Journal of Computing and Security

January 2018, Volume 5, Number 1 (pp. 13–34)

http://www.jcomsec.org

A Provably Secure Variant of ETRU Based on Extended Ideal Lattices Over Direct Product of Dedekind Domains

Reza Ebrahimi Atani [a,*], Shahabaddin Ebrahimi Atani [b], Amir Hassani Karbasi [b],

[a] *Department of Computer Engineering, University of Guilan, P. O. Box 3756, Rasht, Iran.*

[b] *Department of Mathematics, University of Guilan, P. O. Box 1914, Rasht, Iran.*

ARTICLE INFO.

Article history:

Received: 02 November 2016

Revised: 06 July 2018

Accepted: 01 September 2018

Published Online: 26 December 2018

Keywords:

Lattice-Based Cryptography, ETRU, Ideal Lattices, Dedekind Domains, Provable Security.

ABSTRACT

Jarvis and Nevins presented *ETRU* in 2013 which has applausive performance with moderate key-sizes and conjectured resistance to quantum computers. *ETRU*, as an efficient *NTRUEncrypt*-like cryptosystem, is over the ring of Eisenstein integers that is faster with smaller keys for the same or better level of security than does *NTRUEncrypt* which is a desirable alternative to public-key cryptosystems based on factorisation and discrete logarithm problem. However, because of its construction, doubts have regularly arisen on its security. In this paper, we propose how to modify *ETRU* to make it provably secure, under our modified assumption of quantum hardness of standard worst-case lattice problems, restricted to extended ideal lattices related to some extensions of cyclotomic fields structures. We describe the structure of all generated polynomial rings of quotient over direct product of Dedekind domains $\mathbb{Z}$ and $\mathbb{Z}[\zeta_3]$, where ζ_3 is complex cube root of unity. We give a detailed description to show that if the private key polynomials of the *ETRU* are selected from direct product of some Dedekind domains using discrete Gaussians, then the public key, which is their ratio, is statistically indistinguishable from uniform over its range. The security then proves for our main system from the already proven hardness of the R-SIS and R-LWE problems by their extensions.

1 Introduction

Cryptographic structures based on lattices have attracted considerable interest in past years. Lattice cryptography is known with its very strong security proofs based on worst-case hardness and relatively efficient implementations for post-quantum cryptography which has considerable active research area, as well as suitable simplicity and great security against quantum computers. The NTRU encryption scheme (*NTRUEncrypt*), as the fastest lattice-based scheme, proposed by Hoffstein, Pipher and Silverman that it was first presented at the rump session of Crypto'96 [1]. Although its structure relies on computations over the convolution polynomial ring $\frac{\mathbb{Z}_q[x]}{<x^n-1>}$ for n prime and q a small integer and breaking it could be observed as a problem over Euclidean lattices [1]. The NTRU modified by its authors at the ANTS'98 conference and its practical security improved against lattice attacks [2]. *NTRUEncrypt* uses the properties of structured lattices to achieve high efficiency and that makes it a potential practical scheme. It is fundamen-

* Corresponding author.

Email addresses: rebrahimi@guilan.ac.ir (R. E. Atani), ebrahimi@guilan.ac.ir (S. E. Atani), karbasi@phd.guilan.ac.ir (A. H. Karbasi)

https://dx.doi.org/10.22108/jcs.2018.106856.0

ISSN: 2322-4460

tally different from the encryption schemes based on integer factorisation and discrete logarithm over finite fields and elliptic curves, as testified by its inclusion in the IEEE P1363 standard [3]. In addition, it is also believed to be secure against quantum computers [4]. The authors of *NTRUEncrypt* also devised a signature scheme the same as NTRU design (*NTRUSign*). The history of *NTRUSign* began with *NSS* in 2001 [5]. We refer to [6–8] for a series of improvments, cryptanalysis and the survey of *NTRUSign*. We can roughly categorize lattice-based cryptography into two groups:

- Theoretical work for providing security proofs with less efficiency [9–13].
- Applied work for providing efficient size of keys and ciphertext with heuristic security or provable security.

For readers interested in practice, we provide some references to related papers which organized by category:

- Public-key encryption [14, 15],
- Digital signatures [16, 17],
- Group and ring signatures [18],
- Identity-based cryptography [19],
- Homomorphic encryption [20–22],
- Zero-knowledge proofs and identification protocols [23–25].

To further improve the security of the NTRU cryptosystem some variants have been proposed using polynomial rings with coefficients in rings other than $\mathbb{Z}$, including $GF(2^k)[x]$ [26], the non-commutative ring of $k \times k$ matrices of polynomials in $\frac{\mathbb{Z}[x]}{<x^n-1>}$ [27], the non-commutative ring $\mathbf{M} = \frac{M_k\mathbb{Z}[x]}{<X^n-I_{k\times k}>}$, where $\mathbf{M}$ is a matrix ring of $k \times k$ matrices of polynomials in $R = \frac{\mathbb{Z}[x]}{<X^n-1>}$ [28], Dedekind domains such as $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$, *ETRU* ($\mathbb{Z}[\zeta_3]$) and $\mathbb{Z}[\zeta_5]$ [29, 30], QTRU, based on Quaternion algebra [31] and authors' lattice-based schemes [32–34]. Also, pertinent schemes and their variants are proposed in [35–37].

Provably secure lattice-based schemes have a considerable feature that their securities are proved assuming a basic lattice problem is hard in the worst-case. It originated in 1996 with Ajtai's acclaimed worst-case to average-case reduction [38], leading to a collision-resistant hash function that is as hard to break as solving several natural worst-case problems determined over Euclidean lattices. This seminal work of Ajtai is now referred to as the *Small Integer Solution* problem (SIS). Another cutting-edge introduction in the field of provably secure lattice-based cryptography was the definition in 2005 of the *Learning with Errors* problem (LWE) by Regev [14]. LWE is both sufficiently flexible to allow for the design of cryptographic functions, and hard on the standard worst-case lattice problems quantumly reduce to average-case. The SIS and LWE problems have been the foundations for public-key encryption under both chosen-plaintext [14, 32, 39] and chosen-ciphertext [40] attacks, identity-based encryption [19, 41–43], fully homomorphic encryption [44, 45], digital signatures [16, 46, 47], and the surveys [48].

The main drawback of schemes based on SIS and LWE lies in their limited efficiency since a key typically enjoys a random matrix over the ring $\mathbb{Z}_q = \frac{\mathbb{Z}}{q\mathbb{Z}}$ for a small q. Hence the space and computational complexity seem bound to be at least quadratic with respect to the security parameter. The worst-case problem is a restriction of a standard lattice problem to the specific family of structured cyclic lattices. In [49], Micciancio proposed matrices which allow for an interpretation in terms of arithmetic in the ring $\frac{\mathbb{Z}_q[x]}{<x^n-1>}$, where n is the dimension of the worst-case lattices and q is a small prime so Micciancio succeeded in restricting SIS to structured matrices while preserving a worst-case to average-case reduction and this construction leads to a family of pre-image resistant hash functions. However, implementations of this algorithm are extremely slow. In [9, 10], Peikert, Rosen, Lyubashevsky and Micciancio presented to convert the ring to $\frac{\mathbb{Z}_q[x]}{\Phi}$, where Φ is a cyclotomic polynomial (*e.g.*, $\Phi = x^n + 1$ for n a power of 2 or $\Phi = x^n + x^{n-1} + ... + x + 1$ for $n+1$ a prime). The resulting hash function was proven collision-resistant under the assumed hardness of the modified average-case problem, now often called the *Ideal Small Integer Solution* or *Ring Small Integer Solution* problem (R-SIS). The former was itself proven at least as hard as the restriction of standard worst-case lattice problems to a specific family of lattices, called *Ideal Lattices*. In [17], Lyubashevsky suggested an efficient digital signature provably as secure as R-SIS in the random oracle model. Also Stehlé *et al.* [15] introduced a structured (albeit somewhat restricted) variant of LWE, which they proved as hard as R-SIS under a quantum reduction, and allowed for the design of an asymptotically efficient CPA-secure encryption scheme. In concurrent work, Lyubashevsky *et al.* [13] introduced a ring variant of LWE, called R-LWE. Also Stehlé and Steinfield [50] presented provably secure variant of NTRU based on R-LWE and R-SIS, whose great flexibility allows for more natural and efficient cryptographic constructions.

1.1 Our Contribution

ETRU as the fastest *NTRUEncrypt*-like system strongly motivate a theoretically founded research of its security. Actually, its security has remained in doubt, in the absence of such a study so far, over the last 12 years since the initial *ETRU* publication [29, 51]. This work addresses this problem. There-

fore, we propose a modification of *ETRU* that is CPA-secure, under the assumed quantum hardness of standard worst-case problems over ideal lattices, in other words, we give a modified state-of-the-art assumption of quantum hardness of standard worst-case problems over extended ideal lattices for $\Phi = x^n + x^{n-1} + ... + x + 1$ such that $n+1$ is a prime. To this end, we reflect provably secure variant of *NTRUEncrypt* by Stehlé and Steinfield [50] then we convert *ETRU* cryptosystem by Jarvis and Nevins [30] to provably secure scheme over direct product of Dedekind domains based on extended ideal lattices. Note that we can refer to [16, 52, 53] for the use of a discrete Gaussian sampler that ensures for preventing the learning attack [8] in *NTRUSign* thus no secret information is leaked while signing.

To the best of our knowledge, it is the first time that lattice-based cryptographic schemes are designed and analyzed based on a firm theoretical grounding for the security of the NTRU-like schemes, in the asymptotic sense. For practical instantiations of our scheme we add the extra error term to the *ETRU* scheme that is a cheap way to address the lack of IND-CPA security of the original scheme. However, our scheme are likely to be significantly less efficient than the original scheme. Overview of our techniques is explained as follows.

