Provably Secure NTRU Instances over Prime 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. Due to its remarkable performance and potential resistance to quantum attacks, NTRUEncrypt has drawn much attention recently; it also has been standardized by IEEE. However, classical NTRUEncrypt lacks a strong security guarantee and its security still relies on heuristic arguments. At Eurocrypt 2011, Stehlé and Steinfeld first proposed a variant of NTRUEncrypt with a security reduction from standard problems on ideal lattices. This variant is restricted to the family of rings $\mathbb{Z}[X]/(X^n+1)$ with n a power of 2 and its private keys are sampled by rejection from certain discrete Gaussian so that the public key is shown to be almost uniform. Despite the fact that partial operations, especially for RLWE, over $\mathbb{Z}[X]/(X^n+1)$ are simple and efficient, these rings are quite scarce and different from the classical NTRU setting. In this work, we consider a variant of NTRUEncrypt over prime cyclotomic rings, *i.e.* $\mathbb{Z}[X]/(X^{n-1}+\cdots+X+1)$ with n an odd prime, and obtain IND-CPA secure results in the standard model assuming the hardness of worst-case problems on ideal lattices. In our setting, the choice of the rings is much more flexible and the scheme is closer to the original NTRU, as $\mathbb{Z}[X]/(X^{n-1}+\cdots+X+1)$ is a large subring of the NTRU ring $\mathbb{Z}[X]/(X^n-1)$. Some tools for prime cyclotomic rings are also developed.

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

1 Introduction

The well-known public key system NTRU was created and refined by Hoffstein, Pipher and Silverman in [17, 18]. The NTRU encryption scheme, NTRUEncrypt,

[**] Corresponding Author.

is one of the fastest known lattice-based cryptosystems and regarded as an alternative to RSA and ECC due to its potential of countering attacks by quantum computers. The underlying problem of NTRUEncrypt has been used to design various cryptographic primitives including digital signatures [16], identity-based encryption [8] and multi-linear maps [11, 23]. In the course of assessing the security of NTRU, Coppersmith and Shamir first claimed in [5] that one can convert breaking NTRU to solving hard problems on the so-called NTRU lattice. Then an army of cryptanalyses [21, 12, 15, 34, 29, 10, 19, 2, 9, 1, 4, 22] have brought security estimations on NTRU and its variants, and NTRU is still considered secure in practice.

The *Learning With Errors* problem (LWE), introduced by Regev in 2005 [32], is shown to be as hard as certain lattice problems in the worst case. The *Ring Learning With Errors* problem (RLWE) is an algebraic variant of LWE, proposed by Lyubashevsky, Peikert and Regev [25], whose hardness is guaranteed by some hard problems over ideal lattices. Due to its better compactness and efficiency over LWE, RLWE has been used as the foundation of new cryptographic applications. In a celebrated paper [33], Stehlé and Steinfeld first modified NTRUEncrypt by incorporating RLWE and proved that the security of NTRU follows by a reduction from RLWE provided that a right set of parameters are used, which is the first sound theoretical base for the security of NTRU in the asymptotic sense. It is worth noting that several novel ideas and powerful techniques have been developed in [33]. One remarkable contribution is to show that, for n being a power of 2, and private keys f, g sampled according suitable conditions and parameters from the ring $\mathbb{Z}[X]/(X^n + 1)$, the public key $h = \frac{f}{g}$ is close to that uniformly sampled under the statistical distance. Based on the provably secure NTRU scheme, more interesting cryptographic primitives are achieved, such as fully homomorphic encryption [24, 3], proxy re-encryption [30].

In most known ring-based cryptosystems, the rings of the form $\mathbb{Z}[X]/(X^{2^m} + 1)$ are preferred choices. This family of rings has some nice algebraic features and various results on it have been already established. However, as these rings are very scarce, it has a limitation on the choice of the rings. It is noted that another family of rings, the prime cyclotomic rings of the form $\mathcal{R} = \mathbb{Z}[X]/(X^{n-1} + \cdots + X + 1)$ with n being a prime, is also of particular interest in many aspects, especially in the context of RLWE and NTRU. As a large subring, this ring is much closer to the original NTRU ring. It is also remarked that a class of subfield attacks [1] is proposed recently and affects the asymptotic security of NTRU for large moduli q. Note that the subfield attack is not applicable to the setting of [33], but it is still meaningful to consider NTRU over the fields with no subfields of desired relative degree. In this sense, prime cyclotomic ring seems a good choice of the potential to counter the subfield attack. Establishing IND-CPA (*indistinguishability under chosen-plaintext attack*) secure results with respect to this class of rings will be an important topic. Indeed, as stated in [33], the results for $\mathbb{Z}[X]/(X^{2^m} + 1)$ are likely to hold for more general cases including that for prime cyclotomic rings. However, to the best of our knowledge, there were no actual discussions on this issue found in literature.

Our Contribution The main purpose of this paper is to study the problem of provable security of NTRU in a modified setting with respect to prime cyclotomic rings. We show results similar to that of [33] still hold over prime cyclotomic rings. Consequently, to instantiate a provably secure NTRU, the density of usable cyclotomic polynomial degree $n < N$ is increased from $\Theta\left(\frac{\log N}{N}\right)$ to $\Theta\left(\frac{1}{\log N}\right)$. Even though some main ideas of [33] are applicable in our discussion, many technical differences also need to be taken care of. Furthermore, some new results on prime cyclotomic rings developed here might be of general interest. We believe that these results could be used to design more applications based on prime cyclotomic rings.

Organization We start in Section 2 with some notations and basic facts that will be useful to our discussion. We shall develop and prove a series of relevant results over prime cyclotomic rings in Section 3. Section 4 describes a modified $\mathsf{NTRUEncrypt}$ over prime cyclotomic rings and a reduction to its $\mathsf{IND\text{-}CPA}$ security from RLWE which has been proven hard under worst-case assumptions on ideal lattices. We conclude in Section 5. We have a couple of results whose proofs are similar to that in [33], these proofs are included in Appendices A, B and C for completeness.

2 Preliminaries

Lattice A lattice $\mathcal{L}$ is a discrete subgroup of $\mathbb{R}^m$ and represented by a basis, *i.e.* there is a set of linearly independent vectors $\mathbf{b}_1, \cdots, \mathbf{b}_n \in \mathbb{R}^m$ such that $\mathcal{L} = \{\sum_i x_i \mathbf{b}_i | x_i \in \mathbb{Z}\}$. The integer m is the dimension and the integer n is the rank of $\mathcal{L}$. A lattice is full-rank if its rank equals its dimension. 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 the lattice $\mathcal{L}$. More generally, the k-th minimum $\lambda_k(\mathcal{L})$ for $k \leq n$ is the smallest r such that there are at least k linearly independent vectors of $\mathcal{L}$ whose norms are not greater than r. Given a basis $\mathbf{B} = (\mathbf{b}_1, \cdots, \mathbf{b}_n)$ of a full-rank lattice $\mathcal{L}$, the set $\mathcal{P}(\mathbf{B}) = \{\sum_i c_i \mathbf{b}_i | c_i \in [0, 1)\}$ is the fundamental parallelepiped of $\mathbf{B}$ whose volume $|\det(\mathbf{B})|$ is an invariant of $\mathcal{L}$, called the volume of $\mathcal{L}$ and denoted by $\det(\mathcal{L})$. The dual lattice of $\mathcal{L}$ is the lattice $\widehat{\mathcal{L}} = \{\mathbf{c} \in \mathbb{R}^m | \forall i, \langle \mathbf{c}, \mathbf{b}_i \rangle \in \mathbb{Z}\}$ of the same dimension and rank with $\mathcal{L}$.

Given a ring $\mathcal{R}$ with an additive isomorphism θ mapping $\mathcal{R}$ to the lattice $\theta(\mathcal{R})$ in an inner product space and an ideal I of $\mathcal{R}$, we call the sublattice $\theta(I)$ an *ideal lattice*. Due to their smaller space requirement and faster operation speed, ideal lattices have been a popular choice for most lattice-based cryptosystems. More importantly, the hardness of classical lattice problems, SVP(*Shortest Vector Problem*) and γ-SVP(*Approximate Shortest Vector Problem with approximation factor* γ), does not seem to substantially decrease (except maybe very large approximate factors [6]). Thus, it is believed that the worst-case hardness of γ-SVP over ideal lattices, denoted by γ-Ideal-SVP, is against subexponential quantum attacks, for any $\gamma \le \mathrm{poly}(n)$.

Probability and Statistics Let D be a distribution over a discrete domain E. We write $z \hookleftarrow D$ to represent the random variable z that is sampled from the distribution D and denote by $D(x)$ the probability of z evaluates to $x \in E$. We denote by $U(E)$ 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 $\Delta(D_1; D_2) = \frac{1}{2}\sum_{x\in E}|D_1(x) - D_2(x)|$. Two distributions D_1, D_2 are said to be statistically close with respect to n if their statistical distance $\Delta(D_1; D_2) = o(n^{-c})$ for any constant $c > 0$.

Gaussian Measures We denote by $\rho_{r,\mathbf{c}}(\mathbf{x})$ the n-dimensional Gaussian function with center $\mathbf{c} \in \mathbb{R}^n$ and width r, *i.e.* $\rho_{r,\mathbf{c}}(\mathbf{x}) = \exp\left(-\frac{\pi\|\mathbf{x}-\mathbf{c}\|^2}{r^2}\right)$. When the center is $\mathbf{0}$, the Gaussian function is simply written as $\rho_r(\mathbf{x})$. Let S be a subset of $\mathbb{R}^n$, we denote by $\rho_{r,\mathbf{c}}(S)$ (resp. $\rho_r(S)$) the sum $\sum_{\mathbf{x}\in S}\rho_{r,\mathbf{c}}(\mathbf{x})$ (resp. $\sum_{\mathbf{x}\in S}\rho_r(\mathbf{x})$). Let $D_{\mathcal{L},r,\mathbf{c}}$ be the *discrete Gaussian distribution* over a lattice $\mathcal{L}$ with center $\mathbf{c}$ and width r, the probability of a vector $\mathbf{x} \in \mathcal{L}$ under this distribution is $D_{\mathcal{L},r,\mathbf{c}}(\mathbf{x}) = \frac{\rho_{r,\mathbf{c}}(\mathbf{x})}{\rho_{r,\mathbf{c}}(\mathcal{L})}$. For $\delta > 0$, the *smoothing parameter* $\eta_\delta(\mathcal{L})$ is the smallest $r > 0$ such that $\rho_{1/r}(\widehat{\mathcal{L}}) \le 1 + \delta$. The smoothing parameter is bounded in terms of some lattice quantities. The following lemmata will be useful in our discussion.

