Provably Secure NTRUEncrypt over More General Cyclotomic Rings

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

[1] Department of Computer Science and Technology, Tsinghua University, Beijing, 100084, China
y-y13@mails.tsinghua.edu.cn
[2] Department of EE & CS, University of Wisconsin-Milwaukee, Milwaukee, WI 53201, USA
gxu4uwm@uwm.edu
[3] Institute for Advanced Study, Tsinghua University, Beijing, 100084, China
xiaoyunwang@mail.tsinghua.edu.cn

Abstract. NTRUEncrypt is a fast and standardized lattice-based public key encryption scheme, but it lacks a solid security guarantee. In 2011, Stehlé and Steinfeld first proposed a provably secure variant of NTRUEncrypt, denoted by pNE, over power-of-2 cyclotomic rings. The IND-CPA security of pNE is based on the worst-case quantum hardness of classical problems over ideal lattices. Recently, Yu, Xu and Wang constructed 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 and provide asymptotical parameters of pNE over prime power cyclotomic rings. In particular, our result allows tighter parameters for prime cyclotomic rings and improves the existing result. Furthermore, we also discuss a generalization to more general polynomial rings and point out several attributes that affect the selection of parameters. This discussion may be of some value in choosing the underlying ring for cryptographic applications.

Keywords: Lattice-based cryptography, NTRU, Learning With Errors, Provable security.

1 Introduction

NTRU, introduced by Hoffstein, Pipher and Silverman in [20], 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 [19, 11], identity-based encryption [12], fully homomorphic encryption [25, 3] and multilinear maps [15, 24]. In the last 20 years, a batch of cryptanalysis works [8, 22, 16, 30, 14, 21, 13, 1, 5, 23] 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. In 2011, Stehlé and Steinfeld proposed the first provably secure NTRUEncrypt variant [34] that we denote by pNE, and gave a reduction from RLWE(*Ring Learning With Errors*) problem to the IND-CPA security (*indistinguishability under chosen-plaintext attack*) of pNE. RLWE, introduced by Lyubashevsky, Peikert and Regev [26], is an algebraic variant of LWE(*Learning With Errors* [33]) and enjoys more popularity in cryptographic applications than LWE due to its better compactness and efficiency. The hardness of RLWE is based on some worst-case problems over ideal lattices, which provides pNE with a strong security guarantee. Then, a variant of pNE against chosen-ciphertext attacks [36] and a provably secure NTRU signature scheme [35] 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 [38], which allows more flexibility of parameter selections. However, because of size requirements for parameters, the modified pNE is of even less efficiency than the original one.

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 [4], 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 even more general cyclotomic 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 two secret polynomials are sampled from certain Gaussians, which is a remarkable property of pNE originally proposed by Stehlé and Steinfeld in [34]. 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. The sizes of secret keys are asymptotically the same as that in [34] when we restrict to the special case of power-of-2, and these sizes are much smaller than that in [38] for prime cyclotomic rings. Consequently, our generalized pNE scheme is of relatively tight parameters. Our result further enriches the provably secure

NTRU family and allows a more flexible choice of parameters. As by-products, an improved regularity result for general cyclotomic rings and some special properties of prime power cyclotomic rings are shown, which may be of independent interest. While we exploit some ideas shown in [34, 35, 38], many technical differences still need to be treated carefully. Actually in the technical preparation part, we have improved some of the existing results and even developed some new ones in this paper. To the best of our knowledge, concrete discussions for pNE over more general cyclotomic rings have not been found in literature.

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 $P(X)$ mattering the parameter selection. While 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 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. 4. Finally, we further discuss a generalization to some other rings in Sect. 5.

2 Preliminaries

Embeddings and Norms Let $P(X) \in \mathbb{Z}[X]$ be a monic irreducible polynomial of degree n and $\mathbb{K} = \mathbb{Q}[X]/(P(X))$. For any $t = \sum_{i=0}^{n-1} t_i X^i \in \mathbb{K}$, 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 $\mathbb{K}$ to its coefficient vector. We denote by $\|t\|$ (resp. $\|t\|_\infty$) the Euclidean (resp. ℓ_∞) norm of the coefficient vector of t. For $\mathbf{t} = (t^{(1)}, \cdots, t^{(m)}) \in \mathbb{K}^m$, 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 [26, 27]. 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 $\mathbb{K}$ has exactly n embeddings into $\mathbb{C}$ denoted by $\sigma_i : \mathbb{K} \to \mathbb{C}$ where $\sigma_i(t) = t(\omega_i)$ for any $t \in \mathbb{K}$. Then the canonical embedding $\sigma : \mathbb{K} \to \mathbb{C}^n$ is defined as $\sigma(t) = (\sigma_1(t), \cdots, \sigma_n(t))$. In fact, the canonical embedding maps into the space $H = \{(x_1, \cdots, x_n) \mid x_1, \cdots, x_{s_1} \in \mathbb{R}, x_{x_1+k} = \overline{x_{x_1+k+s_2}}, 1 \le k \le s_2\}$ 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 $\mathbf{t} = (t_1, \cdots, t_m) \in \mathbb{K}^m$, 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[4]. 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 $\widehat{\mathcal{L}} = \{\mathbf{c} \in V \mid \forall i, \langle \mathbf{c}, \overline{\mathbf{b}_i} \rangle \in \mathbb{Z}\}$[5]. 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 $k \leq n$, the k-th minimum $\lambda_k(\mathcal{L})$ 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[6] 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 [9]). 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 $\Phi_n(X) = X^{n-1} + X^{n-2} + \cdots + 1$.

