CRPSF and NTRU Signatures over cyclotomic fields

Yang Wang[1] and Mingqiang Wang*[2]

[1,2]School of Mathematics, Shandong University
[1]wyang1114@mail.sdu.edu.cn
[2]wangmingqiang@sdu.edu.cn

Abstract

We propose a detailed construction of Collision Resistance Preimage Sampleable Functions (CRPSF) over any cyclotomic field based on NTRU, hence give a provably secure NTRU Signature scheme (NTRUSign), which is strongly existentially unforgeable under adaptive chosen-message attacks in the random oracle module. The security of CRPSF (NTRUSign) is reduced to the corresponding small integer solution problem over rings (Ring-SIS). More precisely, the security of our scheme is based on the worst-case approximate shortest independent vectors problem (SIVP_γ) over ideal lattices. For any fixed cyclotomic field, we give a probabilistic polynomial time (PPT) key generation algorithm which shows how to extend the secret key of NTRUEncrypt to the secret key of NTRUSign. This conversion is important for constructions of many cryptographic primitives based on NTRU, for example, CRPSF, NTRUSign, identity-based encryption and identity-based signature.

We also delve back into former construction of NTRUEncrypt and enrich the choices of the module q. Some useful results about q-ary lattices, regularity and uniformity of distribution of the public key of NTRUEncrypt are also generalized to more general algebraic field K, as long as K is Galois over $\mathbb{Q}$.

Keywords: NTRU, Ideal lattice, Canonical embedding, Algebraic fields, CRPSF, Ring-LWE, Ring-SIS

1 Introduction

Cryptographic primitives based on NTRU can be traced back to 1996, in this year, the first NTRUEncrypt was devised by Hoffstein, Pipher and Silverman in [22]. NTRUEncrypt is one of the fastest known lattice-based cryptosystems as testified by its inclusion in the IEEE

*Corresponding author

P1363 standard and regarded as an alternative to RSA and ECC, due to its moderate key sizes, remarkable performance and potential capacity of resistance to quantum computers. These properties also hold for other NTRU-based cryptographic primitives, such as identity-based encryption (IBE) [11], fully homomorphic encryption [4, 30], digital signatures [21] and identity-based signature (IBS) [48]. Meanwhile, a batch of cryptanalysis works were proposed aiming at NTRU family [1, 7−9, 12, 14, 16, 19, 24, 26, 45].

Like NTRUEncrypt, the security of early NTRU Signature schemes is also heuristic and lacks a solid mathematical proof. The first construction of NTRU Signature Scheme (NSS) is [23], but it succumbed to attacks showed in [15, 18]. The commonly used and discussed NTRU signature scheme is NTRUSign, which was proposed in [21]. Also, it went through a break-and-repair development history [12, 19, 26, 35, 36]. Provably secure NTRUEncrypt has a relatively short development history [45−47, 49, 50], and to our knowledge, till now, the only provably secure NTRU Signature scheme is proposed in [46]. The NTRUSign constructed by Stehl$\acute{e}$ and Steinfeld is over power-of-two cyclotomic fields. They improved their results in [45] and used a novel technique to bound the Dedekind Zeta function over power-of-two cyclotomic fields. Then they estimated the running time of the traditional key generation algorithm of NTRUSign by relating it to the Dedekind zeta function. In fact, they constructed the first CRPSF [17] over power-of-two cyclotomic fields based on NTRU, then, gave the first provably secure NTRUSign based on CRPSF.

CRPSF is an important cryptographic primitive proposed in [17]. It is a collection of functions with some special properties. The functions are surjective, many-to-one, one-way and collision-resistant trapdoor functions with uniform outputs. The trapdoor inversion algorithm samples from among all the preimages of an image under an appropriate distribution. Meanwhile, for any fixed function f and image y, the conditional probability that sampling a particular preimage x (given f(x)=y) by some domain sampling algorithm is negligible. Thanks to these excellent properties, we can design many cryptographic primitives based on CRPSF, for example, signatures, IBE and IBS.

A natural open problem proposed by Stehl$\acute{e}$ and Steinfeld is that whether their constructions can be extended to more general algebraic fields. Meanwhile, a theoretical study of the security of NTRUEncrypt and NTRUSign is meaningful, due to their high efficiency and industrial standardization. These are the main motivations of our research.

1.1 Our contributions

In this paper, we give concrete constructions of CRPSF and provably secure NTRUSign over any cyclotomic field.

Our main contributions are summarized as follows.

For any fixed cyclotomic field, we theoretically analyze the key generation algorithm of NTRUSign and give an absolute lower bound of success probability of this important algorithm. This algorithm extends a secret key of NTRUEncrypt into a secret key of N-TRUSign. It is standard for many cryptographic primitive constructions based on NTRU, such as CRPSF, NTURSign, IBE and IBS.

Based on this PPT key generation algorithm, we construct a CRPSF over any cyclotomic field. Hence, by [17], we can construct a provably secure NTRUSign, which is strongly existentially unforgeable under adaptive chosen-message attacks in the random oracle module. We also give a detailed construction of claw-free CRPSF as [17].

We revisit [47] and eliminate the requirement of $q = 1 \bmod l$ for $K = \mathbb{Q}(\zeta_l)$ with ζ_l a primitive l-th root of unity. Meanwhile, results about q-ary lattices, regularity (a ring-based leftover hash lemma) and uniformity of the distribution of the public key of NTRUEncrypt are generalized to any algebraic number field K, as long as K is Galois over $\mathbb{Q}$. These results are also useful for many cryptographic primitive constructions.

1.2 Technique Overview

In this subsection, we give a technique overview about our results. Although the main ideas of our NTRUEncrypt, CRPSF and NTRUSign follow Stehl*é* and Steinfeld's routes, there are also many differences. Techniques used in [47] are also vital.

The discussions of q-ary lattices, regularity results and construction of NTRUEncrypt are essentially the same as [47]. The hardness results of Ring-LWE showed in [42] guarantee the security of the corresponding modified NTRUEncrypts. The only slight difference is the requirement of Gaussian parameter σ. The reason why we constrain our NTRUEncrypt schemes in cyclotomic fields is that we want to use the decoding basis of $R^\vee$ (here, $R^\vee$ is the dual lattice of R). These good bases, together with canonical embedding, make it possible to bound the decryption error by using the same method for any cyclotomic field. We don't know if there is such a good basis for general algebraic fields. If a number field K (which is Galois over $\mathbb{Q}$) admits such a basis for $R^\vee$, we can design our NTRUEncrypt in K by using similar techniques.

For NTRUSign, techniques described in [21] and [46] are vital. They showed how to extend a secret key of NTRUEncrypt to a secret key of NTRUSign. This conversion forms the key generation algorithm and is described as follows:

Input: $n, q \in \mathbb{Z}^+$, $\sigma > 0$.

Output: A key pair $(sk, pk) \in R^{2\times 2} \times R_q^\times$.

1. Sample f from $D_{R,\sigma}$, if $(f \bmod q) \notin R_q^\times$, resample.
2. Sample g from $D_{R,\sigma}$, if $(g \bmod q) \notin R_q^\times$, resample.
3. If $||f|| \geq \sqrt{n}\sigma$ or $||g|| \geq \sqrt{n}\sigma$, restart.
4. If $(f, g) \neq R$, restart.
5. Compute $F_q, G_q \in R$ such that $f \cdot G_q - g \cdot F_q = q$, e.g., using a Hermite Normal Form algorithm in [5].
6. Use Babai rounding nearest plane algorithm to approximate (F_q, G_q) in the lattice spanned by (f, g), let $r(f, g)$ be the output, set $(F, G) = (F_q, G_q) - r(f, g)$ for some $r \in R$.
7. If $||(F, G)|| > n\sigma\sqrt{l}$, restart.

8. Return secret key $sk = \begin{bmatrix} f & g \\ F & G \end{bmatrix}$ and public key $pk = h = g \cdot f^{-1} \in R_q^{\times}$.

Here, R is the ring of integers of $K = \mathbb{Q}(\zeta_l)$, $n = \varphi(l)$ and $R_q^{\times}$ is the set of invertible elements of $R_q = R/(qR)$. The elements f and g are the secret key of traditional NTRUEncrypt. Discrete Gaussian distribution ($D_{R,\sigma}$) could insure that elements f and g are short. In fact, the secret key generated by this algorithm is a short basis of the NTRU lattice $\Lambda_h^q = \{(x, y) \in R^2 : \ y = hx \bmod qR\}$, since $\Lambda_h^q = \mathrm{Span}_R\{(f, g), (F, G)\}$. We want to follow the routine of [17], that is to say, a short enough 'trapdoor' basis of Λ_h^q is necessary. This explains the meaning of Step 5 and 6. Meanwhile, Babai's algorithm ensures that Step 7 would pass (this algorithm would not restart in Step 7) with high probability. Gaussian heuristic implies that try to find the secret key only with h is equivalent to solve the SVP_γ problem over Λ_h^q with $\gamma \leq \tilde{O}(n^2)$, which is a very hard problem. The most annoying part is Step 4. We prove that, for appropriate choices of parameters, the probability that Step 4 does not cause a restart is $\approx \frac{1}{\zeta_K(2)}$, where $\zeta_K(2)$ is the Dedekind Zeta function over K. Meanwhile, $\zeta_K(2)$'s have an absolute upper bound for all cyclotomic fields. Therefore, the key generation algorithm is a PPT algorithm, as desired.

The construction of CRPSF is as follows.

1. **TrapGen**$(1^n, q, \sigma)$: By running the key generation algorithm described above, we get a public key $h = g \cdot f^{-1} \in (R_q)^{\times}$ and a private key $sk = \begin{bmatrix} f & g \\ F & G \end{bmatrix}$. The key h defines function $f_h(\boldsymbol{z}) = f_h((z_1, z_2)) = hz_1 - z_2 \in R_q$ with domain $\mathfrak{D}_n = \{\boldsymbol{z} \in R^2 : ||\boldsymbol{z}|| < s\sqrt{2n}\}$ and range $\mathfrak{R}_n = R_q$. The trapdoor string for f_h is sk.
2. **SampleDom**$(1^n, q, s)$: Sample $\boldsymbol{z} \hookleftarrow D_{R^2,s}$, if $||\boldsymbol{z}|| \geq s \cdot \sqrt{2n}$, resample.
3. **SamplePre**(sk, t): To find a preimage in $\mathfrak{D}_n$ for a target $t \in \mathfrak{R}_n = R_q$ under f_h by using the trapdoor sk, sample $\boldsymbol{z} \hookleftarrow D_{\Lambda_h^q + \boldsymbol{c}, s}$ with $\Lambda_h^q = \{(z_1, z_2) \in R^2 : \ z_2 = hz_1 \bmod qR\}$ and $\boldsymbol{c} = (1, h - t)$. Return $\boldsymbol{z}$.

Regularity result over any fixed cyclotomic field guarantees the uniformity of outputs of our CRPSF. Discrete Gaussian sampler [39] makes it possible that we can sample a preimage of any image with trapdoor basis by using **SamplePre** algorithm for appropriate parameters. Meanwhile, note that for any fixed function f_h and any image t, the preimages of t form the set $\Lambda_h^q + \boldsymbol{c}$ for $\boldsymbol{c} = (1, h - t)$, thus the properties of discrete Gaussian distribution ensure that our design fulfils the requirement of minimum entropy. The collision resistance follows from the hardness of corresponding Ring-SIS problem, even with some additional rejection by the key generation algorithm. Once we get a CRPSF, we can give a provably secure NTRUSign that is strongly existentially unforgeable under adaptive chosen-message attacks, by using the constructions in [17] directly. Like NTRUEncrypt, we constrain our construction of CRPSF (NTRUSign) in cyclotomic fields so that we can use the good basis of R (the powerful basis) and $R^{\vee}$ (the decoding basis). These good bases and canonical embedding help us to bound the key generation algorithm (estimate of norms) and get tighter lower bounds of the module q and security parameter γ (SIVP_γ) by using the same method for any cyclotomic field.

Though it may be a little redundant, we still stress that our CRPSF has two crucial properties for security in cryptographic applications as stated in [17]. First, the output is statistically close to uniform over the range. Second, the **SamplePre** algorithm does not just find an arbitrary preimage of t, but actually samples from among all its preimages under a discrete Gaussian over Λ_h^q. These properties imply that there are two (nearly) equivalent ways of choosing a pair $(\boldsymbol{z}, t = f_h(\boldsymbol{z}))$: either choose $\boldsymbol{z}$ from the input distribution and compute $t = f_h(\boldsymbol{z})$, or choose t uniformly at random and sample $\boldsymbol{z}$ from $f_h^{-1}(t)$. These properties make CRPSF 'as good as' trapdoor permutations in certain applications.

In our constructions, the module q is $\tilde{O}(n^8)$ and the security parameter γ is also $\tilde{O}(n^8)$. Like provably secure NTRUEncrypt, they are too large for practicability. This is a common shortcoming for provably secure NTRU families. Though our construction may be less efficiency, it provides an important support for designing NTRUSign over general cyclotomic rings with relative small parameters (with no provably secure guarantee, but the key generation algorithm is PPT by our results) and analyzing the security from the view of attacks. How to reduce the magnitudes of parameters and improve the efficiency of the schemes are important and meaningful open problems.

1.3 Organization

In Section 2, we introduce some notations and basic results that will be used in our discussion. In Section 3, we give a new series of relevant results about some kinds of q-ary lattices and regularity. These are important for us to analyze the key generation algorithm of our NTRUEncrypt and to construct the NTRUEncrypt in Section 4. In Section 5, we mainly analyze the key generation algorithm of CRPSF and NTRUSign. Detailed construction of CRPSF is put in Section 6. In Section 7, we will discuss the NTRU signature scheme.

2 Preliminaries

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

2.1 Notations

Throughout this paper, l and n are positive integers. Set $\hat{l} = l$ when l is odd and $\hat{l} = \frac{l}{2}$ when l is even. Functions $\varphi(n)$ and $\mu(n)$ stand for the Euler function and the Möbius function. We use $[n]$ to denote the set $\{1, 2, \cdots, n\}$. For $p = 1, 2, \cdots, \infty$, we use $||\cdot||_p$ to represent the l_p norm corresponding to the canonical embedding. When $p = 2$, we usually use $||\cdot||$ to represent the l_2 norm. For any matrix $M \in \mathbb{C}^{n\times n}$, we use $\lambda_i(M)$ stand for its eigenvalues and $s_i(M)$ stand for its singular values for $i \in [n]$. We arrange eigenvalues and singular values by their magnitudes, i.e. $\lambda_1(M) \geq \cdots \geq \lambda_n(M)$ and $s_1(M) \geq \cdots \geq s_n(M)$. For two random variables X and Y, $\Delta(X, Y)$ stands for their statistic distance. As usual, $E(X)$ and $Var(X)$ stand for the expectation and the variance of a random variable X. When we write $X \hookleftarrow \xi$, we mean that the random variable X obeys to a distribution ξ. Function rad represents the radical of a positive integer n, i.e. for $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ with different primes p_i, $rad(n) = \prod_{i=1}^{k} p_i$. If S is a finite set, then $|S|$ is its cardinality and $U(S)$ is the uniform distribution over S. Symbols $\mathbb{Z}^+$ and $\mathbb{R}^+$ stand for the sets of positive integers and positive reals. Symbol $\log x$ represents $\log_2 x$ for $x \in \mathbb{R}^+$.

2.2 Algebraic Fields, Space H and Geometry

Through out this paper, we consider the algebraic fields. Assume $[K : \mathbb{Q}] = n := r_1 + 2r_2$ for $r_1, r_2 \in \mathbb{Z}^+$, there are n embeddings from K to $\mathbb{C}$, the number of real embeddings is r_1 and the number of complex embeddings is $2r_2$. We define the canonical embedding σ on K, who maps $x \in K$ to $(\sigma_1(x), \cdots, \sigma_n(x)) \in H$, where H is a kind of Minkowski space in algebraic number theory. Here we order the σ_i and define $H = \{(x_1, \cdots, x_n) \in \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} : \ x_{n+1-i} = \overline{x_{r_1+i}}, \ \forall i \in [r_2]\}$. H is isomorphic to $\mathbb{R}^n$ as an inner product space via the orthonormal basis $\boldsymbol{h}_{i \in [n]}$ defined as follows. Assume $\boldsymbol{e}_j \in \mathbb{C}^n$ be the vector with 1 in its j-th coordinate and 0 elsewhere, $\boldsymbol{i}$ be an imaginary number which satisfies $\boldsymbol{i}^2 = 1$. We then set $\boldsymbol{h}_j = \boldsymbol{e}_j$ for $1 \leq j \leq r_1$, $\boldsymbol{h}_{r_1+j} = \frac{1}{\sqrt{2}}(\boldsymbol{e}_{r_1+j} + \boldsymbol{e}_{n+1-j})$ and $\boldsymbol{h}_{n+1-j} = \frac{\boldsymbol{i}}{\sqrt{2}}(\boldsymbol{e}_{r_1+j} - \boldsymbol{e}_{n+1-j})$ for $1 \leq j \leq r_2$. Moreover, $\sigma(K) \subseteq H \cong K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$.

For any element $x \in K$, we can define the ℓ_p norm of x by $||x||_p = ||\sigma(x)||_p$ for $p < \infty$ and $||x||_\infty = \max_{i \in [n]} |\sigma_i(x)|$. Because multiplication of embedded elements is component-wise, for any $x, y \in K$, we have $||x \cdot y||_p \leq ||x||_\infty \cdot ||y||_p$ for $p \in \{1, \cdots, \infty\}$. The Trace and Norm of $x \in K$ is defined as usual, i.e. $\mathrm{Tr}(x) := \mathrm{Tr}_{K/\mathbb{Q}}(x) = \sum_{i=1}^{n} \sigma_i(x)$ and $\mathrm{N}(x) := \mathrm{N}_{K/\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x)$. The Norm is multiplicative: $\mathrm{N}(x \cdot y) = \mathrm{N}(x) \cdot \mathrm{N}(y)$. The Trace is $\mathbb{Q}$-linear: $\mathrm{Tr}(x + y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$ and $\mathrm{Tr}(c \cdot x) = c \cdot \mathrm{Tr}(x)$ for all $x, y \in K$ and $c \in \mathbb{Q}$. Also note that $\mathrm{Tr}(x \cdot y) = \sum_{i=1}^{n} \sigma_i(x)\sigma_i(y) =< \sigma(x), \overline{\sigma(y)} >$, so $\mathrm{Tr}(x \cdot y)$ is a symmetric bilinear form akin to the inner product of embeddings of x and y.

The discriminant Δ_K of K is a measure of the geometry sparsity of its ring of integers. Let $\alpha_1, \cdots, \alpha_n$ represent a $\mathbb{Z}$ basis of R, we can define $\Delta_K = |(\sigma_i(\alpha_j))_{1 \leq i,j \leq n}|^2$, where $|\cdot|$ represents the determinant of a matrix. In particular, the discriminant of the l-th cyclotomic number field is

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

where p runs over all prime factors of l and $n = \varphi(l)$. An integral ideal $I \subseteq R$ is a usual ideal defined in the ring R and a fractional ideal $J \subseteq K$ is a set such that $dJ \subseteq R$ is an integral ideal for some $d \in R$. It is well known that both I and J admit $\mathbb{Z}$-basis and we can require $d \in \mathbb{Z}$. One can regard integral ideals as special cases of fractional ideals. For any two fractional ideals I and J, the sum $I + J$ is the set of all $a + b$ for $a \in I$ and $b \in J$, and the product ideal $I \cdot J$ is the set of all finite sums of terms ab for $a \in I$ and $b \in J$. Multiplication extends to fractional ideals in the obvious way and the set of fractional ideals forms a group under multiplication. Every fractional ideal can be represented as the quotient of two coprime integral ideals and has an inverse ideal, written I^{-1}, such that $I \cdot I^{-1} = R$.

The norm of an integral ideal is its index as an additive subgroup of R and the norm of a fractional ideal $J = A/B$ is defined as $\mathrm{N}(J) = \frac{\mathrm{N}(A)}{\mathrm{N}(B)}$, where A and B are coprime integral ideals of R.

Assume $K = \mathbb{Q}(\alpha)$, then for any positive prime q, the ideal qR has a prime ideal decomposition of the form $qR = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i}$. More precisely, assume that $\Phi(x)$ is the minimum polynomial of α over $\mathbb{Q}$, if $q \nmid |R/\mathbb{Z}[\alpha]|$, $\Phi(x) = \prod_{i=1}^{g} \Phi_i^{e_i}(x) \bmod q$. Each $\Phi_i(x)$ is a monic irreducible polynomial in $\mathbb{Z}_q[x]$ with $\deg(\Phi_i(x)) = f_i$. $\mathfrak{q}_i = (q, \Phi_i(x))R$ and the norm of $\mathfrak{q}_i$ is q^{f_i}. We also have $\sum_{i=1}^{g} e_i f_i = n$. When $K/\mathbb{Q}$ is a Galois extension, we have $e_1 = \cdots = e_g$ and $f_i = \cdots = f_g$, i.e. $efg = n$.

When $K = \mathbb{Q}(\zeta)$ is a cyclotomic field, where $\zeta = \zeta_l$ is a primitive l-th root of unity with minimal polynomial $\Phi_l(x) = \prod_{i|l}(x^i - 1)^{\mu(\frac{l}{i})}$ of degree $n = \varphi(l)$, we have $[K : \mathbb{Q}] = n = \varphi(l)$, and $K \cong \mathbb{Q}[x]/\Phi_l(x)$. Let $q \in \mathbb{Z}$ be a prime, then the factorization of the ideal qR is as follows. Let $d \geq 0$ be the largest integer such that q^d divides l, let $e = \varphi(q^d)$ and let $f \geq 1$ be the multiplicative order of q modulo l/q^d. Then $qR = \prod_{i=1}^{g} \mathfrak{q}_i^{e}$, where $\mathfrak{q}_i$ are $g = n/(ef)$ different prime ideals, each of norm q^f.

