CRPSF and NTRU Signatures over cyclotomic fields

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

[1,2]School of Mathematics, Shandong University, Jinan, Shandong, 250100, P.R. China
[1]wyang1114@mail.sdu.edu.cn
[2]wangmingqiang@sdu.edu.cn

Abstract

Classical NTRUEncrypt is one of the fastest known lattice-based encryption schemes. Its counterpart, NTRUSign, also has many advantages, such as moderate key sizes, high efficiency and potential of resisting attacks from quantum computers. However, like classical NTRUEncrypt, the security of NTRUSign is also heuristic. Whether we can relate the security of NTRUSign to the worst-case lattice problems like NTRUEncrypt is still an open problem.

Our main contribution is that we propose a detailed construction of Collision Resistance Preimage Sampleable Functions (CRPSF) over any cyclotomic field based on NTRU. By using GPV's construction, we can give a provably secure NTRU Signature scheme (NTRUSign), which is strongly existentially unforgeable under adaptive chosen-message attacks in the (quantum) random oracle model. The security of CRPSF (NTRUSign) is reduced to the corresponding ring small integer solution problem (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 algorithm 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, give a much tighter reduction from decision dual-Ring-LWE problem (where the secret is chosen form the codifferent ideal) to decision primal-Ring-LWE problem (where the secret is chosen form the ring of integers) and give a provably secure NTRUEncrypt over any cyclotomic ring. Some useful results about q-ary lattices, regularity and uniformity of distribution of the public keys of NTRUEncrypt are also extended to more general algebraic fields.

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

*Corresponding author

1 Introduction

Cryptographic primitives based on NTRU can be traced back to 1996, when the first NTRUEncrypt was devised by Hoffstein, Pipher and Silverman in [19]. NTRUEncrypt is one of the fastest known lattice-based cryptosystems as testified by its inclusion in the IEEE 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. Properties like high efficiency and resistance to quantum attacks also hold for other NTRU-based cryptographic primitives, such as identity-based encryption (IBE) [11], fully homomorphic encryption [3, 25], digital signatures [18] and identity-based signature (IBS) [41]. Meanwhile, a batch of cryptanalysis works were proposed aiming at NTRU family [1, 5, 6, 8, 12–14, 21–23, 38].

Like classical 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) was discussed in [20], but it succumbed to attacks showed in [15, 17]. The commonly used and discussed NTRU signature scheme is NTRUSign, which was first proposed in [18]. Also, it went through a break-and-repair development history [12, 21, 23, 29, 30]. Construction of provably secure NTRUEncrypt has a relatively short development history [38−40, 42, 43] and till now, we can construct provably secure NTRUEncrypt over any cyclotomic field [40]. However, to our knowledge, the only provably secure NTRU Signature scheme was proposed in [39]. The NTRUSign constructed by Stehlé and Steinfeld is over power-of-two cyclotomic fields. They improved their results in [38] 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, the same algorithm was also the key generation algorithm of a kind of CRPSF over powers-of-2 cyclotomic rings, thus they constructed the first provably secure CRPSF [16] over power-of-two cyclotomic fields based on NTRU. Then, by using GPV's construction, they gave the first provably secure NTRUSign. As far as we know, CRPSF constructed in [39] was the first one which constructed in rings and used the hardness of worst-case ideal lattice problems over corresponding cyclotomic fields.

CRPSF is an important cryptographic primitive proposed in [16]. 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 as showed in [16], for example, signatures, IBE and IBS.

It is easy to see that the CRPSF and NTRUSign constructed in [39] are lack of flexibilities—only powers-of-2 cyclotomic rings can be used. Also, in this particular rings, there are subfields attacks [1, 6, 23] when the dimension n is large. Meanwhile, due to the good algebraic

structures, hard lattice problems may become easier [9] when using quantum computers. Moreover, as stressed in [27], "powers of 2 are sparsely distributed and the desired concrete security level for an application may call for a ring dimension much smaller than the next-largest power of 2. Restricting to powers of 2 could lead to key sizes and run-times that are at least twice as large as necessary.". A natural open problem given in [39] is that whether their constructions can be extended to more general algebraic fields. Meanwhile, a theoretical study of the security of NTRUEncrypt and NTRUSign over more general fields is meaningful, due to their high efficiency, earlier industrial standardization and possibility of becoming new standards via the call of post-quantum cryptography by NIST (for example NTRU Prime and FALCON) in the post quantum world. These are also 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 initial purpose is to research the theoretical securities of NTRU schemes, especially NTRUSign, over general rings. More details are as follows.

For any fixed cyclotomic field, we first theoretically analyze the key generation algorithm of NTRUSign and give an absolute lower bound of success probability of this important algorithm. This is the main obstacle which constrains the security analysis of classical NTRUSign, since their key generation algorithms are all heuristic. This useful algorithm extends a secret key of NTRUEncrypt into a secret key of NTRUSign. It is also standard for many cryptographic primitive constructions based on NTRU, such as CRPSF, NTURSign, IBE and IBS. We use the canonical embedding and basis-embedding norms used in [40] to overcome the technological dependence on the form of cyclotomic rings.

Based on the above PPT key generation algorithm, we then construct a provably secure CRPSF over any cyclotomic field. Then, by [16], we can construct a provably secure N-TRUSign, which is strongly existentially unforgeable under adaptive chosen-message attacks in the (quantum [44]) random oracle model. The security of CRPSF and NTRUSign follows from the hardness of corresponding Ring-SIS problems. We further give a detailed construction of provably secure claw-free CRPSF whose security depends on corresponding Ring-ISIS problems as [16].

We also revisit NTRUEncrypt [40]. We give a tight reduction from decision dual-Ring-LWE problem to decision primal-Ring-LWE problem over any cyclotomic field. This result shows that, under canonical embedding, reduction from decision dual-Ring-LWE problem to decision primal-Ring-LWE problem over general cyclotomic fields is as simple as that over powers-of-2 cyclotomic fields [10]. We then give a provably secure NTRUEncrypt over cyclotomic rings 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 are generalized to any algebraic fields, so we can reobtain the regularity results (a ring-based leftover hash lemma) showed in [36]. Also, the uniformity of the distribution of the public key of NTRUEncrypt is generalized to more general number fields.

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 Stehlé and Steinfeld's routes, there are also many differences. Techniques used in [40] are also vital.

The discussions of q-ary lattices, regularity results and construction of NTRUEncrypt are essentially the same as [40], so we just give a very simple overview. The hardness results of Ring-LWE showed in [34] guarantee the security of the corresponding modified NTRUEncrypts. The only slight difference is the requirement of Gaussian parameter σ. Reductions from decision dual-Ring-LWE problem to decision primal-Ring-LWE problem are simple, we prove that, in cyclotomic field $K = \mathbb{Q}(\zeta_l)$, we can transfer a dual-Ring-LWE sample to a primal-Ring-LWE problem by multiplying l. This reduction is almost as tight as that over powers-of-2 cyclotomic fields [10]. The reason why we constrain our NTRUEncrypt schemes in cyclotomic fields is that we want to use the powerful basis of $R = \mathcal{O}_K$. These good bases, together with canonical embedding and basis-coefficient norm, 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 admits such a basis for R, we can design our NTRUEncrypt in K by using similar techniques and our improved results about q-ary lattices in this paper.

For NTRUSign, techniques described in [18] and [39] are vital. They showed how to extend a secret key of NTRUEncrypt to a secret key of NTRUSign. The key generation algorithm 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 [7].
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 $R_q = R/(qR)$. Elements f and g can be regarded as 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 [16], 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. We can quantify the quality of secret key by using Gaussian heuristic, which implies that try to find the secret key only with h is equivalent to solve the SVP_γ problem over Λ_h^q with $\gamma \leq \tilde{O}(n^2)$. This is a very hard problem, though in the particular lattice Λ_h^q.

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. Overall, we get that 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 [33] 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 rejections in this key generation algorithm. Once we get a CRPSF, we can give a provably secure NTRUSign which is strongly existentially unforgeable under adaptive chosen-message attacks, by using the constructions in [16] directly.

Construction of Claw-free CRPSF is almost the same as that of CRPSF. 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**$_{f_{h,w}}(sk, t)$. Claw-freeness is based on the hardness of corresponding Ring-ISIS problems. We give a brief reduction from Ring-SIS to Ring-ISIS by using the regularity results. So, security of claw-free CRPSF is also guaranteed by the hardness of worst-case lattice problems.

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 modulus q and security parameter γ (SIVP$_\gamma$) 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 [16]. 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 modulus 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 practice. This is a common shortcoming for provably secure NTRU families. Though our construction may be less efficient, 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 shall give a new series of relevant results about some kinds of q-ary lattices and regularity in any algebraic fields. We will also discuss the generalized construction the NTRUEncrypt. In Section 4, we mainly analyze the key generation algorithm of CRPSF and NTRUSign. Detailed construction of CRPSF is put in Section 5. In Section 6, 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, we set $\hat{l} = l$ when l is odd and $\hat{l} = \frac{l}{2}$ when l is even for some positive integer l. Function $\varphi(n)$ stands for the Euler totient function. We use $[n]$ to denote the set $\{1, 2, \cdots, n\}$. We usually use $||\cdot||$ to represent the l_2 norm over an Euclidean space $\mathbb{R}^n$ or $\mathbb{C}^n$. For any matrix $M \in \mathbb{C}^{n\times n}$, symbols $s_i(M)$ stand for its singular values for $i \in [n]$. We shall arrange the singular values by their magnitudes, i.e. $s_1(M) \geq \cdots \geq s_n(M)$. For two

random variables X and Y, $\Delta(X,Y)$ stands for their statistical 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. 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, especially the cyclotomic fields. Assume $[K:\mathbb{Q}] = n := r_1 + 2r_2$ for some $r_1, r_2 \in \mathbb{Z}^+$, 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 $1 \le j \le r_1$, $\boldsymbol{h}_{r_1+j} = \frac{1}{\sqrt{2}}(\boldsymbol{e}_{r_1+j} + \boldsymbol{e}_{n+1-j})$ and $\boldsymbol{h}_{n+1-j} = \frac{\boldsymbol{i}}{\sqrt{2}}(\boldsymbol{e}_{r_1+j} - \boldsymbol{e}_{n+1-j})$ for $1 \le j \le r_2$. Moreover, $\sigma(K) \subseteq H \cong K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$. Let's denote $\psi : K \mapsto \mathbb{R}^n$ be the composite of the above isomorphism from H to $\mathbb{R}^n$ and the canonical embedding. Then, for any $x \in K$, we have $\psi(x) = U \cdot \sigma(x)$ with $U = \begin{pmatrix} I_{r_1} & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} I_{r_2} & \frac{1}{\sqrt{2}} J_{r_2} \\ 0 & \frac{1}{\sqrt{2}\cdot\boldsymbol{i}} J_{r_2} & -\frac{1}{\sqrt{2}\cdot\boldsymbol{i}} I_{r_2} \end{pmatrix}$, where $I_{r_1} = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}_{r_1 \times r_1}$ and $J_{r_2} = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}_{r_2 \times r_2}$.

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 $||x||_\infty = \max_{i\in[n]} |\sigma_i(x)|$. It is easy to verify that $||\psi(x)|| = ||\sigma(x)||$. Because multiplications in H of embedded elements is component-wise, for any $x, y \in K$, we have $||x \cdot y||_p \le ||x||_\infty \cdot ||y||_p$ 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 $\mathrm{N}(x) := \mathrm{N}_{K/\mathbb{Q}}(x) = \prod_{i=1}^n \sigma_i(x)$. 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 $\Delta_K = |(\sigma_i(\alpha_j))_{1\le i,j\le n}|^2$, here $|\cdot|$ represents the determinant of a matrix. In particular, the discriminant of the l-th cyclotomic number field is

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

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 $a \cdot b$ 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 $K = \mathbb{Q}(\alpha)$ with $n = [K : \mathbb{Q}]$, then for any positive prime q, the ideal qR has a prime ideal decomposition of the form $qR = \prod_{i=1}^{\mathfrak{g}} \mathfrak{q}_i^{\mathfrak{e}_i}$. More precisely, assume that $\Phi(x)$ is the minimum polynomial of α over $\mathbb{Q}$, $q \nmid |R/\mathbb{Z}[\alpha]|$ and $\Phi(x) = \prod_{i=1}^{\mathfrak{g}} \Phi_i^{\mathfrak{e}_i}(x) \bmod q$. Each $\Phi_i(x)$ is a monic irreducible polynomial in $\mathbb{Z}_q[x]$ with $\deg(\Phi_i(x)) = \mathfrak{f}_i$. We have $\mathfrak{q}_i = (q, \Phi_i(\alpha))R$ and the norm of $\mathfrak{q}_i$ is $q^{\mathfrak{f}_i}$. We also have $\sum_{i=1}^{\mathfrak{g}} \mathfrak{e}_i \cdot \mathfrak{f}_i = n$. When $K/\mathbb{Q}$ is a Galois extension, we have $\mathfrak{e}_1 = \cdots = \mathfrak{e}_{\mathfrak{g}}$ and $\mathfrak{f}_i = \cdots = \mathfrak{f}_{\mathfrak{g}}$, i.e. $\mathfrak{e} \cdot \mathfrak{f} \cdot \mathfrak{g} = n$.

