilon'}$ when n is a prime power. The size of Gaussian sample is asymptotically the same as that in [40] when $n = 2^k$, and smaller than that in [44] when n is a prime. We also remark that the regularity result in [33] allows a smaller sample width ($r \geq 2\varphi(n) \cdot q^{\frac{1}{m}+\epsilon'}$), but it seems to work only for the case of $\delta = 2^{-\Theta(n)}$.

From the generalized knapsack function $(t_1, \cdots, t_m) \mapsto \sum_{i=1}^m t_i a_i$, we obtain an isomorphism $\mathbb{Z}^{m\varphi(n)}/\mathbf{a}^\perp(J_\emptyset) \cong \mathcal{R}_q$. Thus Lemma 13 gives immediately the following regularity result.

Theorem 2. *Let* $n > 2, \mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X))$ *and* $n' = \deg(\Theta_n(X))$. *Let* $q = 1 \bmod n$ *be a prime and* $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. *Let* $m \geq 2, \epsilon > 0, \delta \in (0, \frac{1}{2})$ *and* $a_i \hookleftarrow U(\mathcal{R}_q^\times)$ *for any* $i \in \{1, \cdots, m\}$. *Then, for* $\mathbf{t} \hookleftarrow \widetilde{D}_{\mathbb{Z}^{m\varphi(n)},r}$ *with* $r \geq n'\sqrt{\ln(2m\varphi(n)(1+1/\delta))/\pi} \cdot q^{\frac{1}{m}+\epsilon}$, *we have*

$$\Delta\left(\left(a_1, \cdots, a_m, \sum_{i=1}^m t_i a_i\right); U\left((\mathcal{R}_q^\times)^m \times \mathcal{R}_q\right)\right) \leq 2\delta + 2^{(2m+1)\varphi(n)}q^{-\epsilon m\varphi(n)}.$$

4.4 Properties of Prime Power Cyclotomic Rings

Prime power cyclotomic rings are a kind of fundamental cyclotomic rings with a relatively simple form. All cyclotomic rings can be decomposed into the tensor product of prime power cyclotomic rings [33][10]. In this paper, we will construct a class of provably secure NTRU schemes over prime power cyclotomic rings. To this end, we list some useful properties of this kind of rings.

Firstly we prove several basic facts about singular values of the canonical embedding transformation of a prime power cyclotomic ring. These facts profile the geometry of prime power cyclotomic rings under coefficient embedding and canonical embedding.

Lemma 14. *Let* $n = d^\nu$ *with* d *a prime and* $\mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X))$. *Let* $\mathbf{V}$ *be the canonical embedding transformation of* $\mathcal{R}$ *and* $s_1(\mathbf{V}), \cdots, s_{\varphi(n)}(\mathbf{V})$ *be all singular values of* $\mathbf{V}$ *in increasing order. Then* $s_1(\mathbf{V}) = \cdots = s_{\frac{n}{d}}(\mathbf{V}) = \sqrt{\frac{n}{d}}$ *and others equal* $\sqrt{n}$.

[10] This property is useful under canonical embedding, but we may not need to use it in this paper.

Proof. It suffices to calculate the eigenvalues of $\mathbf{U} = \mathbf{V}\mathbf{V}^*$. Let $\omega_1, \cdots, \omega_{\varphi(n)}$ be all roots of $\Phi_n(X)$, then $\mathbf{V} = (\omega_j^{i-1})_{1 \le i,j \le \varphi(n)}$. Let $\mathbf{U} = (u_{ij})_{1 \le i,j \le \varphi(n)}$. By a routine computation, it follows that

$$u_{ij} = \begin{cases} \varphi(n), \text{ for } i = j; \\ -\frac{n}{d}, \quad \text{for } i \neq j \text{ and } i = j \bmod \frac{n}{d}; \\ 0, \qquad \text{for } i \neq j \bmod \frac{n}{d}. \end{cases}$$

Let $\mathbf{e}_i$ be the i-th row of the $\varphi(n)$-dimensional identity matrix. Let $\mathbf{x}_i = \sum_{j=i \bmod \frac{n}{d}} \mathbf{e}_j$ where $i \in \{1, \cdots, \frac{n}{d}\}$ and the subindex j is within $\{1, \cdots, \varphi(n)\}$. It can be verified that all $\frac{n}{d}$ $\mathbf{x}_i$'s are eigenvectors of $\mathbf{U}$ with respect to eigenvalue $\frac{n}{d}$. Let $\mathbf{y}_{ij} = \mathbf{e}_i - \mathbf{e}_{i+\frac{jn}{d}}$ where $i \in \{1, \cdots, \frac{n}{d}\}$ and $j \in \{1, \cdots, d-2\}$. These $\frac{n(d-2)}{d} = \varphi(n) - \frac{n}{d}$ $\mathbf{y}_{ij}$'s are also eigenvectors of $\mathbf{U}$ and corresponding eigenvalues equal n. Notice that all $\mathbf{x}_i$'s and $\mathbf{y}_{ij}$'s are $\varphi(n)$ linearly independent vectors, hence we complete the proof. □

Combining Lemmata 8 and 14, we obtain a tail inequality immediately. It should be remarked that Lemmata 7 and 14 can also yield a tail inequality: the tail bound may be smaller by a logarithmic factor at most but is also likely to be larger by a polynomial factor of n for certain cases, such as $n = d$. Thus we only use the following result in later discussion.

Lemma 15. *Let $n = d^\nu$ with d a prime and $\mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X))$. For $r > 0$, then*

$$\Pr_{f \hookleftarrow \tilde{D}_{\mathbb{Z}^{\varphi(n)}, r}} \left(\|f\| \ge r\sqrt{\frac{2(d-1)}{d} \cdot \omega(\ln n)} \right) \le n^{-\omega(1)}.$$

The multiplicative *expansion factor* of $\mathcal{R}$ is defined as $\gamma_\times(\mathcal{R}) = \max_{f,g \in \mathcal{R}} \frac{\|fg\|}{\|f\|\|g\|}$. For prime and power-of-2 cyclotomic rings, their expansion factors are of size $O(\sqrt{n})$ where n is the order (see [22, 44]). The following lemma indicates that, for general prime power cyclotomic rings, their expansion factors are well-bounded as well.

Lemma 16. *Let $n = d^\nu$ with d a prime and $\mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X))$. For any $f, g \in \mathcal{R}$, we have $\|fg\|_\infty \le 2\|f\|\|g\|$ and $\|fg\| \le 2\sqrt{\varphi(n)}\|f\|\|g\|$.*

Proof. We first consider the multiplication over the ring $\mathcal{R}' = \mathbb{Z}[X]/(X^n - 1)$. Let $f', g' \in \mathcal{R}'$ be the polynomials with the same coefficients as f, g respectively, *i.e.* all leading coefficients are 0. Let $h' \in \mathcal{R}'$ be the product of f' and g'. We denote by $(f'_0, \cdots, f'_{n-1})$, $(g'_0, \cdots, g'_{n-1})$ and $(h'_0, \cdots, h'_{n-1})$ the coefficient vectors of f', g' and h'. It is known that $h'_i = \sum_{j=0}^{n-1} f'_j g'_{(i-j) \bmod n}$. By Cauchy-Schwarz inequality, we have $|h'_i| \le \|f'\|\|g'\| = \|f\|\|g\|$ for any i.