Our main technical contribution in this work is the modification and analysis of the *ETRU* key generation algorithms. The private key in *ETRU* consists of two sparse polynomials of degrees less than n and each coefficient is an Eisenstein integer. The public key is their quotient in the ring $\frac{\mathbb{Z}[\zeta_3]_q[x]}{<x^n-1>}$ that the denominator is resampled if it is not invertible. It is shown that the public key cannot be distributed in the whole ring uniformly. Indeed, in order to use the established hardness of R-SIS and R-LWE to guarantee the uniform distribution we show a problem (weaker distribution property), which still suffices for linking the security to R-SIS and R-LWE. Hence, we exploit a discrete Gaussian with standard deviation $\approx (q^{\frac{1}{2}}, |q'|^{\frac{1}{2}})$ to sample the private key polynomials. An essential ingredient, which may be of independent interest, is a new regularity result for the ring $R_q := \frac{\mathbb{Z}_q[x]}{\Phi}$. For the cyclotomic polynomial $\Phi = x^n + 1$ with n a power of 2 there is n factors modulo prime q and we have $a_1, a_2, ..., a_m$ uniform in R_q so we want $\sum_{i \leq m}(s_i.a_i)$ to be within exponentially small statistical distance to uniformity, with small random s_i's and small m. In [15, 49], proposed regularity bounds do not suffice for $m = O(1)$. To achieve the desired closeness to uniformity, we propose a new regularity result for the quotient ring $R_{(q,q')} := \frac{(\mathbb{Z}\times\mathbb{Z}[\zeta_3])_{(q,q')}[x]}{<(1,1)x^n+(1,1)x^{n-1}+...+(1,1)x+(1,1)>}$ over direct product of Dedekind domains $\mathbb{Z}$ and $\mathbb{Z}[\zeta_3]$, where ${\zeta_3}^3 = 1$ such that $\zeta_3 = \frac{1}{2}(-1 + \sqrt{3}i)$ and the extended cyclotomic polynomial $\Phi = (1,1)x^n + (1,1)x^{n-1} + ... + (1,1)x + (1,1)$ where $n+1$ a prime factors modulo prime (q, q') (we mean the modulo (q, q') denotes the reduction of pairwise coefficients modulo q and q' coordinate-wise and component-wise): Let $(a_1, a'_1), (a_2, a'_2), ..., (a_m, a'_m)$ be uniform among the invertible elements of $R_{(q,q')}$ so we have $\sum_{i \leq m}((t_i, t'_i).(a_i, a'_i))$ then we sample the (t_i, t'_i)'s according to discrete Gaussians with small standard deviation $\approx (q^{\frac{1}{m}}, |q'|^{\frac{1}{m}})$. An additional difficulty in the proof of public key uniformity, which we handle via an inclusion-exclusion argument, is that we need the randomizers (t_i, t'_i) to be invertible in $R_{(q,q')}$ (the denominator of the public key is one such (t_i, t'_i)): we therefore resample according to a discrete Gaussian, if it is not invertible.

Finally, We present a modification of the Gentry *et al.* [16] structured variants of *inversion-based dimension reduction* of the R-SIS/R-LWE instances in the case of R-SIS: Given $(a_i, a'_i)_{i \leq m}$ uniformly and independently chosen in $R_{(q,q')}$, find an $(t, t') \in R^m \setminus (0, 0)$ with $R := \frac{(\mathbb{Z}\times\mathbb{Z}[\zeta_3])[x]}{\Phi}$ such that $\sum_i((t_i, t'_i).(a_i, a'_i)) = (0, 0) \bmod (q, q')$. If q and q' are sufficiently large, the event "(a_m, a'_m) invertible in $R_{(q,q')}$" occurs with non-negligible probability, so the average-case hardness of the problem is essentially unchanged if we divide all (a_i, a'_i)'s by (a_m, a'_m). We can then remove $(a_m, a'_m) = (1, 1)$ from the input, by making it implicit.

In order to get IND-CPA security according to our modified assumption that standard lattice problems are (quantumly) hard to solve in the worst-case for the extended ideal lattice, we make our modifications to the *ETRU* scheme as follows.

(1) We replace R_{ETRU} by $R_{(q,q')} := (\mathbb{Z} \times \mathbb{Z}[\zeta_3])_{(q,q')}[x]/ < x^n + x^{n-1} + ... + x + 1 >$ with $n+1$ a prime. We will exploit the irreducibility of $x^n + x^{n-1} + ... + x + 1$ in $\mathbb{Z}[x]$ and in $\mathbb{Z}[\zeta_3][x]$. Also the fact that R is the ring of integers of an extended cyclotomic number field.

(2) We choose (q, q') as a sufficiently large public prime such that $(q, q') \leq' (Poly(n), Poly(n))$, that is, $((\mathbb{Z} \times \mathbb{Z}[\zeta_3]), \leq')$ is a poset, if we define $(a_i, a'_i) \leq' (b_i, b'_i) \Leftrightarrow [a_i \leq b_i \; and \; a'_i \leq b'_i]$, that $(f = x^n + x^{n-1} + ... + x + 1)$ splits into n distinct linear factors modulo (q, q'). This allows us to use the search to decision reduction for R-LWE with ring $R_{(q,q')} := \frac{R}{<(q,q')>}$ (similar to [13]). This also allows us to take $(p, p') = (2, 2)$.

(3) We sample (f, f') and (g, g') from discrete Gaussians over R, rejecting the samples that are not invertible modulo (q, q'). Then we reflect that $\frac{(g,g')}{(f,f')} \bmod (q, q')$ is essentially uniformly distributed over the set of invertible elements of $R_{(q,q')}$. In order to simplify decryption, it

is choosen $(f, f') = (p, p')(\bar{f}, \bar{f}') + (1, 1)$ with $(\bar{f}, \bar{f}')$ sampled from a discrete Gaussian,.

(4) We add a small error term (e, e') in the encryption: $(C, C') = (h, h')(t, t') + (p, p')(e, e') + (M, M') \bmod (q, q')$, with (t, t') and (e, e') sampled from the R-LWE error distribution. This allows us to derive CPA security from the hardness of a variant of R-LWE.

In practice, these modifications may be expensive to implement which are similar to the modifications from [50] and a variant of R-LWE. A summarization of *ETRU* is explained as fallows.

1.2 *ETRU Cryptosystem*

In order to define the *ETRU* [30], we identify $\Phi = x^n - 1$ so we choose a prime n and set $R_{ETRU} := \frac{\mathbb{Z}[\zeta_3][x]}{<x^n-1>}$, we also choose p' and q' in $\mathbb{Z}[\zeta_3]$ relatively prime, with $|q'|$ much larger than $|p'|$. Since each *ETRU* coefficient is a pair of integers, an element of *ETRU* at degree n is comparable with an element of *NTRUEncrypt* of degree $n' = 2n$. In key generation process, private key consists of two randomly chosen polynomials $f, g \in R = \frac{\mathbb{Z}[\zeta_3][x]}{<x^n-1>}$ with their coefficients in $\mu_6 = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$. We define the inverses $F_{q'} = f^{-1} \in R_{q'}$ and $F_{p'} = f^{-1} \in R_{p'}$, where $R_{q'}$ and $R_{p'}$ are the reduced sets modulo q' and p' respectively. Hence public key is generated by $h = F_{q'} \times g$. The public key h is a polynomial with n coefficients which are reduced modulo q'. Each coefficient consists of two integers can be stored as binary strings of length $\lceil log_2(4.|q'|/3) \rceil$, hence the size of the *ETRU* public key is $K = 2n\lceil log_2(4.|q'|/3)$. An *NTRUEncrypt* public key, corresponding to polynomials with $n' = 2n$ coefficients reduced modulo an integer q, has size $K' = n'\lceil log_2(q) \rceil$. Therefore to maintain the same key size as *NTRUEncrypt* with $n' = 2n$ and $q = 2^k$, we should choose $|q'| \leqslant (3/4)q$ so that $\lceil log_2(4.|q'|/3) \rceil \leqslant \lceil log_2(q) \rceil$. In encryption and decryption process, each encryption requires the user to compute $e = \phi \times p'h + m \bmod q'$, where m is a plaintext and ϕ is a ephemeral key. In total one counts $n'^2 + n' \sim 4n^2 + 2n$ operations for *NTRUEncrypt* encryption at $n' \sim 2n$ in contrast to only $3n^2 + 27n$ operations for *ETRU* encryption. Each decryption requires the user to compute both $a = f \times e \bmod q'$ and $m = F_{p'} \times a \bmod p'$. For decryption, we have $2n'^2 + 2n' \sim 8n^2 + 4n$ operations for *NTRUEncrypt* and only $6n^2 + 29n$ operations for *ETRU*. In [30] is shown that in fact $|q'| \sim (3/8)q$ is an optimal choice in view of security against decryption failure and lattice attacks. Based on this choice the public key size for *ETRU* will be smaller than that of *NTRUEncrypt* public key.

1.3 Related Works and Structure

Regarding theoretical field of provably secure lattice-based schemes over ideal lattices, like Gentry's somewhat homomorphic scheme [20], Stehlé and Steinfeld's scheme [50] admits a security proof under the assumed worst-case hardness of $Poly(n)$-Ideal-SVP against $2^{O(g(n))}$-time quantum algorithms over ideal lattices. Their security analysis allows encrypting and decrypting $\Omega(n)$ plaintext bits for $\tilde{O}(n)$ bit operations, while achieving security against $2^{g(n)}$-time attacks, for any $g(n) \leq o(n)$. This assumption is believed to be valid for any $g(n) = o(n)$. Our modification of the above assumption shows that the security analysis for our modified *ETRU* scheme is close to Stehlé and Steinfeld's scheme, whereas ours seems stronger that is based on pairwise elements that this feature implies a greater density of elements of Dedekind domains and also allows us that we extend *NTRUEncrypt* over $(\mathbb{Z} \times \mathbb{Z}[\zeta_3])$ which has a denser lattice than the Euclidean lattices.

Also, the CCA-secure variant of *NTRUEncrypt* (NAEP) has its security on the random oracle [54] and the security of NAEP has been remained open both quantumly and classically, since the reduction from standard problems over ideal lattices to R-LWE is quantum.

Recently, in [55], it is shown how to adapt the *NTRUSign* trapdoor key generation algorithm from [50] to construct an NTRU-based lossy trapdoor function and use it to upgrade the IND-CPA security of the *NTRUEncrypt* scheme to chosen-ciphertext security (IND-CCA2) in the standard model, while preserving the same asymptotic efficiency, up to constant factors. In addition, an extension of [50] in another direction is given in [56], which shows how to modify *NTRUEncrypt* variant in [50] to achieve a fully-homomorphic multi-key encryption scheme. The security of the scheme in [56] relies, besides the hardness of R-LWE, on the assumed computational indistinguishability of the resulting public key from uniformity.

The structure of this paper is as follows. Notations and norm estimations are described in Section 2. In Section 3, we provide the necessary mathematical background of algebraic number theory, on the R-LWE and R-SIS problems and lattices based on direct product of Dedekind domains. Finally, Section 4 is devoted to the description and security proof of the our modified *ETRU* scheme.