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 $\mathfrak{e} = \varphi(q^d)$ and let $\mathfrak{f} \geq 1$ be the multiplicative order of q modulo l/q^d. Then $qR = \prod_{i=1}^{\mathfrak{g}} \mathfrak{q}_i^{\mathfrak{e}}$, where $\mathfrak{q}_i$ are $\mathfrak{g} = n/(\mathfrak{e} \cdot \mathfrak{f})$ different prime ideals, each of norm $q^{\mathfrak{f}}$.

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 $\Lambda^\vee = \{\boldsymbol{y} \in H : \forall\, \boldsymbol{x} \in \Lambda, < \boldsymbol{x}, \overline{\boldsymbol{y}} >= \sum_{i=1}^n x_i \cdot y_i \in \mathbb{Z}\}$. 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. By our definition in Subsection 2.2, it is easy to verify that $I = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n \iff \sigma(I) = \mathbb{Z}\sigma(\beta_1) + \cdots \mathbb{Z}\sigma(\beta_n) \iff \psi(I) = \mathbb{Z}\psi(\beta_1) + \cdots + \mathbb{Z}\psi(\beta_n)$. Therefore, our definition of lattices in H is equivalent to that in $\mathbb{R}^n$. 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 [26] gives upper and lower bounds on the minimum distance of an ideal lattice in l_2 norm and l_∞ norm.

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

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

and

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

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.

One of the most famous lattice problems is SVP. Given a lattice basis B, one try to find a shortest vector in $\Lambda \backslash \{0\}$, where $\Lambda = \mathcal{L}(B)$. 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 $\gamma \leq \mathrm{poly}(n)$. The (Ideal-$\mathrm{SIVP}_\gamma$) 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 $\max_{1 \leq i \leq n} ||x_i|| \leq \gamma \cdot \lambda_n(\Lambda)$.

Roughly speaking, discretization is to convert a continuous Gaussian into a discrete 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. In our applications, we will use the following simple method to discretize errors. Assume $B = (\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$, we first compute $\boldsymbol{c} - \boldsymbol{x} = \sum_{i=1}^n a_i \cdot \boldsymbol{b}_i \bmod \Lambda$ for some coefficients $a_i \in [-\frac{1}{2}, \frac{1}{2})$ and set $\boldsymbol{f} = \sum_{i=1}^n a_i \cdot \boldsymbol{b}_i$. Then, output $\boldsymbol{y} = \boldsymbol{f} + \boldsymbol{x}$. The results (representative elements of $\Lambda + \boldsymbol{c}$) of this process depends on the basis B of Λ we choose. In our applications, we only set B to be the powerful basis defined in Subection 2.4 when $\Lambda = R$. There are also many different methods to discretize errors. For more details, one can refer to [27].

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, for cyclotomic field $K = \mathbb{Q}(\zeta_l)$, we introduce the powerful basis of R and the decoding basis of $R^\vee$ as in [27]. 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 2.2. *The Powerful basis $\overrightarrow{p}$ of $K = \mathbb{Q}(\zeta_l)$ and $R = \mathbb{Z}[\zeta_l]$ is defined as follows:*

- *For a prime power l, define $\overrightarrow{p}$ 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 $\overrightarrow{p} = \otimes_k \overrightarrow{p_k}$, the tensor product of the power basis $\overrightarrow{p_k}$ of each $K_k = \mathbb{Q}(\zeta_{l_k})$.*

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

Also note that $\tau(\overrightarrow{p})$ 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 [27], which shows the estimates of $s_1(\sigma(\overrightarrow{p}))$ and $s_n(\sigma(\overrightarrow{p}))$. Here, function $rad(n)$ 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, $rad(n) = \prod_{i=1}^{k} p_i$.

Lemma 2.3. *We have* $s_1(\sigma(\overrightarrow{p})) = \sqrt{\hat{l}}$, $s_n(\sigma(\overrightarrow{p})) = \sqrt{\frac{l}{rad(l)}}$, $||\sigma(\overrightarrow{p})_i||_\infty = 1$ *and* $||\sigma(\overrightarrow{p})_i|| = \sqrt{n}$ *for all* $i = 1, \cdots, n$.

We can also give the estimates of $s_1(\sigma(\overrightarrow{d}))$ and $s_n(\sigma(\overrightarrow{d}))$. Assume that $\sigma(\overrightarrow{p}) = T$, Lemma 2.3 shows that $s_1(T) = \sqrt{\hat{l}}$ and $s_n(T) = \sqrt{\frac{l}{rad(l)}}$. By the definitions of $\overrightarrow{d}$ and the dual ideal, an easy computation shows that $\sigma(\overrightarrow{d}) = (T^*)^{-1}$. Hence we have $s_n(\sigma(\overrightarrow{d})) = \frac{1}{\sqrt{\hat{l}}}$, $s_1(\sigma(\overrightarrow{d})) = \sqrt{\frac{rad(l)}{l}}$. Moreover, one can similarly deduce that $||\sigma(\overrightarrow{d})_i|| \leq \sqrt{\frac{rad(l)}{l}}$ for all $i = 1, 2, \cdots, n$. The following definition is also useful [40].

Definition 2.4. *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

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

and

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

When we write $x \bmod qR^\vee$, we use the representative element of the coset $x + qR^\vee$ as $\sum_{i=1}^{n} x_i \overrightarrow{d}_i$ 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 $\sum_{i=1}^{n} x_i \overrightarrow{p}_i$ with $x_i \in [-\frac{q}{2}, \frac{q}{2})$. From now on, we only use the decoding basis of $R^\vee$ and the powerful basis of R.

2.5 Gaussian Distributions

For $s > 0$, $\boldsymbol{c} \in H$, which is taken to be $s = 1$ or $\boldsymbol{c} = \boldsymbol{0}$ when omitted, we 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 $s^{-n} \cdot \rho_{s,\boldsymbol{c}}(\boldsymbol{x})$. Let $\boldsymbol{\sigma} = (\sigma_1, \cdots, \sigma_n) \in (\mathbb{R}^+)^n$ be a vector, we can define the elliptical Gaussian distributions in the basis $\{\boldsymbol{h}_i\}_{i \leq n}$ 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 $\varphi(\sum_{i \in [n]} x_i \boldsymbol{h}_i) = (x_1, \cdots, x_n)$, which is the isomorphism from H to $\mathbb{R}^n$ as we explained in Subsection 2.2, then $D_{\boldsymbol{\sigma}}$ is also an

elliptical Gaussian distribution over $\mathbb{R}^n$. This means that Gaussians over H are equivalent to Gaussians over $\mathbb{R}^n$.

For a lattice $\Lambda \subseteq H$, $\sigma > 0$ and $\boldsymbol{c} \in H$, we define the lattice (discrete) 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 $\boldsymbol{x} \in \Lambda$. It is easy to check that $D_{\Lambda,\sigma,\boldsymbol{c}} = D_{\Lambda-\boldsymbol{c},\sigma}$. Meanwhile, we have $D_{\Lambda,\sigma,\boldsymbol{c}} = D_{\varphi(\Lambda),\sigma,\varphi(\boldsymbol{c})}$, since $\frac{e^{-\pi\frac{||\boldsymbol{x}-\boldsymbol{c}||^2}{\sigma^2}}}{\sum_{\boldsymbol{y}\in\Lambda} e^{-\pi\frac{||\boldsymbol{y}-\boldsymbol{c}||^2}{\sigma^2}}} = \frac{e^{-\pi\frac{||\varphi(\boldsymbol{x})-\varphi(\boldsymbol{c})||^2}{\sigma^2}}}{\sum_{\varphi(\boldsymbol{y})\in\varphi(\Lambda)} e^{-\pi\frac{||\varphi(\boldsymbol{y})-\varphi(\boldsymbol{c})||^2}{\sigma^2}}}$ for any $\boldsymbol{x} \in \Lambda$. So, discrete Gaussians over H are also equivalent to discrete Gaussians over $\mathbb{R}^n$.

For $\delta > 0$, we define the smoothing parameter $\eta_\delta(\Lambda)$ as the smallest $\sigma > 0$ such that $\rho_{\frac{1}{\sigma}}(\Lambda^\vee \setminus \mathbf{0}) \leq \delta$. It was shown that we can efficiently sample from a distribution, which is within a negligible statistical distance from a not too narrow discrete Gaussian [16, 33]. It was further shown that we can actually sample the discrete Gaussian precisely for suitable parameters [4]. 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 $||B|| = \max_i ||b_i||$. Note that we have $||B|| \geq ||\tilde{B}||$.

Theorem 2.5. *There is a probabilistic polynomial time algorithm that, given a basis B of an n-dimensional lattice $\Lambda = \mathcal{L}(B)$, a standard deviation $\sigma \geq ||\tilde{B}|| \cdot \sqrt{\frac{\ln(2n+4)}{\pi}}$, and a $\boldsymbol{c} \in H$, outputs a sample distributed according to $D_{\Lambda+\boldsymbol{c},\sigma}$.*

We will use following lemmas from [28], [32], [2], [16] and [35].

Lemma 2.6. *For any full-rank lattice Λ and positive real $\varepsilon > 0$, we have $\eta_\varepsilon(\Lambda) \leq \sqrt{\frac{\ln(2n(1+\frac{1}{\varepsilon}))}{\pi}} \cdot \lambda_n(\Lambda)$.*

Lemma 2.7. *For any full-rank lattice Λ, $\boldsymbol{c} \in H$, $\varepsilon \in (0,1)$ and $\sigma \geq \eta_\varepsilon(\Lambda)$, we have $\Pr_{\boldsymbol{b}\hookleftarrow D_{\Lambda,\sigma,\boldsymbol{c}}}[||\ \boldsymbol{b}-\boldsymbol{c}|| \geq \sigma\sqrt{n}] \leq \frac{1+\varepsilon}{1-\varepsilon} \cdot 2^{-n}$.*

Lemma 2.8. *For any full-rank lattice Λ and any positive real $\varepsilon > 0$, we have $\eta_\varepsilon(\Lambda) \leq \sqrt{\frac{\ln(2n(1+\frac{1}{\varepsilon}))}{\pi}} \cdot \frac{1}{\lambda_1^\infty(\Lambda^\vee)}$.*

Lemma 2.9. *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, $\Pr_{\boldsymbol{x}\hookleftarrow D_{\Lambda,\sigma}}(||\boldsymbol{x}|| \geq \sqrt{n} \cdot \sigma) < 2^{-2n}$.

Lemma 2.10. *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 2.11. *For any full-rank lattice $\Lambda \subseteq H$, $\boldsymbol{c} \in H$, $\varepsilon \in (0,1)$, $\sigma \geq 2 \cdot \eta_\varepsilon(\Lambda)$ and $\boldsymbol{b} \in \Lambda$, we have $D_{\Lambda,\sigma,\boldsymbol{c}}(\boldsymbol{b}) \leq \frac{1+\varepsilon}{1-\varepsilon} \cdot 2^{-n}$.*

We also need the following adapted result on one-dimensional projections of discrete Gaussians, which is proposed in [39]. It is helpful for us to estimate the norm of x^{-1} with $x \hookleftarrow D_{R,\sigma}$.

Lemma 2.12. *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.