Lemma 1 ([28], Le. 3.3). *Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a full-rank lattice and $\delta \in (0, 1)$. Then $\eta_\delta(\mathcal{L}) \le \sqrt{\frac{\ln(2n(1+1/\delta))}{\pi}} \cdot \lambda_n(\mathcal{L})$.*

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

Lemma 3 ([28], 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 $r \ge \eta_\delta(\mathcal{L})$, we have $\Pr_{\mathbf{b}\hookleftarrow D_{\mathcal{L},r,\mathbf{c}}}(\|\mathbf{b} - \mathbf{c}\| \ge r\sqrt{n}) \le \frac{1+\delta}{1-\delta}2^{-n}$.*

Lemma 4 ([14], Cor. 2.8). *Let $\mathcal{L}' \subseteq \mathcal{L} \subseteq \mathbb{R}^n$ be full-rank lattices and $\delta \in (0, \frac{1}{2})$. For $\mathbf{c} \in \mathbb{R}^n$ 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 ([14], 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.*

Furthermore, we denote by ψ_r the Gaussian distribution with mean 0 and width r over $\mathbb{R}$ and by ψ_r^n the *spherical Gaussian distribution* over $\mathbb{R}^n$ of the vector $(v_1, \cdots, v_n)$ in which each v_i is drawn from ψ_r independently. In this paper, we shall restrict ψ_r over $\mathbb{Q}$ rather than $\mathbb{R}$. As explained in [7], this will only lead to a negligible impact on our results.

Cyclotomic Ring Let ξ_n be a primitive n-th complex root of unity and $\Phi_n(X)$ the n-th cyclotomic polynomial. It is known that $\Phi_n(X) \in \mathbb{Z}[X]$ and is of degree $\varphi(n)$, the totient of n. All roots of $\Phi_n(X)$ form the set $\{\xi_n^i | i \in \mathbb{Z}_n^*\}$. In this paper, we will be working with a cyclotomic ring of the form $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. For any prime n, if a prime q satisfies $q = 1 \bmod n$, then $\Phi_n(X)$ splits into $n-1$ distinct linear factors modulo q. Given n, the existence of infinite such primes is guaranteed by Dirichlet's theorem on arithmetic progressions. Furthermore, by Linnik's theorem, the smallest such q can be bounded by $\operatorname{poly}(n)$ (a more precise bound $O(n^{5.2})$ has been proven in [36]). Another important class of rings involved in our discussion is the family of rings of the form $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. As indicated earlier, our main focus will be *prime cyclotomic rings*, *i.e.* those rings associate with polynomials $\Phi_n(X) = X^{n-1} + X^{n-2} + \cdots + 1$ with n a prime.

Given a positive integer n, we define the polynomial $\Theta_n(X)$ to be $X^n - 1$ if n is odd, and $X^{\frac{n}{2}} + 1$ if n is even. It is easy to see that there is a natural ring extension $\mathcal{R}' = \mathbb{Z}[X]/\Theta_n(X)$ of the cyclotomic ring $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. In particular, when $n > 1$ is a power of 2, $\mathcal{R} = \mathcal{R}'$; when n is a prime, the relation $\Theta_n(X) = \Phi_n(X) \cdot (X-1)$ implies a ring isomorphism $\mathcal{R}' \simeq \mathcal{R} \times \mathbb{Z}$ by the Chinese Remainder Theorem.

Hardness of RLWE The "pure" Ring Learning With Errors problem (RLWE) introduced in [25] involves the dual of the ring. For the ring $\mathbb{Z}[X]/(X^{2^m}+1)$, its dual is just a scaling of itself. Therefore, many RLWE instances are established over such rings to avoid dual. In [7], Ducas and Durmus proposed an "easy-to-use" RLWE setting and instantiated RLWE over prime cyclotomic rings. In this paper, we follow the setting of [7].

Definition 1 (RLWE error distribution in [7]). *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 [7]). *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 $1/\operatorname{poly}(n)$.*

The following theorem indicates that RLWE under the above settings is hard based on the worst-case hardness of γ-Ideal-SVP. The ideal lattices we discuss here are with respect to the so-called *canonical embedding*, *i.e.* $\theta(f) = (f(\xi_n^i))_{i \in \mathbb{Z}_n^*}$.

Theorem 1 ([7], Th. 2). *Let n be an odd prime, and let $\mathcal{R}_q$ be the ring $\mathbb{Z}_q[X]/\Phi_n(X)$ where q is a prime congruent to 1 modulo $2n$. 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 $t = \sqrt{n}\alpha q \left(\frac{(n-1)k}{\log((n-1)k)}\right)^{1/4}$ (with $\gamma = \tilde{O}\left(\frac{\sqrt{n}}{\alpha}\right)$) that runs in time $O(q \cdot \mathrm{poly}(n))$.*

Let $\mathcal{R}_q^\times$ be the set of all invertible elements of $\mathcal{R}_q$. By restricting $A_{s,\psi}$ to $\mathcal{R}_q^\times \times \mathcal{R}_q$, we obtain a modified RLWE distribution and denote it by $A_{s,\psi}^\times$. Replacing $A_{s,\psi}$ and $U(\mathcal{R}_q \times \mathcal{R}_q)$ by $A_{s,\psi}^\times$ and $U(\mathcal{R}_q^\times \times \mathcal{R}_q)$ respectively, we get a variant of RLWE which is denoted by $\mathsf{RLWE}^\times$. When $q = \Omega(n)$, the invertible elements account for a non-negligible fraction in the $\mathcal{R}_q$. Thus $\mathsf{RLWE}^\times$ remains hard. Furthermore, as explained in [33], the nonce s in $A_{s,\psi}^\times$ can be sampled from ψ without incurring security loss. We denote by $\mathsf{RLWE}_{HNF}^\times$ this variant of $\mathsf{RLWE}^\times$.

3 New Results on Prime Cyclotomic Rings

In this section, we will report on a series of results on prime cyclotomic rings. Some of the results are adapted from corresponding conclusions in [33], but the modifications are not trivial considering the differences between the cyclotomic rings of prime and a power of 2 orders. Firstly, we present several notations and basic properties aiming at prime cyclotomic rings.

3.1 Notations and Properties

Let n be a prime and $\mathcal{R}$ be the ring $\mathbb{Z}[X]/\Phi_n(X) = \mathbb{Z}[X]/(X^{n-1} + \cdots + 1)$. For any $f \in \mathcal{R}$, we call a vector $(f_0, \cdots, f_{n-2}) \in \mathbb{Z}^{n-1}$ the coefficient vector of f if $f = \sum_{i=0}^{n-2} f_i X^i$. For any $\mathbf{s} = (s_1, \cdots, s_m) \in \mathcal{R}^m$, we view $\mathbf{s}$ as a $m(n-1)$-dimensional vector in $\mathbb{Z}^{m(n-1)}$ by coefficient embedding. Given $\mathbf{s}, \mathbf{t} \in \mathcal{R}^m$, their Euclidean inner product is denoted by $\langle \mathbf{s}, \mathbf{t} \rangle$. To get a clean expression of $\langle \mathbf{s}, \mathbf{t} \rangle$ as a coefficient of a polynomial related to $\mathbf{s}$ and $\mathbf{t}$, we introduce two operations on $f \in \mathcal{R}$ as follows.

Let $f \in \mathcal{R}$ of coefficient vector $(f_0, \cdots, f_{n-2})$, we define $f^\smile$ to be the polynomial $\sum_{i=0}^{n-2} (\sum_{j=i}^{n-2} f_j) X^i$ and $f^\frown$ the polynomial $\sum_{i=0}^{n-3} (f_i - f_{i+1}) X^i + f_{n-2} X^{n-2}$, respectively. One important consequence is that, regarding $\smile$ and $\frown$ as two functions over $\mathcal{R}$, these operations are inverse to each other, namely

Proposition 1. *Let n be a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$, then*

$$\forall f \in \mathcal{R}, (f^\smile)^\frown = (f^\frown)^\smile = f.$$

Proof. Let $(g_0, \cdots, g_{n-2})$ and $(h_0, \cdots, h_{n-2})$ be the coefficient vectors of the polynomials $f^\smile$ and $f^\frown$ respectively. According to the definitions of these two operations, we have

$$g_i = \sum_{j=i}^{n-2} f_j \text{ for } i \in \{0, \cdots, n-2\}$$

and

$$h_i = f_i - f_{i+1} \text{ for } i < n-2 \quad \text{and} \quad h_{n-2} = f_{n-2}.$$

Then, a straightforward computation leads to that

$$g_i - g_{i+1} = f_i \text{ for } i < n-2 \quad \text{and} \quad g_{n-2} = f_{n-2}$$

and

$$\sum_{j=i}^{n-2} h_j = f_i \text{ for } i \in \{0, \cdots, n-2\}.$$

Thus we conclude that $g^{\frown} = h^{\smile} = f$, *i.e.* $(f^{\smile})^{\frown} = (f^{\frown})^{\smile} = f$. □

The following lemma manifests an expression of the Euclidean inner product of two elements in $\mathcal{R}$.

Lemma 6. *Let n be 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 $(f_0, \cdots, f_{n-2})$ and $g \in \mathcal{R}$ of coefficient vector $(g_0, \cdots, g_{n-2})$. Then*

$$\sum_{i=0}^{n-2} f_i g_i = \textit{the constant coefficient of the polynomial } f(X)g^{\smile}(X^{-1}).$$

Proof. Let $(g'_0, \cdots, g'_{n-2})$ be the coefficient vector of the polynomial $g^{\smile}$. Notice that the term X^n is equivalent to the identity element of $\mathcal{R}$. Hence X^{-1} is equivalent to X^{n-1} when it comes to the algebraic computations over $\mathcal{R}$. Then we have

$$f(X)g^{\smile}(X^{-1}) = f(X)g^{\smile}(X^{n-1}) = \sum_{i,j \in \{0,\cdots,n-2\}} f_i g'_j X^{i+(n-1)j}.$$

The constant coefficient of $f(X)g^{\smile}(X^{-1})$ is only contributed by the term $X^{i+(n-1)j}$ with $i+(n-1)j = 0, n-1 \bmod n$, *i.e.* $i = j$ or $j-1$. Note that $X^{n-1} = -(X^{n-2} + \cdots + 1)$, thus the constant coefficient of $f(X)g^{\smile}(X^{-1})$ equals $\sum_{i=0}^{n-2} f_i g'_i - \sum_{i=0}^{n-3} f_i g'_{i+1} = \sum_{i=0}^{n-3} f_i(g'_i - g'_{i+1}) + f_{n-2}g'_{n-2}$. The terms $\{g'_i - g'_{i+1}\}_{i=0}^{n-3}$ and g'_{n-2} are the coefficients of the polynomial $(g^{\smile})^{\frown} = g$. Consequently, the constant coefficient of $f(X)g^{\smile}(X^{-1})$ equals $\sum_{i=0}^{n-2} f_i g_i$. □

Corollary 1. *Let n be 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*

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

Remark For the ring $\mathbb{Z}[X]/(X^n+1)$, the Euclidean inner product of any two elements f and g equals the constant coefficient of the polynomial $f(X)g(X^{-1})$, which is simpler than the case in our discussion. The rather involved expression of Euclidean inner product contributes to a sequence of technical differences compared to that in [33].

Now we introduce several norms and demonstrate some relations among them. For any $t \in \mathcal{R}$, we define its T_2-*norm* by $\mathrm{T}_2(t)^2 = \sum_{i=1}^{n-1} |t(\xi_n^i)|^2$ and its *algebraic norm* by $\mathrm{N}(t) = \prod_{i=1}^{n-1} |t(\xi_n^i)|$. Also we define the *polynomial norm* $\|t\|$ by the Euclidean norm of the coefficient vector of t.