2 Notations and Definitions

In this section, we refer to [30, 50] for notations, norm estimations and definitions. If (q, q') is a non-zero

element of $(\mathbb{Z} \times \mathbb{Z}[\zeta_3])$, we let $(\mathbb{Z} \times \mathbb{Z}[\zeta_3])_{(q,q')}$ denote the ring of integers with pairwise elements modulo (q, q'), *i.e.*, the set $(\{0, ..., q-1\}, \{0, ..., |q'|^2-1\})$ with addition and multiplication modulo (q, q') for each component. Since ${\zeta_3}^3 - 1 = (\zeta_3 - 1)({\zeta_3}^2 + \zeta_3 + 1) = 0$, we have ${\zeta_3}^2 + \zeta_3 + 1 = 0$ and hence ${\zeta_3}^2 = -1 - \zeta_3$. The ring of *Eisenstein integers*, denoted $\mathbb{Z}[\zeta_3]$, is the set of complex numbers of the form $q' = a + b\zeta_3$ with $a, b \in \mathbb{Z}$. Also we have two choices of embeddings of $\mathbb{Z}[\zeta_3]$ into $\mathbb{R}^2$. The first is via the isomorphism of additive groups $\mathbb{Z}[\zeta_3] \to \mathbb{Z}^2$ mapping $a + b\zeta_3$ to (a, b); under this embedding, right multiplication by $q' = a + b\zeta_3$ is realized by the matrix

$$< q' >= \begin{bmatrix} a & b \\ -b & a-b \end{bmatrix}$$

This is distinct from, and computationally more efficient to use than, the isometric ring monomorphism of $\mathbb{Z}[\zeta_3]$ into $\mathbb{C}$, $(\mathbb{C} \cong \mathbb{R}^2)$, given by $a + b\zeta_3 \mapsto (a - \frac{b}{2}) + i(\frac{\sqrt{3}b}{2})$. In [30] is described that the image of this isometric embedding is also a lattice in $\mathbb{R}^2$ – in fact the two-dimensional sphere-packing lattice with basis $B = \{1, \zeta_3\}$ over $\mathbb{Z}$. For $q' = a + b\zeta_3$ we have $|q'|^2 = a^2 + b^2 - ab$ as magnitude of q'. Write μ_n for the cyclic subgroup of n-th roots of unity in $\mathbb{C}$; then note that $\mu_3 = \{1, \zeta_3, \zeta_3^2 = -1 - \zeta_3\}$ and $\mu_6 = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$ are both contained in $\mathbb{Z}[\zeta_3]$. We have the following results from *ETRU*.

Theorem 1 ([30], Th. 1)**.** *The set μ_6 consists of exactly all units (invertible elements) of $\mathbb{Z}[\zeta_3]$. The primes of $\mathbb{Z}[\zeta_3]$ are (up to multiplication by a unit): $1 - \zeta_3$; rational primes $p' \in \mathbb{Z}$ satisfying $p' \equiv 2$ mod 3; and those $q' \in \mathbb{Z}[\zeta_3]$ for which $|q'|^2 = p'$ is a rational prime satisfying $p' \equiv 1$ mod 3.*

Hence the smallest Eisenstein primes (up to multiplication by a unit) are: $p' = 1 - \zeta_3$, which has $|p'|^2 = 3$; $p' = 2$, with $|p'|^2 = 4$; $p' = 2 + 3\zeta_3$, with $|p'|^2 = 7$.

Theorem 2 ([30], Th. 2)**.** *Let $q' \in \mathbb{Z}[\zeta_3]$ be non-zero and let $< q' >= \{rq' | r \in \mathbb{Z}[\zeta_3]\}$ denote the ideal in $\mathbb{Z}[\zeta_3]$ generated by q'. Then the number of residue classes of $\frac{\mathbb{Z}[\zeta_3]}{<q'>}$ is $|q'|^2$.*

Clearly, over $\mathbb{Z}$, the number of residue classes mod q is simply q. As a consequence of theorem 1 and 2, if q' is prime then $\frac{\mathbb{Z}[\zeta_3]}{<q'>}$ is a finite field with $|q'|^2$ elements. These fields are of the form $\mathbb{Z}_{p'}$ with p' a rational prime which is not congruent to 2 modulo 3, and a quadratic extension field of $\mathbb{Z}_{p'}$ otherwise. Note that if $q' \in \mathbb{Z}[\zeta_3]$, the ideal $< q' >$ is again a lattice, with basis $q'B = \{q', q'\zeta_3\}$.

To define our scheme, we choose an integer n (preferably $n + 1$ a prime) and set $R := \frac{(\mathbb{Z} \times \mathbb{Z}[\zeta_3])[x]}{<x^n + x^{n-1} + ... + x + 1>}$; For any $(p, p') \in (\mathbb{Z} \times \mathbb{Z}[\zeta_3])$, let $R_{(p,p')}$ denote the set of reduced elements of R modulo (p, p'). Note that an element $(f, f') \in R$ is a polynomial $(f_0, f'_0) + (f_1, f'_1)x + ... + (f_{n-1}, f'_{n-1})x^{n-1}$ where each coefficient have first component in $\mathbb{Z}$ and second component in $\mathbb{Z}[\zeta_3]$ as $(f_i, f'_i) = \{(a_i, a'_i) | a_i \in \mathbb{Z}, a'_i \in \mathbb{Z}[\zeta_3]$; where $a'_i = b_i + b'_i\zeta_3$; such that $a'_i = (b_i, b'_i); b_i, b'_i \in \mathbb{Z}\}$. We identify (f, f') with the vector $((a_0, a'_0), (a_1, a'_1), ..., (a_{n-1}, a'_{n-1})) \in \mathbb{Z}^{3n}$. If $a' \in \mathbb{C}$, its real and imaginary parts will be denoted by $\Re(a')$ and $\Im(a')$ respectively. We choose $(p, p') = (2, 2)$ throughout, which has several advantages, *i.e.*, reduction modulo $(2, 2)$ is straightforward.

For a ring $(R, +, \times)$, we let $R^\times$ denote the set of invertible elements of R. If (q, q') is a prime or prime power, we let $\mathbb{F}_{(q,q')}$ denote a finite field with pairwise elements. If $(x, x') \in \mathbb{R}^{3n}$, then $||(x, x')||$ denotes the Euclidean norm of (x, x') of the vector representations of x and x'. The inner product of two vectors (a, a') and (b, b') will be denoted by $< (a, a'), (b, b') >$ that is componentwise. We use $ln(m, m')$ to denote the natural logarithm as $(ln(m), ln(m'))$ and $\sqrt{(m, m')}$ to denote $(\sqrt{m}, \sqrt{m'})$. We can show that $(\mathbb{Z} \times \mathbb{Z}[\zeta_3]), \leq'$) is a partially ordered set, if we define $(a_i, a'_i) \leq' (b_i, b'_i) \Leftrightarrow [a_i \leq b_i \text{ and } a'_i \leq b'_i]$.

An adaptation of the n-dimensional Gaussian function (resp. distribution) with center (0,0) and variance (σ, σ'), will be denoted by $\rho_{(\sigma,\sigma')}(a, a') = (exp(\frac{-\pi||a||^2}{\sigma^2}), exp(\frac{-\pi||a'||^2}{\sigma'^2}))$ (resp. $\nu_{(\sigma,\sigma')}(b, b') = \frac{\rho_{(\sigma,\sigma')}(b,b')}{(\sigma,\sigma')^n}$). If F is a finite set, we let $U(F)$ denote the uniform distribution over F. If a function f over a countable domain F takes non-negative real values, its sum over an arbitrary $G \subseteq F$ will be denoted by $f(G)$. If D_1 and D_2 are two probability distributions over a discrete domain F, their statistical distance is $\Delta(D_1; D_2) = \frac{1}{2}\sum_{(a,a') \in F} |D_1(a, a') - D_2(a, a')|$. We write $z \hookleftarrow D$ when the random variable z is sampled from the distribution D.

We make use of the Landau notations $O(.)$, $\tilde{O}(.)$,$o(.)$,$\omega(.)$,$\Omega(.)$,$\tilde{\Omega}(.)$,$\theta(.)$. A function $f(n)$ is said negligible if $f(n) = n^{-\omega(1)}$. We define that a sequence of events F_n holds with overwhelming probability if $Pr[\neg F_n] \leq' (f(n), g(n))$ for negligible functions f and g. Also, we have the following result for prime elements in direct product of rings.

Lemma 1. *Let R_1 and R_2 be any commutative rings and $R = R_1 \times R_2$. If (q, q') is prime in R, then q is prime in R_1 and q' is prime in R_2.*

Proof. Let $q|ab$ and $q'|cd$ for some $a, b \in R_1$ and $c, d \in R_2$, so $ab = qk$ and $cd = q'k'$ for some $k \in R_1$ and $k' \in R_2$. It follows that $(a, c)(b, d) = (q, q')(k, k')$, and so $(q, q')|(a, c)$ or $(q, q')|(b, d)$. (Because an element $p \in R$ is called prime if $p|ab$, then $p|a$ or $p|b$). If $(q, q')|(a, c)$, then $(q, q') = (a, c)(\lambda_1, \lambda_2)$ for some $\lambda_1 \in R_1$ and $\lambda_2 \in R_2$, so $(q, q') = (a\lambda_1, c\lambda_2)$, there-

fore $q = a\lambda_1$, $q' = c\lambda_2$, then $q|a$, $q'|c$, or if $(q, q')|(b, d)$, then $(q, q') = (b, d)(\lambda_3, \lambda_4)$ for some $\lambda_3 \in R_1$ and $\lambda_4 \in R_2$, so $(q, q') = (b\lambda_3, d\lambda_4)$, therefore $q = b\lambda_3$, $q' = d\lambda_4$, then $q|b$, $q'|d$. □

We refer to [57] for irreducibility of cyclotomic polynomials Φ_n in $\mathbb{Z}[\zeta_3][x]$, where n is prime in $\mathbb{Z}[\zeta_3]$. Hence, there exist rational primes n such that Φ_n is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Z}[\zeta_3][x]$.

3 Reminders on Euclidean Lattices, *ETRU* Lattice and Algebraic Number Theory

We can refer to [50, 51] for reminders on Euclidean lattices and algebraic number theory. Then we give some adaptations of Euclidean lattices and algebraic number theory over direct product of Dedekind domains.