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

[5] 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.

[6] Both coefficient and canonical embedding are an additive isomorphism.

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 [37]).

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 to our results, as explained in [10]. 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 $\mathbf{x} \in \mathcal{L}$. For $\delta > 0$, we denote the *smoothing parameter* by $\eta_\delta(\mathcal{L}) = \min\{r : \rho_{1/r}(\widehat{\mathcal{L}}) \le 1+\delta\}$. We now recall some results which will be used later.

Lemma 1 ([29], Lemma 3.3). *Let $\mathcal{L}$ be an n-dimensional full-rank lattice and $\delta \in (0,1)$. Then $\eta_\delta(\mathcal{L}) \le \sqrt{\ln(2n(1+1/\delta))/\pi}\cdot\lambda_n(\mathcal{L})$.*

Lemma 2 ([31], Lemma 3.5). *Let $\mathcal{L}$ be an n-dimensional full-rank lattice and $\delta \in (0,1)$. Then $\eta_\delta(\mathcal{L}) \le \sqrt{\ln(2n(1+1/\delta))/\pi}/\lambda_1^\infty\left(\widehat{\mathcal{L}}\right)$.*

Lemma 3 ([29], Lemma 4.4). *Let $\mathcal{L} \subseteq V$ be an n-dimensional full-rank lattice and $\delta \in (0,1)$. Then $\Pr_{\mathbf{b}\hookleftarrow D_{\mathcal{L},r,\mathbf{c}}}(\|\mathbf{b}-\mathbf{c}\| \ge r\sqrt{n}) \le \frac{1+\delta}{1-\delta}2^{-n}$ for $\mathbf{c} \in V$ and $r \ge \eta_\delta(\mathcal{L})$.*

Lemma 4 ([18], 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 $r \ge \eta_\delta(\mathcal{L}')$, we have $\Delta(D_{\mathcal{L},r,\mathbf{c}} \bmod \mathcal{L}'; U(\mathcal{L}/\mathcal{L}')) \le 2\delta$.*

Lemma 5 ([18], 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 [26] and shown hard for specific settings. In [10], 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 [10].

Definition 1 (RLWE error distribution in [10]). *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.*

Definition 2 (RLWE **distribution in [10]**). *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 the canonical embedding.

Theorem 1 (**[10], 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* $\gamma = \tilde{O}(\sqrt{n}/\alpha)$ *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 [34], 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 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 [34, 38], our results are of a much wider meaning and some of them are with respect to canonical embedding instead of coefficient embedding.

3.1 Duality Results for Module Lattices

Let $\mathbb{K} = \mathbb{Q}[X]/(\Phi_n(X)) \cong \mathbb{Q}(\xi_n)$ and $\mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X)) \cong \mathbb{Z}[\xi_n]$ be the ring of integers of $\mathbb{K}$. 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 [34].

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 $\mathcal{R}^\vee = \{a \in \mathbb{K} \mid \mathrm{Tr}(a\mathcal{R}) \subseteq \mathbb{Z}\}$ 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 6. *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:*

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

Proof. Let $\mathcal{L}'(\mathbf{a}, J_{\bar{S}}) = \frac{1}{q} \{ (t_1, \cdots, t_m) \in (\mathcal{R}^\vee)^m \mid \exists s \in \mathcal{R}^\vee, \forall i, t_i - \tilde{a_i} s \in J_{\bar{S}} \mathcal{R}^\vee \}$. 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 $\sum_i \langle t_i, \bar{t_i'} \rangle = \sum_i \mathrm{Tr}(t_i t_i') \in \mathbb{Z}$. 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,

$$\sum_i \langle t_i, \bar{t_i'} \rangle = \frac{1}{q} \sum_i \mathrm{Tr}((\tilde{a_i} s + b_i) t_i') = \frac{1}{q} \mathrm{Tr}\left(s \sum_i \tilde{a_i} t_i' \right) + \frac{1}{q} \sum_i \mathrm{Tr}\left(b_i t_i' \right)$$