Lemma 7. *Let n be a prime and $\mathcal{R} = \mathbb{Z}[X]/\varPhi_n(X)$. For any $t \in \mathcal{R}$, we have*

$$\mathrm{N}(t)^{\frac{2}{n-1}} \leq \frac{1}{n-1}\mathrm{T}_2(t)^2 \quad \textit{and} \quad \|t\|^2 = \frac{\mathrm{T}_2(t)^2 + t(1)^2}{n} \geq \frac{\mathrm{T}_2(t)^2}{n}.$$

Proof. The first inequality can be proven directly by arithmetic-geometric inequality. Since $\|t\|^2 = \frac{\sum_{i=0}^{n-1} |t(\xi_n^i)|^2}{n} = \frac{\mathrm{T}_2(t)^2 + t(1)^2}{n}$ is the Parseval's identity [35], the second one follows immediately, as $t(1)^2 \geq 0$. □

Moreover, we present the following result to illustrate that the product of two polynomials in $\mathcal{R}$ is of well-bounded norm.

Lemma 8. *Let n be a prime and $\mathcal{R} = \mathbb{Z}[X]/\varPhi_n(X)$. For any $f, g \in \mathcal{R}$, we have*

$$\|fg\|_\infty \leq 2\|f\|\|g\| \quad \textit{and} \quad \|fg\| \leq 2\sqrt{n-1}\|f\|\|g\|.$$

Proof. Let $\mathcal{R}' = \mathbb{Z}[X]/(X^n - 1)$ and $f', g' \in \mathcal{R}'$ be the polynomials with the same coefficients as f, g respectively, *i.e.* the coefficients of X^{n-1} are 0. Let $h' = \sum_{i=0}^{n-1} h'_i X^i$ be the product of f' and g' in $\mathcal{R}'$ where $h'_i \in \mathbb{Z}$ for $i \in \{0, \cdots, n-1\}$. Let $h = f \cdot g \in \mathcal{R}$. Notice that $\varPhi_n(X)$ is a factor of $X^n - 1$, hence we know that $h' \bmod \varPhi_n(X) = h \in \mathcal{R}$, *i.e.* $h = h' \bmod \varPhi_n(X) = \sum_{i=0}^{n-2}(h'_i - h'_{n-1})X^i$.

Let $(f_0, \cdots, f_{n-2})$ and $(g_0, \cdots, g_{n-2})$ be the coefficient vectors of f and g. We also set $f_{n-1} = g_{n-1} = 0$. For any $i \in \{0, \cdots, n-1\}$, we have $h'_i = \sum_{j=0}^{n-1} f_j g_{(i-j) \bmod n}$. By Cauchy-Schwarz inequality, we know that $|h'_i| \leq \|f\|\|g\|$. Therefore

$$\|h\|_\infty = \max_{0 \leq i \leq n-2} |h'_i - h'_{n-1}| \leq \max_{0 \leq i \leq n-2} (|h'_i| + |h'_{n-1}|) \leq 2\|f\|\|g\|.$$

By equivalence of norms, we conclude that $\|h\| \leq \sqrt{n-1}\|h\|_\infty \leq 2\sqrt{n-1}\|f\|\|g\|$. □

Remark The second inequality indicates that an upper bound of the multiplicative expansion factor of $\mathcal{R}$, which is $\gamma_\times(\mathcal{R}) = \max_{f,g \in \mathcal{R}} \frac{\|fg\|}{\|f\|\|g\|}$, is $2\sqrt{n-1}$. This is comparable to that of power-of-2 cyclotomic rings in the asymptotic sense, as the expansion factor of the ring $\mathbb{Z}[X]/(X^n+1)$ is exactly $\sqrt{n}$ (see [13]).

3.2 Duality Results for Module Lattices

In [33], Stehlé and Steinfeld reveals a nice duality between two module lattices for the n-th cyclotomic ring with n a power of 2. However, that duality cannot be simply generalized to the case of prime cyclotomic rings. Next, we will propose a new duality relationship between two module lattices for a prime cyclotomic ring.

To begin with, we introduce a few families of $\mathcal{R}$-modules. Let q be a prime such that $\Phi_n(X)$ splits into $n-1$ distinct linear factors modulo q and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. We denote by $\{\phi_i\}_{i=1,\cdots,n-1}$ all roots of $\Phi_n(X)$ modulo q. Note that if ϕ is a root of $\Phi_n(X)$ modulo q, then so is $\phi^{-1} \bmod q$. By the Chinese Remainder Theorem, we see that

$$\mathcal{R}_q \simeq \mathbb{Z}_q[X]/(X-\phi_1) \times \cdots \times \mathbb{Z}_q[X]/(X-\phi_{n-1}) \simeq (\mathbb{Z}_q)^{n-1}.$$

From this, we see that each ideal of $\mathcal{R}_q$ is of the form $\prod_{i\in S}(X-\phi_i)\cdot\mathcal{R}_q$ with $S \subseteq \{1,\cdots,n-1\}$, and we denote it by I_S. Let $\mathcal{R}_q^\times$ be the set of all invertible elements of $\mathcal{R}_q$. Given $\mathbf{a} \in \mathcal{R}_q^m$, we define two $\mathcal{R}$-modules $\mathbf{a}^\perp(I_S)$ and $\mathcal{L}(\mathbf{a}, I_S)$ in exactly the same manner as in [33]:

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

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

Then we can define a new $\mathcal{R}$-module $\mathcal{L}^\frown(\mathbf{a}, I_S)$ to be

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

Module lattices $\mathbf{a}^\perp(I_S)$ and $\mathcal{L}^\frown(\mathbf{a}, I_S)$ can be related by duality argument. More precisely,

Lemma 9. *Let n be a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. Let q be a prime such that $\Phi_n(X)$ splits into $n-1$ distinct linear factors modulo q and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Given $S \subseteq \{1,\cdots,n-1\}$ 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 (considering both sets as $m(n-1)$-dimensional lattices by identifying $\mathcal{R}$ with $\mathbb{Z}^{n-1}$)*

$$\widehat{\mathbf{a}^\perp(I_S)} = \frac{1}{q}\mathcal{L}^\frown(\mathbf{a}^\times, I_{\bar{S}}^\times).$$

Proof. Firstly, we prove that $\frac{1}{q}\mathcal{L}^\frown(\mathbf{a}^\times, I_{\bar{S}}^\times) \subseteq \widehat{\mathbf{a}^\perp(I_S)}$. For any $\mathbf{t} = (t_1,\cdots,t_m) \in \mathbf{a}^\perp(I_S)$ and $\mathbf{t}' = (t_1',\cdots,t_m') \in \mathcal{L}^\frown(\mathbf{a}^\times, I_{\bar{S}}^\times)$, Corollary 1 says that their inner product $\langle\mathbf{t},\mathbf{t}'\rangle$ equals the constant coefficient of the polynomial $\sum_{i=1}^m t_i(X)t_i'^\smile(X^{-1})$. According to the definition of $\mathcal{L}^\frown(\mathbf{a}^\times, I_{\bar{S}}^\times)$ and Proposition 1, there exists $s\in\mathcal{R}_q$ such that $(t_i'^\smile \bmod q) = a_i^\times\cdot s + b_i'$ for some $b_i' \in I_{\bar{S}}^\times$. Then we get

$$\sum_{i=1}^m t_i(X)t_i'^\smile(X^{-1}) = s(X^{-1})\cdot\sum_{i=1}^m t_i(X)a_i(X) + \sum_{i=1}^m t_i(X)b_i'(X^{-1}) \bmod q$$

Both two sums in the right hand side evaluate to 0 in $\mathcal{R}_q$, which means that $\langle \mathbf{t}, \mathbf{t}' \rangle = 0 \bmod q$. Therefore, we finish the proof of this part.

Secondly, it suffices to prove that $\widehat{\mathcal{L}^{\frown}(\mathbf{a}^{\times}, I_{\bar{S}}^{\times})} \subseteq \frac{1}{q}\mathbf{a}^{\perp}(I_S)$. For any $\mathbf{t} \in \mathcal{L}^{\frown}(\mathbf{a}^{\times}, I_{\bar{S}}^{\times})$ and $\mathbf{t}' \in \widehat{\mathcal{L}^{\frown}(\mathbf{a}^{\times}, I_{\bar{S}}^{\times})}$, the constant coefficient of $\sum_{i=1}^{m} t_i'(X) t_i^{\smile}(X^{-1}) = \langle \mathbf{t}', \mathbf{t} \rangle$ is an integer due to duality. Notice that if $(t_1, \cdots, t_m) \in \mathcal{L}^{\frown}(\mathbf{a}^{\times}, I_{\bar{S}}^{\times})$, then $\left((t_1^{\smile} \cdot X^k)^{\frown}, \cdots, (t_m^{\smile} \cdot X^k)^{\frown}\right) \in \mathcal{L}^{\frown}(\mathbf{a}^{\times}, I_{\bar{S}}^{\times})$. Thus, for $k \in \{1, \cdots, n-2\}$, the constant coefficient of $\sum_{i=1}^{m} t_i'(X) t_i^{\smile}(X^{-1}) X^{-k}$ is also an integer, which implies that all coefficients of $\sum_{i=1}^{m} t_i'(X) t_i^{\smile}(X^{-1})$ are integers. For any $(t_1, \cdots, t_m) \in \widehat{\mathcal{L}^{\frown}(\mathbf{a}^{\times}, I_{\bar{S}}^{\times})}$, we deduce from the fact $(q^{\frown}, 0, \cdots, 0) \in \mathcal{L}^{\frown}(\mathbf{a}^{\times}, I_{\bar{S}}^{\times})$ that $qt_1 \in \mathbb{Z}^{n-1}$. Let $\nu_{I_{\bar{S}}^{\times}}$ be the polynomial $\prod_{i \in \bar{S}}(X - \phi_i^{-1})$. Since $\left(\nu_{I_{\bar{S}}^{\times}}^{\frown}, 0, \cdots, 0\right) \in \mathcal{L}^{\frown}(\mathbf{a}^{\times}, I_{\bar{S}}^{\times})$, we obtain $qt_1(X) \cdot \nu_{I_{\bar{S}}^{\times}}(X^{-1}) = 0 \bmod \mathcal{R}_q$, that means $(qt_1 \bmod q) \in I_S$. For the same reason, we have $(qt_i \bmod q) \in I_S$ for any $i \in \{1, \cdots, m\}$. If we set $s = 1$, then $(a_1^{\times\frown}, \cdots, a_m^{\times\frown}) \in \mathcal{L}^{\frown}(\mathbf{a}^{\times}, I_{\bar{S}}^{\times})$. It shows that the polynomial $\sum_{i=1}^{m} (qt_i(X) a_i(X)) = q \sum_{i=1}^{m} \left(t_i(X) a_i^{\times}(X^{-1})\right) = 0 \bmod q$. Combining the fact that $(qt_i \bmod q) \in I_S$, we conclude that $q(t_1, \cdots, t_m) \in \mathbf{a}^{\perp}(I_S)$. The proof is completed. □

Remark The above result on the duality is different from that proven in [33], because the inner product has a more involved form. The original ideas of [33] have been exploited here, but we also add more details to treat technical differences.