3.1 Euclidean Lattices, *ETRU* Lattice and Adaptations

A *lattice* is a set of the form $L = \sum_{i\leq n} \mathbb{Z}b_i$, where the b_i's are linearly independent vectors in $\mathbb{R}^n$ and are called a basis of L (full-rank lattices). The integer n is called the *lattice dimension*. The *minimum* $\lambda_1(L)$ (resp. $\lambda_1^\infty(L)$) is the Euclidean (resp. infinity) norm of any shortest non-zero vector of L. If $B = (b_i)_i$ is a basis matrix of L, the *fundamental parallelepiped* of B is the set $\mathcal{P}(B) = \{\sum_{i\leq n} c_i b_i | c_i \in [0, 1)\}$. Determinant L, $(detL)$, is denoted by the volume $|detB|$ of $\mathcal{P}(B)$ that is an invariant of the lattice L. Minkowski's theorem states that $\lambda_1(L) \leq \sqrt{n}(detL)^{\frac{1}{n}}$. In particular, we define the k-th *successive minimum* $\lambda_k(L)$ for any $k \leq n$ as the smallest r such that L contains at least k linearly independent vectors of norm $\leq r$. The Gaussian heuristic estimates the shortest non-zero vector in a lattice L is $\lambda_1(L) = \sqrt{\frac{n}{2\pi e}}(detL)^{\frac{1}{n}}$. The *dual lattice* of L is denoted as $\hat{L} = \{c \in \mathbb{R}^n | \forall i, < c, b_i > \in \mathbb{Z}\}$. The dimension of *ETRU* lattice is $4n$ and it determinant is $\lambda^{2n}|q'|^n$ such that the lattice constant λ is chosen to maximize the efficiency of finding short vectors in the lattice, therefore the shortest expected vector in *ETRU* lattice is $\lambda_1(L) \leq \sqrt{\frac{2n|q'|\lambda}{\pi e}}$ which depends on choice of λ and secret parameters f, g. In *ETRU* lattice the Euclidean and infinity norms are equal.

For our lattice $L \subseteq \mathbb{R}^{3n}$, a real $(\sigma, \sigma') >' (0, 0)$ and a point $(c, c') \in \mathbb{R}^{3n}$, we show the *lattice Gaussian distribution* of support L, deviation (σ, σ') and center (c, c') by $D_{L,(\sigma,\sigma'),(c,c')}(b, b') = \frac{\rho_{(\sigma,\sigma'),(c,c')}(b,b')}{\rho_{(\sigma,\sigma'),(c,c')}(L)}$, for any $(b, b') \in L$. We can omit the subscript (c, c') when it is (0,0). The variance for both the real and imaginary parts in *ETRU* lattice is computable (for example, see [51]). For $(\delta, \delta') >' (0, 0)$, we define the *smoothing parameter* $\eta_{(\delta,\delta')}(L)$ as the smallest $(\sigma, \sigma') >' (0, 0)$ such that $\rho_{\frac{(1,1)}{(\sigma,\sigma')}}(\hat{L}\backslash(0, 0)) \leq' (\delta, \delta')$. Since an element of *ETRU* is comparable with an element of *NTRUEncrypt* and where necessary, by rounding each of the parameter to the nearest integer, then we can use the following adaptations.

Lemma 2 (Adapted from [58], Le. 3.3). *For any full-rank lattice $L \subseteq \mathbb{R}^{3n}$ and $\delta, \delta' \in (0, 1)$, we have* $\eta_{(\delta,\delta')}(L) \leq' (\sqrt{\frac{ln((2n,4n)((1,1)+\frac{(1,1)}{(\sigma,\sigma')}))}{(\pi,\pi)}}.min(\lambda_n(L), \frac{(1,1)}{\lambda_1^\infty(\hat{L})}))$.

Lemma 3 (Adapted from [58], Proof of Le. 4.4). *For any full-rank lattice $L \subseteq \mathbb{R}^{3n}$, $(c, c') \in \mathbb{R}^{3n}$, $\delta, \delta' \in (0, 1)$ and $(\sigma, \sigma') \geq' \eta_{(\delta,\delta')}(L)$, we have $\rho_{(\sigma,\sigma'),(c,c')}(L) = \frac{(\sigma,\sigma')^n}{detL}((1, 1) + (\varepsilon, \varepsilon'))$, with $|(\varepsilon, \varepsilon')| \leq' (\delta, \delta')$. As a consequence, we have $\frac{\rho_{(\sigma,\sigma'),(c,c')}(L)}{\rho_{(\sigma,\sigma')}(L)} \in [\frac{(1,1)-(\delta,\delta')}{(1,1)+(\delta,\delta')}, (1, 1)]$.*

Lemma 4 (Adapted from [58], Le. 4.4). *For any full-rank lattice $L \subseteq \mathbb{R}^{3n}$, $(c, c') \in \mathbb{R}^{3n}$, $\delta, \delta' \in (0, 1)$ and $(\sigma, \sigma') \geq' \eta_{(\delta,\delta')}(L)$, we have $Pr_{(b,b')\hookleftarrow D_{L,(\sigma,\sigma'),(c,c')}}[||(b, b')|| \geq' (\sigma, \sigma')(\sqrt{n}, \sqrt{2n})] \leq' (\frac{(1,1)+(\delta,\delta')}{(1,1)-(\delta,\delta')}).(2^{-n}, 2^{-2n})$.*

Lemma 5 (Adapted from [16], Cor. 2.8). *Let $L' \subseteq L \subseteq \mathbb{R}^{3n}$ be two full-rank lattices. For any $(c, c') \in \mathbb{R}^{3n}$, $\delta, \delta' \in (0, \frac{1}{2})$ and $(\sigma, \sigma') \geq' \eta_{(\delta,\delta')}(L')$, we have $\Delta(D_{L,(\sigma,\sigma'),(c,c')} \bmod L'; U(\frac{L}{L'})) \leq' 2(\delta, \delta')$.*

Lemma 6 (Adapted from [11], Le. 2.11). *For any full-rank lattice $L \subseteq \mathbb{R}^{3n}$, $(c, c') \in \mathbb{R}^{3n}$, $\delta, \delta' \in (0, 1)$ and $(\sigma, \sigma') \geq' 2\eta_{(\delta,\delta')}(L)$ and $(b, b') \in L$, we have $D_{L,(\sigma,\sigma'),(c,c')}(b, b') \leq' (\frac{(1,1)+(\delta,\delta')}{(1,1)-(\delta,\delta')}).(2^{-n}, 2^{-2n})$.*

Lemma 7 (Adapted from [16], Th. 4.1). *There exists a polynomial-time algorithm that takes as input any basis $(b_i, b_i')_i$ of any lattice $L \subseteq \mathbb{Z}^{3n}$ and $\sigma, \sigma' = \omega(\sqrt{lnn})$ $max\,||(b_i, b_i')||$, and returns samples from a distribution whose statistical distance to $D_{L,(\sigma,\sigma')}$ is negligible with respect to $(n, 2n)$.*

Lemma 8 (Adapted from [50], Le. 2.7). *For any full-rank lattice $L \subseteq \mathbb{R}^{3n}$, $(c, c') \in \mathbb{R}^{3n}$, $\delta, \delta' \in (0, 1)$, $t, t' \geq \sqrt{2\pi}$, unit vector $(u, u') \in \mathbb{R}^{3n}$ and $(\sigma, \sigma') \geq' (\frac{(t,t')}{(\sqrt{2\pi},\sqrt{2\pi})}.\eta_{(\delta,\delta')}(L))$, we have:*

$$Pr_{(b,b')\hookleftarrow D_{L,(\sigma,\sigma'),(c,c')}}[| < (b, b') - (c, c'), (u, u') > | \leq' \frac{(\sigma, \sigma')}{(t, t')}] \leq' (\frac{(1, 1) + (\delta, \delta')}{(1, 1) - (\delta, \delta')} \frac{(\sqrt{2\pi e}, \sqrt{2\pi e})}{(t, t')}).$$

Similarly, if $(\sigma, \sigma') \geq' \eta_{(\delta,\delta')}(L)$, we have:

$$Pr_{(b,b')\hookleftarrow D_{L,(\sigma,\sigma'),(c,c')}}[| < (b, b') - (c, c'), (u, u') > | \geq' (t, t')(\sigma, \sigma')] \leq' (\frac{(1, 1) + (\delta, \delta')}{(1, 1) - (\delta, \delta')}(t, t')\sqrt{2\pi e}.(e^{(-\pi t^2)}, e^{(-\pi t'^2)}).$$

3.2 Algebraic Number Theory and Adaptations

3.2.1 Ideal Lattices

Assume $\Phi \in (\mathbb{Z}\times\mathbb{Z}[\zeta_3])$ be a monic degree n irreducible polynomial. We set $R := \frac{(\mathbb{Z}\times\mathbb{Z}[\zeta_3])[x]}{<\Phi>}$, then let I be an (integral) ideal of R, (*i.e.*, a subset of R that is closed under $+$ and $\times$ by arbitrary element of R. We assume $< (r_1, r'_1), ..., (r_k, r'_k) >$ denote the minimal ideal of R containing these elements, and we say that $(r_1, r'_1), ..., (r_k, r'_k)$ generate this ideal. We can reflect I as both an ideal and a lattice because by mapping polynomials to the vectors of their coefficients, we can see that a non-zero ideal I corresponds to a full-rank sublattice of $\mathbb{Z}^{3n}$. An *ideal lattice* for Φ is a sublattice of $\mathbb{Z}^{3n}$ that corresponds to a non-zero ideal $I \subseteq \frac{(\mathbb{Z}\times\mathbb{Z}[\zeta_3])[x]}{<\Phi>}$. This ideal lattice is called Φ-ideal lattice. The *algebraic norm* of a non-zero ideal I is the cardinality of the additive group $\frac{R}{I}$, and is equal to $det(I)$, where I is viewed as an ideal lattice.