Let $h = fg \in \mathcal{R}$. We deduce that $h = h' \bmod \Phi_n(X)$ from the fact that $\Phi_n(X)$ is a factor of $X^n - 1$. Notice that $X^l = -(X^{\frac{n}{d} \cdot (d-2)} + \cdots + X^{\frac{n}{d}} + 1)X^{l-\varphi(n)}$ for

any $l \in [\varphi(n), n)$, hence we have

$$h = \sum_{i=0}^{\varphi(n)-1} \left(h'_i - h'_{\varphi(n)+(i \bmod \frac{n}{d})}\right) X^i.$$

It leads to that

$$\|h\|_\infty = \max_{0 \le i < \varphi(n)} \{|h'_i - h_{\varphi(n)+(i \bmod \frac{n}{d})}|\} \le 2 \max_{0 \le i < n} \{|h'_i|\} \le 2\|f\|\|g\|.$$

Then we conclude that $\|h\| \le \sqrt{\varphi(n)}\|h\|_\infty \le 2\sqrt{\varphi(n)}\|f\|\|g\|$. □

5 pNE over Prime Power Cyclotomic Rings

In this section, we will describe a class of NTRUEncrypt over general prime power cyclotomic rings whose IND-CPA security can be reduced from RLWE and approximate Ideal-SVP. Our scheme is adapted from that in [40, 44] with modified key generation algorithm. We denote by $\mathsf{pNE}(n, d, \nu, q, p, r, \alpha, k)$ the provably secure NTRU specified by the following public parameters.

- Let $\mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X))$ and its order $n = d^\nu$ where d is a prime.
- Let $q = 1 \bmod n$ be a prime and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. The ciphertext space is $\mathcal{R}_q$.
- Let $p \in \mathcal{R}_q^\times$ be of small norm, such as $p = 2$ or $p = x + 3$. The message space is $\mathcal{R}/p\mathcal{R}$.
- The parameter r is the width of discrete Gaussian distribution used for key generation.
- The parameters α and k determine the RLWE error distribution.

Three main algorithms are listed as follows.

- **Key Generation.** Sample f' from $\widetilde{D}_{\mathbb{Z}^{\varphi(n)},r}$; if $f = pf' + 1 \bmod q \notin \mathcal{R}_q^\times$, resample. Sample g from $\widetilde{D}_{\mathbb{Z}^{\varphi(n)},r}$; if $g \bmod q \notin \mathcal{R}_q^\times$, resample. Then return private key $sk = f \in \mathcal{R}_q^\times$ and public key $pk = h = pg/f \in \mathcal{R}_q^\times$.
- **Encryption.** Given message $M \in \mathcal{R}/p\mathcal{R}$, let $t = \sqrt{n'}\alpha q \left(\frac{\varphi(n)k}{\log(\varphi(n)k)}\right)^{1/4}$ where $n' = \deg(\Theta_n(X))$, set $s, e \hookleftarrow \overline{\psi_t^{n'}}$ and return ciphertext $C = hs + pe + M \in \mathcal{R}_q$.
- **Decryption.** Given ciphertext C and private key f, compute $C' = (fC \bmod q)$ and return $C' \bmod p$.

In the rest of this section, we will give an analysis of the above algorithms and propose a set of parameters that make pNE workable and provably secure.

5.1 Key Generation

Gaussian sampler is a core component of the key generation algorithm. Since our parameter conditions are much stronger than that in Lemma 6, we now assume that a polynomial-time perfect discrete Gaussian sampler is available. First, we show that the key generation algorithm terminates in expected polynomial time for selective parameters.

Lemma 17. *Let $n = d^\nu$ with d a prime and $\mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X))$. Let $q = 1 \bmod n$ be a prime and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. For any $\delta \in (0, 1/2)$, choose $r \geq \varphi(n)\sqrt{\ln(2\varphi(n)(1+1/\delta))/\pi} \cdot q^{1/\varphi(n)}$, then we have*

$$\Pr_{f' \hookleftarrow \widetilde{D}_{\mathbb{Z}^{\varphi(n)}, r}} \left((p \cdot f' + a \bmod q) \notin \mathcal{R}_q^\times \right) \leq \varphi(n)(1/q + 2\delta)$$

holds for $a \in \mathcal{R}$ and $p \in \mathcal{R}_q^\times$

Proof. Notice that the norm of $J_{\{k\}}$ is $\mathrm{N}(J_{\{k\}}) = q$ and the discriminant of the cyclotomic field $K = \mathbb{Q}[X]/(\Phi_n(X))$ is $\Delta_K \leq \varphi(n)^{\varphi(n)}$ (see [33] for the latter). The volume of the ideal lattice $\sigma(J_{\{k\}})$ is given by $\mathrm{vol}(\sigma(J_{\{k\}})) = \mathrm{N}(J_{\{k\}})\sqrt{\Delta_K}$. Thus we have that $\lambda_1(\sigma(J_{\{k\}})) \leq \sqrt{\varphi(n)}\,\mathrm{vol}(\sigma(J_{\{k\}}))^{1/\varphi(n)} \leq \varphi(n) q^{1/\varphi(n)}$ by Minkowski's first theorem. Since $\lambda_{\varphi(n)}(\sigma(J_{\{k\}})) = \lambda_1(\sigma(J_{\{k\}}))$, by Lemma 1, we have $r \geq \eta_\delta(\sigma(J_{\{k\}}))$. Together with Lemma 5, it leads to that the probability of $p \cdot f' + a = 0 \bmod J_{\{k\}}$ is at most $1/q + 2\delta$. The final result is proved by using the union bound. □

Next we give a result showing that the sizes of secret polynomials f and g are small with overwhelming probability. Despite that f and g are sampled from Gaussian using T_2-norm, to compare with NTRU, we measure their sizes by Euclidean norms of their coefficient vectors.

Lemma 18. *Let $n = d^\nu$ with d a prime and $q > 8n$ be a prime satisfying $q = 1 \bmod n$. Let $r \geq \varphi(n)\sqrt{\frac{2\ln(6\varphi(n))}{\pi}} \cdot q^{1/\varphi(n)}$. Then with probability $\geq 1 - n^{-\omega(1)}$, the secret key polynomials f, g satisfy*

$$\|f\| \leq \omega\left(\sqrt{n \ln n}\right) \cdot \|p\| r \quad \text{and} \quad \|g\| \leq \omega\left(\sqrt{\ln n}\right) \cdot r.$$

If $\deg p = 0$, then $\|f\| \leq \omega\left(\sqrt{\ln n}\right) \cdot \|p\| r$ with probability $\geq 1 - n^{-\omega(1)}$.

Proof. Applying Lemma 15, we have

$$\Pr_{g \hookleftarrow \widetilde{D}_{\mathbb{Z}^{\varphi(n)}, r}} \left(\|g\| \geq \omega\left(\sqrt{\ln n}\right) \cdot r \right) \leq n^{-\omega(1)}.$$

Let $\delta = \frac{1}{10\varphi(n) - 1}$. Since $r \geq \varphi(n)\sqrt{\ln(2\varphi(n)(1+1/\delta))/\pi} \cdot q^{1/\varphi(n)}$, Lemma 17 yields

$$\begin{aligned}
&\Pr_{g \hookleftarrow \widetilde{D}_{\mathbb{Z}^{\varphi(n)}, r}} \left(\|g\| \geq \omega\left(\sqrt{\ln n}\right) \cdot r \mid g \in \mathcal{R}_q^\times \right) \\
\leq &\frac{\Pr_{g \hookleftarrow \widetilde{D}_{\mathbb{Z}^{\varphi(n)}, r}} \left(\|g\| \geq \omega\left(\sqrt{\ln n}\right) \cdot r \right)}{\Pr_{g \hookleftarrow \widetilde{D}_{\mathbb{Z}^{\varphi(n)}, r}} \left(g \in \mathcal{R}_q^\times \right)} \\
\leq &n^{-\omega(1)} \cdot \frac{1}{1 - \varphi(n)(1/q + 2\delta)} = n^{-\omega(1)}.
\end{aligned}$$

Thus we get that $\|g\| \leq \omega\left(\sqrt{\ln n}\right) \cdot r$ with probability $\geq 1 - n^{-\omega(1)}$. The same argument holds true for the polynomial f' such that $f = p \cdot f' + 1$.