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 7. *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 [27], we have $R^{\vee} = \langle g/n' \rangle$. By Lemma 6, we get the result immediately. □

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

Lemma 8. *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 7, 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 7. 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 $\lambda_1^{\infty}\left(\widehat{\mathbf{a}^{\perp}(J_S)}\right) = \mathrm{T}_{\infty}(\mathbf{v}) = \frac{\mathrm{T}_{\infty}(\mathbf{u}')}{qn'} \geq \frac{\lambda_1^{\infty}(\mathcal{L}(\mathbf{a}, J_{\bar{S}}))}{qn'}$. □

3.2 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 9. *Let $\mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X))$. Let $q = 1 \bmod n$ be a prime and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. 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 $\geq 1 - \frac{2^{4m\varphi(n)}}{q^{\epsilon m \varphi(n)}}$ 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 $p(\mathbf{t},s_j)=\mathrm{Pr}_{\mathbf{a}}(\forall i,t_i-\tilde{a}_i s_j\in J_S)$ and $p_i(t_i,s_j)=\mathrm{Pr}_{a_i}(t_i-\tilde{a}_i s_j\in J_S)$. 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

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

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

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

$$p\leq 2^{(m+1)|S|}\max_{d<\beta\varphi(n)}\frac{N(B,d)^m}{q^{(m-1)(|S|-d)}}\leq 2^{4m\varphi(n)}q^{-\varphi(n)m\epsilon}.$$

We now complete the proof. □

Remark The above proof makes use of ideas from [35], 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.

3.3 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 [28], 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 [34, 38] respectively. However, the results in [34, 38] only focus on two special classes of cyclotomic rings and are under the coefficient embedding. The regularity result with respect to canonical embedding was shown in [27] and applied to general cyclotomic rings, but it has some limitations for certain cryptographic applications.[7] Here, we will give an improved result that applies to general cyclotomic rings and has more flexibility than that in [27].

In the following discussion, when the sampling $\mathbf{t} \hookleftarrow D_{\mathbb{Z}^{m\varphi(n)}, r, \mathbf{c}}$ is mentioned, it means that we view each vector of $\mathbb{Z}^{m\varphi(n)}$ as an element of $\mathcal{R}^m$ (by coefficient embedding) and use T_2-norm in the evaluation of the Gaussian function.

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, 4, 8 and 9.

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 $S \subseteq \{1, \cdots, \varphi(n)\}$, $m \geq 2, \epsilon > 0, \delta \in (0, \frac{1}{2})$. 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 $\mathbf{t} \hookleftarrow D_{\mathbb{Z}^{m\varphi(n)}, r, \mathbf{c}}$. Then for all except a fraction $\leq 2^{4m\varphi(n)} q^{-\epsilon m\varphi(n)}$ 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

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

Remark Let $\mathbf{t} \in \mathcal{R}^m$ be the Gaussian sample in Lemma 10. For $\delta = q^{-cn}$ with $c = O(1)$, Lemma 3 shows that $\mathrm{T}_2(\mathbf{t}) = \widetilde{O}(n^2)\sqrt{m} q^{\frac{1}{m}+\epsilon'}$ with overwhelming probability. We will see from Lemma 11 that $\|\mathbf{t}\| = \widetilde{O}(\sqrt{d} n^{1.5})\sqrt{m} q^{\frac{1}{m}+\epsilon'}$ for the case that n is a prime power[8]. The size of Gaussian sample is asymptotically same to that in [34] when $n = 2^k$, and smaller than that in [38] when n is a prime. Furthermore, the regularity result in [27] allows a smaller sample width $(r \geq 2\varphi(n) \cdot q^{\frac{1}{m}+\epsilon'})$, but it seems to only hold 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 10 gives immediately the following regularity result.

[7] As discussed in [38], it does not suffice to construct pNE only from the regularity result in [27].

[8] We take the upper bound in Lemma 11 directly, but, from the proof, $\|\mathbf{t}\|$ may be about $\widetilde{O}(n^{1.5})\sqrt{m} q^{\frac{1}{m}+\epsilon'}$ in average for large d.