We choose $\Phi = (1,1)x^n + (1,1)x^{n-1} + ... + (1,1)x + (1,1)$ where $n+1$ is a prime. In this restriction, any ideal I of R satisfies $\lambda_n(I) = \lambda_1(I)$. Also we have $R_1 := \frac{\mathbb{Z}[x]}{<x^n+x^{n-1}+...+x+1>}$ and $R_2 := \frac{\mathbb{Z}[\zeta_3][x]}{<x^n+x^{n-1}+...+x+1>}$, so we can refer to [50] and [57] to show that the rings R_1 and R_2 are the maximal order of the corresponding cyclotomic number fields $\mathbb{Q}[\zeta] \cong \frac{\mathbb{Q}[x]}{\Phi}$, where $\zeta \in \mathbb{C}$ is a primitive $n+1$-th root of unity and $\mathbb{Q}[\zeta'] \cong \frac{\mathbb{Q}[\zeta_3][x]}{\Phi}$, where $\zeta' \in \mathbb{C}$ is a primitive $n+1$-th root of unity, respectively. Hence, since this Φ corresponds to the $(n+1, n+1)$-th extended cyclotomic polynomial, the ring $R := \frac{(\mathbb{Z}\times\mathbb{Z}[\zeta_3])[x]}{\Phi}$ is the ring of integers of the corresponding extended cyclotomic number field $\mathbb{Q}[\zeta, \zeta'] = \mathbb{Q}[\zeta](\zeta') = \mathbb{Q}'[\zeta'] \cong \frac{(\mathbb{Q}\times\mathbb{Q}[\zeta_3])[x]}{\Phi} := K$; where $\zeta, \zeta' \in \mathbb{C}$ are primitive $n+1$-th root of unity respectively. We show $(\sigma_i, \sigma'_i)_{i\leq n}$ is extended canonical complex embeddings: Hence, let $(\sigma_i, \sigma'_i) : P \mapsto P(\zeta^{2i+1}, \zeta'^{2i+1})$ for $i \leq n$. For any $(\beta, \beta') \in \mathbb{Q}'[\zeta']$, we define its T_2-norm by $T_2(\beta, \beta')^2 = (\sum_{i\leq n} |\sigma_i(\beta_i)|^2, \sum_{i\leq n} |\sigma'_i(|\beta'_i|)|^2)$ and its algebraic norm by $N(\beta, \beta') = (\prod_{i\leq n} |\sigma_i(\beta_i)|, \prod_{i\leq n} |\sigma'_i(|\beta'_i|)|)$. We have from the arithmetic-geometric inequality: $(N(\beta)^{\frac{2}{n}}, N(\beta')^{\frac{1}{n}}) \leq' (\frac{1}{n}, \frac{1}{2n})T_2(\beta, \beta')^2$. The norm of the coefficient vector of (β, β') when expressed as an element of K denoted by $||(\beta_i, \beta'_i)|| = (\frac{1}{\sqrt{n}}, \frac{1}{\sqrt{2n}})T_2(\beta, \beta')$. For any element $f \in R$, we have $|N(f)| = det < f >$, where $< f >$ is the ideal of R generated by f.

The following adaptation is aconsequence of Lemma 8.

Lemma 9 (Adapted from [50], Le. 2.8)**.** *For any non-zero ideal lattice $I \subseteq R$, $(c, c') \in K$, $\delta, \delta' \in (0, 1)$, $t, t' \geq \sqrt{2\pi}$, $(u, u') \in K$ and $(\sigma, \sigma') \geq' \eta_{(\delta,\delta')}(I)$, we have $Pr_{(b,b')\hookleftarrow D_{I,(\sigma,\sigma'),(c,c')}}[||((b, b') - (c, c') \times (u, u')|| \geq' (t, t')(\sigma, \sigma')||(u, u')||(\sqrt{n}, \sqrt{2n})] \leq' (\frac{(1,1)+(\sigma,\sigma')}{(1,1)-(\sigma,\sigma')}(t, t')(n, 2n)\sqrt{2\pi e}.(e^{(-\pi t^2)}, e^{(-\pi t'^2)})$.*

3.2.2 On the Reduction of the Ring Modulo (q, q')

In *ETRU* [30] is described that based on properties of *Eisenstein integers* and their lattices, one can choose parameters n and q' smaller than those of *NTRUEncrypt* and by using appropriate cryptographic primitives, (*i.e.*, FFT in NTRU-like rings and variants of the Gaussian cumulative distribution function), one can reduce computational copmlexity and probability of *ETRU* decryption failure versus *NTRUEncrypt*, so our computed results for the second components in pairwise elements can be reduced but in this work, we use adaptation of standard models over integers. Let (q, q') be a prime element and $R_{(q,q')} := \frac{R_1}{qR_1} \times \frac{R_2}{q'R_2} = \frac{(\mathbb{Z}\times\mathbb{Z}[\zeta_3])_{(q,q')}[x]}{\Phi}$. For choosing Φ with $n+1$ a prime, we have the factorisation of Φ modulo (q, q') of the form $\Phi = \prod_{i\leq k_{(q,q')}} \Phi_i$. Here, there is an important issue, notice that we have a pairwise system such that all the Φ_i's are irreducible modulo (q, q') over $(\mathbb{Z}\times\mathbb{Z}[\zeta_3])$. Φ_i's share the same degree $d_{(q,q')} = \frac{n}{k_{(q,q')}}$. Using Theorem 1 and 2, an adaptation of the Chinese Remainder Theorem provides a ring isomorphism between $R_{(q,q')}$ and $(\mathbb{F}_{(q,|q'|^2)^{d_{(q,q')}}})^{k_{(q,q')}}$. Choosing such (q, q')'s admit natural FFT for $+$ and $\times$ computations in $\mathbb{F}_{(q,|q'|)}$ (adapted from [12], Se. 2.2), furthermore, Lemma 1 and an adaptation of Dirichlet's and Linnik's theorems assert that infinitely such primes exist and the smallest such prime is $\leq' (Poly(n), Poly(n))$.

3.2.3 Module (q, q')-ary Lattices

We define an m-dimensional lattice L with $(q, q')\mathbb{Z}^m \subseteq L \subseteq \mathbb{Z}^m$, a (q, q')-ary lattice. An R-module is a set of the form $M = \sum_{i\leq d} R\mathbf{b}_i \subseteq K^m$. If the (b_i, b'_i)'s are K-linearly independent, we denote them an R-basis of M. In [59, 60] is mentioned that contrarily to lattice, some R-modules may not admit an R-basis.

Let $(a, a') \in R^m_{(q,q')}$. We define the following families of R-modules:

$$(a, a')^\perp := \{((t_1, t'_1), ..., (t_m, t'_m)) \in R^m : \sum_i (t_i, t'_i)(a_i, a'_i) = (0, 0) \bmod (q, q')\},$$

$$L((a, a')) := \{((t_1, t'_1), ..., (t_m, t'_m)) \in R^m : \exists (s, s') \in R_{(q,q')}, \forall i, (t_i, t'_i) = (a_i, a'_i).(s, s') \bmod (q, q')\}.$$

By mapping an element of R^m to the concatenation of the coefficient vectors (matrices), these modules correspond to $3nm$-dimensional integer lattices and

we call them module (q,q')-ary lattices. In the following adaptation, we use Peikert's algorithm as a significantly faster discrete Gaussian sampler.

Lemma 10 (Adapted from [52]). *There exists a $\tilde{O}(3nm)$-time off-line / on-line algorithm that takes as input an R-basis $(b_1,b'_1),...,(b_m,b'_m)$ of a module (q,q')-ary lattice $L \subseteq R^m$, with $(q,q') = (Poly(n),Poly(n))$, $(c,c') \in \mathbb{Q}^{3nm}$ and $(\sigma,\sigma') = \omega(\sqrt{nm(lnn)})$ max $||(b_i,b'_i)||$, and returns samples from a distribution whose statistical distance to $D_{L,(\sigma,\sigma'),(c,c')}$ is negligible with respect to $(n,2n)$. The complexity bound holds assuming pre-computations (off-line) are performed using $(q,q'),(\sigma,\sigma')$ and $(b_1,b'_1),...,(b_m,b'_m)$, but not (c,c').*

3.3 Computational Problems and Adaptations

3.3.1 The Shortest Vector Problem

SVP is the most important algorithmic problem on lattices. Given a basis of a lattice L, we aim to find a shortest vector in $L \setminus \mathbf{0}$. It can be generalized to γ-SVP by asking for a non-zero vector that is no longer than $\gamma(n)$ times a solution to SVP, for a prescribed function $\gamma(.)$. If we work in the ideal lattices, we have the problem Ideal-SVP (resp. γ-Ideal-SVP), which is implicitly parameterized by a sequence of polynomials Φ of growing degrees. There is no algorithm that performs non-negligibly better for $(\gamma-)$Ideal-SVP than for $(\gamma-)$SVP. It is believed that no subexponential quantum algorithm solves the computational variants of γ-SVP or γ-Ideal-SVP in the worst case, for any γ that is polynomial in the dimension. We refer the reader to [61–63] for the fact that the smallest γ which is known to be achievable in polynomial time is exponential, up to poly-logarithmic factors in the exponent.

3.3.2 The Small Integer Solution Problem Over Rings

We can refer to [9, 11] for R-SIS problem, as an average-case variant of γ-SVP in module q-ary lattices. In the following, we give an adaptation of R-SIS in module (q,q')-ary lattice.

Definition 1. The Ring Small Integer Solution problem with parameters $(q,q'),m,(\beta,\beta')$ and Φ $(R-SIS^{\Phi}_{(q,q'),m,(\beta,\beta')})$ is as follows: Given m polynomials $(a_1,a'_1),...,(a_m,a'_m)$ chosen uniformly and independently in $R_{(q,q')}$, find $(t,t') \in (a,a')^{\perp} \setminus (0,0)$ such that $||(t,t')|| \leq' (\beta,\beta')$.

The average-case hardness of R-SIS is related to the worst-case hardness of Ideal-SVP, as follows.

Theorem 3 (Adapted from [9]). *Let $n+1$ be a prime, $\Phi = x^n + x^{n-1} + ... + x + 1$ and $(\varepsilon,\varepsilon') >' (0,0)$. Let $m > 0, (q,|q'|) >' (0,0)$ such that $(q,|q'|) \geq' (\beta,\beta')(\sqrt{n},\sqrt{2n})\omega(lnn)$ and $m, lnq, ln|q'| \leq Poly(n)$. A polynomial-time algorithm solving $(R-SIS^{\Phi}_{(q,q'),m,(\beta,\beta')})$ with non-negligible probability can be used to solve γ-Ideal-SVP in polynomial-time with $\gamma \geq' (\beta,\beta')(\sqrt{n},\sqrt{2n})\omega(\sqrt{lnn})$.*

3.3.3 The Learning With Errors Problem Over Rings

R-LWE was introduced by Lyubashevsky et al. in [13]. Let $s \in R_q$ and ψ a distribution in R_q, then $A_{s,\psi}$ is defined as the distribution obtained by sampling the pair $(a, as+e)$ with a uniformly chosen in R_q and e sampled independently from ψ. R-LWE is hard for specific error distributions ψ closely related to Gaussian. In the following, we give an adaptation of R-LWE in $R_{(q,q')}$ that it differs from the one of [13], and the noise distributions are discrete.

Definition 2. Let Γ be a distribution over a family of distributions on R. The Ring Learning With Errors Problem with parameters $(q,q'),\Gamma$ and Φ $(R-LWE^{\Phi}_{(q,q'),\Gamma})$ is as follows: Let ψ be sampled from Γ and (s,s') be chosen uniformly in $R_{(q,q')}$. Given access to an oracle O that produces samples in $R_{(q,q')} \times R_{(q,q')}$, distinguish whether O outputs samples from the distribution $A_{(s,s'),\psi}$ or $U(R_{(q,q')} \times R_{(q,q')})$. The distinguishing advantage should be non-negligible over the randomness of the input, the randomness of the samples and the internal randomness of the algorithm.