Lemma 2.13. *Let K be a cyclotomic field with $[K:\mathbb{Q}] = n := 2r$, $R = \mathcal{O}_K$, $\delta \in (0,1)$, $t \geq \sqrt{2\pi}$ and $\sigma \geq \frac{t}{\sqrt{2\pi}} \cdot \eta_\delta(R)$, we have*

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

Proof. Let $\psi : K \mapsto \mathbb{R}^n$ be the composition of σ and the isomorphism from H to $\mathbb{R}^n$ as proposed in Subsection 2.2. Notice that $\mathrm{Re}(\sigma_k(x)) = \mathrm{Re}(\sigma_{n+1-k}(x))$ and $\mathrm{Im}(\sigma_k(x)) = -\mathrm{Im}(\sigma_{n+1-k}(x))$ for any $x \in K$ and $k \in [r]$. So, we have

$$\psi(x) = \begin{pmatrix} \frac{1}{\sqrt{2}} \cdot I_r & \frac{1}{\sqrt{2}} \cdot J_r \\ \frac{1}{\sqrt{2} \cdot \boldsymbol{i}} \cdot J_r & -\frac{1}{\sqrt{2} \cdot \boldsymbol{i}} \cdot I_r \end{pmatrix} \cdot \sigma(x) = \begin{pmatrix} \sqrt{2} \cdot \mathrm{Re}(\sigma_1(x)) \\ \vdots \\ \sqrt{2} \cdot \mathrm{Re}(\sigma_r(x)) \\ -\sqrt{2} \cdot \mathrm{Im}(\sigma_{r+1}(x)) \\ \vdots \\ -\sqrt{2} \cdot \mathrm{Im}(\sigma_n(x)) \end{pmatrix},$$

where $J_r = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}_{r \times r}$. By definition, $x \hookleftarrow D_{R,\sigma}$ is equivalent to $\psi(x) \hookleftarrow D_{\psi(R),\sigma}$. So, by using Lemma 2.12 with $\boldsymbol{u} = \boldsymbol{e}_k$ and $k \in [r]$, we get

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

Therefore, for any $k \in [r]$, we have

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

which implies that

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

Note that $|\sigma_k(x)| = |\sigma_{n+1-k}(x)|$, we can conclude the desired result by taking the union bound. □

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 2.14. *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 (constrained) ring inhomogeneous small integer solution problem* ($\text{R-ISIS}^{\times}_{q,m,\beta}$) *is: given $a_i \hookleftarrow U(R_q^{\times})$ 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 [24].

Theorem 2.15. *For $\varepsilon = \varepsilon(n) = n^{-\omega(1)} \in (0, 1)$, there is a probabilistic polynomial time reduction from solving* 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 $m, \beta, \log q \leq \text{poly}(n)$.*

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

Definition 2.16. *For $s \in R_q^{\vee}$ and an error distribution ψ over $K_{\mathbb{R}}$, the* Ring-LWE *distribution $A^{\vee}_{s,\psi}$ 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 $(a, b = a \cdot s + e \bmod qR^{\vee})$.*

Definition 2.17. *Let Ψ be a family of distributions over $K_{\mathbb{R}}$. The average-case decision* Ring-LWE *problem, denoted D-RLWE$^{\vee}_{q,\Psi}$, is to distinguish (with non-negligible advantage) between independent samples from $A^{\vee}_{s,\psi}$ 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 $R_q \times \mathbb{T}$.*

In [34], a reduction from SIVP_{γ} to decision Ring-LWE over any algebraic number field is given.

Theorem 2.18. *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_{γ} *to* $\text{D-RLWE}^{\vee}_{q,D_{q\cdot\xi}}$*, where $\xi = \alpha \cdot (\frac{nk}{\log(nk)})^{\frac{1}{4}}$ with k the number of samples to be used and $\gamma = \omega(\frac{\sqrt{n} \cdot \log n}{\alpha})$.*

3 Improved Provably Secure NTRUEncrypt

Provably secure NTRUEncrypt was first introduced by Stehlé and Steinfeld [38] over powers-of-2 cyclotomic rings. They proved that for suitable choices of secret keys of classical NTRUEncrypt, the public key would become statistically close to the uniform distribution.

Hence, they could tweak classical NTRUEncrypt slightly and give a worst-case hardness reduction. Recently, provably secure NTRUEncrypt was generalized to any cyclotomic field [40]. In this section, we shall discuss this scheme further and give some generalized results which will be also very useful for designing of many cryptographic primitives, such as the following CRPSF.

3.1 Analysis of q-ary Lattices

In this subsection, we assume that $K = \mathbb{Q}(\alpha)$ is an algebraic field, $[K : \mathbb{Q}] = n$ 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, we assume that the prime ideal decomposition of qR is known (in this setting, we can compute the prime ideal decomposition of qR conveniently, see Theorem 4.8.13. of [7]). All the proofs in this subsection are essentially the same as those in [40], so we put them in Appendix A.

Notice that for general K, R may not be isomorphic to $\mathbb{Z}[x]/(\Phi(x))$ and R usually has no power basis. These are quite different from the cases in cyclotomic fields. While, we have the following prime ideal decomposition [7]. For any fixed prime $q \nmid |R/\mathbb{Z}[\alpha]|$ and $q \nmid \Delta_K$, we have $\Phi(x) = \Phi_1(x) \cdots \Phi_{\mathfrak{g}}(x) \bmod q$ with $\deg(\Phi_i(x)) = \mathfrak{f}_i$ for $i \in [\mathfrak{g}]$. Here, $\Phi_i(x)$ is irreducible polynomial in $\mathbb{Z}_q[x]$ and $\Phi_i(x) \neq \Phi_j(x)$ for any $i \neq j \in [\mathfrak{g}]$. Meanwhile, we have $qR = \mathfrak{q}_1 \cdots \mathfrak{q}_{\mathfrak{g}}$ with $\mathfrak{q}_i = (q, \Phi_i(\alpha))R$ and $\mathrm{N}(\mathfrak{q}_i) = q^{\mathfrak{f}_i}$ for $i = 1, \cdots, \mathfrak{g}$. In particular, we have $\sum_{i=1}^{\mathfrak{g}} \mathfrak{f}_i = n$ and the isomorphism $R_q \cong R/\mathfrak{q}_1 \times \cdots \times R/\mathfrak{q}_{\mathfrak{g}} \cong \mathbb{Z}[x]/(q, \Phi_1(x)) \times \cdots \times \mathbb{Z}[x]/(q, \Phi_{\mathfrak{g}}(x)) \cong \mathbb{Z}_q[x]/(\Phi_1(x)) \times \mathbb{Z}_q[x]/(\Phi_{\mathfrak{g}}(x)) \cong \mathbb{Z}_q[x]/(\Phi(x))$. $\mathbb{Z}_q[x]$ is a principal ideal domain, hence R_q is a principal ideal ring. For any proper ideal $I \subseteq R_q$, 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 $S \subseteq \{1, 2, \cdots, \mathfrak{g}\}$. This is because that $\Phi_i^2(x) \cdot R_q = \Phi_i(x) \cdot R_q$ for any $i \in [\mathfrak{g}]$. In fact, on the one hand, we obviously have $\Phi_i^2(x) \cdot R_q \subseteq \Phi_i(x) \cdot R_q$. On the other hand, note that $\Phi_i(x)$ is prime to $\prod_{k \neq i} \Phi_k(x)$, we have $\Phi_i(x) \cdot r_1(x) + \prod_{k \neq i} \Phi_k(x) \cdot r_2(x) = 1$ for some $r_1(x), r_2(x) \in \mathbb{Z}_q[x]/(\Phi(x))$. Hence, we get $\Phi_i(x) \cdot (\Phi_i(x) \cdot r_1(x) - 1) = 0$ in $\mathbb{Z}_q[x]/(\Phi(x))$, which implies that $\Phi_i(x) \cdot R_q \subseteq \Phi_i^2(x) \cdot R_q$. We will also use I_S to represent the ideal $\prod_{i \in S} \Phi_i(\alpha) R_q$ of R_q. Let $\boldsymbol{a} \in (R_q)^m$, the definitions of the q-ary lattices we need are as followings [40]:

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

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

Here, $R^{\vee} \cdot \boldsymbol{a} = \{t \cdot \boldsymbol{a} = (ta_1, \cdots, ta_m) : t \in R^{\vee}\}$. We also define $\boldsymbol{a}^{\perp}$ and $L(\boldsymbol{a})$ as $\boldsymbol{a}^{\perp}(R_q)$ and $L(\boldsymbol{a}, R_q)$. As in [40], $\boldsymbol{a}^{\perp}(I)$ and $L(\boldsymbol{a}, I)$ have the following dual relations and its proof is independent of the form of algebraic number field.

Lemma 3.1. *Let $\boldsymbol{a}^{\perp}(I)$ and $L(\boldsymbol{a}, I)$ be defined above, then we have $\boldsymbol{a}^{\perp}(I) = q \cdot (L(\boldsymbol{a}, I))^{\vee}$ and $L(\boldsymbol{a}, I) = q \cdot (\boldsymbol{a}^{\perp}(I))^{\vee}$.*[1]

[1]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 $\mathrm{Tr}(\boldsymbol{x} \cdot \boldsymbol{v}) := \sum_{j=1}^{m} \mathrm{Tr}(x_j \cdot v_j) \in \mathbb{Z}$

Let $I_S = \prod_{i\in S}\Phi_i(\alpha)R_q \subseteq R_q$ and $J_S = \prod_{i\in S}\mathfrak{q}_i \subseteq R$ for $S \subseteq \{1, 2, \cdots, \mathfrak{g}\}$. 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 $J_S^{\vee} = \prod_{i\in S}\mathfrak{q}_i^{-1}R^{\vee}$. The next lemma 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 3.2. *Set $q \geq 2$ to be a prime such that $q \nmid \Delta_K$ and $q \nmid |R/\mathbb{Z}(\alpha)|$. Let $m \geq 2$ and $\varepsilon > 0$, assume $\Phi(x) = \prod_{i=1}^{\mathfrak{g}}\Phi_i(x)$ with $\deg(\Phi_i(x)) = \mathfrak{f}_i$ and $I_S = \prod_{i\in S}\Phi_i(\alpha)R_q$ for some $S \subseteq [\mathfrak{g}]$, then we have $\lambda_1^{\infty}(L(\boldsymbol{a}, I_S)) \geq B$ with $B = \frac{q^{\beta}}{|\Delta_K|^{\frac{1}{n}}}$, where $\beta = (1-\frac{1}{m})(1-\frac{\sum_{i\in S}\mathfrak{f}_i}{n}) - \varepsilon$, except with probability $p \leq 2^{2mn+(m+1)\mathfrak{g}}q^{-\varepsilon mn}$ over the uniformly random choice of $\boldsymbol{a} \in (R_q^{\times})^m$.*

Remark 3.3. *When $K = \mathbb{Q}(\zeta_l)$ is a cyclotomic field and $q = 1 \bmod l$, this lemma is the same as Lemma 3.4 in [40].*

The following lemma is a direct consequence of Lemmata 2.8, 2.10, 3.1 and 3.2, which will be used to estimate the distribution of public keys of NTRUEncrypt.

Lemma 3.4. *Let $K = \mathbb{Q}(\alpha)$ be an algebraic field, $R = \mathcal{O}_K$, $m \geq 2$, q is a positive prime such that $q \nmid \Delta_K$ and $q \nmid |R/\mathbb{Z}[\alpha]|$. Assume that the prime ideal decomposition of qR in R is $qR = \mathfrak{P}_1 \cdots \mathfrak{P}_{\mathfrak{g}}$. Set $\delta \in (0, \frac{1}{2})$, $\varepsilon > 0$, $S \subseteq [\mathfrak{g}]$, $\boldsymbol{c} \in R^m$ and $\boldsymbol{t} \hookleftarrow D_{R^m,\sigma,\boldsymbol{c}}$, where $\sigma \geq |\Delta_K|^{\frac{1}{n}}\sqrt{\frac{\ln(2mn(1+\frac{1}{\delta}))}{\pi}} \cdot q^{\frac{\sum_{i\in S}\mathfrak{f}_i}{n}+\frac{1}{m}-\frac{\sum_{i\in S}\mathfrak{f}_i}{mn}+\varepsilon}$. Then for all except a fraction of $2^{2mn+(m+1)\mathfrak{g}}q^{-\varepsilon mn}$ 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 some distribution over R_q and denote $\mathbb{D}_{\chi}$ the distribution of the 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 $U((R_q^{\times})^m \times R_q)$. We can deduce the following result by taking $S = \phi$ and $\boldsymbol{c} = 0$ in Lemma 3.4.