Theorem 2. *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 $m \geq 2, \epsilon > 0, \delta \in (0, \frac{1}{2})$ and $a_i \hookleftarrow U(\mathcal{R}_q^\times)$ for any $i \in \{1, \cdots, m\}$. Then, for $\mathbf{t} \hookleftarrow D_{\mathbb{Z}^{m\varphi(n)}, r}$ with $r \geq n'\sqrt{\ln(2m\varphi(n)(1+1/\delta))/\pi} \cdot q^{\frac{1}{m}+\epsilon}$, we have*

$$\Delta\left(\left(a_1, \cdots, a_m, \sum_{i=1}^{m} t_i a_i\right); U\left((\mathcal{R}_q^\times)^m \times \mathcal{R}_q\right)\right) \leq 2\delta + 2^{4m\varphi(n)} q^{-\epsilon m\varphi(n)}.$$

3.4 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 [27][9]. 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.

The following result shows the quantitative relationship between different norms over prime power cyclotomic rings.

Lemma 11. *Let $n = d^\nu$ with d a prime and $\mathcal{R} = \mathbb{Z}[X]/(\Phi_n(X))$. For any $t \in \mathcal{R}$, we have*

$$\frac{1}{n}\mathrm{T}_2(t)^2 \leq \|t\|^2 \leq \frac{d}{n}\mathrm{T}_2(t)^2.$$

Proof. Let $\omega_1, \cdots, \omega_{\varphi(n)}$ be all roots of $\Phi_n(X)$. Let $\mathbf{V} = (\omega_j^{i-1})_{i,j}$ where $1 \leq i, j \leq \varphi(n)$ and $\mathbf{c}(t)$ be the coefficient vector of t, then $\sigma(t) = \mathbf{c}(t) \cdot \mathbf{V}$. Let $\mathbf{U} = \mathbf{V}\mathbf{V}^*$ where $\mathbf{V}^*$ is the conjugate transpose of $\mathbf{V}$. We have that $\mathbf{U} = (u_{ij})_{i,j}$ is a symmetric matrix where

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

We denote by $\mathbf{e}_i$ the i-th column of the $\varphi(n)$-dimensional identity matrix. Let $\mathbf{x}_i = \sum_{j=i \bmod \frac{n}{d}} \mathbf{e}_i$ where $i \in \{1, \cdots, \frac{n}{d}\}$ and $1 \leq j \leq \varphi(n)$. These $\frac{n}{d}$ $\mathbf{x}_i$'s are eigenvectors of $\mathbf{U}$ and corresponding eigenvalues equal $\frac{n}{d}$. Let $\mathbf{y}_{ij} = \mathbf{e}_i - \mathbf{e}_{i+\frac{jn}{d}}$ where $i \in \{1, \cdots, \frac{n}{d}\}$ and $j \in \{1, \cdots, d-2\}$. It can be verified that these $\frac{n(d-2)}{d} = \varphi(n) - \frac{n}{d}$ $\mathbf{y}_{ij}$'s are also eigenvectors of $\mathbf{U}$ with respect to eigenvalue n and all $\mathbf{x}_i$'s and $\mathbf{y}_{ij}$'s are linearly independent. Thus the largest eigenvalue of $\mathbf{U}$ is at most n and the smallest one is $\frac{n}{d}$, then we have

$$\frac{n}{d} \leq \frac{\mathrm{T}_2(t)^2}{\|t\|^2} = \frac{\|\sigma(t)\|^2}{\|\mathbf{c}(t)\|^2} \leq n.$$

The proof is completed. □

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

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 [17, 38]). The following lemma indicates that, for general prime power cyclotomic rings, their expansion factors are well-bounded as well.

Lemma 12. *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 $\|h\| \le \sqrt{\varphi(n)}\|h\|_\infty \le 2\sqrt{\varphi(n)}\|f\|\|g\|$. □

4 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 [34, 38] 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 $D_{\mathbb{Z}^{\varphi(n)},r}$; if $f = pf' + 1 \bmod q \notin \mathcal{R}_q^\times$, resample. Sample g from $D_{\mathbb{Z}^{\varphi(n)},r}$; if $g \bmod q \notin \mathcal{R}_q^\times$, resample. Then return private key $sk = f \in \mathcal{R}_q^\times$ and public key $pk = h = pg/f \in \mathcal{R}_q^\times$. Note that the Gaussian sampling uses T_2-norm.
– **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.

4.1 Key Generation

Gaussian sampler is a core component of the key generation algorithm. Since our parameter conditions are much stronger than that in Lemma 5, 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 13. *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*

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

holds for $a \in \mathcal{R}$ and $p \in \mathcal{R}_q^\times$ [10].

Proof. Notice that the norm of $J_{\{k\}}$ is $\mathrm{N}(J_{\{k\}}) = q$ and the discriminant of the cyclotomic field $\mathbb{K} = \mathbb{Q}[X]/(\Phi_n(X))$ is $\Delta_\mathbb{K} \leq \varphi(n)^{\varphi(n)}$ (see [27] for the latter). The volume of the ideal lattice $\sigma(J_{\{k\}})$ is given by $\mathrm{vol}(\sigma(J_{\{k\}})) = \mathrm{N}(J_{\{k\}})\sqrt{\Delta_\mathbb{K}}$. 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 4, 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 coincide with NTRU setting, we measure their sizes by Euclidean norms of their coefficient vectors.

