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 quantum worst-case hardness of classical problems over ideal lattices. Recently, Yu, Xu and Wang constructed pNE variants over prime cyclotomic rings. In this paper, we further extend the previous results to the case of general prime power cyclotomic rings, which allows a more flexible choice of parameters. We discover a potential trade-off between the power exponent of the ring order and the minimal magnitude of modulus. Moreover, we discuss the case of pNE over general rings assuming the hardness of corresponding RLWE, and propose three attributes of the ring mattering to parameter selection.

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

1 Introduction

NTRU, introduced by Hoffstein, Pipher and Silverman in [22], is a celebrated public key cryptosystem standardized by IEEE. Its encryption scheme, NTRUEncrypt, is one of the fastest known lattice-based encryption schemes. Based on NTRU, various cryptographic primitives are designed, including digital signature [21, 11], identity-based encryption [12], fully homomorphic encryption [28, 4] and multi-linear maps [16, 27]. In the last 20 years, many cryptanalytic estimations [8, 25, 17, 20, 37, 32, 15, 23, 3, 13, 1, 7, 26] were proposed aiming at NTRU family, and NTRU is still believed to be secure in practice.

⋆ Corresponding Author.

In 2011, Stehlé and Steinfeld proposed the first IND-CPA(*indistinguishability under chosen-plaintext attack*) secure NTRUEncrypt variant, denoted by pNE, over power-of-2 cyclotomic rings in [35]. pNE shows a connection between NTRU and RLWE(*Ring Learning With Errors* problem). RLWE, introduced by Lyubashevsky, Peikert and Regev [29], has been shown to be as hard as some worst-case problems over ideal lattices, which provides pNE with a strong security guarantee. Recently, Yu, Xu and Wang modified pNE to make it work over prime cyclotomic rings [39], which allows more flexibility of parameter selections. Despite these efforts, the choice of the underlying rings for pNE is still an important issue to be addressed.

Contribution In this paper, we study pNE over prime power cyclotomic rings and show that, given appropriate parameters, pNE still holds in this more general case. Our result further enriches the provably secure NTRU family and allows a more flexible choice of parameters. As by-products, some properties of prime power cyclotomic rings are shown, which may be of some independent interest. Unifying the corresponding results of [35]and [39], some of their ideas are also used in this paper. However, it is still not straightforward to deal with all differences in the proofs.

We also study how prime power affects the final parameter selection. Let $n = d^{\nu}$ be the cyclotomic ring order where d is a prime. As ν increases, the magnitude of minimal modulus q in our result (measured by $\log(q)/\log(n)$) decreases, which implies a set of smaller parameters may be used. However, for large ν, the cyclotomic field $\mathbb{Q}[X]/\Phi(X)$ tends to contain more subfields, which might lead to a worrisome structure as shown in [1, 7].

Moreover, we consider the extension of pNE to general rings and propose three attributes of the ring mattering parameter selection. To design a relatively compact pNE, it requires all these attributes to be small. Although the hardness of RLWE over general rings is not well-studied yet, it may be of some value for searching the candidate of cyclotomic rings for lattice-based cryptosystems.

Open Problem In this paper, we work with coefficient embedding as that in the NTRU setting. The canonical embedding, used in the context of RLWE [29, 30], is another possible choice. Under canonical embedding, both addition and multiplication are coordinate-wise, and one may obtain tighter geometric bounds of unified form for all cyclotomic rings. Indeed, regularity results shown in [30] can be generalized to the form discussed in our paper, however, the current theory is not sufficient to lead to "uniform" public key which is the core component of pNE. To design a new key generation algorithm under canonical embedding, some technical difficulties need to be overcome.

Organization In Sect. 2, we introduce some notations and basic results that will be used in our discussion. In Section 3, we show a series of relevant results over prime power cyclotomic rings. Then we describe our pNE scheme over prime power cyclotomic rings and demonstrate parameter requirements in Sect. 4. Finally, we further discuss the problem of ring selection in Sect. 5.

2 Preliminaries

Lattice A lattice is a set of all integer linear combinations of some linearly independent vectors $\mathbf{b}_1, \cdots, \mathbf{b}_n$ in an m-dimensional Euclidean space. We call $\mathbf{B} = (\mathbf{b}_1, \cdots, \mathbf{b}_n)$ a basis and m the dimension of the lattice. When $n = m$, the lattice is full-rank. Let $\mathbf{B}$ be a basis of $\mathcal{L}$, then we denote the volume of $\mathcal{L}$ as $\det(\mathcal{L}) = \sqrt{\det(\mathbf{B}^\top \mathbf{B})}$. The dual lattice of $\mathcal{L}$ is the lattice $\widehat{\mathcal{L}} = \{\mathbf{c} \in \mathbb{R}^m \mid \forall i, \langle \mathbf{c}, \mathbf{b}_i \rangle \in \mathbb{Z}\}$. 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 a ring with an additive isomorphism θ 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 classical lattice problems By restricting SVP(*Shortest Vector Problem*) and γ-SVP(*Approximate Shortest Vector Problem with approximation factor* γ) to ideal lattices, we get Ideal-SVPand γ-Ideal-SVP. These ideal lattice problems do not seem to be substantially easier than the versions for general lattice (except maybe 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 Let $U(E)$ be the uniform distribution over a finite domain E. For two distributions D_1,D_2 over a 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. 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 $z = x$.

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 $\mathbf{c} \in \mathbb{R}^n$ and width r. When $\mathbf{c} = \mathbf{0}$, the Gaussian function is written as $\rho_r(\mathbf{x})$. Let ψ_r be the Gaussian distribution over $\mathbb{R}$ with mean 0 and width r and 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 $\mathbb{Q}$, which only leads to a negligible impact to our results, as explained in [10]. For $S \subset \mathbb{R}^n$, 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 $\eta_\delta(\mathcal{L}) = \min\{r : \rho_{1/r}(\widehat{\mathcal{L}}) \leq 1 + \delta\}$. We now recall some results which will be used later.

Lemma 1 ([31], Le. 3.3). *Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a 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 ([33], Le. 3.5). *Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a 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 ([31], Le. 4.4). *Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a full-rank lattice and $\delta \in (0, 1)$. For $\mathbf{c} \in \mathbb{R}^n$ and $r \geq \eta_\delta(\mathcal{L})$, we have $\Pr_{\mathbf{b} \hookleftarrow D_{\mathcal{L},r,\mathbf{c}}}(\|\mathbf{b} - \mathbf{c}\| \geq r\sqrt{n}) \leq \frac{1+\delta}{1-\delta} 2^{-n}$.*

Lemma 4 ([19], Cor. 2.8). *Let $\mathcal{L}' \subseteq \mathcal{L} \subseteq \mathbb{R}^n$ be full-rank lattices and $\delta \in (0, 1/2)$. For $\mathbf{c} \in \mathbb{R}^n$ 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 5 ([19], Th. 4.1). *There exists a polynomial-time algorithm that, given a basis $(\mathbf{b}_1, \cdots, \mathbf{b}_n)$ of a lattice $\mathcal{L} \subseteq \mathbb{Z}^n$, a parameter $r = \omega(\sqrt{\log n}) \max \|\mathbf{b}_i\|$ and $\mathbf{c} \in \mathbb{R}^n$, outputs samples from a distribution statistically close to $D_{\mathcal{L},r,\mathbf{c}}$ 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 [38]).

Hardness of RLWE The Ring Learning With Errors problem (RLWE) was first proposed in [29] 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 $1/\mathrm{poly}(n)$.*

For certain error distributions, RLWE can be reduced from γ-Ideal-SVP.