We can interpret R-LWE as a problem over module (q,q')-ary lattice. Assume m be the number of samples asked to the oracle, and let $((a_i,a'_i),(b_i,b'_i))_{i\leq m}$ be the samples. Then solving R-LWE consists in assessing whether the vector (b,b') is generated uniformly modulo the (module) lattice $L((a,a'))$ or around the origin according to some Gaussian-like distribution and then reduced modulo the lattice.

Theorem 4 (Adapted from [13]). *Assume that $\alpha(q,|q'|) = \omega(n\sqrt{lnn})$ with $\alpha \in (0,1)$ and $(q,q') = (Poly(n),Poly(n))$ prime. Consider the distribution $\bar{\Gamma}_{\alpha}$ defined below in this section. There exists a randomized polynomial-time quantum reduction from γ-Ideal-SVP to $R-LWE_{(q,q'),\bar{\Gamma}_{\alpha}}$, denoted by $R-LWE_{(q,q'),\alpha}$ in the sequal, with $\gamma = \frac{\omega(n^{1.5}lnn)}{(\alpha,\alpha)}$.*

3.3.4 Variants of R-LWE

For $(s,s') \in R_{(q,q')}$ and ψ a distribution in $R_{(q,q')}$, we define $A^{\times}_{(s,s'),\psi}$ as the distribution obtained by sampling the pair $((a,a'),((a,a')(s,s')+(e,e')))$ with (a,a') uniformly chosen in $R^{\times}_{(q,q')}$ and (e,e') sampled

independently from ψ. Let $(q, |q'|) = (\Omega(n), \Omega(n))$, then the probability for a uniform element of $R_{(q,q')}$ of being invertible is non-negligible, and thus R-LWE remains hard even when $A_{(s,s'),\psi}$ and $U(R_{(q,q')} \times R_{(q,q')})$ are respectively replaced by $A^{\times}_{(s,s'),\psi}$ and $U(R^{\times}_{(q,q')} \times R_{(q,q')})$. The latter variant is called R-LWE$^{\times}$. Also, the nonce (s, s') can be chosen from the error distribution without incurring any security reduction ([64], Le. 2). We call R-LWE$^{\times}_{HNF+}$ the corresponding modification of R-LWE. For completeness, we recall the argument. Assume an algorithm $\mathcal{J}$ can solve R-LWE$^{\times}_{HNF+}$ so we use $\mathcal{J}$ to solve R-LWE$^{\times}$. The concept is to transform samples $((a_i, a'_i), (b_i, b'_i))_i$ into samples $((a_1^{-1}a_i, a_1'^{-1}a'_i), (b_i - a_1^{-1}b_1a_i, b'_i - a_1'^{-1}b'_1a'_i))_i$, where inversion is performed in $R^{\times}_{(q,q')}$. This transformation maps $A^{\times}_{(s,s'),\psi}$ to $A^{\times}_{(-e_1,-e'_1),\psi}$, and $U(R^{\times}_{(q,q')} \times R_{(q,q')})$ to itself. In [65] is proven that a simpler variant of R-LWE with fixed number of samples and fixed spherical noise is hard.

3.3.5 Noise Definition and Noise Generation

We use a modification of Stehlé and Steinfeld's noise generation algorithm [50] such that the samples are small with probability exponentially close to 1, and can be computed in quasi-linear time and the R-LWE problem remains hard. Alternative noise generation techniques for R-LWE are described in [66, 67].

The elliptical Gaussian $\rho_{(\sigma,\sigma')}$ as the row vector of independent Gaussians $(\rho_{(\sigma_1,\sigma'_1)}, ..., \rho_{(\sigma_n,\sigma'_n)})$ is defined, where $(\sigma_i, \sigma'_i) = (\sigma_{i+n/2}, \sigma'_{i+n/2})$ for $1 \leq i \leq n/2$, $(\sigma, \sigma') \in \mathbb{R}^{3n}$ with positive coordinates. A sample from $\rho'_{(\sigma,\sigma')}$ as a sample from $\rho_{(\sigma,\sigma')}$ is defined that multiplied first from the right by:

$$\frac{1}{\sqrt{2}} \begin{pmatrix} (1,1) & (1,1) \\ (i,i) & (-i,-i) \end{pmatrix} \otimes Id_{\frac{3n}{2}} \in \mathbb{C}^{3n \times 3n},$$

and second by $V \in \mathbb{C}^{3n \times 3n}$ with upper half equal to $\frac{1}{n}(\zeta^{(-2j+1)k}, \zeta'^{(-2j+1)k})_{0 \leq j < n/2, 0 \leq k < n}$ and bottom half equal to the complex conjugate of the upper half. We can perform these matrix multiplications for each component with $O(nlnn)$ complex-valued arithmetic operations by the Cooley-Tukey FFT. Note that they are numerically extremely stable. Now a sample from $\bar{\rho'}_{(\sigma,\sigma')}$ is defined: a sample from $\rho'_{(\sigma,\sigma')}$ with absolute error $<' \frac{1}{n^2}$ is computed, then we have it by rounding it to a closest integer and reducing it modulo (q, q'); if it is within distance $\frac{1}{n^2}$ of the middle of two consecutive integers, then restart. Finally, a distribution sampled from $\bar{\Upsilon}_\alpha$ for $\alpha \geq 0$ is defined as $\bar{\rho'}_{(\sigma,\sigma')}$, where $(\sigma_i, \sigma'_i) = (\sigma_{i+n/2}, \sigma'_{i+n/2}) = (\alpha q\sqrt{1 + \sqrt{n}x_i}, \alpha|q'|\sqrt{1 + \sqrt{2n}x'_i})$ with the (x_i, x'_i)'s sampled independently from the distribution $\Gamma(2, 1)$ for $i \leq \frac{n}{2}$ such that the distribution $\Gamma(2, 1)$ has density $(xe^{-x}, x'e^{-x'})$ for $x, x' \geq 0$ and zero for $x, x' < 0$.

Sampling each component from $\bar{\rho'}_{(\sigma,\sigma')}$ and also from $\bar{\Upsilon}_\alpha$ can be obtained in time $\tilde{O}(n)$, and in our cryptographic applications, one could pre-compute such samples off-line. As a result, by taking $(r, r') = (1, 1)$ in the following result, we obtain that with probability $\geq' 1 - n^{-\omega(1)}$, any sample from $\bar{\Upsilon}_\alpha$ in R has Euclidean norm $\leq' (\alpha q n^{1/4}\omega(\sqrt{lnn}), \alpha|q'|2n^{1/4}\omega(\sqrt{lnn}))$.

Lemma 11 (Adapted from [50], Le. 2.10)**.** *Let $(y, y'), (r, r') \in R$, with (r, r') fixed and (y, y') sampled from $\bar{\Upsilon}_\alpha$, with $(\alpha q, \alpha|q'|) \geq' (n^{1/4}, 2n^{1/4})$. Then $Pr[||(y, y')(r, r')|| \geq' (\alpha q n^{1/4}\omega(\sqrt{lnn}), \alpha|q'|2n^{1/4}\omega(\sqrt{lnn}))$. $||(r, r')|| \leq' (n^{-\omega(1)}, n^{-\omega(1)})$ and $Pr[||(y, y')(r, r')||_\infty \geq' (\alpha q n^{-1/4}\omega(lnn), \alpha|q'|2n^{-1/4}\omega(lnn))$ $.||(r, r')||] \leq' (n^{-\omega(1)}, n^{-\omega(1)})$.*

4 A Provably Secure Variant of *ETRU*

In *ETRU*, the public key h is the ratio of the randomly generated private key polynomials f and g, whose coefficients have small magnitudes. We would like to derive the IND-CPA security based on standard lattice assumptions for our revised scheme from the hardness of R-LWE, so we ensure that the distribution of (h, h') is statistically very close to uniform over $R^{\times}_{(q,q')}$. We aim to sample (f, f') and (g, g') from the distribution $D^{\times}_{(\sigma,\sigma')}$, obtained by sampling from $D_{(\mathbb{Z}\times\mathbb{Z}[\zeta_3])^n,(\sigma,\sigma')} = D_{\mathbb{Z}^{3n},(\sigma,\sigma')}$ and rejecting if the sample is not invertible modulo (q, q'). Recall that the invertible elements in $\mathbb{Z}[\zeta_3]$ are sampled from μ_6 (based on fundamental domain). We will eventually choose $(\sigma, \sigma') \approx (n^c q^{1/2}, n^c|q'|^{1/2})$ for some small constant c.

We make the proof that the ratio $\frac{(g,g')}{(f,f')}$ is close to uniform when $(f, f'), (g, g') \hookleftarrow D^{\times}_{(\sigma,\sigma')}$ in the following steps.

We show that each term $|Pr_{(f,f'),(g,g')}[(g, g')/(f, f') = (a, a')] - |R^{\times}_{(q,q')}|^{-1}|$ is $<' |R^{\times}_{(q,q')}|^{-1}.(\varepsilon, \varepsilon')$, with overwhelming probability over the choice of $(a, a') \in R^{\times}_{(q,q')}$. Also for the overwhelming majority of the pairs $((a_1, a'_1), (a_2, a'_2) \in (R^{\times}_{(q,q')})^2)$, we have the equivalent probability $|Pr_{(f,f'),(g,g')}[(f, f')(a_1, a'_1) + (g, g')(a_2, a'_2) = (0, 0)] - |R^{\times}_{(q,q')}|^{-1}| <' |R^{\times}_{(q,q')}|^{-1}.(\varepsilon, \varepsilon')$, that this statement is a consequence of a regularity bound for $((a_1, a'_1), ..., (a_m, a'_m), \sum_i (t_i, t'_i)(a_i, a'_i))$ with $m = 2$. More precisely, we prove a small bound $<' |R^{\times}_{(q,q')}|^{-1}.(\varepsilon, \varepsilon')$ on the statistical distance Δ to uniformity over $(R^{\times}_{(q,q')})^m \times R_{(q,q')}$ of the distribution of $((a_1, a'_1), ..., (a_m, a'_m), \sum_i (t_i, t'_i)(a_i, a'_i))$ where the (a_i, a'_i)'s are sampled uniformly and independently in $R^{\times}_{(q,q')}$ and the (t_i, t'_i)'s are independently sampled

from $D^{\times}_{(\sigma,\sigma')}$. A similar strong regularity was used by Stehlé and Steinfeld in [50]. There is an important fact that the support of the (t_i, t'_i)'s is not a lattice. Recall that the Φ_i's are irreducible factors of Φ modulo (q, q') so with an inclusion-exclusion approach, we can write the support as the lattice $\mathbb{Z}^{3n}$ minus the union of the lattices $L_{\Phi_i} = \{(x, x') \in R : \Phi_i|((x, x') \bmod (q, q'))\}$ corresponding to the ideals $< (q, q'), \Phi_i >$ of R.