2.3 Lattice and Discretization

We define a lattice as a discrete additive subgroup of H and we only deal with full-rank lattices. Assume $B = \{\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\}$ is a basis of a lattice Λ, we have $\Lambda = \mathcal{L}(B) = \{\sum_{i=1}^{n} z_i \boldsymbol{b}_i \ : \ z_i \in \mathbb{Z}\}$. The determinant of a lattice $\mathcal{L}(B)$ is defined as $|\det(B)|$, which is independent of the choice of basis B. The minimum distance $\lambda_1(\Lambda)$ of a lattice is the length of a shortest nonzero lattice vector. We usually use the l_2 norm, i.e. $\lambda_1(\Lambda) = \min_{0 \neq \boldsymbol{x} \in \Lambda} ||\boldsymbol{x}||$. The dual lattice of $\Lambda \subseteq H$ is defined as $\Lambda^\vee = \{\boldsymbol{y} \in H : \ \forall \ \boldsymbol{x} \in \Lambda, \ < \boldsymbol{x}, \overline{\boldsymbol{y}} >= \sum_{i=1}^{n} x_i y_i \in \mathbb{Z}\}$. This is actually the complex conjugate of the dual lattice as usually defined in $\mathbb{C}^n$. All of the properties of the dual lattice that we use also hold for the conjugate dual. It is easy to see that $(\Lambda^\vee)^\vee = \Lambda$. If $B = \{\boldsymbol{b}_i\} \subseteq H$ is a basis of a lattice, its dual basis $D = \{\boldsymbol{d}_j\}$ is characterized by $< \boldsymbol{b}_i, \overline{\boldsymbol{d}_j} >= \delta_{ij}$, where δ_{ij} is the Kronecker delta. It is obvious that $\mathcal{L}(D) = \mathcal{L}(B)^\vee$.

For any fractional ideal I of K, we can represent I as $\mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n$ for some $\beta_i \in K$, $i = 1, \cdots, n$. Then $\sigma(I)$ is a lattice of H, and we call $\sigma(I)$ an ideal lattice and identify I with this lattice and associate with I all the usual lattice quantities. We have $|\Delta_K| = \det(\sigma(R))^2$, the squared determinant of the lattice $\sigma(R)$. We also have $\det(\sigma(I)) = \mathrm{N}(I) \cdot \sqrt{|\Delta_k|}$. The following lemma from [27] gives upper and lower bounds on the minimum distance of an ideal lattice in l_2 norm.

Lemma 2.1. *For any fractional ideal I in a number field K of degree n,*

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

For any fractional ideal I in K, its dual is defined as $I^\vee = \{a \in K : \ \mathrm{Tr}(aI) \subseteq \mathbb{Z}\}$. It is easy to verify $(I^\vee)^\vee = I$, $I^\vee$ is a fractional ideal and $I^\vee$ embeds under σ as the dual lattice of I as defined before. In fact, an ideal of K and its inverse are related by multiplication with the dual ideal $R^\vee$: $I^\vee = I^{-1} \cdot R^\vee$. The factor $R^\vee$ is often called the codifferent, and its inverse $(R^\vee)^{-1}$-the different, which is in fact an ideal in R. For more details, one can refer to [6].

One of the most famous lattice problems is SVP. Given a lattice basis B, try to find a shortest vector in $\Lambda \backslash \{0\}$, where $\Lambda = \mathfrak{L}(B)$. The relaxed problem SVP_γ is asking for a nonzero lattice vector that is no longer than γ times the length of a solution of SVP. By restricting SVP to the ideal lattice, we obtain Ideal-SVP. No polynomial quantum algorithm is known to solve the worst-case SVP_γ problem for $\gamma \leq \mathrm{poly}(n)$ and also no algorithm is known to perform non-negligibly better for ideal lattices than classic lattices. The (Ideal-SIVP_γ) SIVP_γ problem is that given a basis of a lattice Λ of dimension n, try to find n linear independent vectors $x_1, \cdots, x_n \in \Lambda$ such that $\max_{1 \leq i \leq n} ||x_i|| \leq \gamma \cdot \lambda_n(\Lambda)$.

We now consider the discretization. As in [28], the goal of discretization is to convert a continuous Gaussian into a Gaussian-like distribution. Given a lattice $\Lambda = \mathcal{L}(B)$, a point $\boldsymbol{x} \in H$ and a point $\boldsymbol{c} \in H$ representing a lattice coset $\Lambda + \boldsymbol{c}$, we want to discretize $\boldsymbol{x}$ to a point $\boldsymbol{y} \in \Lambda + \boldsymbol{c}$, written $\boldsymbol{y} = \lfloor \boldsymbol{x} \rceil_{\Lambda + \boldsymbol{c}}$. Here $\lfloor \cdot \rceil$ denote some kinds of discretization operations. We hope the length of $\boldsymbol{y} - \boldsymbol{x}$ is not too large. To do this, we can sample a relatively short vector $\boldsymbol{f}$ from $\Lambda + (\boldsymbol{c} - \boldsymbol{x})$, and output $\boldsymbol{y} = \boldsymbol{f} + \boldsymbol{x}$. We require that the method used to choose $\boldsymbol{f}$ be efficient and depend only on the desired coset $\Lambda + (\boldsymbol{c} - \boldsymbol{x})$. Such a procedure is called valid.

Three easy methods were described in [28]. We describe the formal definition as in [32], a modified version of [28]. Define $\lceil x \rceil$ to be the smallest integer that is bigger than or equal to x for any $x \in \mathbb{R}$.

Definition 2.2. *If Bern denotes the Bernoulli distribution, then the univariate Reduction distribution $Red(a) = Bern(\lceil a \rceil - a) - (\lceil a \rceil - a)$ is the discrete probability distribution defined for parameter $a \in \mathbb{R}$ as taking the values*

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

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

We now describe the coordinate-wise rounding discretisation which is easy to use for our applications. One can check the following definition defines a valid discretisation, more details are in [32].

Definition 2.3. *Suppose $\Lambda = \mathcal{L}(B)$ is a n-dimensional lattice in space H. For $\boldsymbol{c} \in H$, the coordinate-wise randomized rounding discretisation $\lfloor \boldsymbol{X} \rceil^B_{\Lambda + \boldsymbol{c}}$ of random variable $\boldsymbol{X}$ to the lattice coset $\Lambda + \boldsymbol{c}$ with respect to the basis B is then defined by the conditional random variable*

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

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

2.4 Basis for R and $R^\vee$

In our application, we hope that the matrices whose columns are consisted of the basis of R or $R^\vee$ have smaller s_1 and larger s_n. So, we introduce the powerful basis and the decoding basis as in [28]. We set τ be the automorphism of K that maps ζ_l to $\zeta_l^{-1} = \zeta_l^{l-1}$, under the canonical embedding it corresponds to complex conjugation $\sigma(\tau(a)) = \overline{\sigma(a)}$.

Definition 2.4. *The Powerful basis $\vec{p}$ of $K = \mathbb{Q}(\zeta_l)$ and $R = \mathbb{Z}[\zeta_l]$ is defined as follows:*

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

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

Also note that $\tau(\vec{p})$ is a $\mathbb{Z}$-basis of R. Different bases of R (or $R^\vee$) are connected by some unimodular matrice, hence the spectral norm (i.e. the s_1) may have different magnitudes. The following lemma comes from [28], which shows the estimates of $s_1(\sigma(\vec{p}))$ and $s_n(\sigma(\vec{p}))$.

Lemma 2.5. *We have $s_1(\sigma(\vec{p})) = \sqrt{\hat{l}}$, $s_n(\sigma(\vec{p})) = \sqrt{\frac{l}{rad(l)}}$, $||\sigma(\vec{p})_i||_\infty = 1$ and $||\sigma(\vec{p})_i|| = \sqrt{n}$ for all $i = 1, \cdots, n$.*

We also need the estimates of $s_1(\sigma(\vec{d}))$ and $s_n(\sigma(\vec{d}))$. Assume that $\sigma(\vec{p}) = T$, Lemma 2.5 shows that $s_1(T) = \sqrt{\hat{l}}$ and $s_n(T) = \sqrt{\frac{l}{rad(l)}}$. By the definitions of $\vec{d}$ and the dual ideal, an easy computation shows that $\sigma(\vec{d}) = (T^*)^{-1}$. Hence we have $s_n(\sigma(\vec{d})) = \frac{1}{\sqrt{\hat{l}}}$, $s_1(\sigma(\vec{d})) = \sqrt{\frac{rad(l)}{l}}$. Moreover, one can similarly deduce that $||\sigma(\vec{d})_i|| \leq \sqrt{\frac{rad(l)}{l}}$ for all $i = 1, 2, \cdots, n$. The following definition is also useful.

Definition 2.6. *Given a basis B of a fractional ideal J, for any $x \in J$ with $x = x_1 b_1 + \cdots + x_n b_n$, the B-coefficient embedding of x is defined as the vector $(x_1, \cdots, x_n)$ and the B-coefficient embedding norm of x is defined as $||x||_B^c = (\sum_{i=1}^n x_i^2)^{\frac{1}{2}}$.*

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

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

and

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

We will omit the subscript $\sigma(\vec{d})$ of $||\cdot||^c_{\sigma(\vec{d})}$ in the following applications.

When we write $x \bmod qR^\vee$, we use the representative element of the coset $x + qR^\vee$ as $\sum_{i=1}^{n} x_i \vec{d_i}$ with $x_i \in [-\frac{q}{2}, \frac{q}{2})$. Similarly, for element $x \in R$, if we write $x \bmod qR$, we use the representative element of the coset $x + qR$ as $\sum_{i=1}^{n} x_i \vec{p_i}$ with $x_i \in [-\frac{q}{2}, \frac{q}{2})$. Notice that $R \subseteq R^\vee$, any element of R can also be represented as a $\mathbb{Z}$-linear combination of the decoding basis. From now on, we only use the decoding basis of $R^\vee$ and the powerful basis of R.

2.5 Gaussian Distributions

For $s > 0$, $\boldsymbol{c} \in H$, define the Gaussian function $\rho_{s,\boldsymbol{c}} : H \to (0, 1]$ as $\rho_{s,\boldsymbol{c}}(\boldsymbol{x}) = e^{-\pi \frac{||\boldsymbol{x}-\boldsymbol{c}||^2}{s^2}}$. By normalizing this function we obtain the continuous Gaussian probability distribution $D_{s,\boldsymbol{c}}$ of parameter s, whose density is given by $s^{-n} \cdot \rho_{s,\boldsymbol{c}}(\boldsymbol{x})$. We usually omit the subscript $\boldsymbol{c}$ when it is $\mathbf{0}$. Let $\boldsymbol{\sigma} = (\sigma_1, \cdots, \sigma_n) \in (\mathbb{R}^+)^n$ be a vector such that $\sigma_{r_1+j} = \sigma_{n+1-j}$ for $j \in \{1, \cdots, r_2\}$, we can define the elliptical Gaussian distributions in the basis $\{\boldsymbol{h}_i\}_{i \le n}$ as follows: a sample from $D_{\boldsymbol{r}}$ is given by $\sum_{i\in[n]} x_i \boldsymbol{h}_i$, where x_i are chosen independently from the Gaussian distribution D_{σ_i} over $\mathbb{R}$. Note that, if we define a map $\varphi : H \to \mathbb{R}^n$ by $\varphi(\sum_{i\in[n]} x_i \boldsymbol{h}_i) = (x_1, \cdots, x_n)$, then $D_{\boldsymbol{\sigma}}$ is also a (elliptical) Gaussian distribution over $\mathbb{R}^n$.

For a lattice $\Lambda \subseteq H$, $\sigma > 0$ and $\boldsymbol{c} \in H$, we define the lattice Gaussian distribution of support Λ, deviation σ and center $\boldsymbol{c}$ by $D_{\Lambda,\sigma,\boldsymbol{c}}(\boldsymbol{x}) = \frac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{\sigma,\boldsymbol{c}}(\Lambda)}$, for any $\boldsymbol{x} \in \Lambda$. For $\delta > 0$, we define the smoothing parameter $\eta_\delta(\Lambda)$ as the smallest $\sigma > 0$ such that $\rho_{\frac{1}{\sigma}}(\Lambda^\vee \setminus \mathbf{0}) \le \delta$. For σ large enough, it is possible to efficiently sample according to a discrete Gaussian distribution. In [39], an efficient algorithm is proposed to sample an element from $D_{\Lambda,\sigma,\boldsymbol{c}}$. Here we use $\tilde{B}$ to represent the Gram-Schmidt orthogonalization of B and regard the columns of B as a set of vectors. For $B = (b_1, \cdots, b_n)$, define $||B|| = \max_i ||b_i||$.

Theorem 2.7. *There is a probabilistic polynomial time algorithm that, given a basis B of an n-dimensional lattice $\Lambda = \mathcal{L}(B)$, a standard deviation $\sigma \ge ||\tilde{B}|| \cdot \sqrt{\log n}$, and a $\boldsymbol{c} \in H$, outputs a sample whose distribution is $D_{\Lambda,\sigma,\boldsymbol{c}}$.*

We will use following lemmas from [33], [38], [3], [17] and [41].

Lemma 2.8. *For any full-rank lattice Λ and positive real $\varepsilon > 0$, we have $\eta_\varepsilon(\Lambda) \le \sqrt{\frac{\ln(2n(1+\frac{1}{\varepsilon}))}{\pi}} \cdot \lambda_n(\Lambda)$.*

Lemma 2.9. *For any full-rank lattice Λ, $\boldsymbol{c} \in H$, $\varepsilon \in (0, 1)$ and $\sigma \ge \eta_\varepsilon(\Lambda)$, we have $\Pr_{\boldsymbol{b} \hookleftarrow D_{\Lambda,\sigma,\boldsymbol{c}}}[||\ \boldsymbol{b} - \boldsymbol{c}|| \ge \sigma\sqrt{n}] \le \frac{1+\varepsilon}{1-\varepsilon} \cdot 2^{-n}$.*

Lemma 2.10. *For any full-rank lattice Λ and any positive real $\varepsilon > 0$, we have $\eta_\varepsilon(\Lambda) \le \sqrt{\frac{\ln(2n(1+\frac{1}{\varepsilon}))}{\pi}} \cdot \frac{1}{\lambda_1^\infty(\Lambda^\vee)}$.*

Lemma 2.11. *Let B_n denote the Euclidean unit open ball. Then for any lattice Λ, $\sigma > 0$ and $c \geq \frac{\sigma}{\sqrt{2\pi}}$, we have*

$$\rho_\sigma(\Lambda \backslash (c\sqrt{n}B_n)) < (\frac{c}{\sigma} \cdot \sqrt{2\pi e} \cdot e^{-\pi \frac{c^2}{\sigma^2}})^n \cdot \rho_\sigma(\Lambda).$$

Hence, $\Pr_{\boldsymbol{x} \hookleftarrow D_{\Lambda,\sigma}}(||\boldsymbol{x}|| \geq \sqrt{n}\sigma) < 2^{-2n}$.

Lemma 2.12. *Let $\Lambda^{'} \subseteq \Lambda$ be full-rank lattices. For any $\boldsymbol{c} \in H$, $\varepsilon \in (0, 1/2)$ and $\sigma \geq \eta_\varepsilon(\Lambda^{'})$, we have $\Delta(D_{\Lambda,\sigma,\boldsymbol{c}} \mod \Lambda^{'}, U(\Lambda/\Lambda^{'})) \leq 2\varepsilon$.*

Lemma 2.13. *For any full-rank lattice $\Lambda \subseteq H$, $\boldsymbol{c} \in H$, $\delta \in (0, 1)$, $\sigma \geq 2\eta_\delta(\Lambda)$ and $\boldsymbol{b} \in \Lambda$, we have $D_{\Lambda,\sigma,\boldsymbol{c}}(\boldsymbol{b}) \leq \frac{1+\delta}{1-\delta} \cdot 2^{-n}$.*

We also need the following adapted result on one-dimensional projections of discrete Gaussians, which is proposed in [46]. It is helpful for us to estimate the norm of x^{-1} with $x \hookleftarrow D_{R,\sigma}$.

Lemma 2.14. *For any full-rank lattice $\Lambda \subseteq H$ (or $\mathbb{R}^n$), $\boldsymbol{c} \in H$ (or $\mathbb{R}^n$), $\delta \in (0, 1)$, $t \geq \sqrt{2\pi}$, unit vector $\boldsymbol{u} \in H$ (or $\mathbb{R}^n$) and $\sigma \geq \frac{t}{\sqrt{2\pi}} \cdot \eta_\delta(\Lambda)$, we have*

$$\Pr_{\boldsymbol{x} \hookleftarrow D_{\Lambda,\sigma,\boldsymbol{c}}}(| < \boldsymbol{x} - \boldsymbol{c}, \boldsymbol{u} > | \leq \frac{\sigma}{t}) \leq \frac{1+\delta}{1-\delta} \cdot \frac{\sqrt{2\pi}}{t} \cdot e^{\frac{1}{2} - \frac{\pi}{t^2}} \leq \frac{1+\delta}{1-\delta} \cdot \frac{\sqrt{2\pi e}}{t}.$$

Similarly, if $\sigma \geq \eta_\delta(\Lambda)$, we have

$$\Pr_{\boldsymbol{x} \hookleftarrow D_{\Lambda,\sigma,\boldsymbol{c}}}(| < \boldsymbol{x} - \boldsymbol{c}, \boldsymbol{u} > | \geq t\sigma) \leq \frac{1+\delta}{1-\delta} \cdot t \cdot \sqrt{2\pi e} \cdot e^{-\pi t^2}.$$

Now we can give a lower bound of $||x^{-1}||$ for $x \hookleftarrow D_{R,\sigma}$ with R the ring of integers of a cyclotomic field K. It is an adapted version of Lemma 4.1 in [46].

Lemma 2.15. *Let K be a cyclotomic field, $R = \mathcal{O}_K$, $\delta \in (0, 1)$, $t \geq \sqrt{2\pi}$ and $\sigma \geq \frac{t}{\sqrt{2\pi}} \cdot \eta_\delta(R)$, we have*

$$\Pr_{x \hookleftarrow D_{R,\sigma}}(||x^{-1}|| \geq \frac{\sqrt{2}t}{\sigma}) \leq \frac{1+\delta}{1-\delta} \cdot \frac{n \cdot \sqrt{2\pi e}}{t}.$$

Proof. For any $x \hookleftarrow D_{R,\sigma}$, assume $x = x_1\alpha_1 + \cdots + x_n\alpha_n$, where $\alpha_1, \cdots, \alpha_n \in I$ are the power basis of R and $x_i \in \mathbb{Z}$ for $i \in [n]$. For any $k \in [n]$, we have $\mathrm{Re}(\sigma_k(x)) = \sum_{j=1}^n x_j \mathrm{Re}(\sigma_k(\alpha_j))$ and $\mathrm{Im}(\sigma_k(x)) = \sum_{j=1}^n x_j \mathrm{Im}(\sigma_k(\alpha_j))$. Let $\mathrm{Re}^2 = \sum_{j=1}^n \mathrm{Re}(\alpha_j)^2$ and $\mathrm{Im}^2 = \sum_{j=1}^n \mathrm{Im}(\alpha_j)^2$. By using Lemma 2.14 twice, setting $\boldsymbol{c} = \sigma(x) - (x_1, \cdots, x_n)^T \in H$, $\boldsymbol{u} = (\frac{(\mathrm{Re}(\sigma_k(\alpha_1))}{\mathrm{Re}}, \cdots, \frac{\mathrm{Re}(\sigma_k(\alpha_n))}{\mathrm{Re}})^T$ or $\boldsymbol{u} = (\frac{\mathrm{Im}(\sigma_k(\alpha_1))}{\mathrm{Im}}, \cdots, \frac{\mathrm{Im}(\sigma_k(\alpha_n))}{\mathrm{Im}})^T$ correspondingly, we obtain $\Pr(\left|\frac{\mathrm{Re}(\sigma_k(x))}{\mathrm{Re}}\right| \leq \frac{\sigma}{t}) \leq \frac{1+\delta}{1-\delta} \cdot \frac{\sqrt{2\pi e}}{t}$ and $\Pr(\left|\frac{\mathrm{Im}(\sigma_k(x))}{\mathrm{Im}}\right| \leq \frac{\sigma}{t}) \leq \frac{1+\delta}{1-\delta} \cdot \frac{\sqrt{2\pi e}}{t}$. Noticing that $\mathrm{Re}^2 + \mathrm{Im}^2 = n$, which implies that $\max(\mathrm{Re}, \mathrm{Im}) \geq \sqrt{\frac{n}{2}}$. Without loss of generality, assume $\mathrm{Re} \geq \mathrm{Im}$, we have

$$\Pr(|\mathrm{Re}(\sigma_k(x))| \leq \frac{\sigma}{t} \cdot \sqrt{\frac{n}{2}}) \leq \Pr(|\mathrm{Re}(\sigma_k(x))| \leq \frac{\sigma}{t} \cdot \mathrm{Re}) \leq \frac{1+\delta}{1-\delta} \cdot \frac{\sqrt{2\pi e}}{t},$$

Therefore, we get

$$\Pr(|\sigma_k(x)| \leq \frac{\sigma \cdot \sqrt{\frac{n}{2}}}{t}) \leq \Pr(|\mathrm{Re}(\sigma_k(x))| \leq \frac{\sigma}{t} \cdot \sqrt{\frac{n}{2}}) \leq \frac{1+\delta}{1-\delta} \cdot \frac{\sqrt{2\pi e}}{t}.$$

This is equivalent to

$$\Pr(|\sigma_k(x^{-1})| \geq \frac{t}{\sigma \cdot \sqrt{\frac{n}{2}}}) \leq \frac{1+\delta}{1-\delta} \cdot \frac{\sqrt{2\pi e}}{t}.$$

Hence, the union bound gives us the estimation that

$$\Pr(||x^{-1}|| \geq \frac{\sqrt{2}t}{\sigma}) \leq \frac{1+\delta}{1-\delta} \cdot \frac{n \cdot \sqrt{2\pi e}}{t},$$

as we desired. □

2.6 Ring-SIS and Ring-LWE Problems

In this subsection, we state some hard lattice problems we need. We first introduce the small integer solution problem over algebraic number fields. The definitions are as follows.