Theorem 1 ([10], Th. 2). *Let n be an integer and $\mathcal{R}_q = \mathbb{Z}_q[X]/\Phi_n(X)$ where q is a prime congruent to 1 modulo n. Also, let $\alpha \in (0,1)$ be a real number such that $\alpha q > \omega(\sqrt{\log n})$. There exists a randomized quantum reduction from γ-Ideal-SVP on ideal lattices in $\mathbb{Z}[X]/\Phi_n(X)$ to $\mathsf{RLWE}_{q,\psi_t^n,k}$ for $t = \sqrt{n'}\alpha q \left(\frac{\varphi(n)k}{\log(\varphi(n)k)}\right)^{1/4}$ where $n' = \deg(\Theta_n(X))$ (with $\gamma = \tilde{O}(\sqrt{n}/\alpha)$) that runs in time $O(q \cdot \mathrm{poly}(n))$.*

Let $\mathcal{R}_q^\times$ be the set of all invertible elements of $\mathcal{R}_q$. As explained in [35], 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 $U(\mathcal{R}_q \times \mathcal{R}_q)$) with same hardness.

3 New Results on Prime Power Cyclotomic Rings

In this section, we will present a series of results on prime power cyclotomic rings. Some results restricted to power-of-2 and prime cyclotomic rings have been discussed in [35, 39]. However, our results are of a wide meaning and partial modifications should be treated carefully.

3.1 Properties of Prime Power Cyclotomic Rings

Let d be a prime and $n = d^\nu$. The degree of $\Phi_n(X)$ is $\varphi(n)$, the totient of n. Let $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. For any $f = \sum_{i=0}^{\varphi(n)-1} f_i X^i \in \mathcal{R}$, the vector $(f_0, \cdots, f_{\varphi(n)-1}) \in \mathbb{Z}^{\varphi(n)}$ is called the coefficient vector of f. For any $\mathbf{s} = (s_1, \cdots, s_m) \in \mathcal{R}^m$, we view $\mathbf{s}$ as a $\varphi(n)m$-dimensional vector in $\mathbb{Z}^{\varphi(n)m}$ by coefficient embedding. We denote by $\langle \mathbf{s}, \mathbf{t} \rangle$ the Euclidean inner product of $\mathbf{s}, \mathbf{t} \in \mathcal{R}^m$. In [35, 39], authors expressed $\langle \mathbf{s}, \mathbf{t} \rangle$ as a coefficient of a polynomial related to $\mathbf{s}$ and $\mathbf{t}$ for the case $d = 2$ and $\nu = 1$ respectively. In this work, we give a similar expression of $\langle \mathbf{s}, \mathbf{t} \rangle$ for general d and ν.

Let $f \in \mathcal{R}$ be with coefficient vector $(f_0, \cdots, f_{\varphi(n)-1})$, we define two polynomials $f^\frown$ and $f^\smile$ as follows. The coefficient vector of $f^\frown$ is $(f_0^\frown, \cdots, f_{\varphi(n)-1}^\frown)$, where

$$f_i^\frown = \begin{cases} f_i - f_{i+\frac{n}{d}}, & \text{for } i < \varphi(n) - \frac{n}{d}; \\ f_i, & \text{for } i \geq \varphi(n) - \frac{n}{d}. \end{cases}$$

The coefficient vector of $f^\smile$ is $(f_0^\smile, \cdots, f_{\varphi(n)-1}^\smile)$, where

$$f_i^\smile = \sum_{j \geq i, j = i \bmod \frac{n}{d}} f_j.$$

For the case n is a power of 2, we have $f^\smile = f^\frown = f$ for any $f \in \mathcal{R}$, because $\varphi(n) = n/2$.For the case n is a prime, these operations are same to that in [39] and proven to be inverse to each other. Actually, the inverse relation still holds for general prime power case.

Lemma 6. *Let $n = d^\nu$ with d a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$, then $(f^\smile)^\frown = (f^\frown)^\smile = f$ for any $f \in \mathcal{R}$.*

Exploiting above operations, we prove that the Euclidean inner product of two elements equals the constant coefficient of a certain polynomial.

Lemma 7. *Let $n = d^\nu$ with d a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. Denote by X^{-1} the inverse of X. Let $f \in \mathcal{R}$ of coefficient vector $(f_0, \cdots, f_{\varphi(n)-1})$ and $g \in \mathcal{R}$ of coefficient vector $(g_0, \cdots, g_{\varphi(n)-1})$. Then*

$$\sum_{i=0}^{\varphi(n)-1} f_i g_i = \textit{the constant coefficient of the polynomial } f(X)g^\smile(X^{-1}).$$

Proof. It is noted that $\Phi_n(X)$ is a factor of $X^n - 1$. Hence X^n is essentially the identity element of $\mathcal{R}$, which implies that X^{-1} is equivalent to X^{n-1} when it is discussed in $\mathcal{R}$. Let $(g'_0, \cdots, g'_{\varphi(n)-1})$ be the coefficient vector of the polynomial $g^\smile$, then

$$f(X)g^\smile(X^{-1}) = f(X)g^\smile(X^{n-1}) = \sum_{i,j \in \{0,\cdots,\varphi(n)-1\}} f_i g'_j X^{i+(n-1)j \bmod n}.$$

For $\varphi(n) \le l < n$, we have $X^l = -(X^{\frac{n}{d}\cdot(d-2)} + \cdots + X^{\frac{n}{d}} + 1)X^{l-\varphi(n)}$ and the degree of the polynomial on the right-hand side is less than $n - \varphi(n) + \frac{n(d-2)}{d} = \varphi(n)$ that is the degree of $\Phi_n(X)$. Therefore, the constant coefficient of $f(X)g^\smile(X^{-1})$ equals $\sum_{i=0}^{\varphi(n)-1} f_i g'_i - \sum_{i=0}^{\varphi(n)-1-\frac{n}{d}} f_i g'_{i+\frac{n}{d}} = \sum_{i=0}^{\varphi(n)-1-\frac{n}{d}} f_i(g'_i - g'_{i+\frac{n}{d}}) + \sum_{\varphi(n)-\frac{n}{d}}^{\varphi(n)-1} f_i g'_i$. The terms $\{g'_i - g'_{i+\frac{n}{d}}\}_{i=0}^{\varphi(n)-1-\frac{n}{d}}$ and $\{g'_i\}_{i \ge \varphi(n)-\frac{n}{d}}$ are exactly the coefficients of the polynomial $(g^\smile)^\frown = g$. Consequently, the constant coefficient of $f(X)g^\smile(X^{-1})$ equals $\sum_{i=0}^{\varphi(n)-1} f_i g_i$. □

Corollary 1. *Let $n = d^\nu$ with d a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. For any $\mathbf{s} = (s_1, \cdots, s_m) \in \mathcal{R}^m$ and $\mathbf{t} = (t_1, \cdots, t_m) \in \mathcal{R}^m$, then*

$$\langle \mathbf{s}, \mathbf{t} \rangle = \textit{the constant coefficient of the polynomial } \sum_{i=1}^{m} s_i(X) t_i^\smile(X^{-1}).$$

Now we are to study quantitative relations among several common norms. For $t \in \mathcal{R}$, we denote by $\|t\|$ the Euclidean norm of the coefficient vector of t. Also, the T_2-norm of t is $\mathrm{T}_2(t) = \sqrt{\sum_{i \in \mathbb{Z}_n^*} |t(\xi_n^i)|^2}$ and the algebraic norm is $\mathrm{N}(t) = \prod_{i \in \mathbb{Z}_n^*} |t(\xi_n^i)|$.