Theorem 3.5. *Let $K = \mathbb{Q}(\alpha)$ be an algebraic field, $R = \mathcal{O}_K$, $m \geq 2$, q is a positive prime such that $q \nmid \Delta_K$ and $q \nmid |R/\mathbb{Z}[\alpha]|$, $\delta \in (0, \frac{1}{2})$, the prime ideal decomposition of qR in R is $qR = \mathfrak{P}_1 \cdots \mathfrak{P}_{\mathfrak{g}}$, $\varepsilon > 0$ 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*

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

Remark 3.6. *By taking $I_S = R_q$ in Lemma 3.2, we can reobtain Lemma 5.2 of [36], as well as the above regularity result. The proofs are almost same. But in [36], they use the isomorphism $R/qR \cong R^{\vee}/qR^{\vee}$ so that they do not to require $q \nmid |R/\mathbb{Z}(\alpha)|$. However, the same method may not work when treating general ideal I_S of R_q since we use the decomposition which was mentioned above Lemma 3.1. Meanwhile, for primes $q||R/\mathbb{Z}(\alpha)|$, the prime ideal decomposition of qR may be very complicated. So, we just remove this case for simplicity. For more details, one can refer to Section 6 of [7].*

for all $\boldsymbol{v} \in M$.

3.2 Construction of NTRUEncrypts

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 2.5. The following lemma shows that the key generation algorithm can terminate with executing in expected time.

We must remark that in the proof of Lemma 3.7, Lemma 3.8 and Lemma 3.9, we use the property $\lambda_1(I) = \lambda_n(I)$ for some ideal $I \subseteq R$, so that we could use Lemma 2.6 with suitable parameters. This property is not true for general fields. If not so, we have to bound the magnitude of λ_n, which may be very difficult. There are many fields satisfy this requirement, for example, cyclotomic fields, extensions of cyclotomic fields. We do not know which are the necessary and sufficient conditions about judging whether a kind of fields satisfies this requirement or not. Also, for simplicity, we assume that K is Galois over $\mathbb{Q}$, so all the $\mathfrak{f}_i$'s are equal. Otherwise, the conditions of these lemmata should be changed- -just replacing the $\mathfrak{f}$ with the maximum (or minimum) value of these $\mathfrak{f}_i$'s.

Lemma 3.7. *Let K and q satisfy the conditions discussed above, set $\sigma \geq |\Delta_K|^{\frac{1}{2n}} \cdot \sqrt{n} \cdot \sqrt{\frac{\ln(2n(1+\frac{1}{\varepsilon}))}{\pi}} \cdot q^{\frac{\mathfrak{f}}{n}}$ for an arbitrary $\varepsilon \in (0, \frac{1}{2})$. Let $a \in R$ and $p \in R_q^\times$. Then*

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

The following lemma bounds the length of the secret keys, which is very useful for us to analyze the decryption error.

Lemma 3.8. *Let K and q satisfy the conditions discussed above, set $\sigma \geq \sqrt{\frac{2\ln(6n)}{\pi}} \cdot |\Delta_K|^{\frac{1}{2n}} \cdot \sqrt{n} \cdot q^{\frac{\mathfrak{f}}{n}}$. Then with probability $\geq 1 - 2^{3-n}$, the secret key f, g satisfy $||f|| \leq 2\sqrt{n} \cdot \sigma \cdot ||p||_\infty$ and $||g|| \leq \sqrt{n} \cdot \sigma$.*

The last lemma of this subsection estimates the statistical distance between the distribution of public keys 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 3.9. *Let $0 < \varepsilon$, $n \geq 5$, $q \geq 8n$ and $\sigma \geq |\Delta_K|^{\frac{1}{n}} \cdot \sqrt{n + \mathfrak{f} \cdot \lfloor n\varepsilon \rfloor} \cdot \sqrt{\frac{\ln(8nq)}{\pi}} \cdot q^{\frac{1}{2}+(1+\frac{\mathfrak{f}}{2})\varepsilon}$. Let $p \in R_q^\times$, $y_i \in R_q$ and $z_i = -y_i \cdot p^{-1} \bmod qR$ for $i \in \{1, 2\}$. Then*

$$\Delta\left[\frac{y_1 + p \cdot D_{\sigma,z_1}^\times}{y_2 + p \cdot D_{\sigma,z_2}^\times} \bmod qR,\ U(R_q^\times)\right] \leq \frac{2^{8n}}{q^{\lfloor \varepsilon n \rfloor}}.$$

Remark 3.10. *In the case $K = \mathbb{Q}(\zeta_l)$ and $q = 1 \bmod l$, this lemma is equivalent to Lemma 13 of* [40].

In the following of this subsection, we constrain $K = \mathbb{Q}(\zeta_l)$ to be a cyclotomic field. It is obvious that till now, we can give a provably secure NTRUEncrypt in $R^\vee$ as [40]. However, we choose to design our schemes in the polynomial ring $R_q \cong Z_q[x]/(\Phi_l(x))$, so that the schemes may enjoy the high computation speed over polynomial rings and become more 'practical' than using the transformation given in Remark 1 of [40]. The requirement $q = 1 \bmod l$ can also be removed.

In fact, the definition of the decision Ring-LWE problem is the so called decision dual-Ring-LWE problem [36], since the secret s is chosen from the dual ideal $R^\vee$ of R. We can also define the decision primal-Ring-LWE problem as in [36].

Definition 3.11. *Let $k = \mathbb{Q}(\zeta_l)$ and $R = \mathcal{O}_K$, Ψ be a set of error distributions on H and $q \geq 2$. For $s \in R_q$ and $\psi \in \Psi$, the Primal-Ring-LWE distribution $A_{s,\psi}$ over $R_q \times K_{\mathbb{R}}/qR$ is sampled by independently choosing a uniformly random $a \hookleftarrow U(R_q)$ and an error term $e \hookleftarrow \psi$, and outputting $(a, b = a \cdot s + e \bmod qR)$. The average-case decision Primal-Ring-LWE problem, denoted by D-RLWE$_{q,\Psi}$, is to distinguish (with non-negligible advantage) between independent samples from $A_{s,\psi}$ for a random choice of $(s, \psi) \hookleftarrow U(R_q) \times \Psi$, and the same number of uniformly random and independent samples from $R_q \times K_{\mathbb{R}}/qR$.*

We have the following hardness results about the decision Primal-Ring-LWE problems. Its proof is a combination of results showed in [27, 36].

Theorem 3.12. *Let K be the l-th cyclotomic number field with dimension $n = \varphi(l)$ and $R = \mathcal{O}_K$ be its ring of integers. Let $\alpha = \alpha(n) \in (0, 1)$ such that $\alpha \leq \sqrt{\frac{\log n}{n}}$, and let $q = q(n) \geq 2$ be an odd prime such that $(q, l) = 1$ and $\alpha \cdot q \geq \omega(1)$. Then there is a polynomial-time quantum reduction from* Ideal-SIVP$_\gamma$ *for any $\gamma = \omega(\frac{\sqrt{n} \cdot \log n}{\alpha})$ over any ideal lattices in K to the problem of solving* D-RLWE$_{q,\psi}$ *given only k samples, where ψ is the Gaussian distribution $D_{\xi \cdot q}$ with $\xi = l \cdot \alpha \cdot (\frac{nk}{\log(nk)})^{\frac{1}{4}}$.*

Proof. By Theorem 2.13 of [36], for any $s \in R_q^\vee$ and $t \in (R^\vee)^{-1}$ such that $tR^\vee + qR = R$, the map $(a, b) \mapsto (a, t \cdot b)$ transforms $A^\vee_{s,D_\alpha}$ to $A_{t \cdot s, D_{\boldsymbol{r}}}$ with $\boldsymbol{r} = (|\sigma_1(t)| \cdot \alpha, \cdots, |\sigma_n(t)| \cdot \alpha)$, and $U(R_q \times K_{\mathbb{R}}/qR^\vee)$ to $U(R_q \times K_{\mathbb{R}}/qR)$.

Let $g = \prod_{p|l}(1 - \zeta_p)$, then we have $g \in R$, $R^\vee = \frac{g}{l} \cdot R$ and $gR + qR = R$ for any prime q such that $(q, l) = 1$ [27]. Hence $(R^\vee)^{-1} = \frac{l}{g} \cdot R$. By taking $t = l$, we get a transformation from $A^\vee_{s,D_{q \cdot \xi'}}$ with $\xi' = \alpha \cdot (\frac{nk}{\log(nk)})^{\frac{1}{4}}$ to $A_{l \cdot s, \psi}$ and from $U(R_q \times K_{\mathbb{R}}/qR^\vee)$ to $U(R_q \times K_{\mathbb{R}}/qR)$. Combining Theorem 2.18, we get the result as desired. □

Remark 3.13. *One can see the reduction loss from* D-RLWE$^\vee$ *to* D-RLWE *in cyclotomic fields is much smaller than that in general algebraic number fields, in which cases we may choose a $t \in (R^\vee)^{-1}$ such that $||t|| \leq \sqrt{n} \cdot q^{\frac{3}{4}}$ (See Theorem 3.1 and Corollary 3.2 of [36]). Big reduction loss is also the main reason that [40] designed their schemes in $R^\vee$. Also note that [42, 43] used the hardness results showed in [10]. However, methods used in [10] to get a hardness result of primal Ring-LWE problems rely heavily on the form of polynomial $\Phi_l(x)$.*

Remark 3.14. *It is well known that when $l = 2^k$ for some positive integer k, reduction form* D-RLWE$^\vee$ *to* D-RLWE *is very convenient and simple [10]. Meanwhile, multiplications are*

very efficient due to NTT algorithms in these special fields. So, in applications, we usually choose powers-of-2 cyclotomic fields. Theorem 3.12 *is simple but meaningful, which shows that reductions from* D-RLWE$^\vee$ *to* D-RLWE *in general cyclotomic fields are also convenient and simple as cases in powers-of-2 cyclotomic fields.*

We can modify the sample (a, b) of primal Ring-LWE distribution to the set $R_q \times R_q$. We discretize the error, by taking $e \hookleftarrow \lfloor D_{q\xi} \rceil_R$. The decision version of primal Ring-LWE problem becomes to distinguish between the modified distribution of $A_{s,\lfloor D_{q\xi} \rceil_R}$ and the uniform samples from $R_q \times R_q$. Notice that by using the same method proposed in [27, 40], we can change the secret s to obey the error's distribution, i.e. $s \hookleftarrow \lfloor D_{q\xi} \rceil_R$. At last, if we restrict $a \in R_q^\times$, the hardness 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 $a \hookleftarrow U(R_q^\times)$, $s \hookleftarrow \lfloor D_{q\xi} \rceil_R$, $e \hookleftarrow \lfloor D_{q\xi} \rceil_R$ and setting $b = a \cdot s + e \bmod qR$. We will use the symbol R-DLWE$^\times_{q,D_{q\xi}}$ to denote the problem of distinguishing the samples chosen from $A^\times_{s,D_{q\xi}}$ and $U(R_q^\times \times R_q)$.

We set the plain-text space to be $\mathcal{P} = R/pR$. Denote $\chi = \lfloor D_{q\xi} \rceil_R$ with $\xi = l \cdot \alpha \cdot (\frac{nk}{\log(nk)})^{\frac{1}{4}}$, where $k = O(1)$ is some positive integer. We will use the powerful basis for element $x \in R$. The NTRUEncrpyt scheme, denoted by NTRUEncrypt(n, q, p, σ), is as follows.

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

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

Decryption: Given a cipher-text c and the secret key f, compute $c_1 = f \cdot c$. Then return $m = (c_1 \bmod qR) \bmod pR$.

One may have notice that if l is a prime power, then the computations of our NTRUEncrypts are just the same as those in polynomial rings $\mathbb{Z}_q[x]/(\Phi_l(x))$, since in this cases, the powerful basis is the power basis. The analysis of decryption process and the security reduction are standard. So, we only state the results and put the proofs in Appendix B. For more details, one can also refer to [40].