If $\deg p = 0$, we have $\|f\| \leq 1 + \|p\|\|f'\| \leq \omega\left(\sqrt{\ln n}\right) \cdot \|p\|r$ with probability $\geq 1 - n^{-\omega(1)}$. For general cases, applying Lemma 16, we know that $\|f\| \leq 1 + 2\sqrt{\varphi(n)}\|p\|\|f'\| \leq \omega\left(\sqrt{n \ln n}\right) \cdot \|p\|r$ with probability $\geq 1 - n^{-\omega(1)}$. □

For power-of-2 and prime cyclotomic rings, sampling f and g with certain width r makes the public key almost uniform over $\mathcal{R}_q^\times$, which is a remarkable property for provably secure NTRU. Similar conclusion holds for general cyclotomic rings as well, by considering the Gaussian sampling with respect to canonical embedding.

Theorem 3. *Let $n > 7$ and $\mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X))$. Let $q = 1 \bmod n$ be a prime and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Let $D_{r,z}^\times$ be the discrete Gaussian $\widetilde{D}_{\mathbb{Z}^{\varphi(n)},r}$ restricted to $z + \mathcal{R}_q^\times + q\mathbb{Z}^{\varphi(n)}$. Let $\epsilon \in (0, 1/3)$ and choose $r \geq n^{1.5}\sqrt{\ln(8nq)} \cdot q^{\frac{1}{2}+\epsilon}$, then we have*

$$\Delta\left(\frac{y_1 + p \cdot D_{r,z_1}^\times}{y_2 + p \cdot D_{r,z_2}^\times} \bmod q; U(\mathcal{R}_q^\times)\right) \leq \frac{65^{\varphi(n)}}{q^{\lfloor \epsilon\varphi(n) \rfloor}}$$

for $p \in \mathcal{R}_q^\times$, $y_i \in \mathcal{R}_q$ and $z_i = -y_i p^{-1} \bmod q$ for $i \in \{1, 2\}$.

Remark The proof essentially follows the same approach in [40], but some differences still need to be treated. Thus we include the proof in Appendix B for reference.

5.2 Decryption

A successful decryption is ensured by the fact that a polynomial with all coefficients within $[-\frac{q}{2}, \frac{q}{2})$ keeps unchanged after the reduction modulo q. In the decryption algorithm, we calculate a middle term $C' = fC = pgs + pfe + fM \bmod q$. We now estimate the ℓ_∞ norms of pgs, pfe and fM respectively.

Both s and e follow the "easy-to-use" RLWE error distribution [14] that is based on spherical Gaussian rather than classical discrete Gaussian. In [44], the authors gave a tail inequality for such error term and used it to estimate the norms of pgs and pfe. We now propose an improved bound for the norms of pgs and pfe. The main idea is to treat pgs as one term rather than consider pg and s separately, which makes a better use of the properties of Gaussian.

Lemma 19. *Let $n = d^\nu > 7$ with d a prime and $\mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X))$. Let $n' = \deg(\Theta_n(X))$. We view each element of $\mathcal{R}$ as its coefficient vector. For any fixed $y \in \mathcal{R}$ and $t \geq \sqrt{n}$, we have*

$$\Pr_{z \hookleftarrow \psi_t^{n'}}\left(\|yz\|_\infty \geq \omega\left(\sqrt{\ln n}\right)\|y\|t\right) \leq n^{-\omega(1)}.$$

Proof. Let $z = z^{(1)} + z^{(2)}$ where $z^{(1)} = z' \bmod \Phi_n(X)$ with $z' \hookleftarrow \psi_t^{n'}$ and $z^{(2)} = \sum_{i=0}^{\varphi(n)-1} \epsilon_i X^i$ with $\epsilon_i \in [-\frac{1}{2}, \frac{1}{2})$ for any i. Next we only prove the case of d being an odd prime and the same argument holds true for $d = 2$.

Let $(z'_0, \cdots, z'_{n-1})$ be the coefficient vector of z' where all z_i's follow ψ_t. Let $\mathcal{R}' = \mathbb{Q}[X]/(\Theta_n(X))$. Let $y' \in \mathcal{R}'$ be the polynomial with the same coefficients as y, *i.e.* all leading coefficients are 0, and $w' = y'z' \in \mathcal{R}'$. We denote by $(y'_0, \cdots, y'_{n-1})$ and $(w'_0, \cdots, w'_{n-1})$ the coefficient vectors of y' and w' respectively. It is known that $w'_i = \sum_{j=0}^{n-1} z'_j y'_{(i-j) \bmod n}$. Notice that $yz^{(1)} = w' \bmod \Phi_n(X)$, we have that the i-th coefficient of $yz^{(1)}$ is $c_i = w'_i - w'_{\varphi(n)+(i \bmod \frac{n}{d})} = \sum_{j=0}^{n-1} z'_j y_{i,j}$ where $y_{i,j} = y'_{(i-j) \bmod n} - y'_{(\varphi(n)+(i \bmod \frac{n}{d})-j) \bmod n}$. Since all z'_j's are independently drawn from ψ_t, the term $\sum_{j=0}^{n-1} z'_j y_{i,j}$ follows the distribution ψ_{Yt} where $Y = \sqrt{\sum_{j=0}^{n-1} y_{i,j}^2} \leq 2\|y\|$. By Gaussian tail inequality (derived from the Chernoff bound), for any i, we have

$$\Pr\left(|c_i| \geq \omega\left(\sqrt{\ln n}\right) \|y\| t\right) \leq n^{-\omega(1)}.$$

By the union bound, it follows that

$$\Pr\left(\|yz^{(1)}\|_\infty \geq \omega\left(\sqrt{\ln n}\right) \|y\| t\right) \leq n^{-\omega(1)}.$$

For $\|yz^{(2)}\|_\infty$, from Lemma 16, we have $\|yz^{(2)}\|_\infty \leq \sqrt{\varphi(n)}\|y\|$. Due to the fact $t \geq \sqrt{n}$ and $\|yz\|_\infty \leq \|yz^{(1)}\|_\infty + \|yz^{(2)}\|_\infty$, we now complete the proof. □

Together with Lemmata 18 and 16, we obtain a bound of the norms of pgs and pfe.

Lemma 20. *In* $\mathsf{pNE}(n, d, \nu, q, p, r, \alpha, k)$, $t = \sqrt{n'}\alpha q \left(\frac{\varphi(n)k}{\log(\varphi(n)k)}\right)^{1/4} > \sqrt{n}$ *where* $n' = \deg(\Theta_n(X))$. *Then we have*

$$\max\{\|pgs\|_\infty, \|pfe\|_\infty\} \leq \omega(n \log n) \|p\|^2 rt$$

with probability at least $1 - n^{-\omega(1)}$. *In particular, if* $\deg p = 0$, *then*

$$\max\{\|pgs\|_\infty, \|pfe\|_\infty\} \leq \omega(\log n) \|p\|^2 rt$$

with probability at least $1 - n^{-\omega(1)}$.

For the term fM, its norm can be bounded as well.

Lemma 21. *In* $\mathsf{pNE}(n, d, \nu, q, p, r, \alpha, k)$, *we have* $\|fM\|_\infty \leq \omega\left(\sqrt{n^3 \log n}\right) \cdot \|p\|^2 r$ *with probability at least* $1 - n^{-\omega(1)}$. *In particular, if* $\deg p = 0$, *then* $\|fM\|_\infty \leq \omega\left(\sqrt{n \log n}\right) \cdot \|p\|^2 r$ *with probability at least* $1 - n^{-\omega(1)}$.

Proof. By reducing modulo the pX^i's, we can write M into $\sum_{i=0}^{\varphi(n)-1} \epsilon_i pX^i$ with $\epsilon_i \in (-\frac{1}{2}, \frac{1}{2}]$ and then get $\|M\| \leq 2\sqrt{\varphi(n)}\|\sum_{i=0}^{\varphi(n)-1} \epsilon_i X^i\|\|p\| \leq \varphi(n)\|p\|$ from Lemma 16. If $\deg p = 0$, we have $\|M\| = \|p\| \cdot \|\sum_{i=0}^{\varphi(n)-1} \epsilon_i X^i\| \leq \frac{\sqrt{\varphi(n)}}{2}\|p\|$. Then, combining Lemmata 18 and 16 with the above result, the proof is completed. □

Combining Lemmata 20 and 21, we give a set of parameters such that pNE enjoys a high probability of successful decryption.