Definition 2.16. *Let R be the ring of integers of K, q, m be positive integers and β be a real number.*

- *The ring small integer solution problem* ($\text{R-SIS}_{q,m,\beta}$) *is: given $a_1, \cdots, a_m \in R_q$ chosen independently from the uniform distribution, find $\boldsymbol{z} = (z_1, \cdots, z_m) \in R^m$ such that $\sum_{i=1}^m a_i z_i = 0 \bmod qR$ and $0 < ||\boldsymbol{z}|| \leq \beta$.*
- *The ring inhomogeneous small integer solution problem* ($\text{R-ISIS}_{q,m,\beta}$) *is: given $a_i \hookleftarrow U(R_q)$ for $i = 1, \cdots, m$ and $u \hookleftarrow U(R_q)$, find $\boldsymbol{z} = (z_1, \cdots, z_m) \in R^m$ such that $\sum_{i=1}^m a_i z_i = u \bmod qR$ and $||\boldsymbol{z}|| \leq \beta$.*

For appropriate parameters, the following theorem shows that the Ring-SIS problem is hard [29].

Theorem 2.17. *For $\varepsilon = \varepsilon(n) = n^{-\omega(1)} \in (0,1)$, there is a probabilistic polynomial time reduction from solving* $\text{Ideal-SIVP}_{\gamma \cdot \sqrt{\frac{\ln(2n(1+\frac{1}{\varepsilon}))}{\pi}}}$ *with high probability in polynomial time in the worst case to solving* $\text{R-SIS}_{q,m,\beta}$ *with non-negligible probability in polynomial time, for any m, q, β, γ such that $\gamma \geq \beta\sqrt{n} \cdot \omega(\sqrt{\log n})$, $q \geq \beta\sqrt{n} \cdot \omega(\log n)$ and $m, \beta, \log q \leq \mathrm{poly}(n)$.*

We also need to introduce the Ring-LWE problem. Let $\mathbb{T} = K_{\mathbb{R}}/R^{\vee}$.

Definition 2.18. *For $s \in R_q^{\vee}$ and an error distribution ψ over $K_{\mathbb{R}}$, the* Ring-LWE *distribution $A_{s,\psi}$ over $R_q \times \mathbb{T}$ is sampled by independently choosing a uniformly random $a \hookleftarrow U(R_q)$ and an error term $e \hookleftarrow \psi$, and outputting $(a, b = \frac{a \cdot s}{q} + e \bmod R^{\vee})$.*

Definition 2.19. *Let Ψ be a family of distributions over $K_{\mathbb{R}}$.*

- *The average-case* Ring-LWE *search problem, denoted R-LWE$_{q,\Psi}$, is given access to arbitrarily many independent samples from $A_{s,\psi}$ for some arbitrary $s \in R_q^\vee$ and $\psi \in \Psi$, find s.*
- *The average-case* Ring-LWE *decision problem, denoted R-DLWE$_{q,\Psi}$, is to distinguish (with non-negligible advantage) between independent samples from $A_{s,\psi}$ for a random choice of $(s, \psi) \hookleftarrow U(R_q^\vee) \times \Psi$, and the same number of uniformly random and independent samples from $R_q \times \mathbb{T}$.*

There is a large disparity between known hardness theorems for search and decision Ring-LWE. From [27] and [29], the reduction from worst-case ideal lattice problems (such as SIVP$_\gamma$) to search Ring-LWE problem is tenable in any algebraic number field and any modulus for approximate parameter choices. While the hardness of decision Ring-LWE is reduced to search Ring-LWE and the search-to-decision reduction works only for cyclotomic fields and requires that the module q 'split' well. Usually, we require $q = 1 \bmod n$ for a n-dimension extension of field. In [42], a reduction from SIVP$_\gamma$ to decision Ring-LWE over any algebraic number field is given. Also, the requirement of q is eliminated.

Theorem 2.20. *Let K be an algebraic number field and $R = \mathcal{O}_K$, $[K : \mathbb{Q}] = n$. Assume $\alpha \in (0, 1)$ such that $\alpha \leq \sqrt{\frac{\log n}{n}}$, and let $q \geq 2$ be an integer such that $\alpha q \geq \omega(1)$. Then there is a polynomial time quantum reduction from Ideal-SIVP$_\gamma$ to R-DLWE$_{q,D_\xi}$, where $\xi = \alpha(\frac{nk}{\log(nk)})^{\frac{1}{4}}$ with k the number of samples to be used and $\gamma = \omega(\frac{\sqrt{n}\cdot\log n}{\alpha})$.*

We can modify the sample (a, b) of Ring-LWE distribution to the set $R_q \times R_q^\vee$ as in [47]. We scale the b component by a factor of q, so that it is an element of $K_{\mathbb{R}}/(qR^\vee)$. The corresponding error distribution is $D_{q\xi}$ with $\xi = \alpha \cdot (\frac{nk}{\log{(nk)}})$ and k the number of samples. Then we discretize the error, by taking $e \hookleftarrow \lfloor D_{q\xi} \rceil$. The decision version of Ring-LWE becomes to distinguish between the modified distribution of $A_{s,\lfloor D_{q\xi} \rceil}$ and the uniform samples from $R_q \times R_q^\vee$. Notice that by using the same method proposed in [28], we can change the secret s to obey the error's distribution, i.e. $s \hookleftarrow \lfloor D_{q\xi} \rceil$. At last, if we restrict $a \in R_q^\times$, the difficult of this problem does not decrease. We use symbol $A^\times_{s,D_{q\xi}}$ to denote the distribution of (a, b) obtained by choosing $a \hookleftarrow U(R_q^\times)$, $s \hookleftarrow \lfloor D_{q\xi} \rceil$, $e \hookleftarrow \lfloor D_{q\xi} \rceil$ and $b = a \cdot s + e$. We will use the symbol R-DLWE$^\times_{q,D_{q\xi}}$ to denote the problem of distinguish the samples from $A^\times_{s,D_{q\xi}}$ and $U(R_q^\times \times R_q^\vee)$.

3 Analysis of q-Ary Lattices and Improved Results of Regularity

In this section, we shall prove some useful results. We assume that $K = \mathbb{Q}(\alpha)$ is an algebraic field which is a Galois extension over $\mathbb{Q}$, $[K : \mathbb{Q}] = n$ and $R = \mathcal{O}_K$. Let $\Phi(x)$

be the minimum polynomial of α over $\mathbb{Q}$, q is a prime such that $q \nmid |R/\mathbb{Z}[\alpha]|$ and $q \nmid \Delta_K$. Meanwhile, assume that the prime ideal decomposition of qR is known. All the proofs in this section are essentially the same as those in [47], so we put them in Appendix A.

We first describe an isomorphism theorem which is helpful for us to analyse the q-ary lattices we need. In some textbooks, it is called the fourth isomorphism theorem or lattice isomorphism theorem. We only describe its ring's version. In the cases of groups and modules, the results are almost the same.

Proposition 3.1. *Let R be a ring and B an ideal of R. Then every subring of R/B is of the form A/B, for some subring A of R such that $B \subseteq A \subseteq R$, the corresponding relation is* 1-1. *In particular, every ideal of R/B is of the form A/B, for some ideal A of R such that $B \subseteq A \subseteq R$.*

We know that $R_q = \mathbb{Z}_q[x]/\Phi(x)$ and $\mathbb{Z}_q[x]$ is a principal ideal domain, hence R_q is a principal ideal ring. Recall that for any fixed prime $q \nmid |R/\mathbb{Z}[\alpha]|$ and $q \nmid \Delta_K$, $\Phi(x) = \Phi_1(x) \cdots \Phi_g(x) \bmod q$ with $\deg(\Phi_i(x)) = f$ for $i \in [g]$. Meanwhile, $qR = \mathfrak{q}_1 \cdots \mathfrak{q}_g$ with $\mathfrak{q}_i = (q, \Phi_i(x))R$ and $\mathrm{N}(\mathfrak{q}_i) = q^f$ for $i = 1, \cdots, g$.

For any proper ideal $I \in R_q$, we can write $I = (f(x))R_q$, where $f(x)$ contains at least one polynomials of $\Phi_i(x)$, i.e. $f(x) = \prod_{i \in S} \Phi_i(x)$ for some non-empty $S \subseteq \{1, 2, \cdots, g\}$. We will use I_S to represent the ideal $\prod_{i \in S} \Phi_i(x) R_q$ of R_q.

3.1 q-Ary Lattices

We first introduce a simple relation. Let I be a proper ideal of R_q, by Proposition 3.1, there is an ideal J of R such that $qR \subseteq J \subseteq R$ and $I = J/qR$. Considering the relation $qJ \subseteq qR \subseteq J \subseteq R$, we get $R^\vee \subseteq J^\vee \subseteq (qR)^\vee \subseteq (qJ)^\vee$, which implies $R^\vee \subseteq J^\vee \subseteq \frac{1}{q}(R)^\vee \subseteq \frac{1}{q}(J)^\vee$. Thus we get an R module inclusion relations

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

Moreover, $R^\vee/qJ^\vee$ is an R submodule of $J^\vee/qJ^\vee$. Notice that for $I_S = \prod_{i \in S} \Phi_i(x) R_q$, we have $J_S = \prod_{i \in S} \mathfrak{q}_i$.

Now, we define the q-ary lattices we need for our analysis of public key distribution in Section 4. Let $\boldsymbol{a} \in (R_q)^m$, the definitions of the q-ary lattices are as followings:

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

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

Here, $R^\vee \cdot \boldsymbol{a} = \{t \cdot \boldsymbol{a} = (ta_1, \cdots, ta_m) : t \in R^\vee\}$. It is easy to see that both $\boldsymbol{a}^\perp(I)$ and $L(\boldsymbol{a}, I)$ are well-defined and are R modules, hence the value s can take over all elements in $R^\vee$. We also define $\boldsymbol{a}^\perp$ and $L(\boldsymbol{a})$ as $\boldsymbol{a}^\perp(R_q)$ and $L(\boldsymbol{a}, R_q)$. The dual $M^\vee$ of a lattice $M \subseteq K^m$ is defined as the set of all $\boldsymbol{x} \in K^m$ such that $\mathrm{Tr}(\boldsymbol{a} \cdot \boldsymbol{v}) := \sum_{j=1}^m \mathrm{Tr}(x_j \cdot v_j) \in \mathbb{Z}$ for all $\boldsymbol{v} \in M$. The following lemma shows the dual relations between $\boldsymbol{a}^\perp(I)$ and $L(\boldsymbol{a}, I)$.

Lemma 3.2. *Let $\boldsymbol{a}^\perp(I)$ and $L(\boldsymbol{a}, I)$ be defined above, then we have $\boldsymbol{a}^\perp(I) = q(L(\boldsymbol{a}, I))^\vee$ and $L(\boldsymbol{a}, I) = q(\boldsymbol{a}^\perp(I))^\vee$.*

3.2 Lower Bound of λ_1^∞ in $L(a, I)$

Let $I_S = \prod_{i \in S} \Phi_i(x) R_q \subseteq R_q$ and $J_S = \prod_{i \in S} \mathfrak{q}_i \subseteq R$ for $S \subseteq \{1, 2, \cdots, g\}$. We have $qR \subseteq J_S \subseteq R$ and $I_S = J_S / qR$. Further, $J_S^{-1} = \prod_{i \in S} \mathfrak{q}_i^{-1}$ and $J_S^\vee = \prod_{i \in S} \mathfrak{q}_i^{-1} R^\vee$.

Now we can give a lemma which shows that for $\boldsymbol{a} \hookleftarrow U((R_q^\times)^m)$, the lattice $L(\boldsymbol{a}, I_S)$ is extremely unlikely to contain unusually short vectors for the infinity norm.

Lemma 3.3. *Let $m \geq 2$ and $\varepsilon > 0$, assume $\Phi(x) = \prod_{i=1}^g \Phi_i(x)$ and $I_S = \prod_{i \in S} \Phi_i(x) R_q$ for any $S \subseteq [g]$, then we have $\lambda_1^\infty(L(\boldsymbol{a}, I_S)) \geq B$ with $B = \frac{q^\beta}{|\Delta_K|^{\frac{1}{n}}}$, where $\beta = (1 - \frac{1}{m})(1 - \frac{|S|}{g}) - \varepsilon$, except with probability $p \leq 2^{2m(n+g)} q^{-\varepsilon mn}$ over the uniformly random choice of $\boldsymbol{a} \in (R_q^\times)^m$.*

Remark 3.4. *When $K = \mathbb{Q}(\zeta_l)$ is a cyclotomic field and $q = 1 \bmod l$, this lemma is essentially the same with Lemma 3.4 in [47]. When $g = n$, we have the exception of $\boldsymbol{a}$ is less than $2^{(3m+1)n} q^{-\varepsilon mn}$.*

Remark 3.5. *This lemma can be regarded as a special case of Lemma 5.2 in [43]. So is the following theorem of the regularity results in Subsection 3.3.*

3.3 Improved Results on Regularity

In this subsection, we discuss the regularity results.

The following result is a direct consequence of Lemmata 2.10, 2.12, 3.2 and 3.3. By Lemma 3.3 and 3.2, we have $\lambda_1^\infty((\boldsymbol{a}^\perp(I_S))^\vee) = \frac{1}{q} \lambda_1^\infty(L(\boldsymbol{a}, I_S)) \geq |\Delta_K|^{-\frac{1}{n}} q^{\frac{|S|}{mg} - \frac{|S|}{g} - \frac{1}{m} - \varepsilon}$ except with a fraction of $2^{2m(n+g)} q^{-\varepsilon mn}$ of $\boldsymbol{a} \in (R_q^\times)^m$ for $S \subseteq [g]$ and $m \geq 2$. Then Lemma 2.10 tells us that $\eta_\delta((a^\perp(I_S))^\vee) \leq |\Delta_K|^{\frac{1}{n}} \sqrt{\frac{\ln(2mn(1+\frac{1}{\delta}))}{\pi}} \cdot q^{\frac{|S|}{g} + \frac{1}{m} - \frac{|S|}{mg} + \varepsilon}$ for any $\delta > 0$. Therefore, Lemma 2.12 gives us the following lemma.

Lemma 3.6. *Let $K = \mathbb{Q}(\alpha)$ be an algebraic field which is Galois over $\mathbb{Q}$, $R = \mathcal{O}_K$, $m \geq 2$, q is a positive prime such that $q \nmid \Delta_K$ and $q \nmid |R/\mathbb{Z}[\alpha]|$, and the prime ideal decomposition of qR in R is $qR = \mathfrak{P}_1 \cdots \mathfrak{P}_g$, $\delta \in (0, \frac{1}{2})$, $\varepsilon > 0$, $S \subseteq [g]$, $\boldsymbol{c} \in R^m$ and $\boldsymbol{t} \hookleftarrow D_{R^m, \sigma, \boldsymbol{c}}$, where $\sigma \geq |\Delta_K|^{\frac{1}{n}} \sqrt{\frac{\ln(2mn(1+\frac{1}{\delta}))}{\pi}} \cdot q^{\frac{|S|}{g} + \frac{1}{m} - \frac{|S|}{mg} + \varepsilon}$. Then for all except a fraction of $2^{2m(n+g)} q^{-\varepsilon mn}$ of $\boldsymbol{a} \in (R_q^\times)^m$, we have*

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

Let χ be a distribution over R_q and denote $\mathbb{D}_\chi$ the distribution of such tuple $(a_1, \cdots, a_m, \sum_{i=1}^m t_i a_i) \in (R_q^\times)^m \times R_q$, where $a_i \hookleftarrow U(R_q^\times)$ are chosen independently and $t_i \hookleftarrow \chi$ for all $i = 1, 2, \cdots, m$. The regularity of the generalized knapsack function $(t_1, \cdots, t_m) \to \sum_{i=1}^m t_i a_i$ is the statistical distance between $\mathbb{D}_\chi$ and $U((R_q^\times)^m \times R_q)$.

In [31], Micciancio discussed the regularity over general rings and used it to design one-way functions. Some improved regularity results are given in [46], [49], [50] and [47]. Here, we can also give an improved result of regularity for any algebraic field which is Galois over $\mathbb{Q}$. Note that for each $\boldsymbol{a} \hookleftarrow U((R_q^\times)^m)$, the map $\boldsymbol{t} \mapsto \sum_{i=1}^m a_i t_i$ induces an isomorphism from the quotient $R^m/\boldsymbol{a}^\perp$ to its range. The latter is R_q, thanks to the invertibility of a_i's. By taking $S = \phi$ and $\boldsymbol{c} = 0$ in Lemma 3.6, we deduce the following result.

Theorem 3.7. *Let $K = \mathbb{Q}(\alpha)$ be an algebraic field which is Galois over $\mathbb{Q}$, $R = \mathcal{O}_K$, $m \geq 2$, q is a positive prime such that $q \nmid \Delta_K$ and $q \nmid |R/\mathbb{Z}[\alpha]|$, $\delta \in (0, \frac{1}{2})$, and the prime ideal decomposition of qR in R is $qR = \mathfrak{P}_1 \cdots \mathfrak{P}_g$, $\varepsilon > 0$ and $a_i \hookleftarrow U(R_q^\times)$ for all $i \in [m]$. Assume $\boldsymbol{t} \hookleftarrow D_{R^m,\sigma}$ with $\sigma \geq |\Delta_K|^{\frac{1}{n}} \sqrt{\frac{\ln(2mn(1+\frac{1}{\delta}))}{\pi}} \cdot q^{\frac{1}{m}+\varepsilon}$. Then we have*

$$\Delta\left((a_1, \cdots, a_m, \sum_{i=1}^m t_i a_i);\ U((R_q^\times)^m \times R_q)\right) \leq 2\delta + 2^{2m(n+g)} q^{-\varepsilon mn}.$$

4 Improved NTRUEncrypt

With the results of Section 3, we can give a construction of NTRUEncrypt over any cyclotomic field. Let $R = \mathcal{O}_K$. The construction is essentially the same as that in [47]. So are the proofs and we put them in Appendix B.

4.1 Key Generation Algorithm

In this subsection, we set $K = \mathbb{Q}(\alpha)$ to be an algebraic number field which is Galois over $\mathbb{Q}$. Assume $n = [K : \mathbb{Q}]$ and q is a positive prime such that $q \nmid \Delta_K$ and $q \nmid |R/\mathbb{Z}[\alpha]|$. Moreover, assume that $qR = \prod_{i=1}^g \mathfrak{q}_i$ with $\mathfrak{q}_i$ the prime ideal of R, the norm of $\mathfrak{q}_i$ is q^f with $f = \frac{n}{g}$.

We first give a key generation algorithm for our NTRUEncrypts and analyze the algorithm in details. The key generation algorithm of the NTRUEncrypts is as follows.

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

Output: A key pair $(sk,\ pk) \in R_q^\times \times R_q^\times$.

- Sample f' from $D_{R,\sigma}$; let $f = p \cdot f' + 1$; if $(f \bmod qR) \notin R_q^\times$, resample.
- Sample g from $D_{R,\sigma}$; if $(g \bmod qR) \notin R_q^\times$, resample.
- Return secret key $sk = f$ and public key $pk = h = pg/f \in R_q^\times$.

Notice that as long as $\sigma \geq ||\tilde{B}|| \cdot \sqrt{\log n}$ for any basis B of R, we can sample an element in polynomial time to obey the distribution $D_{R,\sigma}$ by using Theorem 2.7. The following lemma shows that the key generation algorithm can terminate with executing only several times.

Lemma 4.1. *Let K and q satisfy the conditions at the beginning of this subsection, set $\sigma \geq |\Delta_K|^{-\frac{1}{2n}} \cdot \sqrt{n} \cdot \sqrt{\frac{\ln(2n(1+\frac{1}{\varepsilon}))}{\pi}} \cdot q^{\frac{f}{n}}$ for an arbitrary $\varepsilon \in (0, \frac{1}{2})$. Let $a \in R$ and $p \in R_q^{\times}$. Then*

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

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

Lemma 4.2. *Let K and q satisfy the conditions at the beginning of this subsection, set $\sigma \geq \sqrt{\frac{2\ln(6n)}{\pi}} \cdot |\Delta_K|^{-\frac{1}{2n}} \cdot \sqrt{n} \cdot q^{\frac{f}{n}}$. Then with probability $\geq 1 - 2^{3-n}$, the secret key f, g satisfy $||f|| \leq 2\sqrt{n}\sigma||p||_\infty$ and $||g|| \leq \sqrt{n}\sigma$.*

The last lemma of this subsection estimates the statistic distance between the distribution of public key and the uniform distribution on $R_q^{\times}$. We denote by $D_{\sigma,z}^{\times}$ the discrete Gaussian $D_{R,\sigma}$ restricted to $R_q^{\times} + z$.