Lemma 8. *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*

$$\mathrm{N}(t)^{\frac{2}{\varphi(n)}} \le \frac{\mathrm{T}_2(t)^2}{\varphi(n)} \quad \textit{and} \quad \|t\|^2 = \frac{\mathrm{T}_2(t)^2 + \frac{n}{d}\sum_{k=0}^{\frac{n}{d}-1}\left(\sum_{i=k \bmod \frac{n}{d}} t_i\right)^2}{n} \ge \frac{\mathrm{T}_2(t)^2}{n}.$$

Proof. By arithmetic-geometric inequality, the first inequality follows. We now prove the second inequality. For any $l \in \mathbb{Z}_n^*$, the value of $|t(\xi_n^l)|^2$ can be written as

$$|t(\xi_n^l)|^2 = t(\xi_n^l)t(\xi_n^{-l}) = \sum_{i=0}^{\varphi(n)-1} t_i^2 + \sum_{i\neq j} t_i t_j \xi_n^{l(i-j)} = \|t\|^2 + \sum_{i\neq j} t_i t_j \xi_n^{l(i-j)}.$$

Then, we have

$$\begin{aligned}\mathrm{T}_2^2(t) &= \varphi(n)\cdot\|t\|^2 + \sum_{i\neq j} t_i t_j \sum_{l\in\mathbb{Z}_n^*} \xi_n^{(i-j)l} \\ &= \varphi(n)\cdot\|t\|^2 + \sum_{i\neq j} t_i t_j \left(\sum_{k=1}^{d-1} \xi_n^{(i-j)k}\right)\left(\sum_{k=0}^{\frac{n}{d}-1} \xi_n^{(i-j)dk}\right).\end{aligned}$$

Let $S_1(\xi_n^{i-j}) = \sum_{k=1}^{d-1} \xi_n^{(i-j)k}$ and $S_2(\xi_n^{i-j}) = \sum_{k=0}^{\frac{n}{d}-1} \xi_n^{(i-j)dk}$. The term $\xi_n^{(i-j)d}$ equals 1 if and only if $i = j \bmod \frac{n}{d}$. A routine computation leads to that

$$S_2(\xi_n^{i-j}) = \begin{cases} 0, \text{ for } i \neq j \bmod \frac{n}{d}; \\ \frac{n}{d}, \text{ for } i = j \bmod \frac{n}{d}. \end{cases}$$

Because $i \neq j$ and $|i-j| < \varphi(n)$, the term ξ_n^{i-j} can not be 1. When $i = j \bmod \frac{n}{d}$, we have $S_1(\xi_n^{i-j}) = \frac{\xi_n^{(i-j)d} - \xi_n^{i-j}}{\xi_n^{i-j}-1} = -1$. Combining the expressions of $S_1(\xi_n^{i-j})$ and $S_2(\xi_n^{i-j})$, we obtain

$$\begin{aligned}\mathrm{T}_2^2(t) &= \varphi(n)\cdot\|t\|^2 - \frac{n}{d}\left(\sum_{\substack{i\neq j \\ i=j \bmod \frac{n}{d}}} t_i t_j\right) \\ &= \varphi(n)\cdot\|t\|^2 - \frac{n}{d}\left(\sum_{k=0}^{\frac{n}{d}-1}\left(\sum_{i=k \bmod \frac{n}{d}} t_i\right)^2 - \sum_{i=0}^{\varphi(n)-1} t_i^2\right) \\ &= n\cdot\|t\|^2 - \frac{n}{d}\sum_{k=0}^{\frac{n}{d}-1}\left(\sum_{i=k \bmod \frac{n}{d}} t_i\right)^2.\end{aligned}$$

Thus the second inequality follows immediately. □

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 [18, 39]). The following lemma indicates that, for general prime power cyclotomic rings, their expansion factors are well-bounded as well.

Lemma 9. *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 $\|fg\|_\infty \leq 2\|f\|\|g\|$ and $\|fg\| \leq 2\sqrt{\varphi(n)}\|f\|\|g\|$.*

Proof. We apply the idea of [39] and 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 $|h'_i| \leq \|f'\|\|g'\| = \|f\|\|g\|$ 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

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

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

3.2 Duality Results for Module Lattices

Some duality results with respect to module lattices over power-of-2 and prime cyclotomic rings are presented respectively in [35, 39]. Next we will give a general duality result for all prime power cyclotomic rings.

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 and denote by $\{\phi_i\}_{i=1,\cdots,\varphi(n)}$ all roots of $\Phi_n(X)$ modulo q. 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. Given $\mathbf{a} \in \mathcal{R}_q^m$, three families of $\mathcal{R}$-modules $\mathbf{a}^\perp(I_S)$, $\mathcal{L}(\mathbf{a}, I_S)$ and $\mathcal{L}^\frown(\mathbf{a}, I_S)$ are defined as follows.

$$\mathbf{a}^\perp(I_S) := \left\{(t_1, \cdots, t_m) \in \mathcal{R}^m \mid \forall i, (t_i \bmod q) \in I_S \text{ and } \sum_{i=1}^m t_i a_i = 0 \bmod q\right\},$$

$$\mathcal{L}(\mathbf{a}, I_S) := \{(t_1, \cdots, t_m) \in \mathcal{R}^m \mid \exists s \in \mathcal{R}_q, \forall i, (t_i \bmod q) = a_i \cdot s \bmod I_S\},$$

$$\mathcal{L}^\frown(\mathbf{a}, I_S) := \left\{(t_1, \cdots, t_m) \in \mathcal{R}^m \mid (t_1^\smile, \cdots, t_m^\smile) \in \mathcal{L}(\mathbf{a}, I_S)\right\}.$$

Identifying $\mathcal{R}$ with $\mathbb{Z}^{\varphi(n)}$, these $\mathcal{R}$-modules can be viewed as $m\varphi(n)$-dimensional lattices, called *module lattices*. The definitions and notations of above module lattices look the same as that in [39], but it is worth noting that the ring $\mathcal{R}$ becomes a general prime power cyclotomic ring so that the meanings of $\smile$ and $\frown$ are modified as well. The duality relationship between $\mathbf{a}^\perp(I_S)$ and $\mathcal{L}^\frown(\mathbf{a}, I_S)$ holds for more general cases.

Lemma 10. *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 $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Given $S \subseteq \{1, \cdots, \varphi(n)\}$ and $\mathbf{a} \in \mathcal{R}_q^m$, let $\mathbf{a}^\times \in \mathcal{R}_q^m$ be defined by $a_i^\times = a_i(X^{-1})$ and $I_{\bar{S}}^\times$ be the ideal $\prod_{i \in \bar{S}}(X - \phi_i^{-1}) \cdot \mathcal{R}_q$ where $\bar{S}$ is the complement of S. Then $\widehat{\mathbf{a}^\perp(I_S)} = \frac{1}{q}\mathcal{L}^\frown(\mathbf{a}^\times, I_{\bar{S}}^\times)$.*

Remark The main technique of proof is to associate Euclidean inner product of vectors with certain polynomials as stated in Corollary 1. The above lemma can be proven in a manner similar to [39] and hence we omit the proof here.

3.3 On the Absence of Unusually Short Vector in $\mathcal{L}^{\frown}(\mathbf{a}, I_S)$

Let $\mathcal{R}_q^{\times}$ be the set of all invertible elements of $\mathcal{R}_q$. For $\mathbf{a} \hookleftarrow \mathbf{U}((\mathcal{R}_q^{\times})^m)$, the lattice $\mathcal{L}^{\frown}(\mathbf{a}, I_S)$ is nearly impossible to contain a unusually short vector for the ℓ_∞ norm. We first show a similar result for $\mathcal{L}(\mathbf{a}, I_S)$.

Lemma 11. *Let $n = d^\nu > 7$ 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 $S \subseteq \{1, \cdots, \varphi(n)\}$, $m \geq 2$ and $\epsilon > 0$, set*

$$\beta := 1 - \frac{1}{m} + \frac{1 - \sqrt{1 + 4m(m-1)\left(1 - \frac{|S|}{\varphi(n)}\right) + 4m\epsilon}}{2m} \geq 1 - \frac{1}{m} - \epsilon - (m-1)\left(1 - \frac{|S|}{\varphi(n)}\right),$$

then we have $\lambda_1^{\infty}(\mathcal{L}(\mathbf{a}, I_S)) \geq \frac{1}{\sqrt{n}} q^{\beta}$ with probability $\geq 1 - \frac{2^{\varphi(n)}}{(q-1)^{\epsilon\varphi(n)}}$ over the uniformly random choice of $\mathbf{a}$ in $(\mathcal{R}_q^{\times})^m$.

Remark The proof essentially follows the same approach in [35, 39] but with minor differences on the inequalities for different norms. The concrete relations among norms are shown in Lemma 8. Thus the proof is not included in our paper. Furthermore, this result holds for all prime power cyclotomic rings, but it can be optimized for some special cases. For example, for $n = 2^\nu$, the second inequality in Lemma 8 can be replaced with an identity that $\|t\|^2 = \frac{2\mathrm{T}_2(t)^2}{n}$ so that the threshold length will increase to $\sqrt{\frac{2}{n}} q^{\beta}$.