We obtain the uniformity of $\sum_i (t_i, t'_i)(a_i, a'_i)$ for the (t_i, t'_i)'s sampled from a lattice Gaussian by proving uniformity of the vector (t, t') made of the (t_i, t'_i)'s taken modulo the kernel of the map $(t, t') \mapsto \sum (t_i, t'_i)(a_i, a'_i) \bmod (q, q')$. Notice that the kernel is a lattice.

4.1 Random Module (q, q')-ary Lattice and Some New Results

We have the duality between variants of the $(a, a')^{\perp}$ and $L((a, a'))$ lattices, so we can obtain improved regularity bounds over the ring $R_{(q,q')}$ and its ideals. Now, we define a generalization of the $(a, a')^{\perp}$ and $L((a, a'))$ lattices to incorporate the ideals of $R_{(q,q')}$. Assume $\Phi = \prod_{i \le k_{(q,q')}} \Phi_i$ be the irreducible factors modulo (q, q'). Note that the Φ_i's share the same degree $d_{(q,q')} = \frac{n}{k_{(q,q')}}$. The form of the ideals of $R_{(q,q')}$ is $I_T := (\prod_{i \in T} \Phi_i).R_{(q,q')} = \{(a, a') \in R_{(q,q')} : \forall i \in T, (a, a') = (0, 0) \bmod \Phi_i\}$, with $T \subseteq \{1, ..., k_{(q,q')}\}$. Also assume L_T be the lattice corresponding to the ideal $< (q, q'), \prod_{i \le T} \Phi_i >$ of R, that is, $L_T = \{(x, x') \in R : ((x, x') \bmod (q, q')) \in I_T\}$. For $(a, a') \in R^m_{(q,q')}$ and $T \subseteq \{1, ..., k_{(q,q')}\}$, we define the families of R-modules:

$$(a, a')^{\perp}(I_T) := \{((t_1, t'_1), ..., (t_m, t'_m)) \in R^m : \forall i((t_i, t'_i) \bmod (q, q')) \in I_T \text{ and } \sum_i (t_i, t'_i)(a_i, a'_i) = (0, 0) \bmod (q, q')\},$$

$$L((a, a'), I_T) := \{((t_1, t'_1), ..., (t_m, t'_m)) \in R^m : \exists (s, s') \in R_{(q,q')}, \forall i, ((t_i, t'_i) \bmod (q, q')) = (a_i, a'_i)(s, s') \bmod I_T\},$$

where T is an arbitrary subset of $\{1, ..., k_{(q,q')}\}$. Note that $(a, a')^{\perp}(I_T)$ is the intersection of $(a, a')^{\perp}$ with the direct product of m copies of L_T. If $T = \emptyset$ (resp. $T = \{1, ..., n\}$), then we have $(a, a')^{\perp}(I_T) = (a, a')^{\perp}$ (resp. $L((a, a'), I_T) = L((a, a'))$).

We now show the duality between the modules above. We know in the ring R, (x, x') is invertible. Hence, mapping $(a(x), a'(x')) \in R$ to $(a^*(x), a'^*(x')) = (a(x^{-1}), a'(x'^{-1})) \in R$ provides ring authomorphism, so the map of factors Φ_i to itself is a bijection. Therefore, we have the following useful matrix interpretation: If we let A denote the $3n \times 3n$ matrix having as its i-th row the coefficient vector of $(x^i.a(x), x'^i.a'(x'))$ for $i = 0, ..., 3n-1$, then $(a^*(x), a'^*(x'))$ has coefficient vector the first column of A. For an ideal $I_T = (\prod_{i \in T} \Phi_i).R_{(q,q')}$ of R, we let I^*_T denote the ideal $(\prod_{i \in T} \Phi^*_i).R_{(q,q')}$.

Lemma 12 (Adapted from [50], Le. 3.1)**.** *Let $T \subseteq \{1, ..., k_{(q,q')}\}$ and $(a, a') \in R^m_{(q,q')}$. Let $\bar{T}$ be the complement of T and $(a^*, a'^*) \in R^m_{(q,q')}$ be defined by $(a^*_i, a'^*_i) = (a_i(x^{-1}), a'_i(x'^{-1}))$, for all $i \le m$. Then (considering both sets are considered as $3mn$-dimensional lattices):*

$$\widehat{(a, a')^{\perp}(I_T)} = \frac{(1, 1)}{(q, q')} L((a^*, a'^*), I^*_{\bar{T}}).$$

Proof. At first, we show that $\frac{(1,1)}{(q,q')} L((a^*, a'^*), I^*_{\bar{T}}) \subseteq \widehat{(a, a')^{\perp}(I_T)}$. Let $((t_1, t'_1), ..., (t_m, t'_m)) \in (a, a')^{\perp}(I_T)$ and $((u_1, u'_1), ..., (u_m, u'_m)) \in L((a^*, a'^*), I^*_{\bar{T}})$. We have $(t_i, t'_i) = (\sum_{j<n} t_{i,j} x^j, \sum_{j<n} t'_{i,j} x'^j)$ and $(u_i, u'_i) = (\sum_{j<n} u_{i,j} x^j, \sum_{j<n} u'_{i,j} x'^j)$ for any $i \le m$. We would like to show that $(\sum_{i \le m, j \le n} t_{i,j} u_{i,j}, \sum_{i \le m, j \le n} t'_{i,j} u'_{i,j}) = (0, 0) \bmod (q, q')$. This is equivalent to reflecting that the constant coefficient of the polynomial $(\sum_{i \le m} t_i u^*_i, \sum_{i \le m} t'_i u'^*_i)$ is $(0, 0)$ modulo (q, q'). It thus suffices to prove that $< (t, t'), (u^*, u'^*) >= (0, 0) \bmod (q, q')$. We know from definition of the (u_i, u'_i)'s, there exists $(s, s') \in R_{(q,q')}$ such that $((u_i, u'_i) \bmod (q, q')) = ((a^*_i, a'^*_i).(s, s') + (b_i, b'_i))$ for some $(b_i, b'_i) \in I^*_{\bar{T}}$. We have:

$$< (t, t'), (u^*, u'^*) >= (s^*, s'^*). < (t, t'), (a, a') > + < (t, t'), (b^*, b'^*) >= (0, 0) \bmod (q, q'),$$

where we used that $< (t, t'), (a, a') >= (0, 0) \bmod (q, q')$ by definition of (t, t') and $< (t, t'), (b^*, b'^*) >= (0, 0) \bmod (q, q')$ because $((t_i, t'_i)) \bmod (q, q') \in I_T$ and $(b^*_i, b'^*_i) \in I_{\bar{T}}$ for each $i \le m$. This provides the desired inclusion.

Conversely, by duality the reverse inclusion $\frac{(1,1)}{(q,q')} L((a^*, a'^*), I^*_{\bar{T}}) \supseteq \widehat{(a, a')^{\perp}(I_T)}$ is equivalent to $L(\widehat{(a^*, a'^*)}, I^*_{\bar{T}}) \subseteq \frac{(1,1)}{(q,q')} (a, a')^{\perp}(I_T)$, and it suffices to consider the elements of $L((a^*, a'^*), I_{\bar{T}})$ corresponding to $(s, s') = (1, 1)$. □

We have $det(L(a, a'), I_T) = (q^{(m-1)|T|d_{(q,q')}}, |q'|^{(m-1)|T|d_{(q,q')}})$ because there are

$$(q^{|T|d_{(q,q')} + m(n-|T|d_{(q,q')})}, |q'|^{|T|d_{(q,q')} + m(2n-|T|d_{(q,q')})})$$

points of $L((a, a'), I_T)$ in the rectangular cuboid $([0, q-1]^{mn}, [0, |q'|^2 - 1]^{2mn})$, so we have the Minkowski upper bound for each component

$det(L(a,a'),I_T)^{\frac{1}{mn}} = (q^{(1-\frac{1}{m})\frac{|T|}{k_{(q,q')}}}, |q'|^{(1-\frac{1}{m})\frac{|T|}{k_{(q,q')}}})$ on (the infinity norm) $\lambda_1^\infty(L(a,a'),I_T)$. Hence, we show that for a uniformly chosen $(a,a') \in (R^\times_{(q,q')})^m$, the lattice $L((a,a'),I_T)$ is extremely unlikely to contain unusually short vectors, so we construct two lower bounds as follows.

Lemma 13 (Adapted from [50], Le. 3.2)**.** *Let $n \geq 8$ and $n+1$ be a prime. Let $(q,|q'|) \geq' (5,5)$. Assume that $\Phi = x^n + x^{n-1} + ... + x + 1$ splits into $k_{(q,q')}$ distinct irreducible factors modulo (q,q'), each of degree $d_{(q,q')} = \frac{n}{k_{(q,q')}}$. Then, for $m \geq 2$ and $(\varepsilon,\varepsilon') \geq' 0$, we have:*

$$\lambda_1^\infty(L(a,a'),I_T) \geq'$$
$$\begin{cases} (\frac{1}{\sqrt{n}} q^{(1-\frac{1}{m})\frac{|T|}{k_{(q,q')}}-\varepsilon}, \frac{1}{\sqrt{2n}}|q'|^{(1-\frac{1}{m})\frac{|T|}{k_{(q,q')}}-\varepsilon'}) \\ \text{for any } 0 \leq |T| < k_{(q,q')}, \\ (q^{(1-\frac{1}{m})-k_{(q,q')}\cdot\varepsilon}, |q'|^{(1-\frac{1}{m})-k_{(q,q')}\cdot\varepsilon'}) \\ \text{for } |T| = k_{(q,q')}. \end{cases}$$

except with probability $\leq' (2^{4mn}, 2^{8mn})(q^{-\varepsilon mn}, |q'|^{-\varepsilon' 2mn})$ over the uniformly random choice of (a,a') in $(R^\times_{(q,q')})^m$.