Lemma 4.3. *Let $0 < \varepsilon$, $n \geq 5$, $q \geq 8n$ and $\sigma \geq |\Delta_K|^{\frac{1}{n}} \cdot \sqrt{n} \cdot \sqrt{\ln(8nq)} \cdot q^{\frac{1}{2}+(1+\frac{f}{2})\varepsilon}$. Let $p \in R_q^{\times}$, $y_i \in R_q$ and $z_i = -y_i p^{-1} \bmod qR$ for $i \in \{1, 2\}$. Then*

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

Remark 4.4. *In the case $K = \mathbb{Q}(\zeta_l)$ and $q = 1 \bmod l$, this lemma is equivalent to Lemma* 4.3 *in* [47].

4.2 Construction of NTRUEncrypts

In this subsection, we require $K = \mathbb{Q}(\zeta_l)$ to be a cyclotomic field, $R = \mathcal{O}_K$ and q is a positive prime such that $q \nmid \Delta_K$. The construction of NTRUEncrypt is the same as [47] and the difference is that we do not need to require $q = 1 \bmod l$. Recall that in the construction of [47], the analysis of decryption error depends on the decoding basis of $R^\vee$. It is uncertain that if there exists such a good basis for general algebraic number field. We also set the plaintext message space to be $\mathcal{P} = R^\vee / pR^\vee$. Denote $\chi = \lfloor D_{\xi \cdot q} \rceil_{R^\vee}$ with $\xi = \alpha \cdot (\frac{nk}{\log(nk)})^{\frac{1}{4}}$, where $k = O(1)$ is a positive integer. We will use the decoding basis for element $x \in R \subseteq R^\vee$. One should note that $f = 1 \bmod pR$ implies $f = 1 \bmod pR^\vee$. The NTRUEncrpyt scheme is as follows.

Key generation: Use the algorithm describe in Subsection 4.1, return $sk = f \in R_q^{\times}$ with $f = 1 \bmod pR^\vee$, and $pk = h = pg \cdot f^{-1} \in R_q^{\times}$.

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

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

The analysis of decryption process and the security reduction are standard. The only difference is that we use the result of Ring-LWE in [42] to eliminate the requirement $q = 1 \bmod l$. We only state the results. For more details, one can refer to [47].

Theorem 4.5. *Let l be a positive integer, $n = \varphi(l) \geq 5$, and $K = \mathbb{Q}(\zeta_l)$. Let $q \geq 8n$ be a positive prime of size poly(n) such that $q \nmid \Delta_K$ and the prime ideal decomposition of qR in R is $qR = \mathfrak{P}_1 \cdots \mathfrak{P}_g$ with $fg = n$. Assume that $\alpha \in (0,1)$ satisfies $\alpha q \geq \omega(1)$ and $\alpha \leq \sqrt{\frac{\log n}{n}}$. Let $\xi = \alpha \cdot (\frac{nk}{\log{(nk)}})^{\frac{1}{4}}$ with $k = O(1)$, $\varepsilon \in (0, \frac{1}{2})$ and $p \in R_q^\times$. Moreover, let $\sigma \geq n^{\frac{3}{2}} \cdot \sqrt{\ln{(8nq)}} \cdot q^{\frac{1}{2}+(1+\frac{f}{2})\varepsilon}$ and $\omega(n^{\frac{3}{2}}\sqrt{\log n \log\log n} \cdot \alpha^2 \cdot q^2) \cdot \sigma \cdot ||p||_\infty^2 < \frac{q}{2}$. Then if there exists an* IND-CPA *attack against* NTRUEncrypt(n, q, p, σ, ξ) *that runs in time poly(n) with advantage $\frac{1}{poly(n)}$, there exists a poly(n)-time algorithm solving γ-*Ideal-SIVP *on any ideal lattice of K with $\gamma = \tilde{O}(\frac{\sqrt{n}}{\alpha})$. Moreover, the decryption algorithm succeeds to regain the correct message with probability $1 - n^{-\omega(\sqrt{n \log n})}$ over the choice of the encryption randomness.*

Remark 4.6. *We can modify the NTRUEncrypt to work over an integral ideal $I = \hat{l}R^\vee \subseteq R$, and by using the results of* [43]*, we can also design an NTRUEncrypt over R, as stated in* [47].

5 A Useful Key Generation Algorithm

In this section, we introduce a useful key generation algorithm as in [46] and give a detailed analysis. In fact, this is a method about how to convert a secret key of NTRUEncrypt to a secret key of NTRUSign. This key generation algorithm is standard in the construction of many cryptographic primitives based on NTRU. For example, Collision Resistance Preimage Sampleable Functions and NTRU signatures [46], identity-based encryptions [11], identity-based signatures [48] and so on. We assume $K/\mathbb{Q}$ is a Galois extension with K an algebraic field such that $[K : \mathbb{Q}] = n$.

5.1 Useful Lemmas for Dedekind Zeta Function

In this subsection, we introduce some lemmas we need to analyze the key generation algorithm of CRPSF.

For any ideal $I \in R$, we assume that it has the prime ideal decomposition of the form $(\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$ with $\mathfrak{P}_i$ having norm $\mathrm{N}(\mathfrak{P}_i) = p^f$ for all $i = 1, \cdots, g$. Here, one also have

$efg = n$. The Möbius funciton of I is defined as following:

$$\mu(I) = \begin{cases} 1, & \text{if } \ I = R, \\ (-1)^g, & \text{if } \ I = \mathfrak{P}_1 \cdots \mathfrak{P}_g, \\ 0, & \text{otherwise.} \end{cases}$$

The Dedekind zeta function of the ring R is defined by $\zeta_K(s) = \sum_{I \subseteq R} \frac{1}{\mathrm{N}^s(I)}$ for any complex number s, where I runs over all non-zero integral ideals of R. For $\mathrm{Re}(s) > 1$, it is convergent and we have

$$\zeta_K(s) = \sum_{I \subseteq R} \mathrm{N}(I)^{-s} = \prod_{\mathfrak{P}} (1 - \mathrm{N}(\mathfrak{P})^{-s})^{-1},$$

where $\mathfrak{P}$ runs over all prime ideals of R. Moreover,

$$\zeta_K^{-1}(s) = \prod_{\mathfrak{P}} (1 - \mathrm{N}(\mathfrak{P})^{-s}) = \sum_{I \subseteq R} \mu(I) \cdot \mathrm{N}(I)^{-s}.$$

Recall that, for any prime number $p \in \mathbb{Z}$, the ideal pR ramifies in K if and only if $p | \Delta_K$. For a fixed p with prime ideal decomposition of the form $(\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$, we know that $\mathrm{N}(\mathfrak{P}_i) = p^f$ for all $i = 1, 2, \cdots, g$. Here, g is the number of different prime ideals that divides pR, it is also the number of distinct irreducible factors of $\Phi(x)$ (the minimum polynomial of α over $\mathbb{Q}$, $K = \mathbb{Q}(\alpha)$) over $\mathbb{Z}_p[x]$. Therefore, we have $g \leq \min(p,\ n)$ and $f = \frac{n}{e \cdot g}$. Moreover, $e,\ f,\ g$ depend only on p and K. When $p \nmid \Delta_K$, we have $e = 1$, $g = \frac{n}{f}$.

The following lemma shows an estimate of $\zeta_K(s)$. In order to prove this lemma, we need some results about the sum $\sum_{p \leq x} \frac{1}{p}$ for $x \geq 2$ and prime p. In [40], an accurate estimation is given, which states that for $x \geq 2$, one has

$$\sum_{p \leq x} \frac{1}{p} = \ln \ln x + A + r(x).$$

Here, $|r(x)| < 2(5 \ln 2 + 3) \cdot (\ln x)^{-1}$ and $A = \gamma + \sum_p \{\ln(1 - \frac{1}{p}) + \frac{1}{p}\} = 0.26149721 \cdots$ with γ the Euler constant.

Lemma 5.1. *Let* $[K : \mathbb{Q}] = n \geq 200$ *with* $|\Delta_K| = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$, *assume* $\mathfrak{L}(s) = \prod_{i=1}^t (1 - p_i^{\frac{-sn}{e_i \cdot g_i}})^{-g_i}$ *for* $s > 1$. *Then we have* $\zeta_K(1+\varepsilon) \leq \mathfrak{L}(1+\varepsilon) \cdot e^{\frac{2}{\varepsilon(1-\varepsilon)} \cdot n^{1-\varepsilon}}$, *for any* $\varepsilon \in (0, 1)$, *and* $\zeta_K(2) \leq \mathfrak{L}(2) \cdot e^{6.1}$.

Proof. Notice that $\prod_{p | \Delta_K} \prod_{\mathfrak{P} | p} (1 - \mathrm{N}(\mathfrak{P})^{-s})^{-1} = \prod_{i=1}^t (1 - p_i^{\frac{-sn}{e_i \cdot g_i}})^{-g_i} = \mathfrak{L}(s)$. By the definition of Dedekind Zeta function, we have

$$\zeta_K(s) = \prod_{\mathfrak{P}} (1 - \frac{1}{\mathrm{N}(\mathfrak{P})^s})^{-1} = \prod_p \prod_{\mathfrak{P} | p} (1 - \frac{1}{\mathrm{N}(\mathfrak{P})^s})^{-1} = \mathfrak{L}(s) \cdot \prod_{p \nmid \Delta_K} \prod_{\mathfrak{P} | p} (1 - \frac{1}{\mathrm{N}(\mathfrak{P})^s})^{-1}.$$

For any prime $p \nmid \Delta_K$ and $s > 1$, we have

$$\prod_{\mathfrak{P} | p} (1 - \frac{1}{\mathrm{N}(\mathfrak{P})^s})^{-1} = (1 - p^{-\frac{ns}{g}})^{-g} \leq (1 - p^{-\frac{ns}{\min(n,\ p)}})^{-\min(n,\ p)}.$$

Hence, we get

$$\zeta_K(s) \le \mathfrak{L}(s) \cdot \prod_{p\le n, p\nmid\Delta_K} (1-p^{-\frac{ns}{p}})^{-p} \cdot \prod_{p>n, p\nmid\Delta_K} (1-p^{-s})^{-n}.$$

We first deal with the case $s=2$, where we have

$$\zeta_K(2) \le \mathfrak{L}(2) \cdot \prod_{p\le n, p\nmid\Delta_K} (1-p^{-\frac{2n}{p}})^{-p} \cdot \prod_{p>n, p\nmid\Delta_K} (1-p^{-2})^{-n}.$$

By using the inequality $\ln(1-x) \ge -x-x^2$ for $x\in[0,\frac{1}{2}]$, we get

$$\begin{aligned}
\zeta_K(2) &\le \mathfrak{L}(2) \cdot \prod_{p\le n, p\nmid\Delta_K} (1-p^{-\frac{2n}{p}})^{-p} \cdot \prod_{p>n, p\nmid\Delta_K} (1-p^{-2})^{-n} \\
&= \mathfrak{L}(2) \cdot \exp(-p \sum_{p\nmid\Delta_K, 2\le p\le\frac{n}{2}} \ln(1-p^{-4}) - p \sum_{p\nmid\Delta_K, \frac{n}{2}<p\le n} \ln(1-p^{-2}) \\
&\quad - n \sum_{p\nmid\Delta_K, p>n} \ln(1-p^{-2})) \\
&\le \mathfrak{L}(2) \cdot \exp(\sum_{p\nmid\Delta_K, 2\le p\le\frac{n}{2}} (p^{-3}+p^{-7}) + \sum_{p\nmid\Delta_K, \frac{n}{2}<p\le n} (p^{-1}+p^{-3}) \\
&\quad + n \sum_{p\nmid\Delta_K, p>n} (p^{-2}+p^{-4})).
\end{aligned}$$

We now estimate these sums. One can easily compute that $\sum_{p\nmid\Delta_K, p>n} p^{-4} \le \int_n^\infty x^{-4}\mathrm{d}x = \frac{1}{3n^3}$, $\sum_{p\nmid\Delta_K, p>n} p^{-2} \le \int_n^\infty x^{-2}\mathrm{d}x = \frac{1}{n}$, $\sum_{p\nmid\Delta_K, 2\le p\le\frac{n}{2}} p^{-7} \le \int_1^{\frac{n}{2}} x^{-7}\mathrm{d}x \le \frac{1}{6}$ and $\sum_{p\nmid\Delta_K, p\le n} p^{-3} \le \int_1^n x^{-3}\mathrm{d}x \le \frac{1}{2}$. To estimate the sum $\sum_{p\nmid\Delta_K, \frac{n}{2}<p\le n} \frac{1}{p}$, we have

$$\begin{aligned}
\sum_{p\nmid\Delta_K, \frac{n}{2}<p\le n} \frac{1}{p} \le \sum_{\frac{n}{2}<p\le n} \frac{1}{p} &= \sum_{p\le n} \frac{1}{p} - \sum_{p\le\frac{n}{2}} \frac{1}{p} \\
&= \ln\ln n - \ln\ln\frac{n}{2} + r(n) - r(\frac{n}{2}) \\
&= \ln(1+\frac{\ln 2}{\ln n - \ln 2}) + r(n) - r(\frac{n}{2}) < 5.4,
\end{aligned}$$

where we have used the facts that $\ln(1+\frac{\ln 2}{\ln n-\ln 2}) < 0.15$ and $|r(n)-r(\frac{n}{2})| < 2(5\ln 2+3)(\frac{1}{\ln n}+\frac{1}{\ln n-\ln 2}) < 5.25$ for $n\ge 200$. Hence, we get $\zeta_K(2) \le \mathfrak{L}(2)\cdot e^{6.1}$.

Now we consider the case $s=1+\varepsilon$ for $\varepsilon\in(0,1)$. Similarly, we have

$$\begin{aligned}
\zeta_K(1+\varepsilon) &\le \mathfrak{L}(1+\varepsilon) \cdot \prod_{p\nmid\Delta_K, 2\le p\le n} (1-p^{-\frac{(1+\varepsilon)n}{p}})^{-p} \cdot \prod_{p>n, p\nmid\Delta_K} (1-p^{-(1+\varepsilon)})^{-n} \\
&\le \mathfrak{L}(1+\varepsilon) \cdot \exp(\sum_{p\nmid\Delta_K, 2\le p\le n} (p^{1-\frac{(1+\varepsilon)n}{p}} + p^{1-\frac{2(1+\varepsilon)n}{p}}) \\
&\quad + n \cdot \sum_{p>n, p\nmid\Delta_K} (p^{-(1+\varepsilon)} + p^{-2(1+\varepsilon)})).
\end{aligned}$$

We can estimate these sums by using similar method, i.e. $\sum_{p\nmid\Delta_K, 2\le p\le n}(p^{1-\frac{(1+\varepsilon)n}{p}} + p^{1-\frac{2(1+\varepsilon)n}{p}}) \le 2\int_2^n x^{-\varepsilon}\mathrm{d}x \le \frac{2}{1-\varepsilon}n^{1-\varepsilon}$ and $n\cdot\sum_{p>n, p\nmid\Delta_K}(p^{-(1+\varepsilon)}+p^{-2(1+\varepsilon)}) \le 2n\cdot\int_n^\infty x^{-1-\varepsilon}\mathrm{d}x \le \frac{2}{\varepsilon}n^{1-\varepsilon}$. This gives the claimed bound on $\zeta_K(1+\varepsilon)$. □

Remark 5.2. *We can release the condition of n to $n \geq 3$. In this situation, we have $\sum_{p \nmid \Delta_K, \frac{n}{2} < p \leq n} \frac{1}{p} < 45$ and $\zeta_K(2) \leq \mathfrak{L}(2) \cdot e^{47}$. In the cases $n = 256$, $n = 512$ and $n = 1024$, we have $\zeta_K(2) \leq \mathfrak{L}(2) \cdot e^{5.81}$, $\zeta_K(2) \leq \mathfrak{L}(2) \cdot e^{5.2}$ and $\zeta_K(2) \leq \mathfrak{L}(2) \cdot e^{4.8}$.*

Remark 5.3. *The value of $\mathfrak{L}(2)$ depends on the field discriminant Δ_K. A trivial bound for $\mathfrak{L}(s)$ is $(\frac{|\Delta_K|}{\varphi(|\Delta_K|)})^n$. In the case of cyclotomic field $K = \mathbb{Q}(\zeta_l)$, the bound of $\mathfrak{L}(s)$ is $(\frac{l}{\varphi(l)})^{\varphi(l)} \approx (\log \log l)^l$ for sufficient large l. This upper bound is pretty bad, but it is enough for us to deduce Lemma 5.6. In our application, we hope there is an absolute upper bound for $\mathfrak{L}(2)$. In fact, in the case of cyclotomic fields, we can give an absolute upper bound for $\mathfrak{L}(2)$. See Appendix C.*

Next, we shall give an upper bound of the number of integral ideals whose norms are no more than N.

Lemma 5.4. *Let $N \geq 1$, $\varepsilon \in (0,1)$ and $\mathfrak{L}(s)$ defined as in Lemma 5.1. The number $H(N)$ of ideals $I \subseteq R$ satisfying $\mathrm{N}(I) \leq N$ is bounded as $H(N) \leq \mathfrak{L}(1+\varepsilon) \cdot e^{\frac{2}{\varepsilon(1-\varepsilon)} \cdot n^{1-\varepsilon}} \cdot N^{1+\varepsilon}$.*

Proof. For $k \geq 1$, let $M(k)$ denote the number of ideals of R of norm exactly k. Then for $s > 1$, we have $\zeta_K(s) = \sum_{I \subseteq R} \mathrm{N}(I)^{-s} = \sum_{k \geq 1} M(k) k^{-s} \geq \sum_{k \leq N} M(k) k^{-s}$. Note that $\sum_{k \leq N} M(k) k^{-s} \geq \sum_{k \leq N} M(k) N^{-s} = H(N) N^{-s}$, we obtain that $H(N) \leq \zeta_K(s) \cdot N^s$. By Lemma 5.1, we get the result we need. □

We want to bound the probability that two elements f and g of R chosen from discrete Gaussian distribution are co-prime, i.e. $(f,g) = R$. The argument follows the strategy of [46], which is an adapted version of [44]. The following lemma states a fact proved in the proof of Lemma 4.4 in [33].

Lemma 5.5. *For any full-rank lattice $\Lambda \subseteq H$, $\boldsymbol{c} \in H$, $\delta \in (0,1)$ and $\sigma \geq \eta_\delta(\Lambda)$, we have $\rho_{\sigma,\boldsymbol{c}}(\Lambda) = \frac{\sigma^n}{\det(\Lambda)}(1+\varepsilon)$ with $|\varepsilon| \leq \delta$. As a consequence, we have $\frac{\rho_{\sigma,\boldsymbol{c}}(\Lambda)}{\rho_\sigma(\Lambda)} \in \left[\frac{1-\delta}{1+\delta}, 1\right]$.*

Lemma 5.6. *Assume that K is a cyclotomic field with $R = \mathcal{O}_K$, $\sigma \geq 64 n^{5.7} \log n$, and $\delta \in (0, \frac{1}{2})$. Then we have*

$$\Pr_{f,g \hookleftarrow D_{R,\sigma}}[(f,g) \neq R] \leq 1 - \frac{1 - 2^{-n}}{\zeta_K(2)} + 2^{-n}$$

for $n \geq 500$.

Proof. For $f, g \hookleftarrow D_{R,\sigma}$, we have

$$\Pr[(f,g) \neq R] \leq \Pr[(f,g) \neq R \text{ and } ||f||, ||g|| \neq 0] + \Pr[||f|| = 0 \text{ or } ||g|| = 0].$$

By Lemma 5.5, for any $\sigma \geq \eta_\delta(R)$, we have that $\rho_\sigma(R) = \frac{\sigma^n}{\sqrt{|\Delta_K|}} \cdot (1+\varepsilon)$ with $|\varepsilon| \leq \delta$. Taking $\delta = 2^{-2n}$, we have $D_{R,\sigma}(0) = \frac{1}{\rho_\sigma(R)} \in [\frac{\sqrt{|\Delta_K|}}{\sigma^n(1+2^{-2n})}, \frac{\sqrt{|\Delta_K|}}{\sigma^n(1-2^{-2n})}]$, since $\sigma \geq \eta_{2^{-2n}}(R)$. Therefore,

$$\Pr[(f,g) \neq R] \leq \Pr[(f,g) \neq R \text{ and } ||f||, ||g|| \neq 0] + 2^{-3n \log n}.$$

Let $\mathcal{A}$ denote the event $\{||f|| \neq 0,\ ||g|| \neq 0 \text{ and } (f,g) \neq R\}$ and $\mathcal{B}$ denote the event that occurs with probability

$$p = D^T_{R^2,\sigma}(R^2 \setminus \bigcup_{\text{prime } I \subseteq R} I \times I),$$

where $D^T_{R,\sigma}(J) = D_{R,\sigma}(J) - D_{R,\sigma}(0)$ for any $J \subseteq K$, and the distribution $D_{R^2,\sigma}$ denote the pair $(f,g) \in R^2$, where f and g are sampled from $D_{R,\sigma}$ independently. Notice that $(f,g) \neq R$ implies that there is a prime ideal I of R such that $fR \subseteq I$ and $gR \subseteq I$, since R is a Dedekind domain. By the inclusion-exclusion principle, we have $\Pr[(f,g) \neq R \text{ and } ||f||, ||g|| \neq 0] \leq 1-p$ and $p = \sum_{I \subseteq R} \mu(I) \cdot D^T_{R,\sigma}(I \times I)$.