Next we shall show a quantitative relationship between $\lambda_1^{\infty}(\mathcal{L}(\mathbf{a}, I_S))$ and $\lambda_1^{\infty}(\mathcal{L}^{\frown}(\mathbf{a}, I_S))$.

Lemma 12. *Let $n = d^\nu > 7$ with d a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. Let $q = 1 \bmod n$ be a prime and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Then, for any $\mathbf{a} \in (\mathcal{R}_q^{\times})^m$ and $S \subseteq \{1, \cdots, \varphi(n)\}$, we have*

$$\lambda_1^{\infty}(\mathcal{L}(\mathbf{a}, I_S)) \leq \left\lceil \frac{d-1}{2} \right\rceil \lambda_1^{\infty}(\mathcal{L}^{\frown}(\mathbf{a}, I_S)).$$

Proof. We first prove that $\|X^{\frac{\varphi(n)}{2}} t^{\smile}\|_\infty \leq \left\lceil \frac{d-1}{2} \right\rceil \|t\|_\infty$ for any $t \in \mathcal{R}$. For the case $d = 2$, two elements t and $t^{\smile}$ are same and hence the inequality holds. It suffices to prove the inequality for the case $d > 2$. Let $(t_0, \cdots, t_{\varphi(n)})$, $(t_0^{\smile}, \cdots, t_{\varphi(n)}^{\smile})$ and $(t'_0, \cdots, t'_{\varphi(n)})$ be the coefficient vectors of t, $t^{\smile}$ and $X^{\frac{\varphi(n)}{2}} t^{\smile}$ respectively. By classifying all coefficients according to the residue modulo $\frac{n}{d}$ of indices, we write $t^{\smile}$ as $t^{\smile} = \sum_{i=0}^{\frac{n}{d}-1} \left(\sum_{j=i \bmod \frac{n}{d}} t_j^{\smile} X^j \right)$. Let $S_t(i) = \sum_{j=i \bmod \frac{n}{d}} t_j^{\smile} X^j$. There

must be one and only one $j \in [\frac{\varphi(n)}{2}, \frac{\varphi(n)}{2} + \frac{n}{d})$ such that $j = i \bmod \frac{n}{d}$, denoted by $\bar{i}$. Notice that $\varphi(n) = n - \frac{n}{d}$ and that $\frac{\varphi(n)}{2} = \frac{d-1}{2}\frac{n}{d}$ is a multiple of $\frac{n}{d}$, then

$$\begin{aligned} X^{\frac{\varphi(n)}{2}} S_t(i) &= \sum_{\substack{j=i \bmod \frac{n}{d} \\ j<\frac{\varphi(n)}{2}}} (t_j^{\smile} - t_{\bar{i}}^{\smile}) X^{j+\frac{\varphi(n)}{2}} + \sum_{\substack{j=i \bmod \frac{n}{d} \\ j\geq \frac{\varphi(n)}{2}+\frac{n}{d}}} (t_j^{\smile} - t_{\bar{i}}^{\smile}) X^{j+\frac{\varphi(n)}{2}-n} - t_{\bar{i}}^{\smile} X^{\bar{i}-\frac{n}{d}} \\ &= \sum_{\substack{j=i \bmod \frac{n}{d} \\ \frac{\varphi(n)}{2}\leq j<\varphi(n)}} (t^{\smile}_{j-\frac{\varphi(n)}{2}} - t_{\bar{i}}^{\smile}) X^j + \sum_{\substack{j=i \bmod \frac{n}{d} \\ 0\leq j<\frac{\varphi(n)}{2}-\frac{n}{d}}} (t^{\smile}_{j+\frac{\varphi(n)}{2}+\frac{n}{d}} - t_{\bar{i}}^{\smile}) X^j - t_{\bar{i}}^{\smile} X^{\bar{i}-\frac{n}{d}}. \end{aligned}$$

Combining the definition of operation $\smile$, it can be verified that each t'_i is a sum of t_j's whose indices form an arithmetic progression of common difference $\frac{n}{d}$ and length at most $\frac{d-1}{2}$. Thus $\|X^{\frac{\varphi(n)}{2}} t^{\smile}\|_\infty = \max_i |t'_i| \leq \frac{d-1}{2} \max_i |t_i| = \frac{d-1}{2}\|t\|_\infty$ and then we have $\|X^{\frac{\varphi(n)}{2}} t^{\smile}\|_\infty \leq \left\lceil \frac{d-1}{2} \right\rceil \|t\|_\infty$.

Let $\mathbf{v} = (v_1, \cdots, v_m) \in \mathcal{L}^{\frown}(\mathbf{a}, I_S)$ whose infinity norm equals $\lambda_1^\infty(\mathcal{L}^{\frown}(\mathbf{a}, I_S))$. We know that $(v_1^{\smile}, \cdots, v_m^{\smile}) \in \mathcal{L}(\mathbf{a}, I_S)$ and hence $\mathbf{v}' = (X^{\frac{\varphi(n)}{2}} v_1^{\smile}, \cdots, X^{\frac{\varphi(n)}{2}} v_m^{\smile}) \in \mathcal{L}(\mathbf{a}, I_S)$. Notice that $\|\mathbf{v}'\|_\infty = \max_i \|X^{\frac{\varphi(n)}{2}} v_i^{\smile}\|_\infty \leq \left\lceil \frac{d-1}{2} \right\rceil \max_i \|v_i\|_\infty = \left\lceil \frac{d-1}{2} \right\rceil \|\mathbf{v}\|_\infty$ and $\mathbf{v}' \neq \mathbf{0}$, then we conclude that $\lambda_1^\infty(\mathcal{L}(\mathbf{a}, I_S)) \leq \left\lceil \frac{d-1}{2} \right\rceil \lambda_1^\infty(\mathcal{L}^{\frown}(\mathbf{a}, I_S))$. □

Applying Lemmata 11 and 12, we obtain the following result.

Lemma 13. *Let $n = d^\nu > 7$ 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 $S \subseteq \{1, \cdots, \varphi(n)\}$, $m \geq 2$ and $\epsilon > 0$, set*

$$\beta := 1 - \frac{1}{m} + \frac{1 - \sqrt{1 + 4m(m-1)\left(1 - \frac{|S|}{\varphi(n)}\right) + 4m\epsilon}}{2m} \geq 1 - \frac{1}{m} - \epsilon - (m-1)\left(1 - \frac{|S|}{\varphi(n)}\right),$$

then we have $\lambda_1^\infty(\mathcal{L}^{\frown}(\mathbf{a}, I_S)) \geq \frac{1}{\left\lceil \frac{d-1}{2} \right\rceil \sqrt{n}} q^\beta$ with probability $\geq 1 - \frac{2^{\varphi(n)}}{(q-1)^{\epsilon\varphi(n)}}$ over the uniformly random choice of $\mathbf{a}$ in $(\mathcal{R}_q^\times)^m$.

3.4 Regularity Results

We present some regularity results over prime power cyclotomic rings which may be useful in general cryptographic applications. The following lemma can be proven by combining Lemmata 2, 4, 10 and 13. For NTRU discussed in this paper, it suffices to focus on the case $m = 2$.