Theorem 4. *Let* $t = \sqrt{n'}\alpha q \left(\frac{\varphi(n)k}{\log(\varphi(n)k)}\right)^{1/4} > \sqrt{n}$ *where* $n' = \deg(\Theta_n(X))$. *If* $\omega(n \log n)\|p\|^2 rt/q < 1$ *(resp.* $\omega(\log n)\|p\|^2 rt/q < 1$ *if* $\deg p = 0$*), then the decryption algorithm of* pNE *recovers* M *with probability* $1 - n^{-\omega(1)}$ *over the choice of* s, e, f, g.

5.3 Security Reduction and Parameters

The provable security of pNE is guaranteed by the following theorem. The proof totally follows from that in [44] and thus we omit it.

Lemma 22. *Let* $n = d^\nu > 7$ *with* d *a prime and* $\mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X))$. *Let* $q > 8n$ *be a prime congruent to* 1 *modulo* n *and* $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. *Let* $p \in \mathcal{R}_q^\times$ *and* $t = \sqrt{n'}\alpha q \left(\frac{\varphi(n)k}{\log(\varphi(n)k)}\right)^{1/4} > \sqrt{n}$ *where* $n' = \deg(\Theta_n(X))$. *Let* $\epsilon \in (0, 1/3)$ *and* $r \geq n^{1.5}\sqrt{\ln(8nq)} \cdot q^{\frac{1}{2}+\epsilon}$. *If there exists an* IND-CPA *attack against* pNE *that runs in time* T *and has success probability* $1/2+\delta$, *then there exists an algorithm solving* $\mathsf{RLWE}_{q,\psi,k}$ *with* $\psi = \psi_t^{n'}$ *that runs in time* $T' = T + O(kn)$ *and has success probability* $1/2 + \delta'$ *where* $\delta' = \delta/2 - q^{-\Omega(n)}$.

Combining Lemma 22 with Theorems 4 and 1, we get our main result.

Theorem 5. *Let* $n = d^\nu > 7$ *with* d *a prime and* $\mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X))$. *Suppose* $q = 1 \bmod n$ *is a prime of size* $\mathrm{poly}(n)$ *and* $q^{\frac{1}{2}-\epsilon} = \omega\left(n^{3.25}\log^2 n\|p\|^2\right)$ *(resp.* $q^{\frac{1}{2}-\epsilon} = \omega\left(n^{2.25}\log^2 n\|p\|^2\right)$, *if* $\deg p = 0$*) for any* $\epsilon \in (0, 1/3)$ *and* $p \in \mathcal{R}_q^\times$. *Let* $r = n^{1.5}\sqrt{\ln(8nq)} \cdot q^{\frac{1}{2}+\epsilon}$ *and* $t = \sqrt{n'}\alpha q \left(\frac{\varphi(n)k}{\log(\varphi(n)k)}\right)^{1/4}$ *where* $n' = \deg(\Theta_n(X))$, $k = O(1)$ *and* $\alpha q = \Omega(\log^{0.75} n)$. *If there exists an* IND-CPA *attack against* $\mathsf{pNE}(n, d, \nu, q, p, r, \alpha, k)$ *that runs in time* $\mathrm{poly}(n)$ *and has success probability* $1/2 + 1/\mathrm{poly}(n)$, *then there exists a* $\mathrm{poly}(n)$*-time algorithm solving* γ*-Ideal-*SVP *on ideal lattices in* $\mathbb{Z}[X]/(\Phi_n(X))$ *with* $\gamma = \tilde{O}\left(\sqrt{n}q/\log^{0.75} n\right)$. *Moreover, the decryption success probability exceeds* $1 - n^{-\omega(1)}$ *over the choice of the encryption randomness.*

By choosing $\epsilon = o(1)$ and p to be a constant number, the minimal modulus q for which pNE holds is $\tilde{\Omega}(n^{4.5})$, and the minimal approximate factor γ is $\tilde{O}(n^5)$. For the case $d = 2$, our results are asymptotically the same as the improved version shown in [41] (note that the original version was described in [40]). Our result improves that in [44] by a factor of $\tilde{\Theta}(n^3)$ for the case where n is a prime, as the smallest q and γ shown in [44] are $\tilde{\Omega}(n^{7.5})$ and $\tilde{O}(n^8)$ respectively. Moreover, our result shows that pNE over general prime power cyclotomic rings can achieve asymptotically same efficiency as that over power-of-2 cyclotomic rings that are used widely but scarce. Thus, the NTRU scheme in this paper has better compactness and wider applicability.

6 Some Remarks on Further Extension

A recent paper [38] demonstrates a polynomial-time quantum reduction from worst-case ideal lattice problems to RLWE for general rings, which provides a theoretical grounding for the further extension of pNE.

Given a monic irreducible polynomial $P(X) \in \mathbb{Z}[X]$ of degree n, let $K = \mathbb{Q}[X]/(P(X))$ and $\mathcal{R} = \mathbb{Z}[X]/(P(X))$ be an order in K. Let q be a prime such that $P(X)$ splits into n distinct linear factors modulo q[11]. Let $\mathcal{R}^\vee = \{a \in K \mid \mathrm{Tr}(a\mathcal{R}) \subseteq \mathbb{Z}\}$. We also follow the definitions of $\mathcal{R}$-modules and ideals shown in Sect. 4.

Under above setting, we observe that Lemmata 9 and 12 still can be proved following almost the same approach. It is worth noting that the ideals that we discuss are in $\mathcal{R}$ rather than the ring of integers of K, which is a little different from the setting in [38][12]. It also holds that $\mathrm{N}(t) = |\mathcal{R}/t\mathcal{R}|$ for any $t \in \mathcal{R}$ (see [11]), which ensures that all proofs go through. However, Lemmata 10 and 11 require some modifications to apply to general case. Note that the scaling factor (before $\mathcal{L}(\mathbf{a}, J_{\bar{S}})$) in Lemma 10 is exclusive for cyclotomic rings. For general case, the duality result can be that $\widehat{\mathbf{a}^\perp(J_S)} = \frac{1}{qP'} \cdot \mathcal{L}(\mathbf{a}, J_{\bar{S}})$ where $P' \in \mathcal{R}$ is the derivative of $P(X)$, thanks to the fact $\mathcal{R}^\vee = \frac{1}{P'}\mathcal{R}$ (see [10]). We define a function as

$$\alpha(P) = \min_{s \in \mathcal{R}, s \neq 0} \mathrm{T}_\infty(sP').$$

Using a similar proof of Lemma 11, we can obtain a quantitative relationship (perhaps not optimal)

$$\lambda_1^\infty\left(\widehat{\mathbf{a}^\perp(J_S)}\right) \geq \frac{\lambda_1^\infty(\mathcal{L}(\mathbf{a}, J_{\bar{S}}))}{q\alpha(P)}.$$

As a direct consequence, we get the following regularity result for general rings, which shows that $\alpha(P)$ is relevant to the lower bound of Gaussian width making the public key uniform.

Proposition 1. *Let $P(X) \in \mathbb{Z}[X]$ be a monic irreducible polynomial of degree $n > 2$ and $\mathcal{R} = \mathbb{Z}[X]/(P(X))$. Let $\alpha(P) = \min_{s \in \mathcal{R}, s \neq 0} \mathrm{T}_\infty(sP')$ where P' is the derivative of $P(X)$. Suppose q is a prime such that $P(X)$ splits into n distinct linear factors modulo q. Let $S \subseteq \{1, \cdots, n\}$, $m \geq 2, \epsilon > 0, \delta \in (0, \frac{1}{2})$, and choose $r \geq \alpha(P)\sqrt{\ln(2mn(1+1/\delta))/\pi} \cdot q^{\frac{1}{m}+(1-\frac{1}{m})\frac{|S|}{n}+\epsilon}$, $\mathbf{c} \in \mathbb{R}^{mn}$ and $\mathbf{t} \hookleftarrow \widetilde{D}_{\mathbb{Z}^{mn},r,\mathbf{c}}$. Then for all except a fraction $\leq 2^{(2m+1)n}q^{-\epsilon mn}$ of $\mathbf{a} \in (\mathcal{R}_q^\times)^m$, we have*

$$\Delta\left(\mathbf{t} \bmod \mathbf{a}^\perp(J_S); U(\mathbb{Z}^{mn}/\mathbf{a}^\perp(J_S))\right) \leq 2\delta$$

and

$$\left|\widetilde{D}_{\mathbb{Z}^{mn},r,\mathbf{c}}(\mathbf{a}^\perp(J_S)) - q^{-n-(m-1)|S|}\right| \leq 2\delta.$$

[11] As discussed in [41], a more general case that $P(X)$ splits into distinct factors of same degree may be treated using similar arguments.