Therefore, we have

$$\begin{aligned}
|p - \zeta_K(2)^{-1}| &= |\sum_{I \subseteq R} \mu(I) \cdot D^T_{R,\sigma}(I)^2 - \sum_{I \subseteq R} \mu(I) \cdot \frac{1}{\mathrm{N}(I)^2}| \\
&\leq \sum_{I \subseteq R} |D^T_{R,\sigma}(I)^2 - \frac{1}{\mathrm{N}(I)^2}| \\
&= \sum_{I \subseteq R} |(D_{R,\sigma}(I) - D_{R,\sigma}(0))^2 - \frac{1}{\mathrm{N}(I)^2}|.
\end{aligned}$$

Recall that for any ideal I, $\lambda_n(I) = \lambda_1(I) \leq n \cdot \mathrm{N}^{\frac{1}{n}}(I)$. By Lemma 2.8, we have $\eta_\delta(I) \leq n \cdot \sqrt{\frac{\ln(2n(1+\frac{1}{\delta}))}{\pi}} \cdot \mathrm{N}^{\frac{1}{n}}(I) := B_\delta \cdot \mathrm{N}^{\frac{1}{n}}(I)$. We split the above sum into three parts, depending on the magnitude of $\mathrm{N}(I)$. We shall take $\delta = 2^{-2n}$.

Case 1: Assume $\sigma \geq B_\delta \cdot \mathrm{N}^{\frac{1}{n}}(I)$, this is equivalent to $\mathrm{N}(I) \leq (\frac{\sigma}{B_\delta})^n := C_1$. Then Lemma 5.5 implies that $D_{R,\sigma}(I) = \frac{1}{\mathrm{N}(I)} \cdot \frac{1+\varepsilon_1}{1+\varepsilon_2}$ for $|\varepsilon_1|, |\varepsilon_2| \leq 2^{-2n}$. This is equivalent to say

$$\frac{1}{\mathrm{N}^2(I)} \cdot (\frac{1-2^{-2n}}{1+2^{-2n}})^2 \leq D^2_{R,\sigma}(I) \leq \frac{1}{\mathrm{N}^2(I)} \cdot (\frac{1+2^{-2n}}{1-2^{-2n}})^2.$$

This, together with $D_{R,\sigma}(0) \in [\frac{\sqrt{|\Delta_K|}}{\sigma^n(1+2^{-2n})}, \frac{\sqrt{|\Delta_K|}}{\sigma^n(1-2^{-2n})}]$, means that

$$\begin{aligned}
|(D_{R,\sigma}(I) - D_{R,\sigma}(0))^2 - \frac{1}{\mathrm{N}^2(I)}| &\leq |D^2_{R,\sigma}(I) - \frac{1}{\mathrm{N}^2(I)}| + 2 \cdot D_{R,\sigma}(I) \cdot D_{R,\sigma}(0) + D^2_{R,\sigma}(0) \\
&\leq \frac{1}{\mathrm{N}^2(I)} \cdot \frac{2^{3-2n}}{1-2^{-2n}} + \frac{2\sqrt{|\Delta_K|}}{\mathrm{N}(I) \cdot \sigma^n} \cdot \frac{1+2^{-2n}}{(1-2^{-2n})^2} \\
&\quad + \frac{|\Delta_K|}{\sigma^{2n}} \cdot \frac{1}{(1-2^{-2n})^2}.
\end{aligned}$$

Note that $\sigma^n \geq \mathrm{N}(I) \cdot B^n_{2^{-2n}} \geq \mathrm{N}(I) \cdot (n\sqrt{\frac{n}{4}})^n$, we have

$$\frac{1}{\mathrm{N}^2(I)} \cdot \frac{2^{3-2n}}{1-2^{-2n}} + \frac{2\sqrt{|\Delta_K|}}{\mathrm{N}(I) \cdot \sigma^n} \cdot \frac{1+2^{-2n}}{(1-2^{-2n})^2} \leq \frac{2^{-n}}{\mathrm{N}^2(I)}$$

for $n \geq 5$. Therefore,

$$\begin{aligned}
\sum_{\substack{I \subseteq R \\ \mathrm{N}(I) \leq C_1}} |(D^T_{R,\sigma}(I))^2 - \frac{1}{\mathrm{N}^2(I)}| &\leq \sum_{\substack{I \subseteq R \\ \mathrm{N}(I) \leq C_1}} (\frac{2^{-n}}{\mathrm{N}^2(I)} + \frac{|\Delta_K|}{\sigma^{2n}} \cdot \frac{1}{(1-2^{-2n})^2}) \\
&\leq 2^{-n} \frac{1}{\zeta_K(2)} + H(C_1) \cdot \frac{|\Delta_K|}{\sigma^{2n}} \cdot \frac{1}{(1-2^{-2n})^2}.
\end{aligned}$$

Taking $\varepsilon = 0.1$ in Lemma 5.4, we have $\sum_{\substack{I\subseteq R\\ \mathrm{N}(I)\le C_1}} |(D^T_{R,\sigma}(I))^2 - \frac{1}{\mathrm{N}^2(I)}| \le 2^{-8n} + 2^{-n}\frac{1}{\zeta_K(2)}$ for $n \ge 500$.

Case 2: Assume $\mathrm{N}(I) \ge (\sigma\sqrt{n})^n := C_2$. Notice that $\lambda_1(I) \ge \sqrt{n}\mathrm{N}^{\frac{1}{n}}(I)$ for any fractional ideal I, then $\rho_\sigma(I\backslash\{0\}) = \rho_\sigma(I\backslash\sqrt{n}\cdot \mathrm{N}^{\frac{1}{n}}(I)B_n)$. Hence Lemma 2.11 implies that

$$D_{I,\sigma}(I\backslash\{0\}) = \frac{\rho_\sigma(I\backslash\{0\})}{\rho_\sigma(I)} \le (\frac{\mathrm{N}^{\frac{1}{n}}(I)}{\sigma}\cdot\sqrt{2\pi e}\cdot e^{-\pi\frac{\mathrm{N}^{\frac{2}{n}}(I)}{\sigma^2}})^n.$$

Therefore, we get $D^T_{R,\sigma}(I) = \frac{\rho_\sigma(I\backslash\{0\})}{\rho_\sigma(R)} = \frac{\rho_\sigma(I\backslash\{0\})}{\rho_\sigma(I)}\cdot\frac{\rho_\sigma(I)}{\rho_\sigma(R)} \le (\frac{\mathrm{N}^{\frac{1}{n}}(I)}{\sigma}\cdot\sqrt{2\pi e}\cdot e^{-\pi\frac{\mathrm{N}^{\frac{2}{n}}(I)}{\sigma^2}})^n$. One can check that the condition $\mathrm{N}(I) \ge (\sigma\sqrt{n})^n$ insures $(\frac{\mathrm{N}^{\frac{1}{n}}(I)}{\sigma}\cdot\sqrt{2\pi e}\cdot e^{-\pi\frac{\mathrm{N}^{\frac{2}{n}}(I)}{\sigma^2}})^n \le \frac{\sqrt{2}}{\mathrm{N}(I)}$ for $n \ge 500$. Overall, we have

$$\begin{aligned}\sum_{\substack{I\subseteq R\\ \mathrm{N}(I)\ge C_2}} |(D^T_{R,\sigma}(I))^2 - \frac{1}{\mathrm{N}^2(I)}| &\le \sum_{\substack{I\subseteq R\\ \mathrm{N}(I)\ge C_2}} \frac{1}{\mathrm{N}^2(I)}\\ &\le \sum_{k>\lfloor C_2\rfloor} \frac{H(k)-H(k-1)}{k^2}\\ &= \sum_{k>\lfloor C_2\rfloor}\frac{H(k)}{k^2} - \sum_{k\ge\lfloor C_2\rfloor}\frac{H(k)}{(k+1)^2}\\ &\le \sum_{k>\lfloor C_2\rfloor} H(k)(\frac{1}{k^2}-\frac{1}{(k+1)^2}).\end{aligned}$$

We use Lemma 5.4 by taking $\varepsilon = 0.1$ and have $H(k) \le \mathfrak{L}(1.1)\cdot e^{\frac{200}{9}\cdot n^{0.9}}\cdot k^{1.1} \le \mathfrak{L}(1.1)\cdot 2^{17.3n}\cdot k^{1.1}$ for $n \ge 500$. Therefore, we get

$$\sum_{\substack{I\subseteq R\\ \mathrm{N}(I)\ge C_2}} |(D^T_{R,\sigma}(I))^2 - \frac{1}{\mathrm{N}^2(I)}| \le \mathfrak{L}(1.1)\cdot 2^{17.3n}\sum_{k\ge C_2}\frac{2k+1}{k^{0.9}(k+1)^2}.$$

Since $\frac{2k+1}{k^{0.9}(k+1)^2} \le \frac{2}{k^{1.9}}$, we have $\sum_{k\ge C_2}\frac{2k+1}{k^{0.9}(k+1)^2} \le \frac{20}{9}C_2^{-0.9}$. Overall, we deduce that

$$\sum_{\substack{I\subseteq R\\ \mathrm{N}(I)\ge C_2}} |(D^T_{R,\sigma}(I))^2 - \frac{1}{\mathrm{N}^2(I)}| \le \frac{20}{9}\mathfrak{L}(1.1)\cdot 2^{17.3n}\cdot\frac{1}{(\sigma\sqrt{n})^{0.9n}} \le 2^{-10n}.$$

for $n \ge 500$.

Case 3: Assume now $(\frac{\sigma}{B_\delta})^n < \mathrm{N}(I) < (\sigma\sqrt{n})^n$. Let $k = \lceil\frac{\mathrm{N}(I)^{\frac{1}{n}}}{\sigma/B_\delta}\rceil \ge 1$, then we have $I \subseteq \frac{1}{k}I$, $D^T_{R,\sigma}(I) \le D^T_{R,\sigma}(\frac{1}{k}I\cap R)$ and $\eta_\delta(\frac{1}{k}I) = \frac{1}{k}\eta_\delta(I) \le \sigma$. Hence, we get

$$\begin{aligned}D^T_{R,\sigma}(I) &\le D^T_{R,\sigma}(\frac{1}{k}I\cap R) \le D_{R,\sigma}(\frac{1}{k}I)\\ &= \frac{\rho_\sigma(\frac{1}{k}I)}{\rho_\sigma(R)} \le \frac{k^n}{\mathrm{N}(I)}\cdot\frac{1+2^{-2n}}{1-2^{-2n}}\end{aligned}$$

by Lemma 5.5. Notice that $\frac{B_\delta}{\sigma}\cdot\mathrm{N}(I)^{\frac{1}{n}} \le k \le \frac{2B_\delta}{\sigma}\cdot\mathrm{N}(I)^{\frac{1}{n}}$, we deduce that

$$-(\frac{B_\delta}{\sigma})^{2n} \le D^T_{R,\sigma}(I)^2 - \frac{1}{\mathrm{N}(I)^2} \le (\frac{2B_\delta}{\sigma})^{2n}\cdot(\frac{1+2^{-2n}}{1-2^{-2n}})^2 - \frac{1}{\mathrm{N}(I)^2}.$$

Therefore, we get $|D^T_{R,\sigma}(I)^2 - \frac{1}{\mathrm{N}(I)^2}| \leq (\frac{2B_\delta}{\sigma})^{2n} \cdot (\frac{1+2^{-2n}}{1-2^{-2n}})^2$. Overall, we have

$$\begin{aligned}\sum_{C_1<\mathrm{N}(I)<C_2} |D^T_{R,\sigma}(I)^2 - \frac{1}{\mathrm{N}(I)^2}| &\leq \sum_{C_1<\mathrm{N}(I)<C_2} (\frac{2B_\delta}{\sigma})^{2n} \cdot (\frac{1+2^{-2n}}{1-2^{-2n}})^2 \\ &\leq H((\sigma\sqrt{n})^n) \cdot (\frac{2B_\delta}{\sigma})^{2n} \cdot (\frac{1+2^{-2n}}{1-2^{-2n}})^2.\end{aligned}$$

We still take $\varepsilon = 0.1$ in Lemma 5.4 and get

$$\sum_{C_1<\mathrm{N}(I)<C_2} |D^T_{R,\sigma}(I)^2 - \frac{1}{\mathrm{N}(I)^2}| \leq \mathfrak{L}(1.1) \cdot 2^{17.3n} \cdot (\sigma\sqrt{n})^{1.1n} \cdot (\frac{2B_\delta}{\sigma})^{2n} \cdot (\frac{1+2^{-2n}}{1-2^{-2n}})^2.$$

Since $B_\delta \leq \frac{n^{1.5}}{\sqrt{2}}$ and $\sigma \geq 64n^{5.7}\log n$, we have $\sum_{C_1<\mathrm{N}(I)<C_2} |D^T_{R,\sigma}(I)^2 - \frac{1}{\mathrm{N}(I)^2}| \leq 2^{-1.2n}$ for $n \geq 500$.

In a summary, we have deduce that $|p - \zeta_K(2)^{-1}| \leq \frac{2^{-n}}{\zeta_K(2)} + 2^{-n}$. We get the claimed result. □

Remark 5.7. *The value of σ in this lemma seems a little large. It is essentially decided by the limitation in Case* 3*. For $n \geq 1000$, one can release the condition of σ to $\sigma \geq 64n^5 \log n$. In fact, if we discuss this problem in the sense that n goes to infinity, we can set $\sigma \geq 8n^{3.6}\log n$ and take $\varepsilon = \frac{\ln\ln n}{\ln n}$ in the discuss of Case* 3*. Then, we have $\sum_{C_1<\mathrm{N}(I)<C_2} |D^T_{R,\sigma}(I)^2 - \frac{1}{\mathrm{N}(I)^2}| \leq \frac{1}{2\zeta_K(2)}$ for sufficient large n. Therefore, we have $\Pr_{f,g\hookleftarrow D_{R,\sigma}}[(f,g) \neq R] \leq 1 - \frac{1}{2\zeta_K(2)} + 2^{-n}$ as in* [46].

Remark 5.8. *When $K/\mathbb{Q}$ is a Galois extension of a number field K over $\mathbb{Q}$. The same procedure may also work as long as the discriminant of K, i.e. $|\Delta_K|$ is not too large. When $|\Delta_K| \leq n^n$ for $[K:\mathbb{Q}] = n$, the proof is the same as the case of cyclotomic fields.*

Remark 5.9. *In* [1]*, a sample experiment has been tested in the field $\mathbb{Q}(\zeta_{2^k})$. Their result shows that in applications, the probability of $(f,g) = R$ for $f,g \hookleftarrow D_{R,\sigma}$ is far more larger than the estimate we get. More preciously, they numerically approximated $\zeta_K^{-1}(2)$ for $K = \mathbb{Q}[x]/(x^n+1)$ for $n = 128$ and $n = 256$ by computing the first 2^{22} terms of the Dirichlet series of the Dedekind Zeta function for K and then evaluated the truncated series at* 2*. In both cases they get a density ≈ 0.75. Though the elements are sampled a little different from the uniform distribution, their experiments indicate that $\frac{3}{4}$ is a good approximation of the actual probability of coprimality.*

5.2 NTRU Lattice

Now, let us describe some properties of the NTRU lattice over cyclotomic fields. To avoid confusion, we shall speak of the rank of R-modules and of K-vector spaces when $K \neq \mathbb{Q}$ and restrict the term of dimension to $\mathbb{Z}$-modules and $\mathbb{Q}$-vector spaces as in [1]. We are interested in the R modules in K^2. The dimension of a lattice Λ is the dimension over $\mathbb{Q}$ of the $\mathbb{Q}$ vector space it spans. The rank of an R module $M \subseteq K^2$ is defined as the rank over K of the K

vector space it spans. It is obvious that the rank of an R module M is not necessarily equal to the size of a minimal set of R generators of M. The inner product of K can be extend in a coefficient-wise manner to vectors of K^2: $<(x_1,y_1),(x_2,y_2)>=<x_1,x_2>+<y_1+y_2>$. Therefore, we can view any discrete R module $M \subseteq K^2$ as a lattice.

The NTRU lattice is defined as $\Lambda_h^q = \{(x,y) \in R^2 : \ y = hx \bmod qR\}$, where $h = g \cdot f^{-1} \bmod qR$ and $f, g \hookleftarrow D_{R,\sigma}$ for some $\sigma > 0$. We require $f, g \in R_q^\times$ for convenience. Usually, the NTRU problem over R is finding out a nonzero vector (x,y) such that $||(x,y)|| \leq \tau$ for some target norm τ. In many cases, solving the NTRU problem for some $\tau > \sigma$ is enough to break NTRU-like cryptosystems. The NTRU lattice has dimension $2n$, rank 2 and volume $q^n \cdot \mathrm{Vol}^2(R) = q^n \cdot |\Delta_K|$. In fact, if $\alpha_1, \cdots, \alpha_n$ is a $\mathbb{Z}$ basis of R, one can check that the set $\{(\alpha_1, h \cdot \alpha_1), \cdots, (\alpha_n, h \cdot \alpha_n); (0, q \cdot \alpha_1), \cdots, (0, q \cdot \alpha_n)\}$ is a $\mathbb{Z}$ basis of Λ_h^q and the set $\{(1,h),(0,q)\}$ is a set of R generators of Λ_h^q. Lemma 4.3 shows that for approximate parameters, $h \approx U(R_q^\times)$. Thus the gaussian heuristic predicts the shortest vectors of Λ_h^q have norm $|\Delta_K|^{\frac{1}{2n}} \cdot \sqrt{\frac{nq}{e\pi}}$, which implies that whenever $\sigma < |\Delta_K|^{\frac{1}{2n}} \cdot \sqrt{\frac{q}{2e\pi}}$, the lattice Λ_h^q admits a unusually short vector.

In our applications, the following lemma is also useful.

Lemma 5.10. *Let $f, g \in R_q^\times$ such that $(f,g) = R$. Assume $fG_q - gF_q = q$ for $F_q, G_q \in R$, then we have*

$$\Lambda_h^q = \mathrm{Span}_R\{(f,g),(F_q,G_q)\}.$$

Proof. Note that $\Lambda_h^q = \mathrm{Span}_R\{(1,h),(0,q)\}$ and by coprimality, such F_q, G_q exist. Assume that $M = \mathrm{Span}_R\{(f,g),(F_q,G_q)\}$, we shall prove this lemma by showing $\Lambda_h^q \subseteq M$ and $M \subseteq \Lambda_h^q$.

For any $(x,y) \in M$, $\exists r_1, r_2 \in R$ such that $(x,y) = (r_1 f + r_2 F_q, r_1 g + r_2 G_q)$. Since $gF_q = fG_q \bmod qR$, we have $G_q = hF_q \bmod qR$. Hence, $r_1 g + r_2 G_q = h(r_1 f + r_2 F_q) \bmod qR$. Therefore, $M \subseteq \Lambda_h^q$.

On the other hand, $f(F_q,G_q) - F_q(f,g) = (0,q) \in M$ and $g(F_q,G_q) - G_q(f,g) = (-q,0) \in M$ imply $qR^2 \subseteq M$. Meanwhile, note that $f^{-1}(f,g) = (1,h) \bmod q$ for $f \cdot f^{-1} = 1 \bmod qR$, we have $\Lambda_h^q \subseteq M$. The proof is finished. □

5.3 The Key Generation Algorithm

In this subsection, we assume $K = \mathbb{Q}(\zeta_l)$ is a cyclotomic field with $R = \mathcal{O}_K$ and $n = \varphi(l)$. Now we propose the key generation algorithm as in [46] and give a detailed analysis. The key generation algorithm is as follows:

Input: $n, q \in \mathbb{Z}^+$, $\sigma > 0$.

Output: A key pair $(sk, pk) \in R^{2\times 2} \times R_q^\times$.

1. Sample f from $D_{R,\sigma}$, if $(f \bmod q) \notin R_q^\times$, resample.
2. Sample g from $D_{R,\sigma}$, if $(g \bmod q) \notin R_q^\times$, resample.

3. If $||f|| \geq \sqrt{n}\sigma$ or $||g|| \geq \sqrt{n}\sigma$, restart.
4. If $(f, g) \neq R$, restart.
5. Compute $F_q, G_q \in R$ such that $f \cdot G_q - g \cdot F_q = q$, e.g., using a Hermite Normal Form algorithm in [5].
6. Use Babai rounding nearest plane algorithm to approximate (F_q, G_q) in the lattice spanned by(f, g), let $r(f, g)$ be the output, set $(F, G) = (F_q, G_q) - r(f, g)$ for some $r \in R$.
7. If $||(F, G)|| > n\sigma\sqrt{l}$, restart.
8. Return secret key $sk = \begin{bmatrix} f & g \\ F & G \end{bmatrix}$ and public key $pk = h = g \cdot f^{-1} \in R_q^\times$.

It is easy to check that $\Lambda_h^q = \text{Span}_R\{(f, g), (F, G)\}$ and the lattice $\Lambda = \text{Span}_R\{(f, g)\}$ is a sublattice of Λ_h^q. We assume that $(\alpha_1, \cdots, \alpha_n)$ is the powerful basis of R. Now we give a lemma which is helpful to bound the rejection probability of Step 7 in this key generation algorithm.

Lemma 5.11. *Let $\sigma \geq 8n^{3.6} \log n$. Then, as n grows to infinity,*

$$\Pr_{f,g \hookleftarrow D_{R,\sigma}}(||(F, G)||^2 > \frac{n^2 l\sigma^2}{2} + \frac{q^2\omega(n^2)}{\sigma^2} |(f, g) = R) = o(1),$$

where (F, G) is obtained as in Step 5 and 6.