Lemma 14. *Let $n = d^\nu > 7$ with d a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. Let $q = 1 \bmod n$ be a prime and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Let $S \subseteq \{1, \cdots, \varphi(n)\}$, $m \geq 2, \epsilon > 0, \delta \in (0, \frac{1}{2})$. Let $r \geq \left\lceil \frac{d-1}{2} \right\rceil \sqrt{n \ln(2m\varphi(n)(1 + 1/\delta))/\pi} \cdot q^{\frac{1}{m} + (m-1)\frac{|S|}{\varphi(n)} + \epsilon}$, $\mathbf{c} \in \mathbb{R}^{m\varphi(n)}$ and $\mathbf{t} \hookleftarrow D_{\mathbb{Z}^{m\varphi(n)}, r, \mathbf{c}}$. Then for all except a fraction $\leq 2^{\varphi(n)}(q-1)^{-\epsilon\varphi(n)}$ of $\mathbf{a} \in (\mathcal{R}_q^\times)^m$, we have*

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

For $\mathbf{a} \in (\mathcal{R}_q^\times)^m$, we know that $\det\left(\mathbf{a}^\perp(I_S)\right) = \det\left(\frac{1}{q}\mathcal{L}^\frown(\mathbf{a}^\times, I_{\bar{S}}^\times)\right)^{-1} = q^{\varphi(n)+(m-1)|S|}$. Notice that $|\mathbb{Z}^{m\varphi(n)}/\mathbf{a}^\perp(I_S)| = \det\left(\mathbf{a}^\perp(I_S)\right)$, the following result is an immediate consequence of Lemma 14.

Lemma 15. *Let $n = d^\nu > 7$ with d a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. Let $q = 1 \bmod n$ be a prime and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Let $S \subseteq \{1, \cdots, \varphi(n)\}$, $m \geq 2, \epsilon > 0, \delta \in (0, \frac{1}{2})$. Let $r \geq \left\lceil \frac{d-1}{2} \right\rceil \sqrt{n \ln(2m\varphi(n)(1+1/\delta))/\pi} \cdot q^{\frac{1}{m}+(m-1)\frac{|S|}{\varphi(n)}+\epsilon}$, $\mathbf{c} \in \mathbb{R}^{m\varphi(n)}$ and $\mathbf{t} \hookleftarrow D_{\mathbb{Z}^{m\varphi(n)},r,\mathbf{c}}$. Then for all except a fraction $\leq 2^{\varphi(n)}(q-1)^{-\epsilon\varphi(n)}$ of $\mathbf{a} \in (\mathcal{R}_q^\times)^m$, we have*

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

3.5 Gap of Ideal Lattices

Let I be an ideal of $\mathbb{Z}[X]/\Phi_n(X)$ and $\mathcal{L}_I$ be the ideal lattice generated by I (under the coefficient embedding). For the case $n = 2^\nu$, it is known that $\lambda_{\varphi(n)}(\mathcal{L}_I) = \lambda_1(\mathcal{L}_I)$. For the case $n = d$ is a prime, the gap between $\lambda_{\varphi(n)}(\mathcal{L}_I)$ and $\lambda_1(\mathcal{L}_I)$ is proven to be at most $\sqrt{n}$ (see [39]). Next we are to prove a general result for all prime power cyclotomic rings, which would be of independent interest.

Lemma 16. *Let $n = d^\nu$ with d a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. For any non-zero ideal I of $\mathcal{R}$, we have:*

$$\lambda_{\varphi(n)}(\mathcal{L}_I) \leq \sqrt{d} \cdot \lambda_1(\mathcal{L}_I).$$

Proof. Let $v \in I$ whose coefficient vector $\mathbf{v} = (v_0, \cdots, v_{\varphi(n)-1})$ is a non-zero shortest vector of $\mathcal{L}_I$. We denote by $\mathbf{v}^{(k)} = \left(v_0^{(k)}, \cdots, v_{\varphi(n)-1}^{(k)}\right)$ the coefficient vector of $X^k v$. It is known that $\mathbf{v}^{(k)} \in \mathcal{L}_I$ for any $k \in \{1, \cdots, \varphi(n)-1\}$. Let $\mathcal{R}' = \mathbb{Z}[X]/(X^n - 1)$. Let $\overline{v} \in \mathcal{R}'$ be the polynomial with the same coefficients as v and $\overline{v}^{(k)} = X^k\overline{v} \in \mathcal{R}'$. The coefficient vector of $\overline{v}$ is $(v_0, \cdots, v_{n-1})$ with $v_l = 0$ for $l \geq \varphi(n)$ and that of $\overline{v}^{(k)}$ is denoted by $\left(\overline{v}_0^{(k)}, \cdots, \overline{v}_{n-1}^{(k)}\right)$. We have that $\overline{v}_i^{(k)} = v_{(i-k) \bmod n}$. Since $\Phi_n(X)$ is a factor of $X^n - 1$, we know that $X^k v = \overline{v}^{(k)} \bmod \Phi_n(X)$. By the fact that $X^l = -(X^{\frac{n}{d}\cdot(d-2)} + \cdots + X^{\frac{n}{d}} + 1)X^{l-\varphi(n)}$ for $l > \varphi(n)$, the following result holds:

$$v_i^{(k)} = \overline{v}_i^{(k)} - \overline{v}_{(i \bmod \frac{n}{d})+\varphi(n)}^{(k)} = v_{(i-k) \bmod n} - v_{((i \bmod \frac{n}{d})+\varphi(n)-k) \bmod n}.$$

Let $S_1 = \sum_{i=0}^{\varphi(n)-1} v_{(i-k) \bmod n}^2$, $S_2 = \sum_{i'=0}^{\frac{n}{d}-1} v_{(i'+\varphi(n)-k) \bmod n}^2$. We have that

$$S_1 + S_2 = \sum_{i=0}^{n-1} v_i^2 = \sum_{i=0}^{\varphi(n)-1} v_i^2 = \|\mathbf{v}\|^2 = \lambda_1(\mathcal{L}_I)^2.$$

Let $S_3(i') = \sum_{\substack{j\in\{0,\cdots\varphi(n)-1\}\\ j=i' \bmod \frac{n}{d}}} v_{(j-k) \bmod n}$. A routine computation leads to that

$$\begin{aligned}
\|\mathbf{v}^{(k)}\|^2 &= S_1 + (d-1)S_2 - 2\sum_{i'=0}^{\frac{n}{d}-1} S_3(i') v_{(i'+\varphi(n)-k) \bmod n} \\
&\leq S_1 + (d-1)S_2 + S_2 + \sum_{i'=0}^{\frac{n}{d}-1} S_3(i')^2 \\
&\leq S_1 + dS_2 + (d-1)\sum_{i'=0}^{\frac{n}{d}-1} \left(\sum_{\substack{j\in\{0,\cdots\varphi(n)-1\}\\ j=i' \bmod \frac{n}{d}}} v^2_{(j-k) \bmod n} \right) \\
&= d(S_1 + S_2) = d\lambda_1(\mathcal{L}_I)^2.
\end{aligned}$$

Notice that $\mathbf{v}$ and $\{\mathbf{v}^{(k)}\}_{k=1}^{\varphi(n)-1}$ are linearly independent and of norm within $\sqrt{d}\lambda_1(\mathcal{L}_I)$, then we get that $\lambda_{\varphi(n)}(\mathcal{L}_I) \leq \sqrt{d} \cdot \lambda_1(\mathcal{L}_I)$. □

Interestingly, for prime power cyclotomic rings, it seems to be the prime factor rather than the order that determines the gap of ideal lattices. By combining Minkowski's theorem, we obtain the following corollary.

Corollary 2. *Let $n = d^\nu > 7$ with d a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. Let $q = 1 \bmod n$ be a prime and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Let $S \subseteq \{1, \cdots, \varphi(n)\}$ and denote by $\mathcal{L}_{I_S}$ the lattice generated by the ideal $\langle q, \prod_{i\in S}(X - \phi_i)\rangle$. Then*

$$\lambda_{\varphi(n)}(\mathcal{L}_{I_S}) \leq \sqrt{d} \cdot \lambda_1(\mathcal{L}_{I_S}) \leq \sqrt{d\varphi(n)} \cdot q^{\frac{|S|}{\varphi(n)}}.$$

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 [39] with minor differences. 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 $pk = h = pg/f \in \mathcal{R}_q^\times$.
– **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 $C' = f \cdot C \bmod q$ and return $C' \bmod p$.

Next we analysis the above algorithms and then give a set of parameters to make pNE workable and provably secure.

4.1 Key Generation

The key generation algorithm follows the idea originally proposed by Stehlé and Steinfeld in [35]. Since our parameter conditions are much stronger than that in Lemma 5, we assume that a polynomial-time perfect discrete Gaussian sampler is available. The following lemma shows that the key generation algorithm terminates in expected polynomial time for selective parameters.