[12] If K is a cyclotomic field, its ring of integers is $\mathcal{R}$.

For a fixed Gaussian width r, Lemma 8 implies an attribute relevant to the Euclidean lengths of the secret polynomials:

$$\beta(P) = \sqrt{\sum_{i=1}^{n} \frac{1}{s_i(\mathbf{V})^2}}$$

where $\mathbf{V}$ is the canonical embedding transformation and $s_i(\mathbf{V})$'s are its singular values. More precisely, it holds that $\|f'\|, \|g\| \leq r\beta(P)\omega(\sqrt{\log n})$ with overwhelming probability where $f = pf' + 1$ and g are the secret keys. Moreover, the expansion factor of $\mathcal{R}$, denoted by $\gamma(P) = \gamma_\times(\mathcal{R})$, also affects the sizes of parameters for successful decryption.

In practice, it may be hard to calculate $\alpha(P), \beta(P)$ and $\gamma(P)$, but we can replace them by their upper bounds during estimating parameters. Next we are to discuss some concrete polynomials.

Cyclotomic Polynomial For general cyclotomic polynomials, their $\alpha(P)$ are well-bounded by the cyclotomic indices.

Proposition 2. *For any $n > 0$, $\alpha(\Phi_n) \leq n'$ where $n' = \deg(\Theta_n(X))$.*

Proof. Let $s = \Theta_n(X)/\Phi_n(X)$ and $P(X) = \Phi_n(X)$, then $\alpha(P) \leq \mathrm{T}_\infty(sP'(X))$. Notice that $n'X^{n'-1} = \Theta_n'(X) = sP'(X) + s'P(X)$, we have $\alpha(P) \leq n'$. □

For $\beta(P)$ and $\gamma(P)$, we have discussed the case of prime power cyclotomic rings before. When it comes to general cyclotomic rings, estimating $\beta(P)$ and $\gamma(P)$ will be much more complicated. It is noted that $\beta(P)$ is always $\Omega(1)$, and $\gamma(P)$ could be super-polynomial when n is highly composite.

NTRU *Prime Polynomial* The so-called NTRU Prime polynomial is $P(X) = X^n - X - 1$ where n is a prime. This kind of polynomials were suggested in [5] and discussed in [3, 28]. The following proposition shows that NTRU Prime polynomials have small $\alpha(P)$ and $\gamma(P)$.

Proposition 3. *For $P(X) = X^n - X - 1$, we have $\alpha(P) \leq 2n$ and $\gamma(P) \leq 2\sqrt{n}$.*

Proof. Let $\omega_1 \cdots \omega_n$ be all roots of $P(X)$. It can be verified that $|\omega_i| \leq \frac{n}{n-1}$ for any i. Then it follows that $\alpha(P) \leq \mathrm{T}_\infty(XP'(X)) = \mathrm{T}_\infty(n + (n-1)X) \leq 2n$.

Let $f, g \in \mathcal{R}$ and $h = fg \in \mathcal{R}$. We denote by $(f_0, \cdots, f_{n-1})$, $(g_0, \cdots, g_{n-1})$ and $(h_0, \cdots, h_{n-1})$ the coefficient vectors of f, g and h. By a routine computation, we know that $h_k = \sum_{i=0}^{k} f_i g_{k-i} + \sum_{i=k+1}^{n-1} f_i g_{k+n-i} + \sum_{i=k}^{n-1} f_i g_{k-1+n-i}$ and then $|h_k| \leq 2\|f\|\|g\|$. It follows that $\|h\| \leq 2\sqrt{n}\|f\|\|g\|$. □

For $\beta(P)$, we calculate the values experimentally and plot them in Figure 1. For comparison, we also calculate the tail bound indicated in Lemma 7. We observe that $\beta(P)$ is quite small for NTRU Prime polynomials and the tail bound in Lemma 8 seems much tighter than that of Lemma 7.

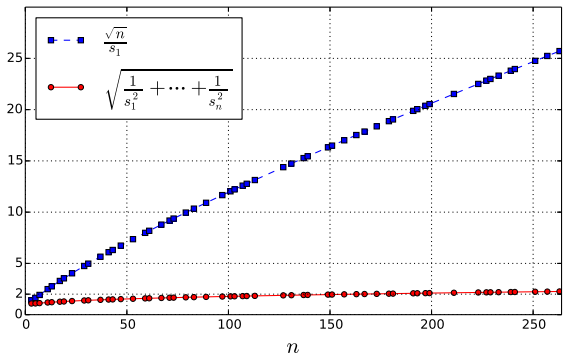

Fig. 1. Experimental measure of $\beta(P)$.

Overall, to design a relatively compact pNE, it may be crucial to find a polynomial $P(X)$ with well-bounded $\alpha(P)$, $\beta(P)$ and $\gamma(P)$. For a certain polynomial, we still need to consider some other factors of pNE, such as RLWE error and the minima of $\mathcal{R}$ (with respect to the T_2-norm). We leave to future work the further investigation of concrete polynomial selections.

A Tail Inequalities for Ellipsoid Gaussians

For an n-dimensional ellipsoid Gaussian, the width r is replaced by a rank-n matrix $\mathbf{R} \in \mathbb{R}^{n\times m}$ and the Gaussian function is defined by $\rho_{\mathbf{R},\mathbf{c}}(\mathbf{x}) = \exp\left(-\pi(\mathbf{x}-\mathbf{c})\left(\mathbf{R}\mathbf{R}^t\right)^{-1}(\mathbf{x}-\mathbf{c})^t\right)$. Let $D_{\mathcal{L},\mathbf{R},\mathbf{c}}$ be the ellipsoid Gaussian over a lattice $\mathcal{L}$ with center $\mathbf{c}$. We omit the subscript $\mathbf{c}$ when $\mathbf{c}=\mathbf{0}$. Let $s_1(\mathbf{R}) \le \cdots \le s_n(\mathbf{R})$ be all singular values of $\mathbf{R}$, then we have the following result.

Lemma 23. *Let $\mathcal{L} \subseteq \mathbb{R}^n$ be an n-dimensional full-rank lattice. For $t > 0$ and a rank-n matrix $\mathbf{R} \in \mathbb{R}^{n\times m}$, then*

$$\Pr_{\mathbf{b}\hookleftarrow D_{\mathcal{L},\mathbf{R}}}\left(\|\mathbf{b}\| \ge t\sqrt{\sum_{i=1}^{n} s_i(\mathbf{R})^2}\right) \le 2n\cdot\exp(-\pi t^2).$$

Proof. Let $\mathbf{U} = \left(\mathbf{R}\mathbf{R}^t\right)^{-1}$, then $\mathbf{U}$ is a rank-n real symmetric matrix. Thus there exist $\mathbf{u}_1,\cdots,\mathbf{u}_n \in \mathbb{R}^n$ satisfying (1) each $\mathbf{u}_i$ is an eigenvector of $\mathbf{U}$ corresponding to the eigenvalue $\frac{1}{s_i(\mathbf{R})^2}$; (2) all these $\mathbf{u}_i$'s are unit vectors and orthogonal to each other. Let $\pi_i(\cdot)$ be the projection to $\mathbf{u}_i$, then $\mathbf{b} = \sum_{i=1}^n \pi_i(\mathbf{b})$ and all $\pi_i(\mathbf{b})$'s are orthogonal to each other.