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

We now show that for $\mathbf{a} \hookleftarrow \mathbf{U}((\mathcal{R}_q^{\times})^m)$, the first minimum of $\mathcal{L}^{\frown}(\mathbf{a}, I_S)$ for the ℓ_∞ norm is overwhelming unlikely unusually small. First we observe that the lattice $\mathcal{L}^{\frown}(\mathbf{a}, I_S)$ is transformed from the lattice $\mathcal{L}(\mathbf{a}, I_S)$. To describe the transformation, we define a matrix $\mathbf{H} \in \mathbb{Z}^{m(n-1) \times m(n-1)}$ as

$$\mathbf{H} = \begin{pmatrix} 1 & & & & \\ -1 & 1 & & & \\ & -1 & \ddots & & \\ & & \ddots & 1 & \\ & & & -1 & 1 \end{pmatrix} \otimes \mathbf{Id}_m,$$

where $\mathbf{Id}_m$ is an m-dimensional identity matrix. Let $\mathbf{B} \in \mathbb{Z}^{m(n-1) \times m(n-1)}$ be a basis of $\mathcal{L}(\mathbf{a}, I_S)$ whose rows correspond to the basis vectors, then $\mathbf{B}' = \mathbf{B} \cdot \mathbf{H}$ is a basis of $\mathcal{L}^{\frown}(\mathbf{a}, I_S)$. It is thus easy to see that $\mathcal{L}^{\frown}(\mathbf{a}, I_S)$ and $\mathcal{L}(\mathbf{a}, I_S)$ are of the same volume, *i.e.* $\det\left(\mathcal{L}^{\frown}(\mathbf{a}, I_S)\right) = \det\left(\mathcal{L}(\mathbf{a}, I_S)\right) = q^{(m-1)|S|}$. This is because there are $q^{m(n-1-|S|)+|S|}$ points of $\mathcal{L}(\mathbf{a}, I_S)$ in the cube $[0, q-1]^{m(n-1)}$. Also, the first minimums of these two lattices may not have a significant difference. Hence we first present a result on $\mathcal{L}(\mathbf{a}, I_S)$ which is a variant on prime cyclotomic rings of Lemma 8 in [33].

Lemma 10. *Let $n \geq 7$ be a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. Let q be a prime such that $\Phi_n(X)$ splits into $n-1$ distinct linear factors modulo q and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. For any $S \subseteq \{1, \cdots, n-1\}$, $m \geq 2$ and $\epsilon > 0$, set*

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

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

Remark The above lemma can be shown by following the original idea but with some slight modifications on the inequalities for different norms in prime cyclotomic rings. For completeness, we give a proof in Appendix A. It is also noted that our statement of the lemma is essentially the same as that in Lemma 8 of [33], this is primarily because there is a simple relation for the Euclidean and algebraic norms in both prime and power-of-2 cyclotomic rings.

Next, we shall show that the first minimum $\lambda_1^{\infty}(\mathcal{L}(\mathbf{a}, I_S))$ is at most $\frac{n}{2}$ times that of $\mathcal{L}^{\frown}(\mathbf{a}, I_S)$.

Lemma 11. *Let $n \geq 7$ be a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. Let q be a prime such that $\Phi_n(X)$ splits into $n-1$ distinct linear factors modulo q and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Then, for any $\mathbf{a} \in (\mathcal{R}_q^{\times})^m$ and $S \subseteq \{1, \cdots, n-1\}$, we have*

$$\lambda_1^{\infty}(\mathcal{L}(\mathbf{a}, I_S)) \leq \frac{n-1}{2} \lambda_1^{\infty}(\mathcal{L}^{\frown}(\mathbf{a}, I_S)).$$

Proof. We first show that $\|X^{\frac{n-1}{2}} t^{\smile}\|_{\infty} \leq \frac{n-1}{2}\|t\|_{\infty}$ for any $t \in \mathcal{R}$. Let $(t_0, \cdots, t_{n-2})$ be the coefficient vector of t. We denote by $(t_0^{\smile}, \cdots, t_{n-2}^{\smile})$ and $(t'_0, \cdots, t'_{n-2})$ the coefficient vectors of the polynomials $t^{\smile}$ and $X^{\frac{n-1}{2}} t^{\smile}$, then:

$$t'_i = \begin{cases} t^{\smile}_{\frac{n+1}{2}+i} - t^{\smile}_{\frac{n-1}{2}}, & i < \frac{n-3}{2} \\ -t^{\smile}_{\frac{n-1}{2}}, & i = \frac{n-3}{2} \\ t^{\smile}_{i-\frac{n-1}{2}} - t^{\smile}_{\frac{n-1}{2}}, & i > \frac{n-3}{2} \end{cases}.$$

From $t_i^{\smile} = \sum_{j=i}^{n-2} t_j$, we get

$$t'_i = \begin{cases} -\sum_{j=\frac{n-1}{2}}^{\frac{n-1}{2}+i} t_j, & i < \frac{n-3}{2} \\ -\sum_{j=\frac{n-1}{2}}^{n-2} t_j, & i = \frac{n-3}{2} \\ \sum_{j=i-\frac{n-1}{2}}^{\frac{n-3}{2}} t_j, & i > \frac{n-3}{2} \end{cases}.$$

Notice that each t'_i is a sum of consecutive t_j's of length at most $\frac{n-1}{2}$, thus $\|X^{\frac{n-1}{2}} t^{\smile}\|_{\infty} = \max_i |t'_i| \leq \frac{n-1}{2} \max_i |t_i| = \frac{n-1}{2}\|t\|_{\infty}$ holds.

For any $\mathbf{s} = (s_1, \cdots, s_m) \in \mathcal{L}^\frown(\mathbf{a}, I_S)$, the vector $\mathbf{s}^\smile = (s_1^\smile, \cdots, s_m^\smile)$ belongs to $\mathcal{L}(\mathbf{a}, I_S)$ and thus the vector $\mathbf{s}' = \left(X^{\frac{n-1}{2}} s_1^\smile, \cdots, X^{\frac{n-1}{2}} s_m^\smile\right)$ is also in $\mathcal{L}(\mathbf{a}, I_S)$. Then

$$\|\mathbf{s}'\|_\infty = \max_i \|X^{\frac{n-1}{2}} s_i^\smile\|_\infty \leq \frac{n-1}{2} \max_i \|s_i\|_\infty = \frac{n-1}{2} \|\mathbf{s}\|_\infty.$$

Since there exists a unique $\mathbf{s} \in \mathcal{L}(\mathbf{a}, I_S)$ such that $\mathbf{r} = \mathbf{s}^\frown$ for any $\mathbf{r} \in \mathcal{L}^\frown(\mathbf{a}, I_S)$, we conclude that $\lambda_1^\infty(\mathcal{L}(\mathbf{a}, I_S)) \leq \frac{n-1}{2} \lambda_1^\infty(\mathcal{L}^\frown(\mathbf{a}, I_S))$. □

Lemmata 10 and 11 lead to the following result on $\mathcal{L}^\frown(\mathbf{a}, I_S)$ immediately.

Lemma 12. *Let $n \geq 7$ be a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. Let q be a prime such that $\Phi_n(X)$ splits into $n-1$ distinct linear factors modulo q and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. For any $S \subseteq \{1, \cdots, n-1\}$, $m \geq 2$ and $\epsilon > 0$, set*

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

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

3.4 Results on Regularity

Let $\mathbb{D}_\chi$ be the distribution of the tuple $(a_1, \cdots, a_m, \sum_{i=1}^m t_i a_i) \in (\mathcal{R}_q^\times)^m \times \mathcal{R}_q$ with a_i's being independent and uniformly random in $\mathcal{R}_q^\times$ and t_i's being sampled from the distribution χ over $\mathcal{R}_q$. We call the statistical distance between $\mathbb{D}_\chi$ and the uniform distribution over $(\mathcal{R}_q^\times)^m \times \mathcal{R}_q$ the *regularity* of the generalized knapsack function $(t_1, \cdots, t_m) \mapsto \sum_{i=1}^m t_i a_i$. In [27], Micciancio gave some results on regularity for general finite rings and constructed a class of one-way functions. In [33], an improved result was claimed for the ring $\mathbb{Z}[X]/(X^n + 1)$ with n a power of 2 and a Gaussian distribution χ.

We can derive the result of the regularity for prime cyclotomic rings. It provides a foundation of security for more cryptographic primitives based on prime cyclotomic rings. In the later part, we will concentrate on NTRU applications corresponding to the case $m = 2$.

Lemma 13. *Let $n \geq 7$ be a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. Let q be a prime such that $\Phi_n(X)$ splits into $n-1$ distinct linear factors modulo q and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Let $S \subseteq \{1, \cdots, n-1\}$, $m \geq 2, \epsilon > 0, \delta \in (0, \frac{1}{2})$, $\mathbf{c} \in \mathbb{R}^{m(n-1)}$ and $\mathbf{t} \hookleftarrow D_{\mathbb{Z}^{m(n-1)}, r, \mathbf{c}}$, with $r \geq \frac{n-1}{2}\sqrt{\frac{n \ln(2m(n-1)(1+1/\delta))}{\pi}} \cdot q^{\frac{1}{m} + (m-1)\frac{|S|}{n-1} + \epsilon}$. Then for all except a fraction $\leq \frac{2^{n-1}}{(q-1)^{\epsilon(n-1)}}$ of $\mathbf{a} \in (\mathcal{R}_q^\times)^m$, we have*

$$\varDelta\left(\mathbf{t} \bmod \mathbf{a}^\perp(I_S); U(\mathbb{Z}^{m(n-1)}/\mathbf{a}^\perp(I_S))\right) \leq 2\delta.$$

In particular, for all except a fraction $\leq 2^{n-1}(q-1)^{-\epsilon(n-1)}$ *of* $\mathbf{a} \in (\mathcal{R}_q^\times)^m$*, we have*

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

Proof. By combining Lemmata 2, 4, 9 and 12, the first part follows. For $\mathbf{a} \in (\mathcal{R}_q^\times)^m$, the lattice $\mathbf{a}^\perp(I_S)$ is of the volume $\det\left(\mathbf{a}^\perp(I_S)\right) = \det\left(\frac{1}{q}\mathcal{L}^\frown(\mathbf{a}^\times, I_{\bar{S}}^\times)\right)^{-1} = q^{m(n-1)}/q^{(m-1)(n-1-|S|)} = q^{n-1+(m-1)|S|}$. Notice that $|\mathbb{Z}^{m(n-1)}/\mathbf{a}^\perp(I_S)| = \det\left(\mathbf{a}^\perp(I_S)\right)$, thus we complete the proof of the second part. □

Remark Our regularity result is under the coefficient embedding. We have also considered the canonical embedding and generalized some results of [26]. In the latter case, for $\delta = q^{-\epsilon n}$ with $\epsilon \in (0,1)$, the polynomial factor of the lower bound of required width gets reduced to $O(n^{1.5})$ from $O(n^2)$ in Lemma 13 and the power exponent can also be slightly smaller. However, our key result, which is Theorem 2 in next section, requires the parameter δ in Lemma 13 to be very small. Under the canonical embedding and with $\delta = q^{-n-\epsilon n}$, a desired result similar to the lemma is not currently available. Thus we only work with the coefficient embedding in this paper and leave the relevant results for our next work.