Theorem 3.15. *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 $qR = \mathfrak{P}_1 \cdots \mathfrak{P}_\mathfrak{g}$ with $\mathfrak{f} \cdot \mathfrak{g} = n$. Assume that $\alpha \in (0, 1)$ satisfies $\alpha q \geq \omega(1)$ and $\alpha \leq \sqrt{\frac{\log n}{n}}$. Let $\xi = l \cdot \alpha \cdot (\frac{nk}{\log(nk)})^{\frac{1}{4}}$ with $k = O(1)$, $\varepsilon \in (0, \frac{1}{2})$ and $p \in R_q^\times$. Moreover, let $\sigma \geq n^{\frac{3}{2}} \cdot \sqrt{\ln(8nq)} \cdot q^{\frac{1}{2}+(1+\frac{\mathfrak{f}}{2})\varepsilon}$ and $3\sqrt{n} \cdot \sigma \cdot (\sqrt{n \cdot \hat{l}} + \sqrt{n} \cdot q \cdot \xi) \cdot ||p||^2_\infty < \frac{q}{2}$. Then if there exists an* IND-CPA *attack against* NTRUEncrypt(n, q, p, σ) *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 $1 - e^{-\Omega(n)}$ over the choice of the encryption randomness.*

Remark 3.16. *The hardness result of Ring-LWE problem we use is relative tight, while the error estimate is somewhat looser, since we consider the general l and use the simplest discretization to give a union bound. Different methods of error discretization may save the some factors on q and γ [39, 40, 42, 43]. However, even in the most special cases ($l = 2^k$),*

the efficiency of provably secure variant of NTRUEncrypt may not be satisfactory [5, 39]. So we don't aim to analyze the errors by using complicated methods. Setting $q = 1 \bmod l$ and p to be a integer, we have $q = [\tilde{O}(n^{6.5}), \tilde{O}(n^{7.5})]$ (due to the factor $\frac{rad(l)}{l}$) and $\gamma \leq \tilde{O}(n^8)$.

4 A Useful Key Generation Algorithm

In this section, we shall introduce a useful key generation algorithm as in [39] 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 [39], identity-based encryptions [11], identity-based signatures [41] and so on. We assume $K/\mathbb{Q}$ is a Galois extension with K an algebraic field such that $[K : \mathbb{Q}] = n$, if we do not give some special assumptions.

4.1 Useful Lemmata for Dedekind Zeta Function

In this subsection, we introduce some lemmata 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 $(\mathfrak{P}_1 \cdots \mathfrak{P}_\mathfrak{g})^\mathfrak{e}$ with $\mathfrak{P}_i$ having norm $\mathrm{N}(\mathfrak{P}_i) = p^\mathfrak{f}$ for all $i = 1, \cdots, \mathfrak{g}$. Here, one also have $\mathfrak{e} \cdot \mathfrak{f} \cdot \mathfrak{g} = n$. The Möbius function of I is defined as following:

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

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 $(\mathfrak{P}_1 \cdots \mathfrak{P}_\mathfrak{g})^\mathfrak{e}$, $\mathfrak{g}$ 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 $\mathfrak{g} \leq \min(n, p)$. Moreover, $\mathfrak{e}, \mathfrak{f}, \mathfrak{g}$ depend only on p and K. When $p \nmid \Delta_K$, we have $\mathfrak{e} = 1$, $\mathfrak{g} = \frac{n}{\mathfrak{f}}$.

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 [31], 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 4.1. *Let $[K : \mathbb{Q}] = n \geq 200$ with $|\Delta_K| = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$, assume $\mathfrak{L}(s) = \prod_{i=1}^{t}(1 - p_i^{\frac{-sn}{\mathfrak{e}_i \cdot \mathfrak{g}_i}})^{-\mathfrak{g}_i}$ 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 $\prod_{p|\Delta_K} \prod_{\mathfrak{P}|p}(1 - \mathrm{N}(\mathfrak{P})^{-s})^{-1} = \prod_{i=1}^{t}(1 - p_i^{\frac{-sn}{\mathfrak{e}_i \cdot \mathfrak{g}_i}})^{-\mathfrak{g}_i} = \mathfrak{L}(s)$. 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

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

Hence, we get

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

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

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

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

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

We now estimate these sums separately. One can easily check that $\sum_{p \nmid \Delta_K, p > n} p^{-4} \leq \int_n^\infty x^{-4} \mathrm{d}x = \frac{1}{3n^3}$, $\sum_{p \nmid \Delta_K, p > n} p^{-2} \leq \int_n^\infty x^{-2} \mathrm{d}x = \frac{1}{n}$, $\sum_{p \nmid \Delta_K, 2 \leq p \leq \frac{n}{2}} p^{-7} \leq \int_1^{\frac{n}{2}} x^{-7} \mathrm{d}x \leq \frac{1}{6}$

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

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

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

Remark 4.3. *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 4.6. 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 $\mathfrak{L}(2)$. Concrete estimates can be found in Appendix C.*

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

Lemma 4.4. *Let $N \ge 1$, $\varepsilon \in (0, 1)$ and $\mathfrak{L}(s)$ defined as in Lemma 4.1. The number $H(N)$ of ideals $I \subseteq R$ satisfying $\mathrm{N}(I) \le N$ is bounded as $H(N) \le \mathfrak{L}(1+\varepsilon) \cdot e^{\frac{2}{\varepsilon(1-\varepsilon)} \cdot n^{1-\varepsilon}} \cdot N^{1+\varepsilon}$.*

Proof. For $k \ge 1$, let $M(k)$ denote the number of ideals of R of norm exactly k. Then for $s > 1$, we have $\zeta_K(s) = \sum_{I\subseteq R} \mathrm{N}(I)^{-s} = \sum_{k\ge 1} M(k)k^{-s} \ge \sum_{k\le N} M(k)k^{-s}$. By noticing that $\sum_{k\le N} M(k)k^{-s} \ge \sum_{k\le N} M(k)N^{-s} = H(N)N^{-s}$, we obtain that $H(N) \le \zeta_K(s) \cdot N^s$. By Lemma 4.1, we get the result we need. □

We want to bound the probability that two elements f and g of R chosen from some discrete Gaussian distributions are co-prime, i.e. $(f, g) = R$. The argument follows the strategy of [39], which is an adapted version of [37]. The following lemma states a fact proved in the proof of Lemma 2.9 and Lemma 4.4 of [28].

Lemma 4.5. *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 4.6. *Assume that K is a cyclotomic field with $R = \mathcal{O}_K$, $\sigma \geq 64n^{5.7} \log n$. Then we have*

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

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 4.5, for any $\sigma \geq \eta_\delta(R)$ with some $\delta \in (0, \frac{1}{2})$, 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 using 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 2.6, 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 4.5 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

$$\frac{1}{\mathrm{N}^2(I)} \cdot \frac{2^{3-2n}}{1-2^{-2n}} + \frac{2\sqrt{|\Delta_K|}}{\mathrm{N}(I) \cdot \sigma^n} \cdot \frac{1+2^{-2n}}{(1-2^{-2n})^2} \leq \frac{2^{-2n+5}}{\mathrm{N}^2(I)}$$

for $n \geq 16$. Therefore,

$$\begin{aligned}
\sum_{\substack{I \subseteq R \\ \mathrm{N}(I) \leq C_1}} |(D^T_{R,\sigma}(I))^2 - \frac{1}{\mathrm{N}^2(I)}| &\leq \sum_{\substack{I \subseteq R \\ \mathrm{N}(I) \leq C_1}} (\frac{2^{-2n+5}}{\mathrm{N}^2(I)} + \frac{|\Delta_K|}{\sigma^{2n}} \cdot \frac{1}{(1-2^{-2n})^2}) \\
&\leq 2^{-2n+5} \cdot \zeta_K(2) + H(C_1) \cdot \frac{|\Delta_K|}{\sigma^{2n}} \cdot \frac{1}{(1-2^{-2n})^2}.
\end{aligned}$$

Note that for cyclotomic field K, there is an absolute upper bound of $\mathfrak{L}(2)$ (See Appendix C). Similarly, we can also get an absolute upper bound of $\mathfrak{L}(1.1)$. Together with Lemma 4.1, we have $\mathfrak{L}(1.1), \zeta_K(2) \leq 2^{12}$. Then, by taking $\varepsilon = 0.1$ in Lemma 4.4, we have $\sum_{\substack{I \subseteq R \\ \mathrm{N}(I) \leq C_1}} |(D^T_{R,\sigma}(I))^2 - \frac{1}{\mathrm{N}^2(I)}| \leq 2^{-2n+18}$ for $n \geq 500$.

Case 2: Assume $\mathrm{N}(I) \geq (\sigma\sqrt{n})^n := C_2$. Notice that $\lambda_1(I) \geq \sqrt{n} \cdot \mathrm{N}^{\frac{1}{n}}(I)$ 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 2.9 implies that

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

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

$n \geq 500$. Overall, we have

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

We use Lemma 4.4 by taking $\varepsilon = 0.1$ and have $H(k) \leq \mathfrak{L}(1.1)\cdot e^{\frac{200}{9}\cdot n^{0.9}}\cdot k^{1.1} \leq \mathfrak{L}(1.1)\cdot 2^{17.3n}\cdot k^{1.1}$ for $n \geq 500$. Therefore, we get

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

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

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

for $n \geq 500$.

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

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

by Lemma 4.5. Notice that $\frac{B_\delta}{\sigma}\cdot\mathrm{N}(I)^{\frac{1}{n}} \leq k \leq \frac{2B_\delta}{\sigma}\cdot\mathrm{N}(I)^{\frac{1}{n}}$, we deduce that

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

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 4.4 and get

$$\sum_{C_1<\mathrm{N}(I)<C_2} |D^T_{R,\sigma}(I)^2 - \frac{1}{\mathrm{N}(I)^2}| \leq \mathfrak{L}(1.1)\cdot 2^{17.3n}\cdot(\sigma\sqrt{n})^{1.1n}\cdot(\frac{2B_\delta}{\sigma})^{2n}\cdot(\frac{1+2^{-2n}}{1-2^{-2n}})^2. \quad (3)$$

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 $|p - \zeta_K(2)^{-1}| \leq 2^{-n}$. We get the claimed result. □

Remark 4.7. *The value of σ in this lemma seems a little large. It is essentially decided by the limitations in Case 3. For $n \geq 1000$, one can relax 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 $\sigma \geq n^{4.1}$ and $\varepsilon = 0.1$ in Case 3, then (3) becomes $\leq C \cdot 2^{18.3n} \cdot n^{3.65n} \cdot \sigma^{-0.9n} \leq C \cdot 2^{18.3n} \cdot n^{-0.04n} \leq 2^{-1.2n}$ as required. We can also set $\sigma \geq 8n^{3.6}\log n$ and take $\varepsilon = \frac{\log\log n}{\log n}$ in Case 3. Then, (3) becomes $\leq C \cdot \mathfrak{L}(1+\varepsilon) \cdot e^{\frac{4n}{\log\log n}} \cdot 2^n \cdot n^{3n+0.5n(1+\varepsilon)} \cdot \sigma^{-n(1-\varepsilon)}$, since $e^{\frac{2n^{1-\varepsilon}}{\varepsilon(1-\varepsilon)}} \leq e^{\frac{4n}{\log\log n}}$, and we can get $\sum_{C_1<\mathrm{N}(I)<C_2} |D^T_{R,\sigma}(I)^2 - \frac{1}{\mathrm{N}(I)^2}| \leq \frac{1}{2\zeta_K(2)}$ 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 [39].*

Remark 4.8. *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.*

In many applications (for example the NTRUSign schemes over different rings, some identity-based schemes [11, 41] and the following CRPSF we construct), one of the checks in the corresponding key generation algorithms is to judge wether $(f,g) = R$. Though the setting of Gaussian parameters could not reach the requirements of Lemma 4.6 (usually much smaller than the requirements of Lemma 4.6), the corresponding key generation algorithms are still PPT in practice. These, together with Remark 4.8, show that the probability that f, g are co-prime may be much higher than the theoretical estimate of Lemma 4.6.

4.2 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 $||(x,y)|| \leq$

τ 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 3.9 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 4.9. *Let $f, g \in R_q^\times$ such that $(f, g) = R$. Assume $fG_q - gF_q = q$ for some $F_q, G_q \in R$, 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, by noticing that $f^{-1}(f, g) = (1, h) \bmod q$ for $f^{-1} \in R_q$ such that $f \cdot f^{-1} = 1 \bmod qR$, we have $\Lambda_h^q \subseteq M$. The proof is finished. □

4.3 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 [39] 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 [7].
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 $\Lambda_h^q = \mathrm{Span}_R\{(f,g),(F,G)\}$ and the lattice $\Lambda = \mathrm{Span}_R\{(f,g)\}$ is a sublattice of Λ_h^q. The proofs of lemmata in this subsection are essentially the same as those in [39], the differences are that we use the powerful basis of R and the canonical embedding, other than the power basis and the coefficient embedding, to get uniform results in any cyclotomic field. We put the proofs in Appendix D.

Now we give a lemma which is helpful to bound the rejection probability of Step 7 in this key generation algorithm.