Proof. Let $(F_q, G_q) = (F_q, G_q)^* + (F_q, G_q)^{pro}$, here $(F_q, G_q)^*$ denotes the projection of (F_q, G_q) orthogonally to the plain $\text{Span}_K\{(f, g)\} = \text{Span}_{\mathbb{Q}}\{(f\alpha_1, g\alpha_1), \cdots, (f\alpha_n, g\alpha_n)\}$ and $(F_q, G_q)^{pro}$ denotes the projection of (F_q, G_q) into $\text{Span}_K\{(f, g)\}$. Then, $(F, G) = (F_q, G_q) - r(f, g) := (F_q, G_q)^* + (e_f, e_g)$ for some $r \in R$ and $||(F_q, G_q)||^2 = ||(F_q, G_q)^*||^2 + ||(e_f, e_g)||^2$.

We first bound $||(F_q, G_q)^*||$. Note that $||(F_q, G_q)^*|| \leq \min_{r \in K} ||(F_q, G_q) - r(f, g)||$, taking $r = f^{-1}F_q$ (here f^{-1} is the inverse of f in K) shows that $||(F_q, G_q)^*|| \leq ||(0, qf^{-1})|| = q||f^{-1}||$. Here, we have used the fact $G_q = qf^{-1} + g(f^{-1}F_q)$. By using Lemma 2.15 with $t = \frac{\omega(n)}{\sqrt{2}}$, we have

$$\Pr_{f \hookleftarrow D_{R,\sigma}}(||f^{-1}|| \geq \frac{\omega(n)}{\sigma}) \leq o(1).$$

This remains the case when conditioning on $(f, g) = R$, since the probability that $(f, g) = R$ is bounded from below by a constant. Overall, we have $||(F_q, G_q)^*|| \leq \frac{q \cdot \omega(n)}{\sigma}$ holds except with probability $\leq o(1)$.

To bound $||(e_f, e_g)||$, note that $||(e_f, e_g)|| \leq \frac{\sqrt{nl}}{2} \cdot ||(f, g)||$. By using Lemma 2.9, we have $\Pr_{f,g \hookleftarrow D_{R,\sigma}}(||(f, g)|| \leq \sqrt{2n}\sigma) \geq 1 - 2^{2-n}$. For the same reason as above, this remains the case when conditioning on $(f, g) = R$. Overall, we get $||(e_f, e_g)|| \leq \frac{n\sqrt{l}}{\sqrt{2}}\sigma$ except with probability $\leq o(1)$. The proof is finished. □

We can now analyze the rejection probability of the key generation algorithm.

Lemma 5.12. *Let $q \geq 64n\zeta_K(2)$ be a prime such that $q \nmid \Delta_K$ and the prime ideal decomposition of qR in R is $qR = \mathfrak{P}_1 \cdots \mathfrak{P}_g$. Assume $\sigma \geq \max\{8n^{3.6}\ln n, \omega(n \ln^{0.5} n) \cdot q^{\frac{1}{g}}, \omega(q^{\frac{1}{2}}l^{-\frac{1}{4}})\}$, then the key generation algorithm terminates in polynomial time for sufficient large n.*

Proof. We only need to bound the rejection probability of the algorithm by $1 - c$ for an absolute constant c for sufficient large n. For $i \in \{3, 4, 7\}$, we use p_i to represent the rejection probability in Step i, i.e.

- p_3 is the probability that $||f|| \geq \sqrt{n}\sigma$ or $||g|| \geq \sqrt{n}\sigma$ with $f, g \hookleftarrow D^{\times}_{R,\sigma}$.
- p_4 is the probability that $(f, g) \neq R$ and $||f||, ||g|| < \sqrt{n}\sigma$ with $f, g \hookleftarrow D^{\times}_{R,\sigma}$.
- p_7 is the probability that $||(F, G)|| > n\sigma\sqrt{l}$, $(f, g) = R$ and $||f||, ||g|| < \sqrt{n}\sigma$ with $f, g \hookleftarrow D^{\times}_{R,\sigma}$.

For $i \in \{3, 4, 7\}$, we define p'_i as p_i except that f and g are independently sampled from $D_{R,\sigma}$ rather than $D^{\times}_{R,\sigma}$. Let p denote the rejeciton probability in Step 1, then, by the union bound, we have the rejection probability of Step 1 and 2 is $\leq 2p$. Hence, for $i \in \{3, 4, 7\}$, we have $p_i \leq \frac{p'_i}{1-2p}$.

By Lemma 4.1 and the choice of σ, we have $p \leq \frac{1}{32\zeta_k(2)}$ for sufficient large n. Lemma 2.11 imply that $p'_3 \leq 2^{1-2n}$. The choice of σ and Lemma 5.6 shows that $p'_4 \leq 1 - \frac{1}{2\zeta_K(2)} + o(1)$. Finally, Lemma 5.11 implies $p'_7 = o(1)$. Therefore, for sufficient large n, we have $p'_3 + p'_4 + p'_7 \leq 1 - \frac{1}{4\zeta_K(2)}$. The total rejection probability satisfies $p_3 + p_4 + p_7 \leq \frac{p'_3+p'_4+p'_7}{1-2p} \leq 1 - \frac{1}{8\zeta_K(2)}$, as required. □

Finally, we conclude the following theorem.

Theorem 5.13. *Let K be a cyclotomic field, $R = \mathcal{O}_K$, $q \geq 64n\zeta_K(2)$ be a prime such that $q \nmid \Delta_K$ and the prime ideal decomposition of qR in R is $qR = \mathfrak{P}_1 \cdots \mathfrak{P}_g$ such that $fg = n$, $\varepsilon > 0$ be an arbitrary positive number. Assume that $\sigma \geq \max\{8n^{3.6}\ln n, \omega(n \ln^{0.5} n) \cdot q^{\frac{1}{g}}, \omega(q^{0.5}l^{-0.25})\}$. Then the key generation algorithm proposed in this subsection terminates in polynomial time, and the output matrix $\begin{bmatrix} f & g \\ F & G \end{bmatrix}$ is an R basis of Λ^q_h for $h = gf^{-1} \bmod qR$. Meanwhile, if $\sigma \geq n^{\frac{3}{2}}\sqrt{\ln(8nq)} \cdot q^{\frac{1}{2}+(1+\frac{f}{2})\varepsilon}$, the distribution of h is rejected with probability $c < 1$ for some absolute constant c from a distribution whose statistical distance from $U(R^{\times}_q)$ is $\leq \frac{2^{9n}}{q^{\lfloor \varepsilon n \rfloor}}$.*

6 Collision Resistance Preimage Sampleable Functions

In [17], a general cryptographic primitive called Collision Resistance Preimage Sampleable Functions is introduced. In this section, we shall give a detailed construction of CRPSF over cyclotomic fields based on the strategy of [46].

6.1 Basic Definitions

First, we recall the definition of CRPSF.

Definition 6.1. *A collection of collision-resistant preimage sampleable functions, when given a security parameter n, is specified by three PPT algorithms* (**TrapGen**, **SampleDom**, **SamplePre**) *such that*

1. *Generating a function with trapdoor:* **TrapGen**(1^n) *outputs (a, t), where a is the description of an efficiently-computable function $f_a : \mathfrak{D}_n \mapsto \mathfrak{R}_n$ (for some efficiently-recognizable domain $\mathfrak{D}_n$ and range $\mathfrak{R}_n$ depending on n), and t is some trapdoor information for f_a. In the following, we fix some pair (a, t) returned by* **TrapGen**(1^n). *Note that the following properties need only hold for a probability negligibly closed to* 1 *over the choice of (a, t) outputted by* **TrapGen**(1^n).
2. *Domain sampling with uniform outputs:* **SampleDom**(1^n) *samples an x from some (possibly nonuniform) distribution over $\mathfrak{D}_n$ for which the distribution of $f_a(x)$ is uniform over $\mathfrak{R}_n$.*
3. *Preimage sampling with trapdoor: for every $y \in \mathfrak{R}_n$,* **SamplePre**(t, y) *samples from the conditional distribution of $x \hookleftarrow$* **SampleDom**(1^n), *given $f_a(x) = y$.*
4. *One-wayness without trapdoor: for any PPT adversary $\mathfrak{A}$, the probability $\mathfrak{A}(1^n, a, y) \in f_a^{-1}(y) \subseteq \mathfrak{D}_n$ is negligible, where the probability is taken over the choice of a, the target value $y \hookleftarrow U(\mathfrak{R}_n)$ and the random coins of $\mathfrak{A}$.*
5. *Preimage min-entropy: for any $y \in \mathfrak{R}_n$, the conditional min-entropy of $x \hookleftarrow$* **SampleDom** (1^n) *given $f_a(x) = y$ is at least $\omega(\log n)$.*
6. *Collision resistance without trapdoor: for any probabilistic polynomial time adversary $\mathfrak{A}$, the probability that $\mathfrak{A}(1^n, y)$ outputs distinct x_1, x_2 such that $f_a(x_1) = f_a(x_2)$ is negligible, where the probability is taken over the choice of a and $\mathfrak{A}$'s random coins.*

When a collection of functions (**TrapGen**, **SampleDom**, **SamplePre**) satisfies the properties of 1-4 Definition 6.1, we call it one-way preimage sampleable functions (PSFs).

In fact, as pointed in [17], properties 5 and 6 of Definition 6.1 implies property 4. For if not, then given a function f_a, one can find a collision as follows: choose an $x \leftarrow$ **SampleDom**(1^n), and obtain a preimage x' of $f_a(x)$ from the adversarial inverter. Then because x has large min-entropy given $f_a(x)$, we have $x \neq x'$ with overwhelming probability, so x and x' form a collision. Therefore, in constructions, we only need to prove a scheme satisfy the properties $1, 2, 3, 5, 6$ of Definition 6.1.

6.2 Detailed Constructions of CRPSF over Cyclotomic Fields

In this subsection, we give a concrete construction of CRPSF. It is essentially the same with the construction proposed in [46]. We use NTRUCRPSR(n, q, σ, s) to represent the corresponding CRPSF. The detailed construction is as follows.

1. **TrapGen**$(1^n, q, \sigma)$: By running the key generation algorithm in Subsection 5.3, we get a public key $h = g \cdot f^{-1} \in (R_q)^\times$ and a private key $sk = \begin{bmatrix} f & g \\ F & G \end{bmatrix}$. The key h defines function $f_h(\boldsymbol{z}) = f_h((z_1, z_2)) = hz_1 - z_2 \in R_q$ with domain $\mathfrak{D}_n = \{\boldsymbol{z} \in R^2 : ||\boldsymbol{z}|| < s\sqrt{2n}\}$ and range $\mathfrak{R}_n = R_q$. The trapdoor string for f_h is sk.
2. **SampleDom**$(1^n, q, s)$: Sample $\boldsymbol{z} \hookleftarrow D_{R^2,s}$, if $||\boldsymbol{z}|| \geq s \cdot \sqrt{2n}$, resample.
3. **SamplePre**(sk, t): To find a preimage in $\mathfrak{D}_n$ for a target $t \in \mathfrak{R}_n = R_q$ under f_h by using the trapdoor sk, sample $\boldsymbol{z} \hookleftarrow D_{\Lambda_h^q + \boldsymbol{c}, s}$ with $\Lambda_h^q = \{(z_1, z_2) \in R^2 : z_2 = hz_1 \bmod qR\}$ and $\boldsymbol{c} = (1, h - t)$. Return $\boldsymbol{z}$.

Notice that for approximate σ and s, Theorem 5.13 shows that **TrapGen** is a PPT algorithm, Theorem 2.7 implies that **SampleDom** and **SamplePre** are also PPT algorithms. The following theorem shows that for approximate parameters, the three algorithms form a valid CRPSF.

Theorem 6.2. *Assume* $\sigma \geq \max\{8n^{3.6} \ln n, \omega(n \ln^{0.5} n) \cdot q^{\frac{1}{g}}, \omega(q^{0.5} l^{-0.25}), n^{\frac{3}{2}} \sqrt{\ln(8nq)} \cdot q^{\frac{1}{2}+\varepsilon}\}$ *for some* $\varepsilon \in (0, \frac{1}{2})$ *and* $s \geq n^{\frac{3}{2}} \cdot \sigma \cdot \omega(\log n)$. *Then the* NTRUCRPSF$(n, q, \sigma, s)$ *is a* CRPSF *as defined in Definition* 6.1 *against* ploy(n) *time adversaries, assuming the hardness of the worst-case* Ideal-SIVP$_\gamma$ *over* K *against* poly(n) *time adversaries, with* $\gamma = \tilde{O}(n \cdot s)$.

Proof. The sets $\mathfrak{D}_n$ and $\mathfrak{R}_n$ are obviously recognizable. Note that $\eta_{2^{-2n}}(R^2) \leq \sqrt{\frac{\ln(4n(1+2^{2n}))}{\pi}} \cdot \lambda_n(R^2)$ and $\lambda_n(R^2) = \lambda_1(R^2) \leq \sqrt{2n} \cdot \det^{\frac{1}{2n}}(R^2) = \sqrt{2n} \cdot (|\Delta_K|)^{\frac{1}{2n}} \leq \sqrt{2} \cdot n$, we have $s \geq \eta_{2^{-2n}}(R^2)$ and Theorem 2.7 implies that such a $\boldsymbol{z}$ can be efficiently sampled in **SampleDom**. Further, Lemma 2.11 shows that $||\boldsymbol{z}|| < s \cdot \sqrt{2n}$ with probability $1 - 2^{-4n}$.

To show property 2 of Definition 6.1, we apply Theorem 3.7 with $\delta = n^{-\omega(1)}$ to conclude that except for a fraction $\leq 2^{7n} \cdot q^{-2n\varepsilon}$ of $(a_1, a_2) \hookleftarrow U((R_q^\times)^2)$, we have $\Delta(a_1 z_1 - a_2 z_2; U(R_q)) \leq 2\delta$ with $(z_1, z_2) \hookleftarrow D_{R^2,s}$. Since the map $f : x \mapsto a_2^{-1}x$ is a bijection of R_q to itself, we have $\Delta(a_1 a_2^{-1} z_1 - z_2; U(R_q)) = \Delta(a_1 z_1 - a_2 z_2; U(R_q)) \leq 2\delta$. Moreover, when $a_1, a_2 \hookleftarrow U(R_q^\times)$ are chosen independently, $h = a_2^{-1} a_1 \hookleftarrow U(R_q^\times)$. We have $\Delta(hz_1 - z_2; U(R_q)) \leq 2\delta$ with $(z_1, z_2) \hookleftarrow D_{R^2,s}$, except for a fraction of $\leq 2^{7n} \cdot q^{-2\varepsilon n}$ of $h \in R_q^\times$. Finally, by Theorem 5.13, the h generated by **TrapGen** is obtained by rejection with constant rejection probability $c < 1$ from a distribution within statistical distance $2^{9n} q^{-\lfloor \varepsilon n \rfloor}$ of $U(R_q^\times)$. It follows that $\Delta(hz_1 - z_2; U(R_q)) \leq 2\delta$ with $(z_1, z_2) \hookleftarrow D_{R^2,a}$ except with probability $\leq \frac{1}{1-c} \cdot (2^{7n} q^{-2\varepsilon n} + 2^{9n} q^{-\lfloor \varepsilon n \rfloor}) = q^{-\Omega(n)}$ over the choice of the public key h, as required.

To show properties 3 and 5 of Definition 6.1, we first observe that, for any fixed $t \in R_q$, the conditional distribution of $\boldsymbol{z} \hookleftarrow D_{R^2,s}$, given $f_h(\boldsymbol{z}) = hz_1 - z_2 = t \in R_q$, is exactly $\frac{\rho_s(\boldsymbol{z})}{\rho_s(\Lambda_h^q + \boldsymbol{c})} = D_{\Lambda_h^q + \boldsymbol{c}, s}(\boldsymbol{z})$ with $\boldsymbol{c} = (1, h - t)$. Second, sample a vector $\boldsymbol{z} \hookleftarrow D_{\Lambda_h^q + \boldsymbol{c}, s}$ is equivalent to sample a vector $\boldsymbol{z'} \hookleftarrow D_{\Lambda_h^q, s, -\boldsymbol{c}}$ and add a vector $\boldsymbol{c}$. We only need to analyze $D_{\Lambda_h^q, s, -\boldsymbol{c}}$. Recall that $\Lambda_h^q = R(f, g) + R(F, G)$. Assume $(\alpha_1, \cdots, \alpha_n)$ is the powerful basis of R, then $(f, g)\alpha_1, \cdots, (f, g)\alpha_n; (F, G)\alpha_1, \cdots, (F, G)\alpha_n$ are a $\mathbb{Z}$-basis of Λ_h^q. Moreover, since for any $i \in [n]$, we have $||\alpha_i||_\infty = 1$, $||(f, g)\alpha_i|| \leq ||\alpha_i||_\infty \cdot ||(f, g)|| < \sqrt{2n} \cdot \sigma$ and $||(F, G)\alpha_i|| \leq n\sigma\sqrt{l}$.

Theorem 2.7 implies we can efficiently get a sample from $D_{\Lambda_h^q,s,\boldsymbol{c}}$ for any $s \geq n^{\frac{3}{2}} \cdot \sigma \cdot \omega(\log n)$. This proved the property 3. Note that $\eta_{2^{-2n}}(\Lambda_h^q) \leq \sqrt{\frac{\ln(2n(1+2^{2n}))}{\pi}} \cdot \sqrt{2n} \cdot \det^{\frac{1}{2n}}(\Lambda_h^q) \leq n^{1.5} \cdot q^{\frac{1}{2}} \cdot \ln^{0.5} n \leq s$ for $n \geq 500$. Lemma 2.13 indicates that $D_{\Lambda_h^q,s,-\boldsymbol{c}}(\boldsymbol{x}) \leq \frac{1+2^{-2n}}{1-2^{-2n}} \cdot 2^{-2n}$ for any $\boldsymbol{x} \in \Lambda_h^q$. Property 5 is also satisfied except with probability $q^{-\Omega(n)}$ over the choice of the public key h by Theorem 5.13 and the proof of property 2.

At the end, we show property 6 of Definition 6.1. Let $\mathfrak{A}$ be a collision-finding algorithm for NTRUCRPSF with running time poly(n) and has advantage $\delta = \frac{1}{\text{poly}(n)}$ over the choice of the public key h and the randomness of $\mathfrak{A}$. By Theorem 5.13, the success probability of $\mathfrak{A}$ over the the choice of $h \hookleftarrow U(R_q^\times)$ and the randomness of $\mathfrak{A}$ is at least $\delta' = (1-c)\delta - 2^{9n}q^{-\lfloor \varepsilon n \rfloor} = \frac{1}{\text{poly}(n)}$. We construct an algorithm for R-SIS$_{q,2,\beta}$ with $\beta = 2\sqrt{2n} \cdot s$. It works as follows: on input $(a_1, a_2) \hookleftarrow U(R_q^2)$, if $(a_1, a_2) \notin (R_q^\times)^2$, aborts. Otherwise, $\mathfrak{B}$ calls $\mathfrak{A}$ on input $h = a_2^{-1}a_1$. If $\mathfrak{A}$ succeeds, it outputs $(z_1, z_2) \neq (z_1', z_2')$ with $||(z_1, z_2)||, ||(z_1', z_2')|| < \sqrt{2n} \cdot s$ such that $a_1(z_1 - z_1') + a_2(z_2' - z_2) = 0 \bmod qR$. Then $\mathfrak{B}$ outputs $\boldsymbol{w} = (z_1 - z_1', z_2' - z_2)$. Note that $\boldsymbol{w}$ is a valid solution of R-SIS$_{q,2,\beta}$. Condition on $(a_1, a_2) \in (R_q^\times)^2$, the distribution of h given to $\mathfrak{A}$ is $U(R_q^\times)$ and thus $\mathfrak{A}$ succeeds with probability $\geq \delta'$. Since $(a_1, a_2) \in (R_q^\times)^2$ with probability $\geq 1 - \frac{2n}{q}$, it follows that $\mathfrak{B}$ succeeds with probability $\geq (1 - \frac{2n}{q})\delta' = \frac{1}{\text{poly}(n)}$. □

6.3 Claw-free CRPSF

We can also define and construct a kind of claw-free pairs of trapdoor functions as in [17]. A collection of claw-free pairs of one-way/collision-resistent PSFs is defined similar to Definition 6.1, but with the following differences: **TrapGen** outputs a pair a, a' describing functions $f_a, f_{a'} : \mathfrak{D}_n \mapsto \mathfrak{R}_n$ (respectively), and their respective trapdoors t, t'. The preimage sampler works the same way for both f_a (given t) and $f_{a'}$ (given t'). Then the hardness condition is that no PPT adversary $\mathfrak{A}$, given a, a', can find a pair $x, x' \in \mathfrak{D}_n$ such that $f_a(x) = f_{a'}(x')$. Each function $f_a, f_{a'}$ may itself also be collision-resistant in the usually way.

Constructing a collection of claw-free pairs of trapdoor functions is very similar. For simplicity, we only describe the differences. The **TrapGen** algorithm produces (h, sk) as above, as well as a uniform $w \hookleftarrow U(R_q)$. It outputs a pair of functions $f_h(\boldsymbol{z}) = hz_1 - z_2 \bmod qR$ and $f_{h,w}(\boldsymbol{z}) = hz_1 - z_2 + w \bmod qR$. The domain, range and the **SampleDom** algorithm are the same as above. The **SamplePre** algorithm for f_h(**SamplePre**$_{f_h}$) is also as above, but the **SamplePre** algorithm for $f_{h,w}$(**SamplePre**$_{f_{h,w}}$) is that for a target $t \in R_q$, set $t' = t - w \in R_q$, then run **SamplePre**$_{f_h}$ for target t'. The output $\boldsymbol{z}$ of **SamplePre**$_{f_h}(sk, t')$ is the required output of **SamplePre**$_{f_{h,w}}(sk, t)$.