By Cholesky decomposition, we know that there exists a full-rank square matrix $\mathbf{V}$ such that $\mathbf{U} = \mathbf{V}\mathbf{V}^t$. Let $\mathbf{b}' = \mathbf{b}\mathbf{V}$ and $\mathbf{u}_i' = \mathbf{u}_i\mathbf{V}^{-t}$, then $\langle \mathbf{b}, \mathbf{u}_i\rangle = \langle \mathbf{b}', \mathbf{u}_i'\rangle$ and

$$\|\mathbf{u}_i'\|^2 = \mathbf{u}_i\mathbf{V}^{-t}\mathbf{V}^{-1}\mathbf{u}_i^t = \mathbf{u}_i\mathbf{U}^{-1}\mathbf{u}_i^t = s_i(\mathbf{R})^2.$$

Notice that $\rho_{\mathbf{R}}(\mathbf{x}) = \exp\left(-\pi \mathbf{x}\mathbf{U}\mathbf{x}^t\right) = \exp\left(-\pi\|\mathbf{x}\mathbf{V}\|^2\right)$, thus the ellipsoid Gaussian $D_{\mathcal{L},\mathbf{R}}$ multiplying $\mathbf{V}$ is equivalent to $D_{\mathcal{L}',1}$ where $\mathcal{L}'$ is the lattice $\{\mathbf{x}\mathbf{V} \mid \mathbf{x} \in \mathcal{L}\}$. It follows from Lemma 4 that

$$\Pr_{\mathbf{b}\hookleftarrow D_{\mathcal{L},\mathbf{R}}}\left(|\langle \mathbf{b}, \mathbf{u}_i\rangle| \geq t \cdot s_i(\mathbf{R})\right) = \Pr_{\mathbf{b}'\hookleftarrow D_{\mathcal{L}',1}}\left(|\langle \mathbf{b}', \mathbf{u}'_i\rangle| \geq t \cdot \|\mathbf{u}'_i\|\right) \leq 2 \cdot \exp(-\pi t^2).$$

By the union bound, we have

$$\begin{aligned}
\Pr_{\mathbf{b}\hookleftarrow D_{\mathcal{L},\mathbf{R}}}\left(\|\mathbf{b}\| \geq t\sqrt{\sum_{i=1}^{n} s_i(\mathbf{R})^2}\right) &= \Pr_{\mathbf{b}\hookleftarrow D_{\mathcal{L},\mathbf{R}}}\left(\sum_{i=1}^{n}\|\pi_i(\mathbf{b})\|^2 \geq \sum_{i=1}^{n} t^2 s_i(\mathbf{R})^2\right) \\
&\leq \sum_{i=1}^{n} \Pr_{\mathbf{b}\hookleftarrow D_{\mathcal{L},\mathbf{R}}}\left(\|\pi_i(\mathbf{b})\|^2 \geq t^2 s_i(\mathbf{R})^2\right) \\
&= \sum_{i=1}^{n} \Pr_{\mathbf{b}\hookleftarrow D_{\mathcal{L},\mathbf{R}}}\left(|\langle \mathbf{b}, \mathbf{u}_i\rangle| \geq t \cdot s_i(\mathbf{R})\right) \\
&\leq 2n \cdot \exp(-\pi t^2).
\end{aligned}$$

We now complete the proof. □

For a general center $\mathbf{c}$, we may also prove a similar result.

Lemma 24. *Let $\mathcal{L} \subseteq \mathbb{R}^n$ be an n-dimensional full-rank lattice and $\delta \in (0,1)$. For $t > 0$, $\mathbf{c} \in \mathbb{R}^n$ and a rank-n matrix $\mathbf{R} \in \mathbb{R}^{n\times m}$ such that $s_1(\mathbf{R}) \geq \eta_\delta(\mathcal{L})$ where $s_1(\mathbf{R})$ is the smallest singular value of $\mathbf{R}$, then*

$$\Pr_{\mathbf{b}\hookleftarrow D_{\mathcal{L},\mathbf{R},\mathbf{c}}}\left(\|\mathbf{b}-\mathbf{c}\| \geq t\sqrt{\sum_{i=1}^{n} s_i(\mathbf{R})^2}\right) \leq 2n\frac{1+\delta}{1-\delta} \cdot \exp(-\pi t^2).$$

We first prove two following lemmata that will be useful in the proof of Lemma 24.

Lemma 25. *Let $\mathcal{L} \subseteq V$ be an n-dimensional full-rank lattice and $\mathbf{c} \in V$. For $r \geq \eta_\delta(\mathcal{L})$, $t > 0$ and any unit vector $\mathbf{v} \in V$, then $\Pr_{\mathbf{b}\hookleftarrow D_{\mathcal{L},r,\mathbf{c}}}(|\langle \mathbf{b}-\mathbf{c}, \mathbf{v}\rangle| \geq rt) \leq 2\frac{1+\delta}{1-\delta} \cdot \exp(-\pi t^2)$.*

Proof. Similar to the proof of Lemma 6 in [28], we write the expectation of $\exp\left(\frac{2\pi t\langle \mathbf{b}-\mathbf{c}, \mathbf{v}\rangle}{r}\right)$ as

$$\mathbb{E}\left[\exp\left(\frac{2\pi t\langle \mathbf{b}-\mathbf{c}, \mathbf{v}\rangle}{r}\right)\right] = \frac{\rho_{r,\mathbf{c}+rt\mathbf{v}}(\mathcal{L})}{\rho_{r,\mathbf{c}}(\mathcal{L})} \cdot \exp\left(\pi t^2\right).$$

By Lemma 2.7 in [23], we have the above expectation belongs to $\left[\frac{1-\delta}{1+\delta}, \frac{1+\delta}{1-\delta}\right] \cdot \exp\left(\pi t^2\right)$. Using Markov's inequality, we immediately obtain the result. □

Lemma 26. *Let $\mathcal{L}$ be an n-dimensional full-rank lattice and $\mathbf{V} \in \mathbb{R}^{n\times n}$ be a full-rank matrix. Let $\mathcal{L}'$ be the lattice $\{\mathbf{xV} \mid \mathbf{x} \in \mathcal{L}\}$ and $s_n(\mathbf{V})$ be the largest singular value of $\mathbf{V}$. Then $s_n(\mathbf{V})\eta_\delta(\mathcal{L}) \geq \eta_\delta(\mathcal{L}')$ for $\delta \in (0,1)$.*

Proof. It can be verified that $\widehat{\mathcal{L}'} = \{\mathbf{xV}^{-t} \mid \mathbf{x} \in \widehat{\mathcal{L}}\}$. Notice that $\|\mathbf{x}\|^2 \leq s_n(\mathbf{V})^2\|\mathbf{xV}^{-t}\|^2$, thus $\rho_{1/s}\left(\widehat{\mathcal{L}}\right) \geq \rho_{1/(s_n(\mathbf{V})s)}\left(\widehat{\mathcal{L}'}\right)$. From the definition of smoothing parameter, we complete the proof. □

*Proof (*Lemma 24*).* Combining the proof of Lemma 23 with Lemmata 25 and 26, the result can be proved directly.

B Proof of Theorem 3

For $a \in \mathcal{R}_q^\times$, we define $\Pr_a = \Pr_{f_1,f_2}((y_1+pf_1)/(y_2+pf_2) = a)$, where $f_i \hookleftarrow D_{r,z_i}^\times$. It suffices to prove that $|\Pr_a - (q-1)^{-\varphi(n)}| \leq \frac{2^{2\varphi(n)+5}}{q^{\lfloor\epsilon\varphi(n)\rfloor}} \cdot (q-1)^{-\varphi(n)} =: \epsilon'$ for all except a fraction $\leq 64^{\varphi(n)}q^{-\epsilon\varphi(n)}$ of $a \in \mathcal{R}_q^\times$.