3.5 Bounded Gap of Ideal Lattices

Let I be an ideal of the n-th cyclotomic ring and $\mathcal{L}_I$ be the ideal lattice corresponding to I (under the coefficient embedding). For the case that n is a power of 2, one has $\lambda_{\varphi(n)}(\mathcal{L}_I) = \lambda_1(\mathcal{L}_I)$. For n being a prime, however, we do not know whether this nice property hold or not, but we are able to show that the gap between $\lambda_{n-1}(\mathcal{L}_I)$ and $\lambda_1(\mathcal{L}_I)$ is bounded by $\sqrt{n}$.

Lemma 14. *Let n be a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. For any non-zero ideal I of $\mathcal{R}$, we have:*

$$\lambda_{n-1}(\mathcal{L}_I) \leq \sqrt{n} \cdot \lambda_1(\mathcal{L}_I).$$

Proof. Let $\mathbf{a} = (a_0, \cdots, a_{n-2})$ be a non-zero shortest vector of $\mathcal{L}_I$ and $a \in \mathcal{R}$ be the polynomial of coefficient vector $\mathbf{a}$. Then the polynomial $X^k \cdot a$ also induces a vector of $\mathcal{L}_I$ denoted by $\mathbf{a}^{(k)} = \left(a_0^{(k)}, \cdots, a_{n-2}^{(k)}\right)$. For any $k \in \{1, \cdots, n-2\}$, the coordinates of $\mathbf{a}^{(k)}$ can be represented by the a_i's as follows:

$$a_i^{(k)} = \begin{cases} a_{n-k+i} - a_{n-1-k}, & i < k-1 \\ -a_{n-1-k}, & i = k-1 \\ a_{i-k} - a_{n-1-k}, & i > k-1 \end{cases}.$$

Then, we have

$$
\begin{aligned}
\|\mathbf{a}^{(k)}\| &= \sqrt{\sum_{i=0}^{n-2} a_i^2 - 2a_{n-1-k}(\sum_{i\neq n-1-k} a_i) + (n-2)a_{n-1-k}^2} \\
&\leq \sqrt{\sum_{i=0}^{n-2} a_i^2 + (n-1)a_{n-1-k}^2 + (\sum_{i\neq n-1-k} a_i)^2} \\
&\leq \sqrt{\sum_{i=0}^{n-2} a_i^2 + (n-1)a_{n-1-k}^2 + (n-2)(\sum_{i\neq n-1-k} a_i^2)} \\
&\leq \sqrt{n} \cdot \|\mathbf{a}\|.
\end{aligned}
$$

All these $\mathbf{a}^{(k)}$'s and $\mathbf{a}$ are linearly independent so that we conclude that $\lambda_{n-1}(\mathcal{L}_{I_S}) \leq \sqrt{n} \cdot \lambda_1(\mathcal{L}_{I_S})$. □

Back to the ring $\mathcal{R}_q$, combining Minkowski's theorem, we obtain the following corollary.

Corollary 2. *Let $n \geq 7$ be a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. Let q be a prime such that $\Phi_n(X)$ splits into $n-1$ distinct linear factors modulo q and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Let $S \subseteq \{1, \cdots, n-1\}$ and denote by $\mathcal{L}_{I_S}$ the lattice generated by the ideal $\langle q, \prod_{i\in S}(X-\phi_i)\rangle$. Then*

$$\lambda_{n-1}(\mathcal{L}_{I_S}) \leq \sqrt{n} \cdot \lambda_1(\mathcal{L}_{I_S}) \leq n \cdot q^{\frac{|S|}{n-1}}.$$

4 Revised NTRUEncrypt over Prime Cyclotomic Rings

In this section, we will describe a variant of NTRUEncrypt over prime cyclotomic rings with provable security under the worst-case hardness assumption. The revised NTRUEncrypt is determined by parameters n, q, p, r, α, k and denoted by NTRUEncrypt (n, q, p, r, α, k). First, we choose a prime $n \geq 7$ and let $\mathcal{R}$ be the ring $\mathbb{Z}[X]/\Phi_n(X)$. Then we pick a prime $q = 1 \bmod n$ so that $\Phi_n(X) = \prod_{i=1}^{n-1}(X-\phi_i) \bmod q$ with distinct ϕ_i's, and let $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. The parameter $p \in \mathcal{R}_q^\times$ is chosen to be of small norm, such as $p = 2, 3$ or $p = x+2$. The parameter r is the width of discrete Gaussian distribution used for key generation. The parameters α and k are used for RLWE error generation. We list below three main components of NTRUEncrypt (n, q, p, r, α, k) :

- **Key Generation.** Sample f' from $D_{\mathbb{Z}^{n-1},r}$; if $f = pf' + 1 \bmod q \notin \mathcal{R}_q^\times$, resample. Sample g from $D_{\mathbb{Z}^{n-1},r}$; if $g \bmod q \notin \mathcal{R}_q^\times$, resample. Then return private key $sk = f \in \mathcal{R}_q^\times$ with $f = 1 \bmod p$ and public key $pk = h = pg/f \in \mathcal{R}_q^\times$.
- **Encryption.** Given message $M \in \mathcal{R}/p\mathcal{R}$, let $t = \sqrt{n}\alpha q \left(\frac{(n-1)k}{\log((n-1)k)}\right)^{1/4}$, 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 explain when and why the scheme works and how to assess its security.

4.1 Key Generation

In the above key generation algorithm, we generate the polynomials f and g by using a discrete Gaussian sampler. Lemma 5 provides a sampler outputting a distribution within exponentially small statistical distance to a certain discrete Gaussian. Actually, the conditions in our results are more demanding than that in Lemma 5. Ignoring the negligible impact, we assume we already have a polynomial-time perfect discrete Gaussian sampler.

To ensure both f and g are invertible modulo q, we may need to resample quite a few times. The following result indicates that the key generation algorithm terminates in expected polynomial time for some selective parameters.

Lemma 15. *Let $n \geq 7$ be a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. Let q be a prime such that $\Phi_n(X)$ splits into $n-1$ distinct linear factors modulo q and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. For any $\delta \in (0, 1/2)$, let $r \geq n\sqrt{\frac{\ln(2(n-1)(1+1/\delta))}{\pi}} \cdot q^{1/(n-1)}$. Then*

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

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

Proof. It suffices to bound the probability that $p \cdot f' + a$ belongs to $I := \langle q, X - \phi_k \rangle$ by $(1/q + 2\delta)$ for any $k \leq n-1$. First we have $\lambda_{n-1}(\mathcal{L}_I) \leq nq^{\frac{1}{n-1}}$ by Corollary 2 since the ideal I corresponds to $I_{\{k\}}$. This, together with Lemma 1, implies that $r \geq \eta_\delta(\mathcal{L}_I)$. Applying Lemma 4, we have that the probability of $p \cdot f' + a = 0 \bmod I$ does not exceed $1/q + 2\delta$. □

Next, we claim that the norms of f and g are small with overwhelming probability.

Lemma 16. *Let $n \geq 7$ be a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. Suppose $q > 8n$ is a prime such that $\Phi_n(X)$ splits into $n-1$ distinct linear factors modulo q and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Let $r \geq n\sqrt{\frac{2\ln(6(n-1))}{\pi}} \cdot q^{1/(n-1)}$. The secret key polynomials f, g satisfy, with probability $\geq 1 - 2^{-n+4}$,*

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

If $\deg p = 0$, then $\|f\| \leq 2\sqrt{n-1} \cdot \|p\|r$ with probability $\geq 1 - 2^{-n+4}$.

Proof. Setting $\delta = \frac{1}{10(n-1)-1}$, then we get $r \geq \sqrt{\frac{\ln(2(n-1)(1+1/\delta))}{\pi}}$ from the assumption. Applying Lemma 1 to $\mathbb{Z}^{n-1}$, we know that $r \geq \eta_\delta(\mathbb{Z}^{n-1})$. Therefore, we can use Lemma 3 to get,

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

Since $r \geq n\sqrt{\frac{\ln(2(n-1)(1+1/\delta))}{\pi}} \cdot q^{1/(n-1)}$, Lemma 15 yields

$$\begin{aligned}\Pr_{g \hookleftarrow D_{\mathbb{Z}^{n-1},r}} \left(\|g\| \geq r\sqrt{n-1} \mid g \in \mathcal{R}_q^\times \right) &\leq \frac{\Pr_{g \hookleftarrow D_{\mathbb{Z}^{n-1},r}} \left(\|g\| \geq r\sqrt{n-1} \right)}{\Pr_{g \hookleftarrow D_{\mathbb{Z}^{n-1},r}} \left(g \in \mathcal{R}_q^\times \right)} \\ &\leq \frac{1+\delta}{1-\delta} 2^{1-n} \cdot \frac{1}{1-(n-1)(1/q+2\delta)} \leq 2^{4-n}.\end{aligned}$$

This means that the norm of the key polynomial g is less than $r\sqrt{n-1}$ with probability $\geq 1 - 2^{4-n}$. The same argument holds true for the polynomial f' such that $f = p \cdot f' + 1$.

If $\deg p = 0$, we have $\|f\| \leq 1 + \|p\|\|f'\| \leq 2\|p\|r\sqrt{n-1}$ with probability $\geq 1 - 2^{4-n}$. For general cases, applying Lemma 8, we know that $\|f\| \leq 1 + \|p\|\|f'\| \leq 1 + 2(n-1)\|p\|r \leq 2n \cdot \|p\|r$ with probability $\geq 1 - 2^{4-n}$. □

We are also able to prove that the public key h, the ratio of pg and $f = pf'+1$, enjoys a favorable uniformity for some well-chosen r's, just like that shown in [33]. We denote by $D_{r,z}^\times$ the discrete Gaussian $D_{\mathbb{Z}^{n-1},r}$ restricted to $\mathcal{R}_q^\times + z$.

Theorem 2. *Let $n \geq 7$ be a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. Suppose $q > 8n$ is a prime such that $\Phi_n(X)$ splits into $n-1$ distinct linear factors modulo q and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Let $0 < \epsilon < \frac{1}{2}$ and $r \geq (n-1)^2\sqrt{\ln(8nq)} \cdot q^{\frac{1}{2}+2\epsilon}$. Then*

$$\Delta\left(\frac{y_1 + p \cdot D_{r,z_1}^\times}{y_2 + p \cdot D_{r,z_2}^\times} \bmod q; U(\mathcal{R}_q^\times) \right) \leq \frac{2^{3(n-1)}}{q^{\lfloor \epsilon(n-1) \rfloor}}$$

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 Our proof follows essentially the same approach as in [33]. For completeness, we include it in Appendix B. This result provides a new instance of Decisional Small Polynomial Ratio(DSPR) assumption introduced in [24].