Lemma 4.10. *Let $\sigma \geq 8n^{3.6}\log n$. Then, as n grows to infinity,*

$$\mathrm{Pr}_{f,g\hookleftarrow D_{R,\sigma}}(||(F,G)||^2 > \frac{n^2 l\sigma^2}{2} + \frac{q^2\omega(n^3)}{\sigma^2}|(f,g) = R) = o(1),$$

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

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

Lemma 4.11. *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 $qR = \mathfrak{P}_1 \cdots \mathfrak{P}_\mathfrak{g}$. Assume $\sigma \geq \max\{8n^{3.6}\log n, \omega(n\ln^{0.5} n) \cdot q^{\frac{1}{\mathfrak{g}}}, \omega(n^{\frac{1}{4}} q^{\frac{1}{2}} l^{-\frac{1}{4}})\}$, then the key generation algorithm terminates in polynomial time for sufficient large n.*

Finally, we conclude the following theorem.

Theorem 4.12. *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 $qR = \mathfrak{P}_1 \cdots \mathfrak{P}_\mathfrak{g}$ such that $\mathfrak{f} \cdot \mathfrak{g} = n$, $\varepsilon > 0$ be an arbitrary positive number. Assume that $\sigma \geq \max\{8n^{3.6}\log n, \omega(n\ln^{0.5} n) \cdot q^{\frac{1}{\mathfrak{g}}}, \omega(n^{0.25} q^{0.5} l^{-0.25})\}$. 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_h^q for $h = g \cdot f^{-1} \bmod qR$. Meanwhile, if $\sigma \geq n^{\frac{3}{2}}\sqrt{\ln(8nq)} \cdot q^{\frac{1}{2}+(1+\frac{1}{2})\varepsilon}$, the distribution of h is rejected with probability $c < 1$ for some absolute constant c from a distribution whose statistical distance from $U(R_q^\times)$ is $\leq \frac{2^{8n}}{q^{\lfloor \varepsilon n \rfloor}}$.*

5 Collision Resistance Preimage Sampleable Functions

In [16], 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 [39].

5.1 Basic Definitions

First, we recall the definition of CRPSF.

Definition 5.1. *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:* $\mathbf{TrapGen}(1^n)$ *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* $\mathbf{TrapGen}(1^n)$*. Note that the following properties need only hold for a probability negligibly closed to* 1 *over the choice of* (a, t) *outputted by* $\mathbf{TrapGen}(1^n)$*.*
2. *Domain sampling with uniform outputs:* $\mathbf{SampleDom}(1^n)$ *samples an* x *from some (possibly non-uniform) 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* $y \in \mathfrak{R}_n$*,* $\mathbf{SamplePre}(t, y)$ *samples from the conditional distribution of* $x \hookleftarrow \mathbf{SampleDom}(1^n)$*, 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* $x \hookleftarrow \mathbf{SampleDom}(1^n)$ *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 5.1, we call it one-way preimage sampleable functions (PSFs).

In fact, as pointed in [16], properties 5 and 6 of Definition 5.1 implies property 4. For if not, then given a function f_a, one can find a collision as follows: choose an $x \leftarrow \mathbf{SampleDom}(1^n)$, 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 5.1.

5.2 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 [39]. We use NTRUCRPSF(n, q, σ, s) to represent the corresponding CRPSF. The detailed construction is as follows.

1. $\mathbf{TrapGen}(1^n, q, \sigma)$: By running the key generation algorithm in Subsection 4.3, 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 $\mathfrak{D}_n = \{\boldsymbol{z} \in R^2 : ||\boldsymbol{z}|| < s \cdot \sqrt{2n}\}$ 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 4.12 shows that **TrapGen** is a PPT algorithm, Theorem 2.5 implies that **SampleDom** and **SamplePre** are also PPT algorithms. The following theorem shows that for approximate parameters, the three algorithms form a valid CRPSF. Its proof is put in Appendix E.

Theorem 5.2. *Assume* $\sigma \geq \max\{8n^{3.6}\log n, \omega(n\ln^{0.5} n)\cdot q^{\frac{1}{9}}, \omega(n^{0.25}q^{0.5}l^{-0.25}), n^{\frac{3}{2}}\sqrt{\ln(8nq)}\cdot q^{\frac{1}{2}+\varepsilon}\}$ *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* 5.1 *against* ploy(n) *time adversaries, assuming the hardness of the worst-case* Ideal-SIVP$_\gamma$ *over* K *against* poly(n) *time adversaries, with* $\gamma = \tilde{O}(n \cdot s)$.

5.3 Claw-free CRPSF

We can also define and construct a kind of claw-free pairs of trapdoor functions as in [16]. A collection of claw-free pairs of one-way/collision-resistent PSFs is defined similar to Definition 5.1, 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 usual 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 5.1 by using the same proof procedure of Theorem 5.2. Claw-freeness is based on the average-case hardness of R-ISIS$^\times_{q,2,\beta}$ with $\beta = 2\sqrt{2n} \cdot s$. 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$^\times_{q,2,\beta}$. For an R-ISIS$^\times$ instance (a_1, a_2, u), we set $h = a_2^{-1} \cdot a_1 \in R_q^\times$ and $w = a_2^{-1} \cdot u \bmod qR$. 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$^\times_{q,2,\beta}$.

There is a trivial reduction from R-SIS$_{q,m,\beta+\sqrt{mn}\cdot s}$ to R-ISIS$^\times_{q,m,\beta}$ for $\beta \geq \sqrt{mn} \cdot s$, by using Theorem 3.5. Suppose that we have an R-ISIS$^\times_{q,m,\beta}$ 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 $\boldsymbol{t} \hookleftarrow D_{R^m,s}$ for appropriate s and sent $(a_1, \cdots, a_m; u = \sum_{i=1}^m a_i \cdot t_i \bmod qR)$ to the oracle $\mathfrak{O}$. Theorem 3.5 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, $\mathfrak{O}$ shall output a valid solution $\boldsymbol{z}$ to R-ISIS$_{q,m,\beta}$ for some β that admits solutions. Then, for appropriate parameters, Lemma 2.11 shows the probability that $\boldsymbol{t} = \boldsymbol{z}$ is negligible. Meanwhile, by Lemma 2.7, $||\boldsymbol{t} - \boldsymbol{z}|| \leq ||\boldsymbol{t}|| + ||\boldsymbol{z}|| \leq \beta + \sqrt{mn} \cdot s$ with overwhelming probability. We have proved the claim.

In our application, we will set $\beta = \sqrt{mn} \cdot s$. Overall, combing the fact $\eta_\varepsilon(R^m) \leq \sqrt{m} \cdot n$, Theorem 2.5 and Theorem 5.2, we get the following theorem.

Theorem 5.3. *Assume* $\sigma \geq \max\{8n^{3.6} \log n, \omega(n \ln^{0.5} n) \cdot q^{\frac{1}{9}}, \omega(n^{0.25} \cdot q^{0.5} \cdot l^{-0.25}), n^{\frac{3}{2}} \sqrt{\ln(8nq)} \cdot q^{\frac{1}{2}+\varepsilon}\}$ *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 5.4. *Note that we can set* $s \approx \tilde{O}(n^{\frac{3}{2}} \cdot \sigma)$, $q \approx \tilde{O}(\beta \cdot \sqrt{n})$ *and* $\beta \approx \tilde{O}(s \cdot \sqrt{n})$. *Hence, by our choice of parameters in Theorem* 5.2 *and Theorem* 5.3, *we both have* $s = \tilde{O}(n^7)$, $q = \tilde{O}(n^8)$ *and* $\gamma = \tilde{O}(n^8)$. *Combining Remark* 4.7, *the same estimate of* s, q, γ *is true for any* $n \geq 1000$ *(i.e.* $\sigma \geq n^{4.1}$*).*

6 NTRU Signatures over Cyclotomic Fields

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

In [16], 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 [16]. 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).
- **Verify**$(a, m, (r, \sigma))$: if $\sigma \in \mathfrak{D}_n$, $r \in \{0,1\}^k$ and $f_a(\sigma) = H(m||r)$, accept. Else, reject.

Proposition 6.1. *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 [39], 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 6.2. *Let $\varepsilon, n, q, \sigma$ and s satisfy the condition in Theorem* 5.2 *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. The authors are supported by National Cryptography Development Fund (Grant No. MMJJ20180210), NSFC Grant 61832012, NSFC Grant 61672019 and the Fundamental Research Funds of Shandong University (Grant No. 2016JC029).

References

[1] Martin Albrecht, Shi Bai, and Léo Ducas. A subfield lattice attack on overstretched ntru assumptions. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO 2016*, pages 153–178, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

[2] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(1):625–635, 1993.

[3] Joppe W. Bos, Kristin Lauter, Jake Loftus, and Michael Naehrig. Improved security for a ring-based fully homomorphic encryption scheme. In Martijn Stam, editor, *Cryptography and Coding*, pages 45–64, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[4] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In *Proceedings of the Forty-fifth Annual ACM Symposium on Theory of Computing*, STOC '13, pages 575–584, New York, NY, USA, 2013. ACM.

[5] Daniel Cabarcas, Patrick Weiden, and Johannes Buchmann. On the efficiency of provably secure ntru. In Michele Mosca, editor, *Post-Quantum Cryptography*, pages 22–39, Cham, 2014. Springer International Publishing.

[6] Jung Hee Cheon, Jinhyuck Jeong, and Changmin Lee. An algorithm for ntru problems and cryptanalysis of the ggh multilinear map without a low-level encoding of zero. *LMS Journal of Computation and Mathematics*, 19(A):255266, 2016.

[7] Henri Cohen. *A Course in Computational Algebraic Number Theory*. 0072-5285. Springer, Berlin, Heidelberg, 1993.

[8] Don Coppersmith and Adi Shamir. Lattice attacks on ntru. In Walter Fumy, editor, *Advances in Cryptology — EUROCRYPT '97*, pages 52–61, Berlin, Heidelberg, 1997. Springer Berlin Heidelberg.

[9] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. Recovering short generators of principal ideals in cyclotomic rings. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology – EUROCRYPT 2016*, pages 559–585, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

[10] Léo Ducas and Alain Durmus. Ring-lwe in polynomial rings. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *Public Key Cryptography – PKC 2012*, pages 34–51, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[11] Léo Ducas, Vadim Lyubashevsky, and Thomas Prest. Efficient identity-based encryption over ntru lattices. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology – ASIACRYPT 2014*, pages 22–41, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

[12] Léo Ducas and Phong Q. Nguyen. Learning a zonotope and more: Cryptanalysis of ntrusign countermeasures. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology – ASIACRYPT 2012*, pages 433–450, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[13] Nicolas Gama and Phong Q. Nguyen. New chosen-ciphertext attacks on ntru. In Tatsuaki Okamoto and Xiaoyun Wang, editors, *Public Key Cryptography – PKC 2007*, pages 89–106, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[14] Craig Gentry. Key recovery and message attacks on ntru-composite. In Birgit Pfitzmann, editor, *Advances in Cryptology — EUROCRYPT 2001*, pages 182–194, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[15] Craig Gentry, Jakob Jonsson, Jacques Stern, and Michael Szydlo. Cryptanalysis of the ntru signature scheme (nss) from eurocrypt 2001. In Colin Boyd, editor, *Advances in Cryptology — ASIACRYPT 2001*, pages 1–20, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[16] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC '08, pages 197–206, New York, NY, USA, 2008. ACM.

[17] Craig Gentry and Mike Szydlo. Cryptanalysis of the revised ntru signature scheme. In Lars R. Knudsen, editor, *Advances in Cryptology — EUROCRYPT 2002*, pages 299–320, Berlin, Heidelberg, 2002. Springer Berlin Heidelberg.

[18] Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H. Silverman, and William Whyte. Ntrusign: Digital signatures using the ntru lattice. In Marc Joye, editor, *Topics in Cryptology — CT-RSA 2003*, pages 122–140, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

[19] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. Ntru: A ring-based public key cryptosystem. In Joe P. Buhler, editor, *Algorithmic Number Theory*, pages 267–288, Berlin, Heidelberg, 1998. Springer Berlin Heidelberg.

[20] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. Nss: An ntru lattice-based signature scheme. In Birgit Pfitzmann, editor, *Advances in Cryptology — EUROCRYPT 2001*, pages 211–228, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[21] Nick Howgrave-Graham. A hybrid lattice-reduction and meet-in-the-middle attack against ntru. In Alfred Menezes, editor, *Advances in Cryptology - CRYPTO 2007*, pages 150–169, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[22] Éliane Jaulmes and Antoine Joux. A chosen-ciphertext attack against ntru. In Mihir Bellare, editor, *Advances in Cryptology — CRYPTO 2000*, pages 20–35, Berlin, Heidelberg, 2000. Springer Berlin Heidelberg.