[10] In this subsection, the Gaussian sampling from $D_{\mathbb{Z}^{\varphi(n)},r}$ is with respect to the T_2-norm.

Lemma 14. *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 $\geq 1 - 2^{-\varphi(n)+3}$, the secret key polynomials f, g satisfy*

$$\|f\| \leq 2\sqrt{dn} \cdot \|p\| r \quad \text{and} \quad \|g\| \leq \sqrt{d-1} \cdot r.$$

If $\deg p = 0$, then $\|f\| \leq 2\sqrt{d-1} \cdot \|p\| r$ with probability $\geq 1 - 2^{-\varphi(n)+3}$.

Proof. Let $\delta = \frac{1}{10\varphi(n)-1}$, then $r \geq \sqrt{\ln(2\varphi(n)(1+1/\delta))/\pi} \cdot \varphi(n) q^{1/\varphi(n)}$. From Lemma 1, it can be verified that $r \geq \eta_\delta(\mathbb{Z}^{\varphi(n)})$. Applying Lemma 3, we have

$$\Pr_{g \hookleftarrow D_{\mathbb{Z}^{\varphi(n)}, r}} \left(\mathrm{T}_2(g) \geq r\sqrt{\varphi(n)} \right) \leq \frac{1+\delta}{1-\delta} 2^{-\varphi(n)}.$$

Since $r \geq \varphi(n)\sqrt{\ln(2\varphi(n)(1+1/\delta))/\pi} \cdot q^{1/\varphi(n)}$, Lemma 13 yields

$$\begin{aligned}
&\Pr_{g \hookleftarrow D_{\mathbb{Z}^{\varphi(n)}, r}} \left(\mathrm{T}_2(g) \geq r\sqrt{\varphi(n)} \mid g \in \mathcal{R}_q^\times \right) \\
\leq &\frac{\Pr_{g \hookleftarrow D_{\mathbb{Z}^{\varphi(n)}, r}} \left(\mathrm{T}_2(g) \geq r\sqrt{\varphi(n)} \right)}{\Pr_{g \hookleftarrow D_{\mathbb{Z}^{\varphi(n)}, r}} \left(g \in \mathcal{R}_q^\times \right)} \\
\leq &\frac{1+\delta}{1-\delta} 2^{-\varphi(n)} \cdot \frac{1}{1 - \varphi(n)(1/q + 2\delta)} \leq 2^{3-\varphi(n)}.
\end{aligned}$$

Combined with Lemma 11, it follows that $\|g\| \leq r\sqrt{d-1}$ with probability $\geq 1 - 2^{3-\varphi(n)}$. The same argument holds true for the polynomial f' such that $f = p \cdot f' + 1$.

If $\deg p = 0$, we have $\|f\| \leq 1 + \|p\|\|f'\| \leq 2\|p\| r\sqrt{d-1}$ with probability $\geq 1 - 2^{3-\varphi(n)}$. For general cases, applying Lemma 12, we know that $\|f\| \leq 1 + 2\sqrt{\varphi(n)(d-1)}\|p\| r \leq 2\sqrt{dn} \cdot \|p\| r$ with probability $\geq 1 - 2^{3-\varphi(n)}$. □

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 the T_2-norm.

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 $D_{\mathbb{Z}^{\varphi(n)}, r}$ 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*

$$\Delta\left(\frac{y_1 + p \cdot D_{r,z_1}^\times}{y_2 + p \cdot D_{r,z_2}^\times} \bmod q; U(\mathcal{R}_q^\times) \right) \leq \frac{2^{10\varphi(n)}}{q^{\lfloor \epsilon\varphi(n) \rfloor}}$$

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 [34], but some differences still need to be treated. Thus we include the proof in Appendix A for reference.

4.2 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 [10] that is based on spherical Gaussian rather than classical discrete Gaussian. In [38], 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 15. *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 12, 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 14 and 12, we obtain a bound of the norms of pgs and pfe.

Lemma 16. *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 for* $\kappa > 0$, *we have*

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

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

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

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

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

Lemma 17. *In* $\mathsf{pNE}(n, d, \nu, q, p, r, \alpha, k)$, *we have* $\|fM\|_\infty \leq 4\sqrt{dn^3} \cdot \|p\|^2 r$ *with probability at least* $1 - 2^{-\varphi(n)+3}$. *In particular, if* $\deg p = 0$, *then* $\|fM\|_\infty \leq 2\sqrt{dn} \cdot \|p\|^2 r$ *with probability at least* $1 - 2^{-\varphi(n)+3}$.