4.2 Decryption

Just like in the classical NTRUEncrypt, the correctness of decryption is based on the fact that a polynomial of ℓ_∞ norm $< q/2$ is invariant under modulo q reduction. In our decryption procedure, we have $C' = f \cdot C = pgs + pfe + fM \bmod q$. When $\|pgs + pfe + fM\|_\infty < \frac{q}{2}$, C' is in fact $pgs + pfe + fM$ and hence $C' \bmod p = fM \bmod p = M$ due to $f = 1 \bmod p$, *i.e.* the decryption succeeds. Now we are to confirm that, given a set of proper parameters, the ℓ_∞

norms of pgs, pfe and fM will be small enough (e.g., less than $\frac{q}{6}$) with high probability. This ensures a successful decryption.

We first show that the polynomial drawn from RLWE error distribution has a relatively small norm with a high probability.

Lemma 17. *Let $n \geq 7$ be a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. For $t > 1$ and $u > 0$, we have*

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

Proof. We will need the following inequality in our proof:

$$\lfloor x \rceil^2 \leq \frac{1}{4\epsilon} + \frac{1}{1-\epsilon} x^2.$$

In fact, for $x \in \mathbb{R}$, we have $(\lfloor x \rceil - x)^2 \leq \frac{1}{4}$. For any $\epsilon \in (0,1)$, we have $\lfloor x \rceil^2 \leq \frac{1}{4} - x^2 + 2\lfloor x \rceil x \leq \frac{1}{4} - x^2 + \frac{1}{1-\epsilon}x^2 + (1-\epsilon)\lfloor x \rceil^2 = \frac{1}{4} + \frac{\epsilon}{1-\epsilon}x^2 + (1-\epsilon)\lfloor x \rceil^2$. A routine computation leads to the result.

Let $\mathbf{b} = \lfloor \mathbf{b}' \bmod \Phi_n(X) \rceil \in \mathcal{R}$ with $\mathbf{b}' \hookleftarrow \psi_t^n$. Let vector $\mathbf{v} = \frac{1}{t}(b_0, \cdots, b_{n-1})$ where $(b_0, \cdots, b_{n-1})$ is the coefficient vector of $\mathbf{b}'$. Then we obtain

$$\|\mathbf{b}\|^2 \leq \frac{1}{1-\epsilon} \sum_{i=0}^{n-2} (b_i - b_{n-1})^2 + \frac{n-1}{4\epsilon} = \frac{t^2}{1-\epsilon}\|\mathbf{M}\mathbf{v}\|^2 + \frac{n-1}{4\epsilon},$$

where

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

Let $\Sigma = \mathbf{M}^\top \mathbf{M}$, we have

$$\Sigma = \begin{pmatrix} 1 & & & & -1 \\ & 1 & & & -1 \\ & & \ddots & & \vdots \\ & & & 1 & -1 \\ -1 & -1 & \cdots & -1 & (n-1) \end{pmatrix} \in \mathbb{R}^{n \times n}.$$

In our estimation, we need traces $\mathbf{tr}(\Sigma)$, $\mathbf{tr}(\Sigma^2)$ and the operator norm $\|\Sigma\|$. It is easy to check that $\mathbf{tr}(\Sigma) = 2(n-1)$, $\mathbf{tr}(\Sigma^2) = (n-1)(n+2)$. It can be calculated that the characteristic polynomial of Σ is $\lambda(\lambda-1)^{n-2}(\lambda-n)$, so n is the largest eigenvalue of Σ and hence $\|\Sigma\| = n$.

All coordinates of $\mathbf{b}'$ follow the distribution ψ_t independently, so the coordinates of $\mathbf{v}$ follow standard Gaussian independently. As shown in [20], an tail bound for $\|\mathbf{M}\mathbf{v}\|^2$ holds

$$\begin{aligned} &\Pr\left(\|\mathbf{M}\mathbf{v}\|^2 > 2(n-1) + 2\sqrt{(n-1)(n+2)u} + 2nu\right) \\ =&\Pr\left(\|\mathbf{M}\mathbf{v}\|^2 > \mathbf{tr}\left(\Sigma\right) + 2\sqrt{\mathbf{tr}\left(\Sigma^2\right) u} + 2\|\Sigma\|u\right) \leq \exp(-u). \end{aligned}$$

Let

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

and

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

Then it can be verified that

$$A = \sqrt{2(n-1) + 2\sqrt{(n-1)(n+2)u} + 2nu} + \sqrt{\frac{n-1}{4t^2}} < \sqrt{2n}(\sqrt{u}+2),$$

thus we have

$$\begin{aligned}
&\Pr_{\mathbf{b}\hookleftarrow\overline{\psi_t^n}}\left(\|\mathbf{b}\| \geq \left(\sqrt{2n}(\sqrt{u}+2)\right)t\right)\\
\leq &\Pr_{\mathbf{b}\hookleftarrow\overline{\psi_t^n}}(\|\mathbf{b}\| > At)\\
\leq &\Pr_{\mathbf{v}\hookleftarrow\psi_1^n}\left(\frac{1}{1-\epsilon}\|\mathbf{M}\mathbf{v}\|^2 + \frac{n-1}{4t^2\epsilon} > A^2\right)\\
= &\Pr\left(\|\mathbf{M}\mathbf{v}\|^2 > 2(n-1) + 2\sqrt{(n-1)(n+2)u} + 2nu\right)\\
\leq &\exp(-u).
\end{aligned}$$

□

Setting u in Lemma 17 to $\Theta(\log^{1+\kappa} n)$ and applying Lemmata 16,8, we are able to get the following:

Lemma 18. *In* NTRUEncrypt (n,q,p,r,α,k)*, let* $t = \sqrt{n}\alpha q\left(\frac{(n-1)k}{\log((n-1)k)}\right)^{1/4} > 1$*. Then for* $\kappa > 0$*, we have*

$$\|pgs\|_\infty, \|pfe\|_\infty \leq 8\sqrt{2}n^2\mathbf{\Theta}\left(\log^{\frac{1+\kappa}{2}} n\right)\|p\|^2 rt$$

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

Furthermore, if $\deg p = 0$*,then*

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

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

It is also hoped that fM has smaller norm. Indeed, we can prove

Lemma 19. *In* NTRUEncrypt (n,q,p,r,α,k)*, we have*

1. $\|M\| \leq (n-1)\|p\|$.
2. $\|fM\|_\infty \leq 4n^2\|p\|^2 r$ *with probability at least* $1 - 2^{-n+4}$.

Furthermore, if $\deg p = 0$*, we have* $\|M\| \leq \frac{\sqrt{n-1}}{2}\|p\|$ *holds, and with probability at least* $1 - 2^{-n+4}$, $\|fM\|_\infty \leq 2n\|p\|^2 r$ *holds.*

Proof. By reducing modulo the pX^i's, we can write M into $\sum_{i=0}^{n-2} \epsilon_i p X^i$ with $-1/2 < \epsilon_i \leq 1/2$. Using Lemma 8, we have

$$\|M\| \leq 2\sqrt{n-1}\|\sum_{i=0}^{n-2} \epsilon_i X^i\|\|p\| \leq (n-1)\|p\|.$$

For the case $\deg p = 0$, we have $\|M\| = \|p\| \cdot \|\sum_{i=0}^{n-2} \epsilon_i X^i\| \leq \frac{\sqrt{n-1}}{2}\|p\|$. Then, combining Lemmata 16 and 8 with the above result, the proof is completed. □

Overall, we give a set of parameters such that NTRUEncrypt decrypts correctly with high probability.

Theorem 3. *If* $\omega\left(n^2 \log^{0.5} n\right)\|p\|^2 rt/q < 1$*(resp.* $\omega\left(n \log^{0.5} n\right)\|p\|^2 rt/q < 1$ *if* $\deg p = 0$*) and* $t = \sqrt{n}\alpha q \left(\frac{(n-1)k}{\log((n-1)k)}\right)^{1/4} > 1$*, then the decryption algorithm of* NTRUEncrypt *recovers* M *with probability* $1 - n^{-\omega(1)}$ *over the choice of* s, e, f, g.

4.3 Security Reduction and Parameters

In a manner similar to [33], we are able to establish a security reduction of NTRUEncrypt from the decisional $\mathsf{RLWE}^{\times}_{HNF}$. One technical idea is that one can produce a legal pair of public key and ciphertext pair $(h = pa, C = pb + M = hs + pe + M)$ by using the pair $(a, b = as + e)$ sampled from RLWE distribution. The proof of Lemma 20 is shown in Appendix C.

Lemma 20. *Let* $n \geq 8$ *be a prime and* $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$*. Suppose* $q > 8n$ *is a prime such that* $\Phi_n(X)$ *splits into* $n-1$ *distinct linear factors modulo* q *and* $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$*. Let* $\epsilon, \delta > 0$, $p \in \mathcal{R}_q^\times$, $t = \sqrt{n}\alpha q \left(\frac{(n-1)k}{\log((n-1)k)}\right)^{1/4}$*, and* $r \geq (n-1)^2\sqrt{\ln(8nq)} \cdot q^{\frac{1}{2}+\epsilon}$*. If there exists an* IND-CPA *attack against the variant of* NTRUEncrypt *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* $\frac{1}{2} + \delta'$ *where* $\delta' = \frac{\delta}{2} - q^{-\Omega(n)}$.

Now we integrate all above results and discuss the parameter requirements. To ensure the uniformity of public keys, the parameters r, n and q should satisfy the condition claimed in Theorem 2, *i.e.* $r \geq (n-1)^2\sqrt{\ln(8nq)} \cdot q^{\frac{1}{2}+2\epsilon}$ for $0 < \epsilon < \frac{1}{2}$. To ensure a high probability of success decryption, we need that $t = \sqrt{n}\alpha q \left(\frac{(n-1)k}{\log((n-1)k)}\right)^{1/4} > 1$ and $\omega\left(n^2 \log^{0.5} n\right)\|p\|^2 rt/q < 1$ (resp. $\omega\left(n \log^{0.5} n\right)\|p\|^2 rt/q < 1$ if $\deg p = 0$) as stated in Theorem 3. To satisfy the condition of RLWE (Theorem 1), it requires that $\alpha q > \omega(\sqrt{\log n})$. From these requirements, to obtain a variant of NTRUEncrypt with provable security against IND-CPA attack, we may set main parameters as follows.

- $q = \mathrm{poly}(n)$, $\epsilon \in \left(0, \frac{1}{2}\right)$, and $q^{\frac{1}{2}-\epsilon} = \omega\left(n^{4.75} \log^{1.5} n \|p\|^2\right)$,
- $r = n^2 \sqrt{\ln(8nq)} \cdot q^{\frac{1}{2}+\epsilon}$,
- $k = O(1)$, $\alpha q = \Omega(\log^{0.75} n)$ and $t = \sqrt{n}\alpha q \left(\frac{(n-1)k}{\log((n-1)k)}\right)^{1/4} = \Omega(n^{0.75} \log^{0.5} n)$.

If p is set to be an integer($i.e.$ $\deg p = 0$) which is a most routine case used in NTRUEncrypt scheme, the parameters may be relaxed:

- $q = \mathrm{poly}(n)$, $\epsilon \in \left(0, \frac{1}{2}\right)$, and $q^{\frac{1}{2}-\epsilon} = \omega\left(n^{3.75} \log^{1.5} n \|p\|^2\right)$,
- $r = n^2 \sqrt{\ln(8nq)} \cdot q^{\frac{1}{2}+\epsilon}$,
- $k = O(1)$, $\alpha q = \Omega(\log^{0.75} n)$ and $t = \sqrt{n}\alpha q \left(\frac{(n-1)k}{\log((n-1)k)}\right)^{1/4} = \Omega(n^{0.75} \log^{0.5} n)$.