[23] Paul Kirchner and Pierre-Alain Fouque. Revisiting lattice attacks on overstretched ntru parameters. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology – EUROCRYPT 2017*, pages 3–26, Cham, 2017. Springer International Publishing.

[24] Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for module lattices. *Designs, Codes and Cryptography*, 75(3):565–599, 2015.

[25] Adriana López-Alt, Eran Tromer, and Vinod Vaikuntanathan. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In *Proceedings of the Forty-fourth Annual ACM Symposium on Theory of Computing*, STOC '12, pages 1219–1234, New York, NY, USA, 2012. ACM.

[26] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, pages 1–23, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[27] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. A toolkit for ring-lwe cryptography. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology – EUROCRYPT 2013*, pages 35–54, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[28] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM J. Comput.*, 37(1):267–302, 2007.

[29] Phong Q. Nguyen. A note on the security of ntrusign. Cryptology ePrint Archive, Report 2006/387, 2006.

[30] Phong Q. Nguyen and Oded Regev. Learning a parallelepiped: Cryptanalysis of ggh and ntru signatures. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006*, pages 271–288, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[31] Cheng-dong Pan and Cheng-biao Pan. *Elementary number theory*. Peking University press, 2011.

[32] Chris Peikert. Limits on the hardness of lattice problems in ℓ_p norms. In *Proceedings of the Twenty-Second Annual IEEE Conference on Computational Complexity*, CCC '07, pages 333–346, Washington, DC, USA, 2007. IEEE Computer Society.

[33] Chris Peikert. An efficient and parallel gaussian sampler for lattices. In Tal Rabin, editor, *Advances in Cryptology – CRYPTO 2010*, pages 80–97, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[34] Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. Pseudorandomness of ring-lwe for any ring and modulus. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017, pages 461–473, New York, NY, USA, 2017. ACM.

[35] Chris Peikert and Alon Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In Shai Halevi and Tal Rabin, editors, *Theory of Cryptography*, pages 145–166, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[36] Miruna Rosca, Damien Stehlé, and Alexandre Wallet. On the ring-lwe and polynomial-lwe problems. Cryptology ePrint Archive, Report 2018/170, 2018.

[37] Brian D. Sittinger. The probability that random algebraic integers are relatively r-prime. *Journal of Number Theory*, 130(1):164 – 171, 2010.

[38] Damien Stehlé and Ron Steinfeld. Making ntru as secure as worst-case problems over ideal lattices. In Kenneth G. Paterson, editor, *Advances in Cryptology – EUROCRYPT 2011*, pages 27–47, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[39] Damien Stehlé and Ron Steinfeld. Making ntruencrypt and ntrusign as secure as standard worst-case problems over ideal lattices. Cryptology ePrint Archive, Report 2013/004, 2013.

[40] Yang Wang and Mingqiang Wang. Provably secure ntruencrypt over any cyclotomic field. In Carlos Cid and Michael J. Jacobson Jr., editors, *Selected Areas in Cryptography – SAC 2018*, pages 391–417, Cham, 2019. Springer International Publishing.

[41] Jia Xie, Yu-pu Hu, Jun-tao Gao, and Wen Gao. Efficient identity-based signature over ntru lattice. *Frontiers of Information Technology & Electronic Engineering*, 17(2):135–142, 2016.

[42] Yang Yu, Guangwu Xu, and Xiaoyun Wang. Provably secure ntru instances over prime cyclotomic rings. In Serge Fehr, editor, *Public-Key Cryptography – PKC 2017*, pages 409–434, Berlin, Heidelberg, 2017. Springer Berlin Heidelberg.

[43] Yang Yu, Guangwu Xu, and Xiaoyun Wang. Provably secure ntruencrypt over more general cyclotomic rings. Cryptology ePrint Archive, Report 2017/304, 2017.

[44] Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology – CRYPTO 2012*, pages 758–775, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

A Missing Proofs in Section 3

Proof of Lemma 3.1: 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 the equation $\boldsymbol{a}^{\perp}(I) = q(L(\boldsymbol{a}, I))^{\vee}$.

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 3.2: 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 $< B = \frac{q^{\beta}}{|\Delta_K|^{\frac{1}{n}}}$. 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 $S^{'} = [\mathfrak{g}] \setminus S$. 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 $p_i(t_i, s) \neq 0$, 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 $p_i(t_i, s) = 0$, 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 $j \in [\mathfrak{g}] \backslash S'$, the value of a_i can be arbitrary. Hence, overall, we get $p_i(t_i, s) = \frac{\prod_{j \in S \cup S''} (q^{\mathfrak{f}_j} - 1)}{\prod_{j=1}^{\mathfrak{g}} (q^{\mathfrak{f}_j} - 1)} =$

$\prod_{j\in S'\setminus S''}(q^{\mathfrak{f}_j}-1)^{-1}$. Set $\mathfrak{h}=\prod_{i\in S''}\mathfrak{q}_i R^\vee$ with $S^{''}\subseteq S^{'}$ and define a set $\mathfrak{D}=\{d:1\leq d\leq d_{S'}$ and $\exists S^{''}\subseteq S^{'}$ s.t. $d=\sum_{i\in S''}\mathfrak{f}_i\}$, where $d_{S'}=\sum_{i\in S'}\mathfrak{f}_i$. Then, we can rewrite the sum's conditions by

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

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 $d\geq\beta\cdot n$. 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, $|\mathrm{N}(t)|=\mathrm{N}((t))\geq\mathrm{N}(\mathfrak{h})\geq\mathrm{N}(\prod_{i\in S''}\mathfrak{q}_i\cdot R^\vee)=(\prod_{i\in S''}\mathrm{N}(\mathfrak{q}_i))\mathrm{N}(R^\vee)=q^d\cdot|\Delta_K|^{-1}$. Thus $|\mathrm{N}(t)|\geq\frac{q^d}{|\Delta_K|}$. We conclude that $||t||_\infty\geq\frac{1}{\sqrt{n}}||t||\geq|\mathrm{N}^{\frac{1}{n}}(t)|\geq\frac{q^{\frac{d}{n}}}{|\Delta_K|^{\frac{1}{n}}}\geq\frac{q^\beta}{|\Delta_K|^{\frac{1}{n}}}=B$.

Case 2: Suppose now that $d<\beta\cdot n$. 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, $N(B,d)\leq\frac{vol(\mathfrak{B}(B+\lambda,0))}{vol(\mathfrak{B}(\lambda,0))}=(\frac{B}{\lambda}+1)^n\leq(2q^{\beta-\frac{d}{n}}+1)^n\leq 2^{2n}q^{n\beta-d}$, where we have used the fact that $\lambda_1^\infty(\mathfrak{h})\geq\frac{q^{\frac{d}{n}}}{|\Delta_K|^{\frac{1}{n}}}$.

We claim that the number of $s\in R^\vee/(qJ_S^\vee)$ and $s\in\mathfrak{h}$ is $q^{d^{'}}$, where $d^{'}=\sum_{i\in S'\setminus S''}\mathfrak{f}_i$. 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

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

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

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

Therefore, we have

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

We finish the proof.

Proof of Lemma 3.7**:** 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 $\frac{1}{q^{\mathfrak{f}}}+2\varepsilon$, for any $i\leq\mathfrak{g}$. By Lemma 2.1 and the properties of ideal lattices, we have $\lambda_1(\mathfrak{q}_i)=\lambda_n(\mathfrak{q}_i)\leq\sqrt{n}N(\mathfrak{q}_i)^{\frac{1}{n}}(\sqrt{|\Delta_K|})^{\frac{1}{n}}$. By Lemma 2.6 and 2.10, 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 $\leq\frac{1}{q^{\mathfrak{f}}}+2\varepsilon$ as we need.

Proof of Lemma 3.8**:** Set $\varepsilon=\frac{1}{3n-1}$. Note that $\lambda_n(R)=\lambda_1(R)\leq\sqrt{n}\cdot(\sqrt{|\Delta_K|})^{\frac{1}{n}}$. By Lemma 2.6, we have $\eta_\varepsilon(R)\leq\sqrt{\frac{2\ln(6n)}{\pi}}\cdot\sqrt{n}\cdot|\Delta_K|^{\frac{1}{2n}}$. Hence, $\Pr_{x\hookleftarrow D_{R,\sigma}}(||x||\geq\sqrt{n}\cdot\sigma)\leq\frac{3n}{3n-2}2^{-n}$. Meanwhile, σ satisfies the condition in Lemma 3.7, so we get

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

Hence, we have $||f^{'}||,\ ||g||\leq\sqrt{n}\cdot\sigma$ with probability $\geq 1-2^{3-n}$. Then we conclude that $||f||\leq 1+||p||_\infty\cdot||f^{'}||\leq 2\sqrt{n}\cdot\sigma\cdot||p||_\infty$ with the same probability.

Proof of Lemma 3.9**:** 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 $|\Pr_a-(q^{\mathfrak{f}}-1)^{-\mathfrak{g}}|\leq 2^{2n+5}q^{-\lfloor\varepsilon n\rfloor}\cdot(q^{\mathfrak{f}}-1)^{-\mathfrak{g}}=:\varepsilon'$ except a fraction $\leq 2^{7n}q^{-2n\varepsilon}$ 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 $R_q^\times$. Meanwhile, $-a_2/a_1 \hookleftarrow U(R_q^\times)$ when $\boldsymbol{a} \hookleftarrow U(R_q^\times)^2$, so 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 $(f_1, f_2) \in R^2$, $f_i \hookleftarrow D^\times_{\sigma,z_i}$, 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 $\boldsymbol{t} \in \boldsymbol{a}^\perp$, $t_2 = -t_1\frac{a_1}{a_2} \bmod qR$, so t_1 and t_2 are in the same ideal I of R_q. It follows that $\boldsymbol{a}^{\perp\times} = \boldsymbol{a}^\perp \setminus (\cup_{I\subseteq R_q}\boldsymbol{a}^\perp(I)) = \boldsymbol{a}^\perp \setminus (\cup_{S\subseteq[\mathfrak{g}],S\neq\phi}\boldsymbol{a}^\perp(I_S))$. Similarly, we have $R_q^\times + qR = R \setminus (\cup_{S\subseteq[\mathfrak{g}],S\neq\phi}(I_S + qR))$. Using the inclusion-exclusion principal, we get

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

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

In the rest of the proof, we show that, except for a fraction $\leq 2^{7n}q^{-2n\varepsilon}$ of $\boldsymbol{a} \in (R_q^\times)^2$:

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

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

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

Handling (4): When $|S| \leq \varepsilon n$, we apply Lemma 3.4 with $m = 2$ and $\delta = q^{-n-\mathfrak{f}\lfloor\varepsilon n\rfloor}$. 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 $|\boldsymbol{a}^\perp(I_S)/(qR^2)| = |I_S| = q^{n-\mathfrak{f}|S|}$, since $|R_q|/|I_S| = |R_q/I_S| = q^{\mathfrak{f}|S|}$. Therefore for all except a fraction $\leq \frac{2^{7n}}{q^{2n\varepsilon}}$ of $\boldsymbol{a} \in (R_q^\times)^2$,

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

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 $D_{R^2,\sigma,-\boldsymbol{z}}(\boldsymbol{a}^\perp(I_S)) \leq 2\delta + q^{-n-\mathfrak{f}\lfloor\varepsilon n\rfloor}$. Overall, we get

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

for all except a fraction $\leq \frac{2^{7n}}{q^{2n\varepsilon}}$ of $\boldsymbol{a} \in (R_q^\times)^2$, since the are $2^{\mathfrak{g}}$ choices of S. The δ_0 satisfies $|\delta_0| \leq \frac{q^{2n}}{(q^{\mathfrak{f}}-1)^{\mathfrak{g}}}2^{\mathfrak{g}+1}(\delta + q^{-n-\mathfrak{f}\lfloor\varepsilon n\rfloor}) = (\frac{q^{\mathfrak{f}}}{q^{\mathfrak{f}}-1})^{\mathfrak{g}} \cdot 2^{\mathfrak{g}+2} \cdot q^{-\mathfrak{f}\lfloor\varepsilon n\rfloor} \leq 2^{2\mathfrak{g}+2}q^{-\mathfrak{f}\lfloor\varepsilon n\rfloor} \leq 2^{2n+2}q^{-\lfloor\varepsilon n\rfloor}$ as required.