Lemma 17. *Let $n = d^\nu > 7$ with d a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. Let $q = 1 \bmod n$ be a prime and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Let $r \geq \sqrt{d\varphi(n)\ln(2\varphi(n)(1+1/\delta))/\pi} \cdot q^{1/\varphi(n)}$, for any $\delta \in (0, 1/2)$. Then $\Pr_{f' \hookleftarrow D_{\mathbb{Z}^{\varphi(n)},r}}\left((p \cdot f' + a \bmod q) \notin \mathcal{R}_q^\times\right) \leq \varphi(n)(1/q + 2\delta)$ holds for $a \in \mathcal{R}$ and $p \in \mathcal{R}_q^\times$.*

Proof. Let I_k be the ideal $\langle q, X - \phi_k\rangle$ for any $k \in \{1, \cdots, \varphi(n)\}$. Corollary 2 shows that $\lambda_{\varphi(n)}(\mathcal{L}_{I_k}) \leq \sqrt{d\varphi(n)} \cdot q^{\frac{1}{\varphi(n)}}$. By Lemma 1, we have $r \geq \eta_\delta(\mathcal{L}_{I_k})$. Together with Lemma 4, it leads to that the probability of $p \cdot f' + a = 0 \bmod I_k$ is at most $1/q + 2\delta$. By the union bound, the proof is completed. □

Next we prove that the norms of secret polynomials f and g are small.

Lemma 18. *Let $n = d^\nu > 7$ with d a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. Let $q = 1 \bmod n$ be a prime and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Let $r \geq \sqrt{d\varphi(n)\ln(6\varphi(n))/\pi} \cdot q^{1/\varphi(n)}$. The secret key polynomials f, g satisfy, with probability $\geq 1 - 2^{-\varphi(n)+3}$,*

$$\|f\| \leq 3\varphi(n)\|p\|r \quad \text{and} \quad \|g\| \leq \sqrt{\varphi(n)} \cdot r.$$

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

Proof. Combining Lemmata 3 and 17, we have that $\|g\|$ is less than $r\sqrt{\varphi(n)}$ with probability $\geq 1 - 2^{-\varphi(n)+3}$ and so is $\|f'\|$. Since $\|f\| \leq 1 + \|pf'\|$, together with Lemma 9, we complete the proof. □

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. This conclusion holds for general prime power cyclotomic rings as well.

Theorem 2. *Let $n = d^\nu > 7$ with d a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. Let $q = 1 \bmod n$ be a prime and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Let $D^{\times}_{r,z}$ the discrete Gaussian $D_{\mathbb{Z}^{\varphi(n)},r}$ restricted to $\mathcal{R}_q^{\times} + z$. Let $0 < \epsilon < \frac{1}{2}$ and $r \geq \left\lceil \frac{d-1}{2} \right\rceil \sqrt{n\varphi(n)}\sqrt{\ln(8nq)} \cdot q^{\frac{1}{2}+2\epsilon}$. Then*

$$\Delta\left(\frac{y_1 + p \cdot D^{\times}_{r,z_1}}{y_2 + p \cdot D^{\times}_{r,z_2}} \bmod q; U(\mathcal{R}_q^{\times})\right) \leq \frac{2^{3\varphi(n)}}{q^{\lfloor \epsilon\varphi(n) \rfloor}}$$

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 To prove the above theorem, it suffices to follow the same approach in [35] and treat the difference caused by the new regularity result shown in Lemma 15. Thus we omit the proof.

4.2 Decryption

The successful decryption is ensured by the fact that a polynomial of ℓ_∞ norm less than $q/2$ keeps unchanged after modulo q reduction. In the decryption algorithm, we calculate a middle term $C' = f \cdot C = pgs + pfe + fM \bmod q$. We now estimate the ℓ_∞ norms of pgs, pfe and fM respectively.

We first study the sizes of e and s which follow RLWE error distribution.

Lemma 19. *Let $n = d^\nu > 7$ with d a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. For $t > 1$ and $u > 0$, we have*

$$\Pr_{\mathbf{b} \hookleftarrow \overline{\psi_t^n}}\left(\|\mathbf{b}\| \geq \left(2\sqrt{2n} + \sqrt{2du}\right) t\right) \leq \exp(-u).$$

Proof. To begin with, we recall some results that will be useful in our proof.

Proposition 1. *For any $x \in \mathbb{R}$, we have $\lfloor x \rceil^2 \leq \frac{1}{4\epsilon} + \frac{1}{1-\epsilon}x^2$.*

Proposition 2. *Let $\Sigma = \mathbf{M}^\top\mathbf{M}$ where*

$$\mathbf{M} = \begin{pmatrix} 1 & & & -1 \\ & 1 & & -1 \\ & & \ddots & \vdots \\ & & & 1 \ -1 \\ & & & 0 \end{pmatrix} \in \mathbb{R}^{d \times d}.$$

Then we have $\mathbf{tr}(\Sigma) = 2(d-1)$, $\mathbf{tr}(\Sigma^2) = (d-1)(d+2)$ and $\|\Sigma\| = d$.

Proposition 3. *Let $\mathbf{B} \in \mathbb{R}^{n \times n}$ and $\Sigma = \mathbf{B}^\top\mathbf{B}$. Let $\mathbf{v}$ be a vector drawn from ψ_1^n. For any $u > 0$, we have*

$$\Pr\left(\|\mathbf{Bv}\|^2 > \mathbf{tr}\left(\Sigma\right) + 2\sqrt{\mathbf{tr}\left(\Sigma^2\right) u} + 2\|\Sigma\|u\right) \leq \exp(-u).$$

Two first propositions are shown in the proof of Lemma 17 in [39] and the third one is shown in [24].

For the case $d = 2$, we have $\Theta_n(X) = \Phi_n(X)$. Let $\mathbf{b} = \lfloor \mathbf{b}' \bmod \Phi_n(X) \rceil = \lfloor \mathbf{b}' \rceil \in \mathcal{R}$ with $\mathbf{b}' \hookleftarrow \psi_t^{\frac{n}{2}}$ and $\mathbf{v} = \frac{1}{t} \cdot \mathbf{b}'$. By Proposition 1, we have

$$\|\mathbf{b}\|^2 \leq \frac{t^2}{1-\epsilon}\|\mathbf{v}\|^2 + \frac{n}{8\epsilon}.$$

Applying Proposition 3, we get

$$\Pr\left(\|\mathbf{v}\|^2 > n/2 + \sqrt{2nu} + 2u\right) \leq \exp(-u).$$

Let $\epsilon = \left(1 + \sqrt{8t^2\left(n/2 + \sqrt{2nu} + 2u\right)/n}\right)^{-1} \in (0,1)$ and

$$A = \sqrt{\frac{\frac{n}{2} + \sqrt{2nu} + 2u}{1-\epsilon} + \frac{n}{8t^2\epsilon}}.$$

We can verify that $A = \sqrt{n/2 + \sqrt{2nu} + 2u} + \sqrt{n/(8t^2)} < 2\sqrt{2n} + \sqrt{2du}$ and then we have

$$\begin{aligned}
&\Pr_{\mathbf{b} \hookleftarrow \overline{\psi_t^n}}\left(\|\mathbf{b}\| \geq \left(2\sqrt{2n} + \sqrt{2du}\right)t\right) \\
\leq &\Pr_{\mathbf{b} \hookleftarrow \overline{\psi_t^n}}(\|\mathbf{b}\| > At) \\
\leq &\Pr_{\mathbf{v} \hookleftarrow \psi_1^n}\left(\frac{1}{1-\epsilon}\|\mathbf{v}\|^2 + \frac{n}{8t^2\epsilon} > A^2\right) \\
= &\Pr\left(\|\mathbf{v}\|^2 > n/2 + \sqrt{2nu} + 2u\right) \\
\leq &\exp(-u).
\end{aligned}$$