Combining with Theorem 1, we have obtained our main result.

Theorem 4. *Let $n \geq 8$ be a prime and $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$. Suppose $q = \mathrm{poly}(n)$ is a prime such that $\Phi_n(X)$ splits into $n-1$ distinct linear factors modulo q and $q^{\frac{1}{2}-\epsilon} = \omega\left(n^{4.75} \log^{1.5} n \|p\|^2\right)$ (resp. $q^{\frac{1}{2}-\epsilon} = \omega\left(n^{3.75} \log^{1.5} n \|p\|^2\right)$, if $\deg p = 0$), for arbitrary $\epsilon \in \left(0, \frac{1}{2}\right)$ and $p \in \mathcal{R}_q^\times$. Let $r = n^2 \sqrt{\ln(8nq)} \cdot q^{\frac{1}{2}+\epsilon}$ and $t = \sqrt{n}\alpha q \left(\frac{(n-1)k}{\log((n-1)k)}\right)^{1/4}$ where $k = O(1)$ and $\alpha q = \Omega(\log^{0.75} n)$. If there exists an IND-CPA attack against the variant of NTRUEncrypt (n, q, p, r, α, k) that runs in time $\mathrm{poly}(n)$ and has success probability $\frac{1}{2} + \frac{1}{\mathrm{poly}(n)}$, then there exists a $\mathrm{poly}(n)$-time algorithm solving γ-Ideal-SVP on ideal lattices in $\mathbb{Z}[X]/\Phi_n(X)$ with $\gamma = O\left(\sqrt{n}q/\log^{0.75} n\right)$. Moreover, the decryption success probability exceeds $1 - n^{-\omega(1)}$ over the choice of the encryption randomness.*

In the modified NTRUEncrypt, the parameter r is $\tilde{\Omega}(n^2 \cdot q^{\frac{1}{2}+\epsilon})$ and that in [33] is $\tilde{\Omega}(n \cdot q^{\frac{1}{2}+\epsilon})$. Note tha the term $q^{\frac{1}{2}+\epsilon}$ is much greater than its polynomial coefficient n^2 or n, thus, in this sense, our result is close to that for power-of-2 cyclotomic rings. By setting $\epsilon = o(1)$ and p to be of degree 0, the smallest modulus q and approximate factor γ reach $\tilde{\Omega}(n^{7.5})$ and $\tilde{\Omega}(n^8)$ respectively. These compare to $\tilde{\Omega}(n^5)$ and $\tilde{\Omega}(n^{5.5})$ for NTRUEncrypt over power-of-2 cyclotomic rings.

5 Conclusion and Future Work

In this paper, we extended the provable security of an NTRU variant, originally proposed by Stehlé and Steinfeld for power-of-2 cyclotomic rings, to the family of prime cyclotomic rings. As this class of rings is closer to the original NTRU rings, the results here may bring a new security estimation for the original NTRU settings. We also developed a series of tools for prime cyclotomic rings that provide a foundation to generalize more cryptosystems to this class of rings. These tools might be of some independent interest.

We present a theoretical construction with suggested parameters in the asymptotic sense. There are a batch of cryptanalyses work aiming at NTRU, such as hybrid attack [19], subfield attack [1] and straightforward attack [22]. Detailed analyses of our NTRU variant against these attacks should be well-considered.

Furthermore, the operations over the rings $\mathbb{Z}[X]/(X^n \pm 1)$ are still more efficient than that over prime cyclotomic rings. The further investigation of the relation between the prime cyclotomic ring and NTRU ring may improve the efficiency of related cryptosystems. We leave them to the future work.

As shown in [26, 25], canonical embedding provides a neat description of the geometry of cyclotomic rings, which may lead to more compact and general results. To get similar conclusions with respect to the canonical embedding, we need to develop more powerful tools and that is left as a future investigation.

The ideal lattices (under the coefficient embedding) over prime cyclotomic rings are not (anti-)circulant, thus to study the gap between their minimums could be useful in cryptanalysis. Another interesting problem is a finer estimation of Euclidean norm of elements in an ideal of the prime cyclotomic ring, as it is useful in reducing some complexity estimations.

Acknowledgements. We thank Léo Ducas, Dianyan Xiao and the anonymous PKC'17 reviewers for their helpful comments. This work is supported in part by China's 973 Program (No. 2013CB834205), the Strategic Priority Research Program of the Chinese Academy of Sciences (No. XDB01010600) and NSF of China (No. 61502269).

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

[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] Cheon, J.H., Jeong, J., Lee, C.: An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without an encoding of zero. Cryptology ePrint Archive, Report 2016/139 (2016), http://eprint.iacr.org/2016/139

[5] Coppersmith, D., Shamir, A.: Lattice attacks on NTRU. In: EUROCRYPT 1997. pp. 52–61 (1997)

[6] Cramer, R., Ducas, L., Wesolowski, B.: Short Stickelberger class relations and application to Ideal-SVP. Cryptology ePrint Archive, Report 2016/885 (2016), http://eprint.iacr.org/2016/885

[7] Ducas, L., Durmus, A.: Ring-LWE in polynomial rings. In: PKC 2012. pp. 34–51 (2012)

[8] Ducas, L., Lyubashevsky, V., Prest, T.: Efficient identity-based encryption over NTRU lattices. In: ASIACRYPT 2014. pp. 22–41 (2014)

[9] Ducas, L., Nguyen, P.Q.: Learning a zonotope and more: Cryptanalysis of NTRUSign countermeasures. In: ASIACRYPT 2012. pp. 433–450 (2012)

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

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

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

[13] Gentry, C.: Fully homomorphic encryption using ideal lattices. In: STOC 2009. pp. 169–178 (2009)

[14] Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: STOC 2008. pp. 197–206 (2008)

[15] Gentry, C., Szydlo, M.: Cryptanalysis of the revised NTRU signature scheme. In: EUROCRYPT 2002. pp. 299–320. Springer (2002)

[16] 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)

[17] Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A new high speed public key cryptosystem. p. Presented at the rump session of Crypto'96

[18] Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A ring-based public key cryptosystem. In: ANTS 1998. pp. 267–288 (1998)

[19] Howgrave-Graham, N.: A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. In: CRYPTO 2007. pp. 150–169 (2007)

[20] 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)

[21] Jaulmes, E., Joux, A.: A chosen-ciphertext attack against NTRU. In: CRYPTO 2000. pp. 20–35 (2000)

[22] Kirchner, P., Fouque, P.A.: Comparison between subfield and straightforward attacks on NTRU. Cryptology ePrint Archive, Report 2016/717 (2016), http://eprint.iacr.org/2016/717

[23] Langlois, A., Stehlé, D., Steinfeld, R.: GGHLite: More efficient multilinear maps from ideal lattices. In: EUROCRYPT 2014. pp. 239–256 (2014)

[24] 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)

[25] Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: EUROCRYPT 2010. pp. 1–23 (2010)

[26] 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

[27] Micciancio, D.: Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. Computational Complexity 16(4), 365–411 (2007)

[28] Micciancio, D., Regev, O.: Worst-case to average-case reductions based on gaussian measures. SIAM Journal on Computing 37(1), 267–302 (2007)

[29] Nguyen, P.Q., Regev, O.: Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. In: EUROCRYPT 2006. pp. 271–288 (2006)

[30] Nuñez, D., Agudo, I., Lopez, J.: NTRUReEncrypt: An efficient proxy re-encryption scheme based on NTRU. In: ASIACCS 2015. pp. 179–189 (2015)

[31] Peikert, C.: Limits on the hardness of lattice problems in ℓ_p norms. Computational Complexity 17(2), 300–351 (2008)

[32] Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: STOC 2005. pp. 84–93 (2005)

[33] Stehlé, D., Steinfeld, R.: Making NTRU as secure as worst-case problems over ideal lattices. In: EUROCRYPT 2011. pp. 27–47 (2011)

[34] Szydlo, M.: Hypercubic lattice reduction and analysis of GGH and NTRU signatures. In: EUROCRYPT 2003. pp. 433–448 (2003)

[35] Terras, A.: Fourier Analysis on Finite Groups and Applications. Cambridge University Press (1999)

[36] Xylouris, T.: On Linnik's constant (2009), `http://arxiv.org/abs/0906.2749`

A Proof of Lemma 10

Let p be the probability over the randomness of $\mathbf{a}$ that $\lambda_1^\infty(\mathcal{L}(\mathbf{a}, I_S)) < B$, where $B = \frac{1}{\sqrt{n}} q^\beta$. For a non-zero vector $\mathbf{t}$ of ℓ_∞ norm $< B$ and $s \in \mathcal{R}_q/I_S$, let $p(\mathbf{t}, s) = \Pr_{\mathbf{a}}(\forall i, t_i = a_i s \bmod I_S)$ and $p_i(t_i, s) = \Pr_{a_i}(t_i = a_i s \bmod I_S)$, then we have $p(\mathbf{t}, s) = \prod_{i=1}^m p_i(t_i, s)$.

Let ν_{I_S} be the polynomial $\prod_{i \in S}(X - \phi_i)$. We only need to consider such $(\mathbf{t}, s)$ pairs that $\gcd(t_i, \nu_{I_S}) = \gcd(s, \nu_{I_S})$ for all $i \in \{1, \cdots, m\}$: if not so, we can prove $p(\mathbf{t}, s) = 0$ due to the invertibility of a_i. For each such pair, we denote by d the degree of $\gcd(s, \nu_{I_S})$. Notice that there are $(q-1)^{d+n-1-|S|}$ distinct a_i's in $\mathcal{R}_q^\times$ such that $t_i = a_i s \bmod I_S$, *i.e.* $p_i(t_i, s) = (q-1)^{d-|S|}$, then we have $p(\mathbf{t}, s) = \prod_{i=1}^m p_i(t_i, s) = (q-1)^{m(d-|S|)}$.

The probability p is bounded by

$$\begin{aligned} p &\le \sum_{s \in \mathcal{R}_q/I_S} \sum_{0 < \|\mathbf{t}\|_\infty < B} p(\mathbf{t}, s) \\ &\le \sum_{0 \le d \le |S|} \sum_{\substack{S' \subseteq S, |S'| = d \\ h = \prod_{i \in S'}(X - \phi_i)}} \sum_{\substack{s \in \mathcal{R}_q/I_S \\ h | s}} \sum_{\substack{\mathbf{t} \in \mathcal{R}_q^m \\ \forall i, 0 < \|t_i\|_\infty < B \\ h | t_i}} (q-1)^{m(d-|S|)}. \end{aligned}$$

For $h = \prod_{i \in S'}(X - \phi_i)$ of degree d, let $N(B, d)$ be the number of $t \in \mathcal{R}_q$ such that $\|t\|_\infty \in (0, B)$ and $t = ht'$ for $t' \in \mathcal{R}_q$ of degree $< n - 1 - d$. We now show two bounds for $N(B, d)$ depending on d.