Handling (5): Note that for any $S \in [g]$, $\det(I_S + qR) = |R/J_S| \cdot \sqrt{|\Delta_K|} = q^{\mathfrak{f}|S|} \cdot \sqrt{|\Delta_K|}$, where J_S is the ideal of R such that $J_S/(qR) = I_S$. By Minkowski's Theorem, we have $\lambda_1(I_S+qR) = \lambda_n(I_S+qR) \leq |\Delta_K|^{\frac{1}{2n}} \cdot \sqrt{n} \cdot q^{\frac{\mathfrak{f}|S|}{n}}$. Lemma 2.6 implies that $\sigma > \eta_\delta(I_S+qR)$ for any $|S| \leq \frac{\mathfrak{g}}{2}$ with $\delta = q^{-\frac{n}{2}}$. Therefore, Lemma 2.10 shows that $|D_{R,\sigma,-z_i}(I_S+qR) - q^{-\mathfrak{f}|S|}| \leq 2\delta$. For the case $|S| > \frac{\mathfrak{g}}{2}$, we can choose $S^{'} \subseteq S$ with $|S| \leq \frac{\mathfrak{g}}{2}$. Using the same argument above, we get $D_{R,\sigma,-z_i}(I_S^{'} + qR) \leq D_{R,\sigma,-z_i}(I_S + qR) \leq 2\delta + q^{-\frac{\mathfrak{f}\cdot\mathfrak{g}}{2}}$. Therefore,

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

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

B Proof of Theorem 3.15

We first show the following lemmata. Note that in general, we require that $q \cdot \alpha \geq \omega(1)$.

Lemma B.1. *For $\boldsymbol{x} \hookleftarrow \chi$, we have* $\Pr[||\boldsymbol{x}|| \geq (\frac{\sqrt{n\cdot\hat{l}}}{2} + \sqrt{n} \cdot q \cdot \xi)] \leq e^{-\Omega(n)}$.

Proof. Note that $\boldsymbol{x} = \lfloor \boldsymbol{x}' \rceil_R$ for some $\boldsymbol{x}' \hookleftarrow D_s$ with $s = q \cdot \xi$. Meanwhile, we have $E(e^{t\cdot||\boldsymbol{x}'||^2}) = (\sqrt{\frac{\pi}{\pi - t\cdot s^2}})^n$ for any $\boldsymbol{x'} \hookleftarrow D_s$ and $0 < t < \frac{\pi}{s^2}$. Therefore, by taking $t = \frac{3\pi}{4s^2}$ and using the Markov's inequality, we get $\Pr[||\boldsymbol{x}'|| > \sqrt{n} \cdot s \cdot \sqrt{\frac{4}{3\pi}}] \leq e^{n\cdot(\ln 2 - 1)} = e^{-\Omega(n)}$. By our definition, we also have $\boldsymbol{x} = \sum_{k=1}^n \lfloor x_k' \rceil \cdot \overrightarrow{p}_k$, where $\boldsymbol{x}' = \sum_{k=1}^n x_k' \cdot \overrightarrow{p}_k$. Then, $||\boldsymbol{x} - \boldsymbol{x}'|| \leq \frac{\sqrt{n\cdot\hat{l}}}{2}$, which implies that $||\boldsymbol{x}|| \leq ||\boldsymbol{x}'|| + \frac{\sqrt{n\cdot\hat{l}}}{2}$. We get the claimed result. □

Lemma B.2. *We have* $||f \cdot c||_\infty^c \leq 3\sqrt{n} \cdot \sigma \cdot (\sqrt{n \cdot \hat{l}} + \sqrt{n} \cdot q \cdot \xi) \cdot ||p||_\infty^2$ *with probability* $\geq 1 - e^{-\Omega(n)}$.

Proof. Note that $f \cdot c = pgs + pfe + fm$, we have $||f \cdot c||_\infty^c \leq ||f \cdot c||^c \leq C_1 \cdot ||f \cdot c|| \leq C_1 \cdot (||pgs|| + ||pfe|| + ||fm||)$, where $C_1 = \sqrt{\frac{rad(l)}{l}}$. Meanwhile, we have $||pgs|| \leq ||p||_\infty \cdot ||g|| \cdot ||s|| \leq ||p||_\infty \cdot \sqrt{n} \cdot \sigma \cdot (\frac{\sqrt{n\cdot\hat{l}}}{2} + \sqrt{n} \cdot q \cdot \xi)$ and $||pfe|| \leq ||p||_\infty^2 \cdot 2\sqrt{n} \cdot \sigma \cdot (\frac{\sqrt{n\cdot\hat{l}}}{2} + \sqrt{n} \cdot q \cdot \xi)$ with probability $\geq 1 - e^{-\Omega(n)}$. Since $m \in R_p$, by reducing modulo the $p \cdot \sigma(\overrightarrow{p}_k)$'s, we can represent m as $\sum_{k=1}^n \varepsilon_k \cdot p \cdot \overrightarrow{p}_k$ with $\varepsilon_k \in (-\frac{1}{2}, \frac{1}{2}]$. Therefore, we have $||fm|| \leq ||f|| \cdot ||m|| \leq 2\sqrt{n} \cdot \sigma \cdot ||p||_\infty^2 \cdot \frac{\sqrt{n\cdot\hat{l}}}{2}$. Overall, we conclude that $||f \cdot c||_\infty^c \leq 3\sqrt{n} \cdot \sigma \cdot (\sqrt{n \cdot \hat{l}} + \sqrt{n} \cdot q \cdot \xi) \cdot ||p||_\infty^2$ with probability $\geq 1 - e^{-\Omega(n)}$, since $C_1 \leq 1$. □

Lemma B.2 means that we can decrypt successfully whenever $3\sqrt{n} \cdot \sigma \cdot (\sqrt{n \cdot \hat{l}} + \sqrt{n} \cdot q \cdot \xi) \cdot ||p||_\infty^2 < \frac{q}{2}$. The CPA security can be proved easily through the same process as Lemma 16 of [40] by using Lemma 3.9 and Theorem 3.12.

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 $\mathfrak{L}(2) = \prod_{i=1}^{t}(1 - p_i^{-2\cdot \mathfrak{f}_i})^{-\mathfrak{g}_i}$, where $\mathfrak{f}_i$ is the order of $p_i \bmod l/p_i^{\alpha_i}$ and $\mathfrak{g}_i = \frac{\varphi(l/p_i^{\alpha_i})}{\mathfrak{f}_i}$. Meanwhile, $\mathfrak{e}_i \cdot \mathfrak{f}_i \cdot \mathfrak{g}_i = n$, where $\mathfrak{e}_i = \varphi(p_i^{\alpha_i})$.

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

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

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 $g_t = \varphi(p_1^{\alpha_1} \cdots p_{t-1}^{\alpha_{t-1}})$. We set $K = p_1^{\alpha_1} \cdots p_{t-1}^{\alpha_{t-1}}$. Note that, in this case, $p_t = 1 \bmod p_1^{\alpha_1} \cdots p_{t-1}^{\alpha_{t-1}}$, i.e. $p_t = N \cdot K + 1$ for some $N \geq 1$. Therefore, $(1 + \frac{1}{p_t^2-1})^{g_t} = (1 + \frac{1}{N^2 \cdot K^2 + 2N \cdot K})^{\varphi(K)} < (1 + \frac{1}{\varphi(K)})^{\varphi(K)} < e$, 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 $e^{1+\frac{1}{2}+\frac{1}{6}}$.

D Missing Proofs in Subsection 4.3

Proof of Lemma 4.10**:** 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 $\mathrm{Span}_K\{(f, g)\} = \mathrm{Span}_{\mathbb{Q}}\{(f \cdot \overrightarrow{p}_1, g \cdot \overrightarrow{p}_1), \cdots, (f \cdot \overrightarrow{p}_n, g \cdot \overrightarrow{p}_n)\}$ and $(F_q, G_q)^{pro}$ denotes the projection of (F_q, G_q) into $\mathrm{Span}_K\{(f, g)\}$. Then, $(F, G) = (F_q, G_q) - r(f, g) := (F_q, G_q)^* + (e_f, e_g)$ for some $r \in R$ and $||(F, G)||^2 = ||(F_q, G_q)^*||^2 + ||(e_f, e_g)||^2$.

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 2.13 with $t = \frac{\omega(n)}{\sqrt{2}}$, we have

$$\Pr_{f\hookleftarrow D_{R,\sigma}}(||f^{-1}|| \geq \frac{\omega(n^{\frac{3}{2}})}{\sigma}) \leq o(1).$$

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 $||(F_q, G_q)^*|| \leq \frac{q\cdot\omega(n^{\frac{3}{2}})}{\sigma}$ 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 2.7, we can deduce that $\Pr_{f,g \hookleftarrow D_{R,\sigma}}(||(f, g)|| \leq \sqrt{2n}\sigma) \geq 1 - 2^{2-n}$. 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.

Proof of Lemma 4.11**:** 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 3.7 and the choice of σ, we have $p \leq \frac{1}{32\zeta_k(2)}$ for sufficient large n. Lemma 2.9 imply that $p'_3 \leq 2^{1-2n}$. The choice of σ and Lemma 4.6 shows that $p'_4 \leq 1 - \frac{1}{2\zeta_K(2)} + o(1)$. Finally, Lemma 4.10 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.

E Proof of Theorem 5.2

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 2.5 implies that such a $\boldsymbol{z}$ can be efficiently sampled in **SampleDom**. Further, Lemma 2.9 shows that $||\boldsymbol{z}|| < s \cdot \sqrt{2n}$ with probability $1 - 2^{-4n}$.

To show property 2 of Definition 5.1, we apply Theorem 3.5 with $\delta = n^{-\omega(1)}$ to conclude that except for a fraction $\leq 2^{7n} \cdot q^{-2n\varepsilon}$ of $(a_1, a_2) \hookleftarrow U((R^{\times}_q)^2)$, we have $\Delta(a_1z_1 - a_2z_2; U(R_q)) \leq 2\delta$ 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 $\Delta(a_1a_2^{-1}z_1 - z_2; U(R_q)) = \Delta(a_1z_1 - a_2z_2; U(R_q)) \leq 2\delta$. Moreover, when $a_1, a_2 \hookleftarrow U(R^{\times}_q)$ are chosen independently, $h = a_2^{-1}a_1 \hookleftarrow U(R^{\times}_q)$. 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 $h \in R^{\times}_q$. Finally, by Theorem 4.12, the h generated by **TrapGen** is obtained by rejection with constant rejection probability $c < 1$ from a distribution within statistical distance $2^{8n}q^{-\lfloor \varepsilon n \rfloor}$ of $U(R^{\times}_q)$. 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 $\leq \frac{1}{1-c} \cdot (2^{7n}q^{-2\varepsilon n} + 2^{8n}q^{-\lfloor \varepsilon n \rfloor}) = q^{-\Omega(n)}$ over the choice of the public key h, as required.

To show properties 3 and 5 of Definition 5.1, 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 $\boldsymbol{c}$. One of $\mathbb{Z}$-bases of Λ_h^q is $(f,g)\overrightarrow{p}_1, \cdots, (f,g)\overrightarrow{p}_n; (F,G)\overrightarrow{p}_1, \cdots, (F,G)\overrightarrow{p}_n$. Moreover, since for any $i \in [n]$, we have $||\overrightarrow{p}_i||_\infty = 1$, $||(f,g)\overrightarrow{p}_i|| \leq ||\overrightarrow{p}_i||_\infty \cdot ||(f,g)|| < \sqrt{2n}\cdot\sigma$ and $||(F,G)\overrightarrow{p}_i|| \leq n\cdot\sigma\cdot\sqrt{l}$. Theorem 2.5 implies we can efficiently get a sample from $D_{\Lambda_h^q+\boldsymbol{c},s}$ 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 2.11 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 4.12 and the proof of property 2.

At the end, we show property 6 of Definition 5.1. Let $\mathfrak{A}$ be a collision-finding algorithm for NTRUCRPSF with running time $\mathrm{poly}(n)$ and has advantage $\delta = \frac{1}{\mathrm{poly}(n)}$ over the choice of the public key h and the randomness of $\mathfrak{A}$. By Theorem 4.12, 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 $\delta' = (1-c)\delta - 2^{8n}q^{-\lfloor \varepsilon n \rfloor} = \frac{1}{\mathrm{poly}(n)}$. 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 $\geq (1 - \frac{2n}{q})\delta' = \frac{1}{\mathrm{poly}(n)}$.