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 12. 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 14 and 12 with the above result, the proof is completed. □

Combining Lemmata 16 and 17, 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* $\omega\left(n\sqrt{d\log n}\right)\|p\|^2 rt/q < 1$ *(resp.* $\omega\left(\sqrt{d\log n}\right)\|p\|^2 rt/q < 1$ *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.

4.3 Security Reduction and Parameters

The provable security of pNE is guaranteed by the following theorem. The proof totally follows from that in [38] and thus we omit it.

Lemma 18. *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 18 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 $q^{\frac{1}{2}-\epsilon} = \omega\left(d^{0.5} n^{3.25} \log^{1.5} n \|p\|^2\right)$ (resp. $q^{\frac{1}{2}-\epsilon} = \omega\left(d^{0.5} n^{2.25} \log^{1.5} n \|p\|^2\right)$, 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 $\deg p = 0$, the minimal modulus q for which pNE holds is $\tilde{\Omega}(dn^{4.5})$, and the minimal approximate factor γ is $\tilde{O}(dn^5)$. For the case $d = 2$, our results are asymptotically the same as the improved version shown in [35] (note that the original version was described in [34]). For the case that n is a prime, the smallest q and γ shown in [38] are $\tilde{\Omega}(n^{7.5})$ and $\tilde{O}(n^8)$ respectively which are asymptotically larger than ours by a factor of n^2. That means the NTRU scheme in this paper has a better compactness and wider applicability.

Furthermore, it is interesting to note that the final parameters are not only affected by the size of n, but also by its prime factor d. Actually, as shown in the proof of Lemma 11, for large d, most eigenvalues of $\mathbf{U}$ are n rather than $\frac{n}{d}$. That seems to indicate that $\|t\|$ tends close to $\sqrt{\frac{1}{n}}\mathrm{T}_2(t)$ (the "average" value) rather than $\sqrt{\frac{d}{n}}\mathrm{T}_2(t)$ (the worst-case upper bound). As a consequence, the parameters may be improved further when d is large.

5 Further Analysis for General Rings

A very recent paper [32] demonstrates a polynomial-time quantum reduction from worst-case ideal lattice problems to RLWE for general ring, 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, we denote by $\omega_1, \omega_2, \cdots, \omega_n$ its complex roots. Let $\mathbb{K} = \mathbb{Q}[X]/(P(X))$ and $\mathcal{R} = \mathbb{Z}[X]/(P(X))$ be an order in $\mathbb{K}$. Let q be a prime such that $P(X)$ splits into n distinct linear factors modulo q[11]. We view the element of $\mathcal{R}$ as it canonical embedding and let $\mathcal{R}^\vee = \{a \in \mathbb{K} \mid \mathrm{Tr}(a\mathcal{R}) \subseteq \mathbb{Z}\}$. We also follow the definitions of $\mathcal{R}$-modules and ideals shown in Sect. 3.

Under above setting, we observe that Lemmata 6 and 9 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 $\mathbb{K}$, which is a little different

[11] As discussed in [35], a more general case that $P(X)$ splits into distinct factors of same degree may be treated using similar arguments.

from the setting in [32][12]. It also holds that $\mathrm{N}(t) = |\mathcal{R}/t\mathcal{R}|$ for any $t \in \mathcal{R}$ (see [7]), which ensures that all proofs go through. However, Lemmata 7 and 8 require some modifications to apply to general case. Note that the scaling factor (before $\mathcal{L}(\mathbf{a}, J_{\bar{S}})$) in Lemma 7 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 [6]). We define a function mapping $\mathbb{Z}[X]$ to $\mathbb{R}$ as

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

Using a similar proof of Lemma 8, 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.

Lemma 19. *Let $P(X) \in \mathbb{Z}[X]$ be a monic irreducible polynomial of degree n 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 $\mathbf{t} \hookleftarrow D_{\mathbb{Z}^{mn},r,\mathbf{c}}$. Then for all except a fraction $\leq 2^{4mn}q^{-\epsilon mn}$ 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

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

While it may be hard to calculate $\alpha(P)$ in practice, we can replace $\alpha(P)$ with its upper bound and obtain an approximate result. Below are two examples.

- If $P(X) = \Phi_n(X)$, by choosing $s = \Theta_n(X)/\Phi_n(X)$, then $\alpha(P) \leq \mathrm{T}_{\infty}(s\Phi_n'(X))$. Notice that $\Theta_n'(X) = s\Phi_n'(X) + s'\Phi_n(X)$, we have $\alpha(P) \leq n'$ where $n' = \deg(\Theta_n(X))$;
- If $P(X) = X^n - X - 1$ as suggested in [2], by choosing $s = X$, then $\alpha(P) \leq \mathrm{T}_{\infty}(X(nX^{n-1} - 1)) = \mathrm{T}_{\infty}(n + (n-1)X)$. It can be verified that $|\omega_i| \leq \frac{n}{n-1}$ for any i, which implies $\alpha(P) \leq 2n$.