Suppose that $d \ge \beta(n-1)$, then $N(B, d) = 0$. Indeed, for any $t = ht'$ with $t' \in \mathcal{R}_q$, the ideal $\langle t \rangle$ is a full-rank sub-ideal of the ideal $\langle h, q \rangle$. Thus, we have $\mathrm{N}(t) = \mathrm{N}(\langle t \rangle) \ge \mathrm{N}(\langle h, q \rangle) = q^d$. Combined with Lemma 7 and equivalence of norms, we conclude that $\|t\|_\infty \ge \frac{\|t\|}{\sqrt{n-1}} \ge \frac{\mathrm{T}_2(t)}{\sqrt{n(n-1)}} \ge \frac{\mathrm{N}(t)^{1/(n-1)}}{\sqrt{n}} \ge \frac{q^\beta}{\sqrt{n}}$, which implies $N(B, d) = 0$ when $d \ge \beta(n-1)$.

Suppose that $d < \beta(n-1)$, then $N(B,d) \leq (2B)^{n-1-d}$. Let $t = \sum_{i=0}^{n-2} t_i X^i$, $h = \sum_{i=0}^{d} h_i X^i$ and $t' = \sum_{i=0}^{n-2-d} t'_i X^i$. From $t = ht'$, we have

$$(t_0, \cdots, t_{n-2-d}) = (t'_0, \cdots, t'_{n-2-d}) \begin{pmatrix} h_0 & h_1 & \cdots & & h_{n-2-d} \\ & h_0 & h_1 & & \vdots \\ & & h_0 & \ddots & \\ & & & \ddots & h_1 \\ & & & & h_0 \end{pmatrix}$$

The constant coefficient of h_0 is non-zero modulo prime q, so the polynomial t' will be determined once the $(n-1-d)$ low-order coefficients of t are determined, and vice versa. Thus each possible t is uniquely decided by its $(n-1-d)$ low-order coefficients and this leads to $N(B,d) \leq (2B)^{n-1-d}$.

Notice that the number of subsets of S is $2^{|S|}$ and the number of $s \in \mathcal{R}_q / I_S$ divisible by $h = \prod_{i \in S'} (X - \phi_i)$ of degree d is $q^{|S|-d}$. Thus the probability p can be bounded as follows:

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

Since $n \geq 7$, $q = 1 \bmod n$ and $\beta \leq 1 - \frac{1}{m}$, we have $(2B)^m (\frac{q}{q-1}) < (q-1)^{\beta m}$ and then

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

We now complete the proof.

B Proof of Theorem 2

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

To translate Pr_a into a more straightforward form, we introduce another probability $Pr_{\mathbf{a}} = Pr_{f_1,f_2}[a_1 f_1 + a_2 f_2 = a_1 z_1 + a_2 z_2]$ for $\mathbf{a} = (a_1, a_2) \in (\mathcal{R}_q^\times)^2$, and then obtain $Pr_{\mathbf{a}} = Pr_{-a_2 \cdot a_1^{-1}}$ after a simple computation. For $(a_1, a_2) \in (\mathcal{R}_q^\times)^2$, we consider the equation $a_1 f_1 + a_2 f_2 = a_1 z_1 + a_2 z_2$ of the pair (f_1, f_2). All its solutions form the set $\mathbf{z} + \mathbf{a}^{\perp\times}$, where $\mathbf{z} = (z_1, z_2)$ and $\mathbf{a}^{\perp\times} = \mathbf{a}^\perp \bigcap (\mathcal{R}_q^\times + q\mathbb{Z}^{n-1})^2$. Then, we have

$$Pr_{\mathbf{a}} = \frac{\mathbf{D}_{\mathbb{Z}^{2(n-1)},r}(\mathbf{z} + \mathbf{a}^{\perp\times})}{\mathbf{D}_{\mathbb{Z}^{n-1},r}(z_1 + \mathcal{R}_q^\times + q\mathbb{Z}^{n-1}) \cdot \mathbf{D}_{\mathbb{Z}^{n-1},r}(z_2 + \mathcal{R}_q^\times + q\mathbb{Z}^{n-1})}.$$

Thanks to $\mathbf{a} \in (\mathcal{R}_q^\times)^2$, for any $(x_1, x_2) \in \mathbf{a}^\perp$, the elements x_1 and x_2 lie in the same ideal I_S of $\mathcal{R}_q$. To circumvent the restriction on invertibility, we exploit the inclusion-exclusion principle and change the three above sums into the following forms.

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

$$\mathbf{D}_{\mathbb{Z}^{n-1},r}(z_i + \mathcal{R}_q^\times + q\mathbb{Z}^{n-1}) = \sum_{S \subseteq \{1,\cdots,n-1\}} (-1)^{|S|} \cdot \mathbf{D}_{\mathbb{Z}^{2(n-1)},r}(z_i + I_S + q\mathbb{Z}^{n-1}), \text{for } i \in \{1,2\} \quad (2).$$

First, let's prove the Equation (1). For $\mathbf{D}_{\mathbb{Z}^{2(n-1)},r}(\mathbf{z} + \mathbf{a}^\perp(I_S))$ with $|S| \leq \epsilon(n-1)$, let $\delta = q^{-(n-1)-\lfloor \epsilon(n-1) \rfloor}$ and $m = 2$, then Lemma 13 implies that, for all except a fraction $\leq \frac{2^{n-1}}{(q-1)^{\epsilon(n-1)}}$ of $\mathbf{a} \in (\mathcal{R}_q^\times)^2$,

$$\left| \mathbf{D}_{\mathbb{Z}^{2(n-1)},r}(\mathbf{z} + \mathbf{a}^\perp(I_S)) - q^{-(n-1)-|S|} \right| = \left| \mathbf{D}_{\mathbb{Z}^{2(n-1)},r,-\mathbf{z}}(\mathbf{a}^\perp(I_S)) - q^{-(n-1)-|S|} \right| \leq 2\delta.$$

For the case $|S| > \epsilon(n-1)$, we can find $S' \subseteq S$ with $|S'| = \lfloor \epsilon(n-1) \rfloor$. Because $\mathbf{a}^\perp(I_S) \subseteq \mathbf{a}^\perp(I_{S'})$, we have $\mathbf{D}_{\mathbb{Z}^{2(n-1)},r,-\mathbf{z}}(\mathbf{a}^\perp(I_S)) \leq \mathbf{D}_{\mathbb{Z}^{2(n-1)},r,-\mathbf{z}}(\mathbf{a}^\perp(I_{S'}))$. Using the result proven before, we conclude that $\mathbf{D}_{\mathbb{Z}^{2(n-1)},r,-\mathbf{z}}(\mathbf{a}^\perp(I_S)) \leq 2\delta + q^{-(n-1)-\lfloor \epsilon(n-1) \rfloor}$. Therefore, the following inequality holds

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

for all except a fraction $\leq \frac{2^{2(n-1)}}{(q-1)^{\epsilon(n-1)}}$ of $\mathbf{a} \in (\mathcal{R}_q^\times)^2$.

Next, we are to prove the Equation (2). Let $\delta = q^{-(n-1)/2}$. Lemma 2 shows that $\lambda_{n-1}(\mathcal{L}_{I_S}) \leq n \cdot q^{|S|/(n-1)}$. For S of cardinality $\leq (n-1)/2$, by Lemma 1, we get that $r \geq \eta_\delta(I_S + q\mathbb{Z}^{n-1})$. Using Lemma 4, we know $|\mathbf{D}_{\mathbb{Z}^{n-1},r,-z_i}(I_S + q\mathbb{Z}^{n-1}) - q^{-|S|}| \leq 2\delta$. For the case $|S| > (n-1)/2$, using the same argument, we have $\mathbf{D}_{\mathbb{Z}^{n-1},r,-z_i}(I_S + q\mathbb{Z}^{n-1}) \leq 2\delta + q^{-(n-1)/2}$. Therefore,

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

Overall, we prove that, except for a fraction $\leq \frac{2^{2(n-1)}}{(q-1)^{\epsilon(n-1)}}$ of $\mathbf{a} \in (\mathbb{R}_q^\times)^2$,

$$\mathbf{D}_{\mathbb{Z}^{2(n-1)},r}(\mathbf{z} + \mathbf{a}^{\perp\times}) = (1 + \delta_0) \cdot \frac{(q-1)^{n-1}}{q^{2(n-1)}},$$
$$\mathbf{D}_{\mathbb{Z}^{n-1},r}(z_i + \mathcal{R}_q^\times + q\mathbb{Z}^{n-1}) = (1 + \delta_i) \cdot \frac{(q-1)^{n-1}}{q^{n-1}}, \text{for } i \in \{1, 2\}.$$

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

C Proof of Lemma 20

Let $\mathcal{A}$ be the given IND-CPA attack algorithm. Given oracle $\mathcal{O}$ that outputs k samples drawn from either $U(\mathcal{R}_q^\times \times \mathcal{R}_q)$ or $A_{s,\psi}^\times$ for previously chosen $s \hookleftarrow \psi$. We construct an algorithm $\mathcal{B}$ to solve $\mathsf{RLWE}_{HNF}^\times$. Algorithm $\mathcal{B}$ first calls $\mathcal{O}$ to get k samples $(h'_1, C'_1), \cdots, (h'_k, C'_k)$. Then algorithm $\mathcal{B}$ picks $i \hookleftarrow U(\{1, \cdots, k\})$ and calculates the public key $h_i = p \cdot h'_i$. When $\mathcal{A}$ outputs a challenge message pair (M_0, M_1), $\mathcal{B}$ picks $b \hookleftarrow U(\{0, 1\})$, computes the challenge ciphertext $C_i = p \cdot C'_i + M_b$ and sends it to $\mathcal{A}$. Finally, $\mathcal{A}$ outputs its guess b', and then $\mathcal{B}$ outputs 1 if $b' = b$ and 0 otherwise.

All h'_i's are uniformly random in $\mathcal{R}_q^\times$, and thus so are the public keys h_i's due to $p \in \mathcal{R}_q^\times$. Theorem 2 shows that the statistical distance between the distribution of the public key given to $\mathcal{A}$ and that in the genuine attack is $q^{-\Omega(n)}$. Furthermore, if $\mathcal{O}$ outputs samples from $A_{s,\psi}^\times$, the pair (h_i, C_i) is of the form $(h_i, h_i s + pe + M_b)$ which corresponds to actual "public key and ciphertext" pair in the IND-CPA attack. Therefore $\mathcal{A}$ succeeds and $\mathcal{B}$ outputs 1 with probability $\geq \frac{1}{2} + \delta - q^{-\Omega(n)}$.

If $\mathcal{O}$ outputs samples from $U(\mathcal{R}_q^\times \times \mathcal{R}_q)$, then C_i is uniformly random in $\mathcal{R}_q$ and independent of b. Algorithm $\mathcal{B}$ outputs 1 with probability 1/2 in this case. Thus the advantage of $\mathcal{B}$ in distinguishing $U(\mathcal{R}_q^\times \times \mathcal{R}_q)$ and $A_{s,\psi}^\times$ is greater than $\delta/2 - q^{-\Omega(n)}$.