For $\mathbf{a} = (a_1, a_2) \in (\mathcal{R}_q^\times)^2$, let $\Pr_{\mathbf{a}} = \Pr_{f_1,f_2}[a_1f_1 + a_2f_2 = a_1z_1 + a_2z_2]$, then we have $\Pr_{\mathbf{a}} = \Pr_{-a_2\cdot a_1^{-1}}$. We consider the equation $a_1f_1 + a_2f_2 = a_1z_1 + a_2z_2$ of the pair (f_1, f_2). All its solutions form the set $\mathbf{z} + \mathbf{a}^{\perp\times}$ where $\mathbf{z} = (z_1, z_2)$ and $\mathbf{a}^{\perp\times} = \mathbf{a}^\perp \bigcap (\mathcal{R}_q^\times + q\mathbb{Z}^{\varphi(n)})^2$. Then it leads to that

$$\Pr_{\mathbf{a}} = \frac{\widetilde{D}_{\mathbb{Z}^{2\varphi(n)},r}(\mathbf{z}+\mathbf{a}^{\perp\times})}{\widetilde{D}_{\mathbb{Z}^{\varphi(n)},r}(z_1+\mathcal{R}_q^\times+q\mathbb{Z}^{\varphi(n)})\cdot\widetilde{D}_{\mathbb{Z}^{\varphi(n)},r}(z_2+\mathcal{R}_q^\times+q\mathbb{Z}^{\varphi(n)})}.$$

Due to the invertibility of a_1, a_2, for any $(x_1, x_2) \in \mathbf{a}^\perp$, the elements x_1 and x_2 belong to the same ideal J_S. Using the inclusion-exclusion principle, we have

$$\widetilde{D}_{\mathbb{Z}^{2\varphi(n)},r}(\mathbf{z}+\mathbf{a}^{\perp\times}) = \sum_{S\subseteq\{1,\cdots,\varphi(n)\}} (-1)^{|S|}\cdot\widetilde{D}_{\mathbb{Z}^{2\varphi(n)},r}(\mathbf{z}+\mathbf{a}^\perp(J_S)),$$

$$\widetilde{D}_{\mathbb{Z}^{\varphi(n)},r}(z_i+\mathcal{R}_q^\times+q\mathbb{Z}^{\varphi(n)}) = \sum_{S\subseteq\{1,\cdots,\varphi(n)\}} (-1)^{|S|}\cdot\widetilde{D}_{\mathbb{Z}^{\varphi(n)},r}(z_i+J_S), \forall i \in \{1,2\}.$$

Now we are to estimate $\widetilde{D}_{\mathbb{Z}^{2\varphi(n)},r}(\mathbf{z}+\mathbf{a}^{\perp\times})$ by considering each $\widetilde{D}_{\mathbb{Z}^{2\varphi(n)},r}(\mathbf{z}+\mathbf{a}^\perp(J_S))$ respectively. For the case $|S| \leq \epsilon\varphi(n)$, let $\delta = q^{-\varphi(n)-\lfloor\epsilon\varphi(n)\rfloor}$ and $m = 2$, then Lemma 13 implies that, for all except a fraction $\leq 32^{\varphi(n)}q^{-\epsilon\varphi(n)}$ of $\mathbf{a} \in (\mathcal{R}_q^\times)^2$,

$$\left|\widetilde{D}_{\mathbb{Z}^{2\varphi(n)},r}(\mathbf{z}+\mathbf{a}^\perp(J_S)) - q^{-\varphi(n)-|S|}\right| \leq 2\delta.$$

For the case $|S| > \epsilon\varphi(n)$, we can find $S' \subseteq S$ with $|S'| = \lfloor\epsilon\varphi(n)\rfloor$. Because $\mathbf{a}^\perp(J_S) \subseteq \mathbf{a}^\perp(J_{S'})$, we have $\widetilde{D}_{\mathbb{Z}^{2\varphi(n)},r,-\mathbf{z}}(\mathbf{a}^\perp(J_S)) \leq \widetilde{D}_{\mathbb{Z}^{2\varphi(n)},r,-\mathbf{z}}(\mathbf{a}^\perp(J_{S'}))$. From the previous result, we conclude that $\widetilde{D}_{\mathbb{Z}^{2\varphi(n)},r,-\mathbf{z}}(\mathbf{a}^\perp(J_S)) \leq 2\delta + q^{-\varphi(n)-\lfloor\epsilon\varphi(n)\rfloor}$.

Therefore, the following inequality holds:

$$\begin{aligned}
&\left|\widetilde{D}_{\mathbb{Z}^{2\varphi(n)},r}(\mathbf{z}+\mathbf{a}^{\perp\times}) - \frac{(q-1)^{\varphi(n)}}{q^{2\varphi(n)}}\right| \\
=&\left|\sum_{S\subseteq\{1,\cdots,\varphi(n)\}} (-1)^{|S|}\cdot\left(\widetilde{D}_{\mathbb{Z}^{2\varphi(n)},r}(\mathbf{z}+\mathbf{a}^{\perp}(J_S)) - q^{-\varphi(n)-|S|}\right)\right| \\
\leq& 2^{\varphi(n)+1}\delta + 2\sum_{k=\lceil\epsilon\varphi(n)\rceil}^{\varphi(n)}\binom{\varphi(n)}{k} q^{-\varphi(n)-\lfloor\epsilon\varphi(n)\rfloor} \leq 2^{\varphi(n)+2}q^{-\varphi(n)-\lfloor\epsilon\varphi(n)\rfloor},
\end{aligned}$$

for all except a fraction $\leq 64^{\varphi(n)}q^{-\epsilon\varphi(n)}$ of $\mathbf{a}\in(\mathcal{R}_q^\times)^2$.

Next, we are to estimate $\widetilde{D}_{\mathbb{Z}^{\varphi(n)},r}(z_i+\mathcal{R}_q^\times+q\mathbb{Z}^{\varphi(n)})$. Let Δ_K be the discriminant of the cyclotomic field $K=\mathbb{Q}[X]/(\Phi_n(X))$. As shown in [32], we have $\Delta_K\leq\varphi(n)^{\varphi(n)}$. The volume of the ideal lattice $\sigma(J_S)$ is $\mathrm{vol}(\sigma(J_S))=\mathrm{N}(J_S)\cdot\sqrt{\Delta_K}$ and then we have $\lambda_{\varphi(n)}(\sigma(J_S))=\lambda_1(\sigma(J_S))\leq\sqrt{\varphi(n)}\,\mathrm{vol}(\sigma(J_S))^{1/\varphi(n)}\leq\varphi(n)q^{|S|/\varphi(n)}$. Let $\delta=q^{-\varphi(n)/2}$. For S of cardinality $\leq\varphi(n)/2$, by Lemma 1, we get that $r\geq\eta_\delta(\sigma(J_S))$. Using Lemma 5, we know $|\widetilde{D}_{\mathbb{Z}^{\varphi(n)},r,-z_i}(J_S)-q^{-|S|}|\leq 2\delta$. For the case $|S|>\varphi(n)/2$, using the same argument, we have $\widetilde{D}_{\mathbb{Z}^{\varphi(n)},r,-z_i}(J_S)\leq 2\delta+q^{-\varphi(n)/2}$. Therefore, the following inequality holds:

$$\begin{aligned}
&\left|\widetilde{D}_{\mathbb{Z}^{\varphi(n)},r}(z_i+\mathcal{R}_q^\times+q\mathbb{Z}^{\varphi(n)}) - \frac{(q-1)^{\varphi(n)}}{q^{\varphi(n)}}\right| \\
=&\left|\sum_{S\subseteq\{1,\cdots,\varphi(n)\}} (-1)^{|S|}\cdot\left(\widetilde{D}_{\mathbb{Z}^{\varphi(n)},r,-z_i}(J_S) - q^{-|S|}\right)\right| \\
\leq& 2^{\varphi(n)+1}(\delta+q^{-\varphi(n)/2}) = 2^{\varphi(n)+2}q^{-\varphi(n)/2}.
\end{aligned}$$

Overall, we prove that, except for a fraction $\leq 64^{\varphi(n)}q^{-\epsilon\varphi(n)}$ of $\mathbf{a}\in(\mathcal{R}_q^\times)^2$,

$$\widetilde{D}_{\mathbb{Z}^{2\varphi(n)},r}(\mathbf{z}+\mathbf{a}^{\perp\times}) = (1+\delta_0)\cdot\frac{(q-1)^{\varphi(n)}}{q^{2\varphi(n)}},$$

$$\widetilde{D}_{\mathbb{Z}^{\varphi(n)},r}(z_i+\mathcal{R}_q^\times+q\mathbb{Z}^{\varphi(n)}) = (1+\delta_i)\cdot\frac{(q-1)^{\varphi(n)}}{q^{\varphi(n)}}, \forall i\in\{1,2\}.$$

where $|\delta_i|\leq 2^{2\varphi(n)+2}q^{-\lfloor\epsilon\varphi(n)\rfloor}$ for $i\in\{0,1,2\}$, which implies that $|\Pr_a-(q-1)^{-\varphi(n)}|\leq\epsilon'$.