Furthermore, to determine the final parameters of pNE, we also need to consider two following functions:

$$\beta(P) = \max_{t \in \mathbb{K}, t \neq 0} \frac{\|t\|^2}{\mathrm{T}_2(t)^2} \quad \text{and} \quad \gamma(P) = \gamma_{\times}(\mathcal{R}).$$

It is known that $\beta(P)$ is the inverse of the smallest eigenvalue of the (real) matrix $\mathbf{V}\mathbf{V}^*$ where $\mathbf{V} = (\omega_j^{i-1})_{i,j}$ for $1 \leq i, j \leq n$ and $\mathbf{V}^*$ is the conjugate transpose of

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

V. Similar to $\alpha(P)$, two values of $\beta(P)$ and $\gamma(P)$ can be replaced by their upper bounds during the parameter selection. 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 $\gamma(P)$.

A 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 $|\Pr_a - (q-1)^{-\varphi(n)}| \le \frac{2^{2\varphi(n)+5}}{q^{\lfloor \epsilon\varphi(n)\rfloor}} \cdot (q-1)^{-\varphi(n)} =: \epsilon'$ for all except a fraction $\le 2^{9\varphi(n)} q^{-\epsilon\varphi(n)}$ 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 forms 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

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

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

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

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

Now we are to estimate $D_{\mathbb{Z}^{2\varphi(n)},r}(\mathbf{z}+\mathbf{a}^{\perp\times})$ by considering each $D_{\mathbb{Z}^{2\varphi(n)},r}(\mathbf{z}+\mathbf{a}^\perp(J_S))$ respectively. For the case $|S|\le\epsilon\varphi(n)$, let $\delta = q^{-\varphi(n)-\lfloor\epsilon\varphi(n)\rfloor}$ and $m=2$, then Lemma 10 implies that, for all except a fraction $\le 2^{8\varphi(n)}q^{-\epsilon\varphi(n)}$ of $\mathbf{a}\in(\mathcal{R}_q^\times)^2$,

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

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 $D_{\mathbb{Z}^{2\varphi(n)},r,-\mathbf{z}}(\mathbf{a}^\perp(J_S)) \le D_{\mathbb{Z}^{2\varphi(n)},r,-\mathbf{z}}(\mathbf{a}^\perp(J_{S'}))$. From the previous result, we conclude that $D_{\mathbb{Z}^{2\varphi(n)},r,-\mathbf{z}}(\mathbf{a}^\perp(J_S)) \le 2\delta + q^{-\varphi(n)-\lfloor\epsilon\varphi(n)\rfloor}$. Therefore, the following inequality holds.

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

for all except a fraction $\leq 2^{9\varphi(n)}q^{-\epsilon\varphi(n)}$ of $\mathbf{a} \in (\mathcal{R}_q^\times)^2$.

Next, we are to estimate $D_{\mathbb{Z}^{\varphi(n)},r}(z_i + \mathcal{R}_q^\times + q\mathbb{Z}^{\varphi(n)})$. Let $\Delta_{\mathbb{K}}$ be the discriminant of the cyclotomic field $\mathbb{K} = \mathbb{Q}[X]/(\Phi_n(X))$. As shown in [26], we have $\Delta_{\mathbb{K}} \leq \varphi(n)^{\varphi(n)}$. The volume of the ideal lattice J_S is $\mathrm{vol}(J_S) = \mathrm{N}(J_S) \cdot \sqrt{\Delta_{\mathbb{K}}}$ and then we have $\lambda_{\varphi(n)}(J_S) = \lambda_1(J_S) \leq \sqrt{\varphi(n)}\,\mathrm{vol}(J_S)^{1/\varphi(n)} \leq \varphi(n)q^{|S|/\varphi(n)}$. Let $\delta = q^{-\varphi(n)/2}$. For S of cardinality $\leq \varphi(n)/2$, by Lemma 1, we get that $r \geq \eta_\delta(J_S)$. Using Lemma 4, we know $|D_{\mathbb{Z}^{\varphi(n)},r,-z_i}(J_S) - q^{-|S|}| \leq 2\delta$. For the case $|S| > \varphi(n)/2$, using the same argument, we have $D_{\mathbb{Z}^{\varphi(n)},r,-z_i}(J_S) \leq 2\delta + q^{-\varphi(n)/2}$. Therefore, the following inequality holds.