For the case $d > 2$, we have $\Theta_n(X) = X^n - 1$. Let $\mathbf{b} = \lfloor \mathbf{b}' \bmod \Phi_n(X) \rceil \in \mathcal{R}$ with $\mathbf{b}' \hookleftarrow \psi_t^n$. Let $(b_0, \cdots, b_{\varphi(n)-1})$ and $(b'_0, \cdots, b'_{n-1})$ be the coefficient vector of $\mathbf{b}$ and $\mathbf{b}'$ respectively. For any $k \in \{0, \cdots, \frac{n}{d} - 1\}$, the vector $\mathbf{b}'^{(k)} = \left(b'_k, b'_{k+\frac{n}{d}}, \cdots, b'_{k+\frac{n(d-1)}{d}}\right)$ can be viewed as a vector sampled from ψ_t^d and then the vector $\mathbf{b}^{(k)} = \left(b_k, b_{k+\frac{n}{d}}, \cdots, b_{k+\frac{n(d-2)}{d}}\right)$ is equivalent to a vector drawn from $\overline{\psi_t^d}$. Let $\mathbf{v} = \frac{1}{t}\left(\mathbf{b}'^{(0)} || \cdots || \mathbf{b}'^{(\frac{n}{d}-1)}\right) \in \mathcal{R}^n$. By Proposition 1, a straightforward computation leads to that

$$\|\mathbf{b}\|^2 = \sum_{k=0}^{\frac{n}{d}-1} \|\mathbf{b}^{(k)}\|^2 \leq \frac{t^2}{1-\epsilon}\|\mathbf{M}'\mathbf{v}\|^2 + \frac{n - \frac{n}{d}}{4\epsilon},$$

where $\mathbf{M}' = \mathbf{M} \otimes \mathbf{Id}_{\frac{n}{d}}$ and $\mathbf{M}$ is defined in Proposition 2. Let $\Sigma' = \mathbf{M}'^{\top}\mathbf{M}'$. We deduce from Proposition 2 that $\mathbf{tr}(\Sigma') = 2(n - \frac{n}{d})$, $\mathbf{tr}(\Sigma'^2) = (n - \frac{n}{d})(d+2)$

and $\|\Sigma'\| = d$. Then, by Proposition 3, we have

$$\Pr\left(\|\mathbf{M}'\mathbf{v}\|^2 > 2(n - \frac{n}{d}) + 2\sqrt{(n - \frac{n}{d})(d+2)u} + 2du\right) \leq \exp(-u).$$

Let

$$\epsilon = \left(1 + \sqrt{\frac{4t^2\left(2(n - \frac{n}{d}) + 2\sqrt{(n - \frac{n}{d})(d+2)u} + 2du\right)}{n - \frac{n}{d}}}\right)^{-1} \in (0, 1)$$

and

$$A = \sqrt{\frac{2(n - \frac{n}{d}) + 2\sqrt{(n - \frac{n}{d})(d+2)u} + 2du}{1 - \epsilon} + \frac{n - \frac{n}{d}}{4t^2\epsilon}}.$$

We can verify that

$$A = \sqrt{2(n - \frac{n}{d}) + 2\sqrt{(n - \frac{n}{d})(d+2)u} + 2du} + \sqrt{\frac{n - \frac{n}{d}}{4t^2}} < 2\sqrt{2n} + \sqrt{2du}$$

and then we have

$$\begin{aligned}
&\Pr_{\mathbf{b} \hookleftarrow \psi_t^n}\left(\|\mathbf{b}\| \geq \left(2\sqrt{2n} + \sqrt{2du}\right)t\right) \\
\leq &\Pr_{\mathbf{b} \hookleftarrow \psi_t^n}\left(\|\mathbf{b}\| > At\right) \\
\leq &\Pr_{\mathbf{v} \hookleftarrow \psi_1^n}\left(\frac{1}{1-\epsilon}\|\mathbf{M}'\mathbf{v}\|^2 + \frac{n - \frac{n}{d}}{4t^2\epsilon} > A^2\right) \\
= &\Pr\left(\|\mathbf{M}\mathbf{v}\|^2 > 2(n - \frac{n}{d}) + 2\sqrt{(n - \frac{n}{d})(d+2)u} + 2du\right) \\
\leq &\exp(-u).
\end{aligned}$$

Combining two above cases, we complete the proof. □

Let $u = \Theta(\log^{1+\kappa} n)$, together with Lemmata 18 and 9, we obtain a bound of the norms of pgs and pfe.

Lemma 20. *In* $\mathsf{pNE}(n, d, \nu, q, p, r, \alpha, k)$, $t = \sqrt{n'}\alpha q\left(\frac{\varphi(n)k}{\log(\varphi(n)k)}\right)^{1/4} > 1$ *where* $n' = \deg(\Theta_n(X))$. *Then for* $\kappa > 0$, *we have*

$$\|pgs\|_\infty, \|pfe\|_\infty \leq 12\sqrt{2}\varphi(n)\sqrt{n\varphi(n)}\Theta\left(\log^{\frac{1+\kappa}{2}} n\right)\|p\|^2 rt$$

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

$$\|pgs\|_\infty, \|pfe\|_\infty \leq 4\sqrt{2}\sqrt{n\varphi(n)}\Theta\left(\log^{\frac{1+\kappa}{2}} n\right)\|p\|^2 rt$$

with probability at least $1 - n^{-\Theta(\log^\kappa n)}$.

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* $\|fM\|_\infty \leq 6\varphi(n)^2\|p\|^2 r$ *with probability at least* $1 - 2^{-\varphi(n)+3}$*. In particular, if* $\deg p = 0$*, then* $\|fM\|_\infty \leq 2\varphi(n)\|p\|^2 r$ *with probability at least* $1 - 2^{-\varphi(n)+3}$*.*

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

Theorem 3. *Let* $t = \sqrt{n'}\alpha q \left(\frac{\varphi(n)k}{\log(\varphi(n)k)}\right)^{1/4} > 1$ *where* $n' = \deg(\Theta_n(X))$*. If* $\omega\left(\sqrt{\varphi(n)^3 n \log n}\right)\|p\|^2 rt/q < 1$ *(resp.* $\omega\left(\sqrt{\varphi(n) n \log n}\right)\|p\|^2 rt/q < 1$ *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 [39] 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* $\epsilon, \delta > 0$*,* $p \in \mathcal{R}_q^\times$ *and* $t = \sqrt{n'}\alpha q \left(\frac{\varphi(n)k}{\log(\varphi(n)k)}\right)^{1/4} > 1$ *where* $n' = \deg(\Theta_n(X))$*. Let* $r \geq \left\lceil \frac{d-1}{2} \right\rceil \sqrt{n\varphi(n)}\sqrt{\ln(8nq)} \cdot q^{\frac{1}{2}+\epsilon}$*. If there exists an* $\mathsf{IND\text{-}CPA}$ *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* $\psi = \overline{\psi_t^n}$ *that runs in time* $T' = T + O(kn)$ *and has success probability* $1/2 + \delta'$ *where* $\delta' = \delta/2 - q^{-\Omega(n)}$*.*

Combining Lemmata 22 with Theorem 3 and 1, we get the main result.

Theorem 4. *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* $q^{\frac{1}{2}-\epsilon} = \omega\left(dn^{3.75}\log^{1.5} n\|p\|^2\right)$ *(resp.* $q^{\frac{1}{2}-\epsilon} = \omega\left(dn^{2.75}\log^{1.5} n\|p\|^2\right)$*, if* $\deg p = 0$*) for any* $\epsilon \in (0, 1/2)$ *and* $p \in \mathcal{R}_q^\times$*. Let* $r = dn\sqrt{\ln(8nq)} \cdot q^{\frac{1}{2}+\epsilon}$ *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* $\mathsf{IND\text{-}CPA}$ *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 $\tilde{\Omega}(d^2 n^{5.5})$, and the minimal approximate factor γ is $\tilde{\Omega}(d^2 n^6)$. For the case $d = 2$, the smallest q and γ shown in [35] are $\tilde{\Omega}(n^5)$ and $\tilde{\Omega}(n^{5.5})$ respectively which are smaller than our results by a factor of $\sqrt{n}$. That is because we follow a different RLWE setting to work on more general cyclotomic rings.