References

[1] Aggarwal, D., Dadush, D., Regev, O., Stephens-Davidowitz, N.: Solving the shortest vector problem in 2^n time via discrete Gaussian sampling. CoRR abs/1412.7994 (2014), http://arxiv.org/abs/1412.7994

[2] Agrawal, S., Gentry, C., Halevi, S., Sahai, A.: Discrete Gaussian leftover hash lemma over infinite domains. In: ASIACRYPT 2013. pp. 97–116 (2013)
[3] Albrecht, M., Bai, S., Ducas, L.: A subfield lattice attack on overstretched NTRU assumptions: Cryptanalysis of some FHE and graded encoding schemes. In: CRYPTO 2016. pp. 153–178 (2016)
[4] Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Post-quantum key exchange—a new hope. In: USENIX Security 16. pp. 327–343 (2016)
[5] Bernstein, D.J., Chuengsatiansup, C., Lange, T., van Vredendaal, C.: NTRU Prime: reducing attack surface at low cost. In: SAC 2017 (2017)
[6] Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Stehlé, D.: CRYSTALS – Kyber: a CCA-secure module-lattice-based KEM. Cryptology ePrint Archive, Report 2017/634 (2017), http://eprint.iacr.org/2017/634
[7] Bos, J.W., Lauter, K., Loftus, J., Naehrig, M.: Improved security for a ring-based fully homomorphic encryption scheme. In: 14th IMA International Conference on Cryptography and Coding. pp. 45–64 (2013)
[8] Cabarcas, D., Weiden, P., Buchmann, J.A.: On the efficiency of provably secure NTRU. In: PQCrypto 2014. pp. 22–39 (2014)
[9] 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 Journal of Computation & Mathematics 19(A), 255–266 (2016)
[10] Conrad, K.: The different ideal http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/different.pdf
[11] Conrad, K.: Ideal factorization http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/idealfactor.pdf
[12] Coppersmith, D., Shamir, A.: Lattice attacks on NTRU. In: EUROCRYPT 1997. pp. 52–61 (1997)
[13] Cramer, R., Ducas, L., Wesolowski, B.: Short Stickelberger class relations and application to Ideal-SVP. In: EUROCRYPT 2017. pp. 324–348 (2017)
[14] Ducas, L., Durmus, A.: Ring-LWE in polynomial rings. In: PKC 2012. pp. 34–51 (2012)
[15] Ducas, L., Durmus, A., Lepoint, T., Lyubashevsky, V.: Lattice signatures and bimodal Gaussians. In: CRYPTO 2013. pp. 40–56 (2013)
[16] Ducas, L., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D.: CRYSTALS – Dilithium: Digital signatures from module lattices. Cryptology ePrint Archive, Report 2017/633 (2017), http://eprint.iacr.org/2017/633
[17] Ducas, L., Lyubashevsky, V., Prest, T.: Efficient identity-based encryption over NTRU lattices. In: ASIACRYPT 2014. pp. 22–41 (2014)
[18] Ducas, L., Nguyen, P.Q.: Learning a zonotope and more: Cryptanalysis of NTRUSign countermeasures. In: ASIACRYPT 2012. pp. 433–450 (2012)
[19] Gama, N., Nguyen, P.Q.: New chosen-ciphertext attacks on NTRU. In: PKC 2007. pp. 89–106 (2007)
[20] Garg, S., Gentry, C., Halevi, S.: Candidate multilinear maps from ideal lattices. In: EUROCRYPT 2013. pp. 1–17 (2013)

[21] Gentry, C.: Key recovery and message attacks on NTRU-composite. In: EUROCRYPT 2001. pp. 182–194 (2001)
[22] Gentry, C.: Fully homomorphic encryption using ideal lattices. In: STOC 2009. pp. 169–178 (2009)
[23] Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: STOC 2008. pp. 197–206 (2008)
[24] Hoffstein, J., Howgrave-Graham, N., Pipher, J., Silverman, J.H., Whyte, W.: NTRUSign: Digital signatures using the NTRU lattice. In: CT-RSA 2003. pp. 122–140 (2003)
[25] Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A ring-based public key cryptosystem. In: ANTS 1998. pp. 267–288 (1998)
[26] Howgrave-Graham, N.: A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. In: CRYPTO 2007. pp. 150–169 (2007)
[27] Jaulmes, E., Joux, A.: A chosen-ciphertext attack against NTRU. In: CRYPTO 2000. pp. 20–35 (2000)
[28] Kirchner, P., Fouque, P.A.: Revisiting lattice attacks on overstretched NTRU parameters. In: EUROCRYPT 2017. pp. 3–26 (2017)
[29] Langlois, A., Stehlé, D.: Worst-case to average-case reductions for module lattices. Designs, Codes and Cryptography 75(3), 565–599 (2015)
[30] Langlois, A., Stehlé, D., Steinfeld, R.: GGHLite: More efficient multilinear maps from ideal lattices. In: EUROCRYPT 2014. pp. 239–256 (2014)
[31] López-Alt, A., Tromer, E., Vaikuntanathan, V.: On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In: STOC 2012. pp. 1219–1234 (2012)
[32] Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: EUROCRYPT 2010. pp. 1–23 (2010)
[33] Lyubashevsky, V., Peikert, C., Regev, O.: A toolkit for Ring-LWE cryptography. Cryptology ePrint Archive, Report 2013/293 (2013), http://eprint.iacr.org/2013/293
[34] Micciancio, D.: Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. Computational Complexity 16(4), 365–411 (2007)
[35] Micciancio, D., Regev, O.: Worst-case to average-case reductions based on Gaussian measures. SIAM Journal on Computing 37(1), 267–302 (2007)
[36] Nguyen, P.Q., Regev, O.: Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. In: EUROCRYPT 2006. pp. 271–288 (2006)
[37] Peikert, C.: Limits on the hardness of lattice problems in ℓ_p norms. Computational Complexity 17(2), 300–351 (2008)
[38] Peikert, C., Regev, O., Stephens-Davidowitz, N.: Pseudorandomness of Ring-LWE for any ring and modulus. In: STOC 2017 (2017), To appear
[39] Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: STOC 2005. pp. 84–93 (2005)
[40] Stehlé, D., Steinfeld, R.: Making NTRU as secure as worst-case problems over ideal lattices. In: EUROCRYPT 2011. pp. 27–47 (2011)
[41] Stehlé, D., Steinfeld, R.: Making NTRUEncrypt and NTRUSign as secure as standard worst-case problems over ideal lattices. Cryptology ePrint Archive, Report 2013/004 (2013), http://eprint.iacr.org/2013/004

[42] Steinfeld, R., Ling, S., Pieprzyk, J., Tartary, C., Wang, H.: NTRUCCA: How to strengthen NTRUEncrypt to chosen-ciphertext security in the standard model. In: PKC 2012. pp. 353–371 (2012)
[43] Xylouris, T.: On Linnik's constant (2009), http://arxiv.org/abs/0906.2749
[44] Yu, Y., Xu, G., Wang, X.: Provably secure NTRU instances over prime cyclotomic rings. In: PKC 2017. pp. 409–434 (2017)