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

Overall, we prove that, except for a fraction $\leq 2^{9\varphi(n)}q^{-\epsilon\varphi(n)}$ of $\mathbf{a} \in (\mathbb{R}_q^\times)^2$,

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

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

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] 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)

[2] Bernstein, D.J., Chuengsatiansup, C., Lange, T., van Vredendaal, C.: NTRU prime. Cryptology ePrint Archive, Report 2016/461 (2016), http://eprint.iacr.org/2016/461

[3] 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)

[4] Cabarcas, D., Weiden, P., Buchmann, J.A.: On the efficiency of provably secure NTRU. In: PQCrypto 2014. pp. 22–39 (2014)

[5] 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)

[6] Conrad, K.: The different ideal http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/different.pdf
[7] Conrad, K.: Ideal factorization http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/idealfactor.pdf
[8] Coppersmith, D., Shamir, A.: Lattice attacks on NTRU. In: EUROCRYPT 1997. pp. 52–61 (1997)
[9] Cramer, R., Ducas, L., Wesolowski, B.: Short Stickelberger class relations and application to Ideal-SVP. In: EUROCRYPT 2017. pp. 324–348 (2017)
[10] Ducas, L., Durmus, A.: Ring-LWE in polynomial rings. In: PKC 2012. pp. 34–51 (2012)
[11] Ducas, L., Durmus, A., Lepoint, T., Lyubashevsky, V.: Lattice signatures and bimodal gaussians. In: CRYPTO 2013. pp. 40–56 (2013)
[12] Ducas, L., Lyubashevsky, V., Prest, T.: Efficient identity-based encryption over NTRU lattices. In: ASIACRYPT 2014. pp. 22–41 (2014)
[13] Ducas, L., Nguyen, P.Q.: Learning a zonotope and more: Cryptanalysis of NTRUSign countermeasures. In: ASIACRYPT 2012. pp. 433–450 (2012)
[14] Gama, N., Nguyen, P.Q.: New chosen-ciphertext attacks on NTRU. In: PKC 2007. pp. 89–106 (2007)
[15] Garg, S., Gentry, C., Halevi, S.: Candidate multilinear maps from ideal lattices. In: EUROCRYPT 2013. pp. 1–17 (2013)
[16] Gentry, C.: Key recovery and message attacks on NTRU-composite. In: EUROCRYPT 2001. pp. 182–194 (2001)
[17] Gentry, C.: Fully homomorphic encryption using ideal lattices. In: STOC 2009. pp. 169–178 (2009)
[18] Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: STOC 2008. pp. 197–206 (2008)
[19] 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)
[20] Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A ring-based public key cryptosystem. In: ANTS 1998. pp. 267–288 (1998)
[21] Howgrave-Graham, N.: A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. In: CRYPTO 2007. pp. 150–169 (2007)
[22] Jaulmes, E., Joux, A.: A chosen-ciphertext attack against NTRU. In: CRYPTO 2000. pp. 20–35 (2000)
[23] Kirchner, P., Fouque, P.A.: Revisiting lattice attacks on overstretched NTRU parameters. In: EUROCRYPT 2017. pp. 3–26 (2017)
[24] Langlois, A., Stehlé, D., Steinfeld, R.: GGHLite: More efficient multilinear maps from ideal lattices. In: EUROCRYPT 2014. pp. 239–256 (2014)
[25] 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)
[26] Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: EUROCRYPT 2010. pp. 1–23 (2010)
[27] 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

[28] Micciancio, D.: Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. Computational Complexity 16(4), 365–411 (2007)
[29] Micciancio, D., Regev, O.: Worst-case to average-case reductions based on gaussian measures. SIAM Journal on Computing 37(1), 267–302 (2007)
[30] Nguyen, P.Q., Regev, O.: Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. In: EUROCRYPT 2006. pp. 271–288 (2006)
[31] Peikert, C.: Limits on the hardness of lattice problems in ℓ_p norms. Computational Complexity 17(2), 300–351 (2008)
[32] Peikert, C., Regev, O., Stephens-Davidowitz, N.: Pseudorandomness of Ring-LWE for any ring and modulus. In: STOC 2017 (2017), To appear
[33] Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: STOC 2005. pp. 84–93 (2005)
[34] Stehlé, D., Steinfeld, R.: Making NTRU as secure as worst-case problems over ideal lattices. In: EUROCRYPT 2011. pp. 27–47 (2011)
[35] 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
[36] 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)
[37] Xylouris, T.: On Linnik's constant (2009), http://arxiv.org/abs/0906.2749
[38] Yu, Y., Xu, G., Wang, X.: Provably secure NTRU instances over prime cyclotomic rings. In: PKC 2017. pp. 409–434 (2017)