5 Further Analysis

5.1 Prime vs Prime Power

In pNE scheme, the parameter r matters to the sizes of secret keys directly and a feasible value of r is $\tilde{\Omega}(dn \cdot q^{\frac{1}{2}+\epsilon})$ shown in Theorem 4. For two special cases, *i.e.* power-of-2 and prime cyclotomic rings, this value becomes $\tilde{\Omega}(n \cdot q^{\frac{1}{2}+\epsilon})$ and $\tilde{\Omega}(n^2 \cdot q^{\frac{1}{2}+\epsilon})$ respectively, which coincides with the results of [35] and [39] in the asymptotic sense.

To ensure successful decryption, a large r induces a large modulus q, which dominantly impacts the efficiency of pNE(see [5]). Notice that $n = d^\nu$ and then the polynomial factor dn can be written as $n^{1+\frac{1}{\nu}}$. Thus, assume n is of fixed bit length, the larger ν is, the relatively smaller dn is, and the more efficient pNE is. On the other hand, for large ν, the field $\mathbb{Q}(X)/\Phi_n(X)$ tends to have more subfields of proper relative degree, which may lead to a class of subfield attacks as shown in [1, 7]. Even though, for NTRU over any ring, a more efficient lattice attacks was proposed in a very recent paper [26], the presence of subfields is still considered as a worrisome algebraic structure. Overall, it seems a trade-off between the compactness of parameters and the robustness of ring structures.

5.2 pNE on Other Rings

Next we are to discuss what kinds of rings we can construct pNE over, under the assumed hardness of corresponding RLWE. Let $P(X) \in \mathbb{Z}[X]$ is a monic irreducible polynomial of degree n and $\mathcal{R} = \mathbb{Z}[X]/P(X)$. Let $\xi_1, \xi_2, \cdots, \xi_n$ be all complex roots of $P(X)$. Let $\smile$ and $\frown$ be a pair of inverse operations over $\mathcal{R}$ such that Lemma 7 and 10 holds. Let q be a prime such that $P(X)$ splits into k irreducible factors modulo q and each of degree $d = n/k$. Note that we require $k = n$ to ensure the security reduction from RLWE in our pNE and the case $k < n$ was discussed in [36]. We assume RLWE with error distribution χ over $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$ is hard. We define $\alpha(P), \beta(P), \gamma(P) > 0$ as follows:

- Let $\alpha(P) = \max_{t \in \mathcal{R}} \frac{\mathrm{T}_2(t)}{\|t\|}$ where $\mathrm{T}_2(t) = \sqrt{\sum_{i=1}^{n} |t(\xi_i)|^2}$.
- Let $\beta(P) = \min_{s \in \mathcal{R}, s \neq 0} \left\{ \max_{t \in \mathcal{R}} \frac{\|st^\smile\|_\infty}{\|t\|_\infty} \right\}$.
- Let $\gamma(P)$ be the expansion factor $\gamma_\times(\mathcal{R})$.

To make public key close to uniform, we can set $r = \tilde{\Omega}(\sqrt{n}\alpha(P)\beta(P) \cdot q^{0.5+2\epsilon})$. To ensure correct decryption, we can set $q = \tilde{\Omega}(\sqrt{n}\gamma(P)e(\chi)\|p\|^2 r)$, where p is set to be an integer and $e(\chi)$ is a threshold upper bound such that $\|e\| \leq e(\chi)$ with probability $\geq 1 - n^{\omega(1)}$, if $e \hookleftarrow \chi$. Combining these two conditions, to build a relative efficient pNE, we need to choose a polynomial $P(X)$ of small $\alpha(P), \beta(P)$ and $\gamma(P)$. In this sense, the ring $\mathbb{Z}[X]/(X^n - X - 1)$ suggested in [2] may be worth considering. Conversely, for some cyclotomic rings of highly composite order, the value $\gamma(P)$ can be super-polynomial of n and hence pNE over such rings is extremely impractical. We highlight again that above discussions are under the assumed hardness of RLWE over $\mathcal{R}$. A very recent paper [34] 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. This reduction applies to any fixed ring, but some RLWE instances may still be weak [14, 6]. Therefore, it is a priority to find a nice polynomial ring with solid RLWE hardness.

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] Bi, J., Cheng, Q.: Lower bounds of shortest vector lengths in random NTRU lattices. In: TAMC 2012. pp. 143–155 (2012)

[4] 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)

[5] Cabarcas, D., Weiden, P., Buchmann, J.: On the Efficiency of Provably Secure NTRU

[6] Castryck, W., Iliashenko, I., Vercauteren, F.: Provably weak instances of Ring-LWE revisited. In: EUROCRYPT 2016. pp. 147–167. Springer (2016)

[7] 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)

[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. p. To appear (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] Elias, Y., Lauter, K.E., Ozman, E., Stange, K.E.: Provably weak instances of Ring-LWE. In: CRYPTO 2015. pp. 63–92 (2015)

[15] Gama, N., Nguyen, P.Q.: New chosen-ciphertext attacks on NTRU. In: PKC 2007. pp. 89–106 (2007)

[16] Garg, S., Gentry, C., Halevi, S.: Candidate multilinear maps from ideal lattices. In: EUROCRYPT 2013. pp. 1–17 (2013)

[17] Gentry, C.: Key recovery and message attacks on NTRU-composite. In: EUROCRYPT 2001. pp. 182–194 (2001)

[18] Gentry, C.: Fully homomorphic encryption using ideal lattices. In: STOC 2009. pp. 169–178 (2009)
[19] Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: STOC 2008. pp. 197–206 (2008)
[20] Gentry, C., Szydlo, M.: Cryptanalysis of the revised NTRU signature scheme. In: EUROCRYPT 2002. pp. 299–320. Springer (2002)
[21] 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)
[22] Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A ring-based public key cryptosystem. In: ANTS 1998. pp. 267–288 (1998)
[23] Howgrave-Graham, N.: A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. In: CRYPTO 2007. pp. 150–169 (2007)
[24] Hsu, D., Kakade, S.M., Zhang, T.: A tail inequality for quadratic forms of subgaussian random vectors. Electronic Communications in Probability 17(25), 1–6 (2011)
[25] Jaulmes, E., Joux, A.: A chosen-ciphertext attack against NTRU. In: CRYPTO 2000. pp. 20–35 (2000)
[26] Kirchner, P., Fouque, P.A.: Revisiting lattice attacks on overstretched NTRU parameters. In: EUROCRYPT 2017. p. To appear (2017)
[27] Langlois, A., Stehlé, D., Steinfeld, R.: GGHLite: More efficient multilinear maps from ideal lattices. In: EUROCRYPT 2014. pp. 239–256 (2014)
[28] 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)
[29] Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: EUROCRYPT 2010. pp. 1–23 (2010)
[30] 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`
[31] Micciancio, D., Regev, O.: Worst-case to average-case reductions based on gaussian measures. SIAM Journal on Computing 37(1), 267–302 (2007)
[32] Nguyen, P.Q., Regev, O.: Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. In: EUROCRYPT 2006. pp. 271–288 (2006)
[33] Peikert, C.: Limits on the hardness of lattice problems in ℓ_p norms. Computational Complexity 17(2), 300–351 (2008)
[34] Peikert, C., Regev, O., Stephens-Davidowitz, N.: Pseudorandomness of Ring-LWE for any ring and modulus. In: STOC 2017. p. To appear (2017)
[35] Stehlé, D., Steinfeld, R.: Making NTRU as secure as worst-case problems over ideal lattices. In: EUROCRYPT 2011. pp. 27–47 (2011)
[36] 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`
[37] Szydlo, M.: Hypercubic lattice reduction and analysis of GGH and NTRU signatures. In: EUROCRYPT 2003. pp. 433–448 (2003)

[38] Xylouris, T.: On Linnik's constant (2009), http://arxiv.org/abs/0906.2749
[39] Yu, Y., Xu, G., Wang, X.: Provably secure NTRU instances over prime cyclotomic rings. In: PKC 2017. pp. 409–434 (2017)