It is easy to check that the constructed Claw-free CRPSF satisfies the requirements $1, 2, 3, 5, 6$ of Definition 6.1 by using the same proof procedure of Theorem 6.2. Claw-freeness is based on the average-case hardness of R-ISIS$_{q,2,2\sqrt{2n}\cdot s}$. Suppose that an adversary $\mathfrak{A}$ can find a claw $(\boldsymbol{z}, \boldsymbol{z}') \in \mathfrak{D}_n^2$ for f_h and $f_{h,w}$ efficiently, we can construct a PPT algorithm to solve R-ISIS$_{q,2,\beta}$ for $\beta = 2\sqrt{2n} \cdot s$. For an R-ISIS instance (a_1, a_2, u), if $(a_1, a_2) \notin (R_q^\times)^2$, abort. Otherwise, we set $h = a_2^{-1}a_1 \in R_q^\times$ and $w = a_2^{-1}u \bmod qR$. Then we call $\mathfrak{A}$ to get a claw $(\boldsymbol{z}, \boldsymbol{z}') \in \mathfrak{D}_n^2$ for f_h and $f_{h,w}$. Note that we get $hz_1 - z_2 = hz_1' - z_2' + w \bmod qR$, hence, $a_1(z_1 - z_1') + a_2(z_2' - z_2) = u \bmod qR$. Meanwhile, $||(z_1 - z_1', z_2' - z_2)|| \leq 2\sqrt{2n} \cdot s$, it is a valid solution for R-ISIS$_{q,2,\beta}$.

There is a trivial reduction from R-SIS$_{q,m,\beta+\sqrt{mn}\cdot s}$ to R-ISIS$_{q,m,\beta}$ for $\beta \geq \sqrt{mn} \cdot s$, by using Theorem 3.7. Suppose that we have an R-ISIS$_{q,m,\beta}$ oracle $\mathfrak{O}$, the reduction is as follows. For an R-SIS$_{q,m,\beta}$ instance $(a_1, \cdots, a_m)$, if $(a_1, \cdots, a_m) \notin (R_q^\times)^m$, abort. Otherwise, we choose $u \hookleftarrow U(R_q)$ send $(a_1, \cdots, a_m; u)$ to the oracle $\mathfrak{O}$. Theorem 3.7 implies that $\Delta((a_1, \cdots, \alpha_m; \sum_{i=1}^m a_i \cdot t_i), U((R_q^\times)^m \times R_q)) \leq 2\delta + 2^{4mn} q^{-\varepsilon mn}$ for $\boldsymbol{t} \hookleftarrow D_{R^m,s}$, where $s \geq n \cdot \sqrt{\frac{\ln{(2mn(1+\frac{1}{\delta}))}}{\pi}} \cdot q^{\frac{1}{m}+\varepsilon}$ for some $\delta \in (0, \frac{1}{2})$ and $\varepsilon > 0$. Thus for appropriate parameters, $\mathfrak{O}$ output a valid solution $\boldsymbol{z}$ to R-ISIS$_{q,m,\beta}$ for some β that admits solutions. Moreover, since the solutions of $\sum_{i=1}^m a_i \cdot x_i = u \bmod qR$ make up the set $\boldsymbol{z} + \boldsymbol{a}^\perp$, we can sample a vector $\boldsymbol{x} \hookleftarrow D_{\boldsymbol{z}+\boldsymbol{a}^\perp,s}$ and we claim that $\boldsymbol{x} - \boldsymbol{z}$ is a valid solution to R-SIS$_{q,m,\beta}$. Note that sample a vector $\boldsymbol{x} \hookleftarrow D_{\boldsymbol{z}+\boldsymbol{a}^\perp,s}$ is equivalent to sample a vector $\boldsymbol{x}' \hookleftarrow D_{\boldsymbol{a}^\perp,s,-\boldsymbol{z}}$ and then add $\boldsymbol{z}$. Lemma 2.13 shows that for $\beta \geq \sqrt{mn} \cdot s$, the probability that $\boldsymbol{x} = \boldsymbol{z}$ is negligible. Meanwhile, by Lemma 2.9, $||\boldsymbol{x} - \boldsymbol{z}|| \leq ||\boldsymbol{x}|| + ||\boldsymbol{z}|| \leq \beta + \sqrt{mn} \cdot s$ with overwhelming probability. We have proved the claim.

Overall, combing Theorem 2.7 and Theorem 6.2, we get the following theorem.

Theorem 6.3. *Assume* $\sigma \geq \max\{8n^{3.6}\ln n, \omega(n \ln^{0.5} n) \cdot q^{\frac{1}{g}}, \omega(q^{0.5} l^{-0.25}), n^{\frac{3}{2}}\sqrt{\ln(8nq)} \cdot q^{\frac{1}{2}+\varepsilon}\}$ *for some* $\varepsilon \in (0, \frac{1}{2})$ *and* $s \geq n^{\frac{3}{2}} \cdot \sigma \cdot \omega(\log n)$. *Then the constructed* Claw-free NTRUCRPSF(n, q, σ, s) *is a* Claw-free CRPSF *as defined against* ploy(n) *time adversaries, assuming the hardness of the worst-case* Ideal-SIVP$_\gamma$ *over* K *against* poly(n) *time adversaries, with* $\gamma = \tilde{O}(n \cdot s)$.

Remark 6.4. *In Theorem* 6.2 *and Theorem* 6.3, *we both have* $s = \tilde{O}(n^7)$, $q = \tilde{O}(n^8)$ *and* $\gamma = \tilde{O}(n^8)$.

7 NTRU Signatures over Cyclotomic Fields

In this section, we describe the NTRU signatures over any cyclotomic field.

In [17], a method of constructing signature schemes through the collision-resistant preimage sampleable functions is proposed. Moreover, the constructed signature scheme is strongly existentially unforgeable under adaptive chosen-message attacks. We shall use the Probabilistic Full-Domain Hash scheme constructed in [17]. The parameter k is the randomizer length, we can set $k = n$ for simplicity. In fact, any $k = \omega(\log n)$ will suffice for asymptotic security. In this section, $H : \{0,1\}^* \mapsto \mathfrak{R}_n$ is a random oracle. Given a CRPSF(**TrapGen**, **SampleDom**, **SamplePre**), the detailed construction of signature schemes is as follows.

- **SigKeyGen**(1^n): let $(a, t) \leftarrow$**TrapGen**(1^n). The verification key is a and the signing key is t.
- **Sign**(t, m): choose $r \hookleftarrow U(\{0,1\}^k)$, let $\sigma =$**SamplePre**$(t, H(m||r))$ and output (r, σ).

- **Verity**$(a, m, (r, \sigma))$: if $\sigma \in \mathfrak{D}_n$, $r \in \{0,1\}^k$ and $f_a(\sigma) = H(m||r)$, accept. Else, reject.

Proposition 7.1. *The signature scheme above is strongly existentially unforgeable under adaptive chosen-message attack.*

Since we have constructed the NTRUCRPSF, we can use the NTRUCRPSF to design a NTRU signature over any cyclotomic field. Note that applying the construction above directly to our NTRUCRPSF, the signature of a message m is $(\sigma_1, \sigma_2) \in R^2$ and a randomizer $r \in \{0,1\}^k$ satisfying $h\sigma_1 - \sigma_2 = H(m||r)$. As observed in [46], we can reduce the signature length by eliminating the σ_2 from the signature, since it can be easily recovered from the remaining information. Given a NTRUCRPSF(**TrapGen**, **SampleDom**, **SamplePre**), the NTRUSign(n, q, σ, s, k) is as follows.

- **SigKeyGen**$(1^n, q, \sigma, k)$: run **TrapGen**$(1^n, q, \sigma)$ of NTRUCRPSF(n, q, σ, s) to get a verification key $h \in R_q^\times$ and a signing key sk for the function $f_h : \mathfrak{D}_n \mapsto \mathfrak{R}_n$. Here, $\mathfrak{D}_n = \{(z_1, z_2) \in R^2 : ||(z_1, z_2)|| < \sqrt{2n} \cdot s\}$, $\mathfrak{R}_n = R_q$ and $f_h((z_1, z_2)) = hz_1 - z_2 \bmod qR$. Return the secret sk and public key $pk = h$.
- **Sign**(sk, m): choose $r \hookleftarrow U(\{0,1\}^k)$, let $(\sigma_1, \sigma_2) \leftarrow$**SamplePre**$(sk, H(m, r))$. Return (r, σ_1).
- **Verify**$(pk, m, (r, \sigma_1))$: Compute $t = H(m, r)$ and $\sigma_2 = h\sigma_1 - t \bmod qR$. If $(\sigma_1, \sigma_2) \in \mathfrak{D}_n$ and $r \in \{0,1\}^k$, accept. Otherwise, reject.

Theorem 7.2. *Let $\varepsilon, n, q, \sigma$ and s satisfy the condition in Theorem* 6.2 *and $k = \omega(\log n)$. Then, under the random oracle model and the hardness assumption of the worst-case* Ideal-SIVP$_\gamma$ *over K with $\gamma = \tilde{O}(n \cdot s)$, the* NTRUSign$(n, q, \sigma, s, k)$ *defined above is strongly existentially unforgeable against adaptive chosen message attack.*

Acknowledgement

The authors would like to express their gratitude to Bin Guan and Damien Stehlé for helpful discussions.

References

[1] M. Albrecht, S. Bai, L. Ducas: *A subfield lattice attack on overstretched NTRU assumptions: Cryptanalysis of some FHE and graded encoding schemes.* CRYPTO 2016, LNCS, vol. 9814, 153-178, (2016).

[2] L. Babai: *On Lovász lattice reduction and the nearest lattice point problem.* Combinatorica, 6, 1-13, (1986).

[3] W. Banaszczyk: *New bounds in some transference theorems in the geometry of numbers.* Math. Ann., **296**(4), 625-635, (1993).

[4] J. W. Bos, K. Lauter, J. Loftus, M. Naehrig: *Improved security for a ring based fully homomorphic encryption scheme.* IMACC 2013, LNCS, vol. 8308, 45-64, (2013).

[5] H. Cohen: *A course in computational algebraic number theory, 2nd edition.* Springer, (1995).

[6] K. Conrad: *The different ideal. Http://www.math.uconn.edu/∼kconrad/blurbs/.*

[7] J. H. Cheon, J. Jeong, C. Lee: *An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low-level encoding of zero.* LMS J. Comput. Math., **19**(A), 255-266, (2016).

[8] D. Coppersmith, A. Shamir: *Lattice attacks on NTRU.* EUROCRYPT 1997, LNCS, vol. 1233, 52-61, (1997).

[9] D. Cabarcas, P. Weiden, J. A. Buchmann: *On the efficiency of provably secure NTRU.* PQCrypto 2014, LNCS, vol. 8772, 22-39, (2014).

[10] L. Ducas, A. Durmus, T. Lepoint, V. Lyubashevsky: *Lattice signatures and bimodal gaussians.* CRYPTO 2013, LNCS, vol. 8042, 40-56, (2013).

[11] L. Ducas, V. Lyubashevsky, T. Prest: *Efficient identity-based encryption over NTRU lattices.* ASIACRYPT 2014, LNCS, vol. 8874, 22-41, (2014).

[12] L. Ducus, P. Q. Nguyen: *Learning a zonotope and more: Cryptanalysis of NTRUSign countermeasures.* ASIACRYPT 2012, LNCS, vol. 7658, 433-450, (2012).

[13] K. Q. Feng: *Algebraic number theory.* Science Press, (2000).

[14] C. Gentry: *Key recovery and message attacks on NTRU-composite.* EUROCRYPT 2001, LNCS, vol. 2045, 182-194, (2001).

[15] C. Gentry, J. Jonsson, J. Stern, M. Szydlo: *Cryptanalysis of the NTRU signature scheme (NSS) from Eurocrypt 2001.* ASIACRYPT 2001, LNCS, vol. 2248, 1-20, (2001).

[16] N. Gama, P. Q. Nguyen: *New chosen-ciphertext attacks on NTRU.* PKC 2007, LNCS, vol. 4450, 89-106, (2007).

[17] C. Gentry, C. Peikert, V. Vaikuntanathan: *Trapdoors for hard lattices and new cryptographic constructions.* Proc. of STOC, ACM, New York, 197-206, (2008).

[18] C. Gentry, M. Szydlo: *Cryptanalysis of the revised NTRU signature Scheme.* EUROCRYPT 2002, LNCS, vol. 2332, 299-320, (2002).

[19] N. Howgrave-Graham: *A hybrid lattice-reduction and meet-in-the-middle attack against NTRU.* CRYPTO 2007, LNCS, vol. 4622, 150-169, (2007).

[20] J. Hoffstein, N. A. Howgrave-Graham, J. Pipher, J. H. Silverman: *Practical lattice-based cryptography: NTRUEncrypt and NTRUSign.* In [37]. (2009).

[21] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. H. Silverman, W. Whyte: *NTRUSign: Digital signatures using the NTRU lattice.* CT-RSA 2003, LNCS, vol. 2612, 122-140, (2003).

[22] J. Hoffstein, J. Pipher, J. H. Silverman: *NTRU: A ring-based public key cryptosystem.* ANTS 1998, LNCS, vol. 1423, 267-288, (1998).

[23] J. Hoffstein, J. Pipher, J. H. Silverman, W. Whyte: *NSS: The NTRU signature scheme.* EUROCRYPT 2001, LNCS, vol. 2612, 211-228, (2001).

[24] E. Jaulmes, A. Joux: *A chosen-ciphertext attack against NTRU.* CRYPTO 2000, LNCS, vol. 1880, 20-35, (2000).

[25] A. W. Knapp: *Basic algebra.* Birkhãuser Boston, (2006).

[26] P. Kirchner, P. A. Fouque: *Revisiting lattice attacks on overstretched NTRU parameters.* EUROCRYPT 2017, LNCS, vol. 10210, 3-26, (2017).

[27] V. Lyubashevsky, C. Peikert, O. Regev: *On ideal lattices and learning with errors over rings.* EUROCRYPT 2010, LNCS, vol. 6110, 1-23, (2010).

[28] V. Lyubashevsky, C. Peikert, O. Regev: *A Toolkit for Ring-LWE Cryptography.* Crypto. ePrint Archive, 2013:293, (2013).

[29] A. Langlois, D. Stehlé: *Worst-case to average-case reductions for module lattices.* Des. Codes Cryptogr., **75**(3), 565-599, (2015).

[30] A. López-Alt, E. Tromer, V. Vaikuntanathan: *On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption.* Proc. of STOC, ACM, New York, 1219-1234, (2012).

[31] D. Micciancio: *Generalized compact knapsacks, cyclic lattices, and efficient oneway functions.* Comput. Complex. **16**(4), 365-411, (2007).

[32] S. Murphy, R. Player: *Noise Distributions in Homomorphic Ring-LWE.* Crypto. ePrint Archive, 2017:698, (2017).

[33] D. Micciancio, O. Regev: *Worst-case to average-case reductions based on gaussian measures.* SIAM J. Comput., **37**(1), 267-302, (2007).

[34] D. Micciancio, O. Regev: *Trapdoor for lattices: Simpler, tighter, faster, smaller.* EUROCRYPT 2012, LNCS, vol. 7237, 700-718, (2012).

[35] P. Q. Nguyen: *A Note on the Security of NTRUSign.* Crypto. ePrint Archive, 2006:387, (2006).

[36] P. Nguyen, O. Regev: *Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures.* EUROCRYPT 2006, LNCS, vol. 4004, 271-288, (2006).

[37] P. Q. Nguyen, B. Vallée (Eds.): *The LLL algorith: Survey and Applications.* Information Security and Cryptography. Springer, (2010).

[38] C. Peikert: *Limits on the hardness of lattice problems in ℓ_p nroms.* Comput. Complex., **2**(17), 300-351, (2008).

[39] C. Perkert: *An efficient and parallel Gaussian sampler for lattices.* CRYPTO 2010, LNCS, vol. 6223, 80-97, (2010).

[40] C. D. Pan, C. B. Pan: *Elementary number theory, Second Edition*(in Chinese). Peking University press, (2011).

[41] C. Peikert, A. Rosen: *Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices.* TCC, LNCS, vol. 3876, 145-166, (2006).

[42] C. Peikert, O. Regev, N. Stephens-Davidowitz: *Pseudorandomness of Ring-LWE for any ring and modulus.* STOC 2017, 461-473, (2017).

[43] M. Rosca, D. Stehlé, A. Wallet: *On the Ring-LWE and Polynomial-LWE Problems.* Crypto. ePrint Archive, 2018:170, (2018).

[44] B. D. Sittinger: *The probability that random algebraic integers are relatively r-prime.* J. Number Theory, 130, 164-171, (2010).

[45] D. Stehlé, R. Steinfeld: *Making NTRU as secure as worst-case problems over ideal lattices.* EUROCRYPT 2011, LNCS, vol. 6632, 27-47 (2011).

[46] D. Stehlé, R. Steinfeld: *Making NTRUEncrypt and NTRUSign as secure as worst-case problems over ideal lattices.* Crypto. ePrint Archive, 2013:004, (2013).

[47] Y. Wang, M. Q. Wang: *Efficient provably secure NTRUEncrypt over any cyclotomic field.* Crypto. ePrint Archive, 2017:1104, (2017).

[48] J. Xie, Y. P. Hu, J. T. Gao, W. Gao: *Efficient identity-based signature over NTRU lattice.* Front. Inf. Technol. Electron. Eng., **17**(2), 135-142, (2016).

[49] Y. Yu, G. W. Xu, X. Y. Wang: *Provably Secure NTRU Instances over Prime Cyclotomic Rings.* PKC 2017, LNCS, vol. 10174, 409-434, (2017).

[50] Y. Yu, G. W. Xu, X. Y. Wang: *Provably Secure NTRUEncrypt over More General Cyclotomic Rings.* Crypto. ePrint Archive, 2017:304, (2017).

A Missing proofs in Section 3

Proof of Lemma 3.2: We only need to prove $\boldsymbol{a}^{\perp}(I) = q(L(\boldsymbol{a}, I))^{\vee}$, since the other equality can be easily deduced by taking dual in both side of $\boldsymbol{a}^{\perp}(I) = q(L(\boldsymbol{a}, I))^{\vee}$.

We start with showing that $\boldsymbol{a}^{\perp}(I) \subseteq q(L(\boldsymbol{a}, I))^{\vee}$. For any $\boldsymbol{t} \in \boldsymbol{a}^{\perp}(I)$ and $\boldsymbol{z} \in L(\boldsymbol{a}, I)$, we only need to show $\sum_{i=1}^{m} \mathrm{Tr}(t_i \cdot z_i) = 0 \bmod q\mathbb{Z}$. Note that $z_i = a_i \cdot s + q \cdot z_i^{'}$ for some $z_i^{'} \in J^{\vee}$, we have

$$\sum_{i=1}^{m} \mathrm{Tr}(t_i \cdot z_i) = \mathrm{Tr}(s \cdot \sum_{i=1}^{m} t_i \cdot a_i) + q \cdot \sum_{i=1}^{m} \mathrm{Tr}(t_i \cdot z_i^{'}).$$

By the definition, $\sum_{i=1}^{m} t_i \cdot a_i = q \cdot r$ for some $r \in R$. Thus $\sum_{i=1}^{m} \mathrm{Tr}(t_i \cdot z_i) \in q\mathbb{Z}$.

To complete the proof, we will show $q(L(\boldsymbol{a}, I))^{\vee} \subseteq \boldsymbol{a}^{\perp}(I)$. For any $\boldsymbol{x} \in (L(\boldsymbol{a}, I))^{\vee}$, we need to show $q \cdot x_i \in J$ for all $i \in [m]$ and $\sum_{i=1}^{m} qx_i \cdot a_i \in qR$. Note that $q(J^{\vee})^m \subseteq L(\boldsymbol{a}, I)$, we can take $\boldsymbol{v^{(i)}}$ be the vectors in $L(\boldsymbol{a}, I)$ such that the i-th coordinate is $q \cdot s^{'}$ with $s^{'} \in J^{\vee}$ and 0 elsewhere. We have $\mathrm{Tr}(\boldsymbol{x} \cdot \boldsymbol{v^{(i)}}) = \mathrm{Tr}(x_i \cdot q \cdot s^{'}) \in \mathbb{Z}$, hence $q \cdot x_i \in J$. Note that $\forall$ $\boldsymbol{t} \in L(\boldsymbol{a}, I)$, $\sum_{i=1}^{m} \mathrm{Tr}(x_i \cdot t_i) \in \mathbb{Z}$. We write t_i as $a_i \cdot s + q \cdot t_i^{'}$ with $t_i^{'} \in J^{\vee}$, then

$$\sum_{i=1}^{m} \mathrm{Tr}(x_i \cdot t_i) = \mathrm{Tr}(s \cdot \sum_{i=1}^{m} a_i \cdot x_i) + \sum_{i=1}^{m} \mathrm{Tr}(qx_i \cdot t_i^{'}),$$

the latter sum is in $\mathbb{Z}$, hence $\mathrm{Tr}(s \cdot \sum_{i=1}^{m} a_i \cdot x_i) \in \mathbb{Z}$ and we get $\sum_{i=1}^{m} a_i \cdot x_i \in R$. Therefore we have proved $\boldsymbol{a}^{\perp}(I) = q(L(\boldsymbol{a}, I))^{\vee}$. We finish the proof.

Proof of Lemma 3.3: Let p denote the probability, over the randomness of $\boldsymbol{a}$, that $L(\boldsymbol{a}, I_S)$ contains a non-zero vector $\boldsymbol{t}$ of infinity norm $< B = \frac{q^\beta}{n}$. Recall that, $\boldsymbol{t} \in L(\boldsymbol{a}, I_S)$ if and only if there is an $s \in R^\vee$ such that $t_i = a_i \cdot s \bmod qJ_S^\vee$ for all $i \in [m]$. Meanwhile, for any $s \in R^\vee$, all the elements of the coset $s + qJ_S^\vee$ satisfy the equation $t_i = a_i \cdot s \bmod qJ_S^\vee$ for the same t_i. We give an upper bound of p by the union bound, summing the probabilities $p(\boldsymbol{t}, s) = \Pr_{\boldsymbol{a}}[\ t_i = a_i \cdot s \bmod qJ_S^\vee,\ \forall i \in\ [m]]$ over all possible values of $\boldsymbol{t}$ of infinity norm $< B$ and $s \in R^\vee/(qJ_S^\vee)$. Since the $\{a_i\}_{i=1}^m$ are independent, we have $p(\boldsymbol{t}, s) = \prod_{i \le m} p_i(t_i, s)$, where $p_i(t_i, s) = \Pr_{a_i}[t_i = a_i \cdot s \bmod qJ_S^\vee]$. So, we have

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

Note that $qJ_S^\vee = q\prod_{i\in S} \mathfrak{q}_i^{-1} R^\vee = q \cdot \prod_{i \in S} \mathfrak{q}_i^{-1} \cdot R \cdot R^\vee = \prod_{i\in S'} \mathfrak{q}_i \cdot R^\vee$, where $S^{'} = [g] \setminus S$. We have an isomorphism between $J_S^\vee/qJ_S^\vee$ and $J_S^\vee/(\mathfrak{q}_{i_1}R^\vee) \oplus \cdots \oplus J_S^\vee/(\mathfrak{q}_{i_{|S'|}}R^\vee)$.

We claim that for the case $p_i(a_i, s) \neq 0$, there must be a set $S'' \subseteq S'$ such that $s, t_i \in \prod_{i\in S''} \mathfrak{q}_i R^\vee$ and $s, t_i \notin \mathfrak{q}_j R^\vee$ for all $j \in S' \setminus S''$. Otherwise, there are some $j \in S'$ such that either $s = 0 \bmod \mathfrak{q}_j R^\vee$ and $t_i \neq 0 \bmod \mathfrak{q}_j R^\vee$, or $s \neq 0 \bmod \mathfrak{q}_j R^\vee$ and $t_i = 0 \bmod \mathfrak{q}_j R^\vee$. In both cases, we have $p_i(a_i, s) = 0$, since $a_i \in R_q^\times$. Then, for $j \in S''$, we have $t_i = a_i \cdot s = 0 \bmod \mathfrak{q}_j R^\vee$, regardless of the value of $a_i \in R_q^\times$. For any $j \in S' \setminus S''$, we have $t_i = a_i \cdot s \neq 0 \bmod \mathfrak{q}_j R^\vee$, the value of a_i is unique, since $s \neq 0 \bmod \mathfrak{q}_j R^\vee$ and $a_i \in R_q^\times$. For $j \in [n] \setminus S'$, the value of a_i can be arbitrary. Hence, overall, if we set $|S^{''}| = d$, we get $p_i(t_i, s) = \frac{(q^f-1)^{g-|S'|} \cdot (q^f-1)^d}{(q^f-1)^g} = (q^f - 1)^{d-|S^{'}|}$. Therefore, we can rewrite the sum's conditions by

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

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

Case 1: Suppose that $d \ge \frac{\beta \cdot n}{f}$. Since $t \in \mathfrak{h} = \prod_{i \in S''} \mathfrak{q}_i R^\vee$, $\mathfrak{h}$ is a fractional ideal, we have $(t) = tR^\vee \subseteq \mathfrak{h}$ and (t) is a full-rank R-submodule of $\mathfrak{h}$. Hence, $\mathrm{N}(t) = \mathrm{N}((t)) \ge \mathrm{N}(\mathfrak{h}) \ge \mathrm{N}(\prod_{i\in S''} \mathfrak{q}_i \cdot R^\vee) = (\prod_{i \in S''} \mathrm{N}(\mathfrak{q}_i))\mathrm{N}(R^\vee) = q^{df} \cdot \Delta_K^{-1}$. Thus $\mathrm{N}(t) \ge \frac{q^{df}}{|\Delta_K|}$. We conclude that $||t||_\infty \ge \frac{1}{\sqrt{n}}||t|| \ge \mathrm{N}^{\frac{1}{n}}(t) \ge \frac{q^{\frac{df}{n}}}{|\Delta_K|^{\frac{1}{n}}} \ge \frac{q^\beta}{|\Delta_K|^{\frac{1}{n}}} = B$.

Case 2: Suppose now that $d < \frac{\beta \cdot n}{f}$. Define $\mathfrak{B}(l, \boldsymbol{c}) = \{\boldsymbol{x} \in H :\ ||\boldsymbol{x} - \boldsymbol{c}||_\infty < l\}$. Note that $\sigma(\mathfrak{h})$ is a lattice of H, we get $N(B, d)$ is at most the number of points of $\sigma(\mathfrak{h})$ in the region $\mathfrak{B}(B, 0)$. Let $\lambda = \frac{\lambda_1^\infty(\mathfrak{h})}{2}$, then for any two elements $\boldsymbol{v_1}$ and $\boldsymbol{v_2} \in \mathfrak{h}$, we have $\mathfrak{B}(\lambda, \boldsymbol{v_1}) \cap \mathfrak{B}(\lambda, \boldsymbol{v_2}) = \phi$. For any $\boldsymbol{v} \in \mathfrak{B}(B, 0)$, we also have $\mathfrak{B}(\lambda, \boldsymbol{v}) \subseteq \mathfrak{B}(B + \lambda, 0)$. Therefore, $N(B, d) \le \frac{vol(\mathfrak{B}(B+\lambda,0))}{vol(\mathfrak{B}(\lambda,0))} = (\frac{B}{\lambda} + 1)^n \le (2q^{\beta - \frac{df}{n}} + 1)^n \le 2^{2n}q^{n\beta - df}$, where we have used the fact that $\lambda_1^\infty(\mathfrak{h}) \ge \frac{q^{\frac{df}{n}}}{|\Delta_K|^{\frac{1}{n}}}$.

We claim that the number of $s \in R^\vee/(qJ_S^\vee)$ and $s \in \mathfrak{h}$ is $q^{(|S^{'}|-d)f}$. In fact, if s satisfies the above conditions, $s \in \mathfrak{h}/(qJ_S^\vee)$. Using a kind of isomorphism relation which states that for any fractional ideals $\mathfrak{a}$, $\mathfrak{b}$ and integral ideal $\mathfrak{c}$ with $\mathfrak{b} \subseteq \mathfrak{a}$, $\mathfrak{ac}/\mathfrak{bc} \cong \mathfrak{a}/\mathfrak{b}$, we have

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

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

$$p \le \left(\sum_{0 \le d < \frac{\beta \cdot n}{f}} + \sum_{\frac{\beta \cdot n}{f} \le d \le |S'|} \right) \sum_{\substack{S^{''} \subseteq S^{'} \\ |S^{''}| = d \\ \mathfrak{h} = \prod_{i \in S''} \mathfrak{q}_i R^\vee}} \sum_{\substack{s \in R^\vee/(qJ_S^\vee) \\ s \in \mathfrak{h}}} \sum_{\substack{\boldsymbol{t} \in (J_S^\vee)^m \\ \forall i,\ 0 < ||t_i||_\infty < B \\ t_i \in \mathfrak{h}}} \mathfrak{P}$$

Therefore, we have

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

We finish the proof.

B Missing proofs in Section 4

Proof of Lemma 4.1: Thanks to the Chinese Remainder Theorem, we only need to bound the probability that $p \cdot f^{'} + a \in \mathfrak{q}_i$ is no more than $\frac{1}{q^f} + 2\varepsilon$, for any $i \le g$. By Lemma 2.1 and the properties of ideal lattices, we have $\lambda_1(\mathfrak{q}_i) = \lambda_n(\mathfrak{q}_i) \le \sqrt{n} N(\mathfrak{q}_i)^{\frac{1}{n}} (\sqrt{|\Delta_K|})^{\frac{1}{n}}$. By Lemma 2.8 and 2.12, we know that $f^{'} \bmod \mathfrak{q}_i$ is within distance 2ε to uniformity on $R/\mathfrak{q}_i$, so we have $f^{'} = -a/p \bmod \mathfrak{q}_i$ with probability $\le \frac{1}{q^f} + 2\varepsilon$ as we need.

Proof of Lemma 4.2: Set $\varepsilon = \frac{1}{3n-1}$. Note that $\lambda_n(R) = \lambda_1(R) \le \sqrt{n} \cdot (\sqrt{|\Delta_K|})^{\frac{1}{n}}$. By Lemma 2.8, we have $\eta_\varepsilon(R) \le \sqrt{\frac{2\ln(6n)}{\pi}} \cdot \sqrt{n} \cdot |\Delta_K|^{-\frac{1}{2n}}$. Hence, $\Pr_{x \hookleftarrow D_{R,\sigma,\mathbf{c}}}(||x|| \ge \sqrt{n}\sigma) \le$

$\frac{3n}{3n-2}2^{-n}$. Meanwhile, σ satisfies the condition in Lemma 4.1, so we get

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

Hence, we have $||f^{'}||$, $||g|| \le \sqrt{n}\sigma$ with probability $\ge 1-2^{3-n}$. Then we can estimate $||f|| \le 1 + ||p||_\infty \cdot ||f^{'}|| \le 2\sqrt{n}\sigma||p||_\infty$.

Proof of Lemma 4.3**:** For $a \in R_q^\times$, we define $\Pr_a = \Pr_{f_1,f_2}[(y_1+pf_1)/(y_2+pf_2) = a]$, where $f_i \hookleftarrow D_{\sigma,z_i}^\times$. It is suffice to show that $|\Pr_a - (q^f-1)^{-g}| \le 2^{2n+5}q^{-\lfloor \varepsilon n \rfloor} \cdot (q-1)^{-g} =: \varepsilon^{'}$ except a fraction $\le 2^{8n}q^{-2n\varepsilon}$ of $a \in R_q^\times$. Note that $a_1f_1 + a_2f_2 = a_1z_1 + a_2z_2$ is equivalent to $(y_1+pf_1)/(y_2+pf_2) = -a_2/a_1$ in $R_q^\times$ and $-a_2/a_1 \hookleftarrow U(R_q^\times)$ when $\boldsymbol{a} \hookleftarrow U(R_q^\times)^2$, we get $\Pr_{\boldsymbol{a}} := \Pr_{f_1,f_2}[a_1f_1 + a_2f_2 = a_1z_1 + a_2z_2] = \Pr_{-a_2/a_1}$ for $\boldsymbol{a} \in (R_q^\times)^2$.

The set of solutions $(f_1, f_2) \in R^2$, $f_i \hookleftarrow D_{\sigma,z_i}^\times$, to the equation $a_1f_1 + a_2f_2 = a_1z_1 + a_2z_2 \bmod qR$ is $\boldsymbol{z} + \boldsymbol{a}^{\perp\times}$, where $\boldsymbol{z} = (z_1, z_2)$ and $\boldsymbol{a}^{\perp\times} = \boldsymbol{a}^\perp \cap (R_q^\times + qR)^2$. Therefore

$$\Pr_{\boldsymbol{a}} = \frac{D_{R^2,\sigma}(\boldsymbol{z} + \boldsymbol{a}^{\perp\times})}{D_{R,\sigma}(z_1 + R_q^\times + qR) \cdot D_{R,\sigma}(z_2 + R_q^\times + qR)}.$$

Note that $\boldsymbol{a} \in (R_q^\times)^2$, we know for any $\boldsymbol{t} \in \boldsymbol{a}^\perp$, $t_2 = -t_1\frac{a_1}{a_2}$, so t_1 and t_2 are in the same ideal I of R_q. It follows that $\boldsymbol{a}^{\perp\times} = \boldsymbol{a}^\perp \setminus (\cup_{I \subseteq R_q}\boldsymbol{a}^\perp(I)) = \boldsymbol{a}^\perp \setminus (\cup_{S\subseteq[g],S\neq\phi}\boldsymbol{a}^\perp(I_S))$. Similarly, we have $R_q^\times + qR = R \setminus (\cup_{S\subseteq[g],S\neq\phi}(I_S + qR))$. Using the inclusion-exclusion principal, we get

$$D_{R^2,\sigma}(\boldsymbol{z} + \boldsymbol{a}^{\perp\times}) = \sum_{S\subseteq[g]} (-1)^{|S|} \cdot D_{R^2,\sigma}(\boldsymbol{z} + \boldsymbol{a}^\perp(I_S)), \tag{4}$$

$$D_{R,\sigma}(z_i + R_q^\times + qR) = \sum_{S\subseteq[g]} (-1)^{|S|} \cdot D_{R,\sigma}(z_i + I_S + qR), \quad \forall\ i \in \{1,\ 2\}. \tag{5}$$

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

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

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

where $|\delta_i| \le 2^{2n+2}q^{-\lfloor \varepsilon n \rfloor}$ for $i \in \{0,1,2\}$. These imply that $|Pr_a - (q^f-1)^{-g}| \le \varepsilon^{'}$.

Handling (4): When $|S| \le \varepsilon n$, we apply Lemma 3.6 with $m = 2$ and $\delta = q^{-n-f\lfloor \varepsilon n \rfloor}$. Note that $qR^2 \subseteq \boldsymbol{a}^\perp(I_S) \subseteq R^2$, we have $|R^2/\boldsymbol{a}^\perp(I_S)| = \frac{|R^2/(qR^2)|}{|\boldsymbol{a}^\perp(I_S)/(qR^2)|}$. Meanwhile, $|R^2/(qR^2)| = q^{2n}$ and $|\boldsymbol{a}^\perp(I_S)/(qR^2)| = |I_S| = q^{n-f|S|}$, since $|R_q|/|I_S| = |R_q/I_S| = q^{f|S|}$. Therefore for all except a fraction $\le \frac{2^{7n}}{q^{2n\varepsilon}}$ of $\boldsymbol{a} \in (R_q^\times)^2$,

$$\left|D_{R^2,\sigma}(\boldsymbol{z} + \boldsymbol{a}^\perp(I_S)) - q^{-n-f|S|}\right| = |D_{R^2,\sigma,-\boldsymbol{z}}(\boldsymbol{a}^\perp(I_S)) - q^{-n-f|S|}| \le 2\delta.$$

When $|S| > \varepsilon n$, we can choose $S^{'} \subseteq S$ with $|S^{'}| = \lfloor \varepsilon n \rfloor$. Then we have $\boldsymbol{a}^{\perp}(I_S) \subseteq \boldsymbol{a}^{\perp}(I_{S'})$ and hence $D_{R^2,\sigma,-\boldsymbol{z}}(\boldsymbol{a}^{\perp}(I_S)) \leq D_{R^2,\sigma,-\boldsymbol{z}}(\boldsymbol{a}^{\perp}(I_{S'}))$. Using the result proven above, we conclude that $D_{R^2,\sigma,-\boldsymbol{z}}(\boldsymbol{a}^{\perp}(I_S)) \leq 2\delta + q^{-n-f\lfloor \varepsilon n \rfloor}$. Overall, we get

$$\begin{aligned}
\left| D_{R^2,\sigma}(\boldsymbol{z} + \boldsymbol{a}^{\perp\times}) - \frac{(q^f-1)^g}{q^{2n}} \right| &= \left| D_{R^2,\sigma}(\boldsymbol{z} + \boldsymbol{a}^{\perp\times}) - \sum_{k=0}^{g} (-1)^k \tbinom{g}{k} q^{-n-fk} \right| \\
&\leq 2^{g+1}\delta + 2 \sum_{k=\lceil \varepsilon n \rceil}^{g} \tbinom{g}{k} q^{-n-f\lfloor \varepsilon n \rfloor} \\
&\leq 2^{g+1}(\delta + q^{-n-f\lfloor \varepsilon n \rfloor})
\end{aligned}$$

for all except a fraction $\leq \frac{2^{8n}}{q^{2n\varepsilon}}$ of $\boldsymbol{a} \in (R_q^{\times})^2$, since the are 2^g choices of S. The δ_0 satisfies $|\delta_0| \leq \frac{q^{2n}}{(q^f-1)^g} 2^{g+1}(\delta + q^{-n-f\lfloor \varepsilon n \rfloor}) = (\frac{q^f}{q^f-1})^g \cdot 2^{g+2} \cdot q^{-f\lfloor \varepsilon n \rfloor} \leq 2^{2g+2} q^{-f\lfloor \varepsilon n \rfloor} \leq 2^{2n+2} q^{-\lfloor \varepsilon n \rfloor}$ as required.

Handling (5): Note that for any $S \in [g]$, $\det(I_S + qR) = |R/J_S| \cdot \sqrt{|\Delta_K|} = q^{f|S|} \cdot \sqrt{|\Delta_K|}$, where J_S is the ideal of R such that $J_S/(qR) = I_S$. By Minkowski's Theorem, we have $\lambda_1(I_S+qR) = \lambda_n(I_S+qR) \leq |\Delta_K|^{\frac{1}{2n}} \cdot \sqrt{n} \cdot q^{\frac{f|S|}{n}}$. Lemma 2.8 implies that $\sigma > \eta_\delta(I_S+qR)$ for any $|S| \leq \frac{g}{2}$ with $\delta = q^{-\frac{n}{2}}$. Therefore, Lemma 2.12 shows that $|D_{R,\sigma,-z_i}(I_S+qR) - q^{-f|S|}| \leq 2\delta$. For the case $|S| > \frac{g}{2}$, we can choose $S^{'} \subseteq S$ with $|S| \leq \frac{g}{2}$. Using the same argument above, we get $D_{R,\sigma,-z_i}(I_S^{'} + qR) \leq D_{R,\sigma,-z_i}(I_S + qR) \leq 2\delta + q^{-\frac{fg}{2}}$. Therefore,

$$\begin{aligned}
\left| D_{R,\sigma}(z_i + R_q^{\times} + qR) - \frac{(q^f-1)^g}{q^n} \right| &= \left| D_{R,\sigma}(z_i + R_q^{\times} + qR) - \sum_{k=0}^{g} (-1)^k \tbinom{g}{k} q^{-fk} \right| \\
&\leq 2^{g+1}\delta + 2 \sum_{k=\frac{g}{2}}^{g} \tbinom{g}{k} q^{-fk} \\
&\leq 2^{g+1}(\delta + q^{-\frac{n}{2}})
\end{aligned}$$

which leads to the desired bound on δ_i, $i = 1,\ 2$.

C Absolute Upper bound of $\mathfrak{L}(2)$ over Cyclotomic Fields

For cyclotomic field $K = \mathbb{Q}(\zeta_l)$ with $l = p^k$, we have $\mathfrak{L}(2) = \frac{p^2}{p^2-1} < 2$. For general cyclotomic fields $K = \mathbb{Q}(\zeta_l)$ with $l = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ and $n = \varphi(l)$, assume $p_1 < \cdots < p_t$, then $\mathfrak{L}(2) = \prod_{i=1}^{t}(1 - p_i^{-2\cdot f_i})^{-g_i}$, where f_i is the order of $p_i \bmod l/p_i^{\alpha_i}$ and $g_i = \frac{\varphi(l/p_i^{\alpha_i})}{f_i}$. Meanwhile, $e_i \cdot f_i \cdot g_i = n$, where $e_i = \varphi(p_i^{\alpha_i})$.

Case 1: ($f_i \geq 2$ **for all** $i = 1, \cdots, t$). Note that $g_i \leq \min\{p_i, n\}$, we have

$$\begin{aligned}
\mathfrak{L}(2) = \prod_{i=1}^{t}(1 - p_i^{-2\cdot f_i})^{-g_i} &= \exp(-g_i \sum_{i=1}^{t} \ln(1 - p_i^{-2\cdot f_i})) \\
&\leq \exp(-p_i \sum_{i=1}^{t} \ln(1 - p_i^{-4})) \\
&\leq \exp(\sum_{i=1}^{t}(p_i^{-3} + p_i^{-7})) \leq e^{\frac{1}{2}+\frac{1}{6}}.
\end{aligned}$$

That is to say, in this case, there is an absolute upper bound $e^{\frac{1}{2}+\frac{1}{6}}$ for $\mathfrak{L}(2)$.

Case 2: (There are some i **such that** $f_i = 1$**).** In fact, in this annoying case, there is exactly one $i \in [t]$ such that $f_i = 1$. It is t. Then, we have

$$\mathfrak{L}(2) \leq e^{\frac{1}{2}+\frac{1}{6}} \cdot (1 + \frac{1}{p_t^2 - 1})^{g_t},$$

where $g_t = \varphi(p_1^{\alpha_1} \cdots p_{t-1}^{\alpha_{t-1}})$. The term $(1 + \frac{1}{p_t^2-1})^{g_t} = (1 + \frac{1}{p_t^2-1})^{\frac{n}{p_t^{\alpha_t-1}(p_t-1)}}$. Note that, in this case, $p_t = 1 \bmod p_1^{\alpha_1} \cdots p_{t-1}^{\alpha_{t-1}}$. Therefore, $p_t > \sqrt{l}$ and $(1 + \frac{1}{p_t^2-1})^{g_t} \leq (1 + \frac{1}{l-1})^{g_t} \leq (1 + \frac{1}{l-1})^{l-1} < e$, where we have used that the function $(1 + \frac{1}{x})^x$ is a monotone increasing function and $\lim_{x\to\infty}(1 + \frac{1}{x})^x = e$. Hence, in this case, an absolute upper bound for $\mathfrak{L}(2)$ is $e^{1+\frac{1}{2}+\frac{1}{6}}$.