Proof. By the Chinese Remainder Theorem (CRT), we know that $R_{(q,q')}$ (resp. $R^\times_{(q,q')}$) is isomorphic to $(\mathbb{F}_{(q,|q'|^2)^{(d_{(q,q')})}})^{k_{(q,q')}}$ (resp. $(\mathbb{F}^\times_{(q,|q'|^2)^{(d_{(q,q')})}})^{k_{(q,q')}}$). Let $\Phi_T = \prod_{i\in T}\Phi_i$ be a degree $|T|d_{(q,q')}$ generator of I_T.

Let p denote the probability that $L((a,a'),I_T)$ contains a non-zero vector (t,t') of infinity norm $<' (B,B')$. We bound p from above by using the union bound, summing the probabilities $p((t,t'),(s,s')) = Pr_{(a,a')}[\forall i, (t_i,t_i') = (a_i,a_i')(s,s') \bmod I_T]$ over all possible values for (t,t') of infinity norm $<' (B,B')$ and $(s,s') \in \frac{R_{(q,q')}}{I_T}$. Since the (a_i,a_i')'s are independent, we get $p((t,t'),(s,s')) = \prod_{i\leq m} p_i((t_i,t_i'),(s,s'))$, where $p_i((t_i,t_i'),(s,s')) = Pr_{(a_i,a_i')}[(t_i,t_i') = (a_i,a_i')(s,s') \bmod I_T]$.

We show that $gcd((s,s'),\Phi_T) = gcd((t_i,t_i'),\Phi_T)$ up to multiplication by an element of $\mathbb{F}^\times_{(q,|q'|^2)^{d_{(q,q')}}}$. If not, there exists $j \leq n$ such that either $(t_i,t_i') \bmod \Phi_j = (0,0)$ and $(s,s') \bmod \Phi_j \neq (0,0)$, or $(t_i,t_i') \bmod \Phi_j \neq (0,0)$ and $(s,s') \bmod \Phi_j = (0,0)$; In both cases, we have $p_i((t_i,t_i'),(s,s')) = (0,0)$ since $(a_i,a_i') \in R^\times_{(q,q')}$. We can perform Euclidean algorithm from [51] for Eisenstein integers, so we assume that $gcd((s,s'),\Phi_T) = gcd((t_i,t_i'),\Phi_T) = \Phi_{T'}$ for some $T' \subseteq T$ of cardinality $0 \leq k \leq |T|$. For any $j \in T'$, we have $(t_i,t_i') = (a_i,a_i')(s,s') = (0,0) \bmod \Phi_j$ regardless of the value of $(a_i,a_i') \bmod \Phi_j$ such that $(t_i,t_i') = (a_i,a_i')(s,s') \bmod \Phi_j$. Also, for any $j \notin T$, the value of $(a_i,a_i') \bmod \Phi_j$ can be arbitrary in $\mathbb{F}^\times_{(q,|q'|^2)^{d_{(q,q')}}}$. Therefore, there are $((q,|q'|)^{d_{(q,q')}} - (1,1))^{k_{(q,q')}+k-|T|}$ distinct (a_i,a_i')'s in $R^\times_{(q,q')}$ such that $(t_i,t_i') = (a_i,a_i')(s,s') \bmod I_T$. So, $p_i((t_i,t_i'),(s,s')) = ((q,|q'|)^{d_{(q,q')}} - (1,1))^{k-|T|}$.

So far, we have shown that the probability p can be bounded by:

$$p \leq' \sum_{0\leq k\leq|T|} \sum_{\substack{T'\subseteq T \\ |T'|=k}} \sum_{\substack{(s,s')\in\frac{R_{(q,q')}}{I_T} \\ \Phi_{T'}|(s,s')}} \sum_{\substack{(t,t')\in(R_{(q,q')})^m \\ \forall i,(0,0)<'||(t_i,t_i')||_\infty<'(B,B') \\ \forall i,\Phi_{T'}|(t_i,t_i')}} ((q,|q'|)^{d_{(q,q')}}-(1,1))^{m(k-|T|)}$$

For $|T'| = k$, let $n((B,B'),k)$ denote the number of $(t,t') \in R_{(q,q')}$ such that $||(t,t')||_\infty <' (B,B')$ and $(t,t') = \Phi_{T'}(t,t')'$ for some $(t,t')' \in R_{(q,q')}$ of degree $< n - kd_{(q,q')} = n(1-\frac{k}{k_{(q,q')}})$. From two upper bounds for $n((B,B'),k)$, we get the claimed bounds on $\lambda_1^\infty(L((a,a'),I_T))$.

As our first bound for $n((B,B'),k)$, with $(B,B') = (\frac{1}{\sqrt{n}}q^\beta, \frac{1}{\sqrt{2n}}|q'|^\beta)$, we claim that $n((B,B'),k) \leq' (2^{2n},2^{4n})(q^{(\beta-\frac{k}{k_{(q,q')}})n}, |q'|^{(\beta-\frac{k}{k_{(q,q')}})2n})$ for $k < \beta.k_{(q,q')}$ and $n((B,B'),k) = (0,0)$ for $k \geq \beta.k_{(q,q')}$. Hence, we can see that $n((B,B'),k)$ is the number of points of the lattice $I_{T'} + (q,q')\mathbb{Z}^{3n} =< \Phi_{T'},(q,q') >$ in the hyper rectangular cuboid $RC(2B,2B')$ of sidelengths $2B$ and $2B'$, where $RC(2B,2B') = \{(v,v') \in \mathbb{R}^{3n} : ||(v,v')||_\infty <' (B,B')\}$. Let $(\lambda,\lambda') := \lambda_1^\infty(I_{T'} + (q,q')\mathbb{Z}^{3n})$. If we center a hyper rectangular cuboid $RC(\lambda,\lambda')$ of sidelengths λ and λ' on each of the $n((B,B'),k)$ points of $I_{T'} + (q,q')\mathbb{Z}^{3n}$ in $RC(2B,2B')$, the resulting $n((B,B'),k)$ hyper rectangular cuboids do not intersect, and yet are all contained within the enlarged hyper rectangular cuboid $RC(2B+\lambda,2B'+\lambda')$. It follows that $n((B,B'),k) \leq' \frac{vol(RC(2B+\lambda,2B'+\lambda'))}{vol(RC(\lambda,\lambda'))} = ((\frac{2B}{\lambda}+1)^n, (\frac{2B'}{\lambda'}+1)^{2n})$. Now we can show a derivation of lower bound on (λ,λ'), notice that for any $(t,t') \in I_{T'}$, we have $N(t,t') = N(< t,t' >) \geq' N(< \Phi_{T'},(q,q') >) = (q,|q'|)^{kd_{(q,q')}}$, where the inequality is because the ideal $< (t,t') >$ is a sub-ideal of $< \Phi_{T'},(q,q') >$, and the last equality is because $deg\Phi_{T'} = kd_{(q,q')}$, so, $||(t,t')|| = (\frac{1}{\sqrt{n}}T_2(t), \frac{1}{\sqrt{2n}}T_2(t')) \geq' (N(t)^{1/n}, N(t')^{1/2n}) \geq' (q^{\frac{k}{k_{(q,q')}}}, |q'|^{\frac{k}{k_{(q,q')}}})$. By equivalence of norms, we have $||(t,t')||_\infty \geq' (\lambda,\lambda') \geq' (\frac{1}{\sqrt{n}}q^{\frac{k}{k_{(q,q')}}}, \frac{1}{\sqrt{2n}}|q'|^{\frac{k}{k_{(q,q')}}})$. Therefore, using $(B,B') = (\frac{1}{\sqrt{n}}q^\beta, \frac{1}{\sqrt{2n}}|q'|^\beta)$, for $k \geq \beta.k_{(q,q')}$, we conclude that $(\lambda,\lambda') \geq' (B,B')$ so $n((B,B'),k) = (0,0)$, while for $k < \beta.k_{(q,q')}$,

we have $n((B,B'),k) \leq' ((\frac{2B}{\lambda}+1)^n, (\frac{2B'}{\lambda'}+1)^{2n}) \leq' ((2q^{\beta-\frac{k}{k_{(q,q')}}}+1)^n, (2|q'|^{\beta-\frac{k}{k_{(q,q')}}}+1)^{2n}) \leq' (2^{2n},2^{4n})(q^{(\beta-\frac{k}{k_{(q,q')}})n}, |q'|^{(\beta-\frac{k}{k_{(q,q')}})2n})$, as claimed.

As our second bound for $n((B,B'),k)$, we claim that $n((B,B'),k) \leq' (2B^{n-kd_{(q,q')}}, 2B'^{2n-kd_{(q,q')}}) = (2B^{n(1-\frac{k}{k_{(q,q')}})}, 2B'^{2n(1-\frac{k}{k_{(q,q')}})})$. Since the degree of $\Phi_{T'}$ is $kd_{(q,q')}$, each component of the vector $(t,\bar{t}')$ formed by the $n-kd_{(q,q')}$ low-order coefficients of $(t,t') = \Phi_{T'}(t,t')'$ is related to the vector $(t,\bar{t}')'$ formed by the $n-kd_{(q,q')}$ low-order coefficients of $(t,t')'$ by a lower triangular $(3n-3kd_{(q,q')}) \times (3n-3kd_{(q,q')})$ matrix whose diagonal coefficients are equal to the non-zero constant coefficient of $\Phi_{T'}$. So this matrix is non-singular modulo (q,q') and the mapping from $(t,\bar{t}')'$ to $(t,\bar{t}')$ is one-to-one. Hence, this provides the claim.

We know the number of subsets of T is $2^{|T|}$, and the number of $(s,s') \in \frac{R_{(q,q')}}{I_T}$ divisible by $\Phi_{T'}$ is $(q,|q'|)^{d_{(q,q')}(|T|-k)}$, then we have:

$$p \leq' (2^{(m+1)|T|}, 2^{(m+1)|T|}) \times max_{0\leq k\leq |T|} \frac{n((B,B'),k)^m}{(q^{(m-1)(|T|-k)d_{(q,q')}}, |q'|^{(m-1)(|T|-k)d_{(q,q')}})}$$

Based on our first bound, we get:

$$p \leq' (2^{(m+1)(|T|+2n)}, 2^{(m+1)(|T|+4n)}) \times max_{0\leq k\leq \beta.k_{(q,q')}} (q^{n(m(\beta-\frac{k}{k_{(q,q')}})-(m-1)\frac{|T|-k}{k_{(q,q')}})}, |q'|^{2n(m(\beta-\frac{k}{k_{(q,q')}})-(m-1)\frac{|T|-k}{k_{(q,q')}})})$$

observed as a function of k, for $k=0$, the exponent is maximized. It then has the value $(-mn\varepsilon, -2mn\varepsilon')$, when $\beta = (1-\frac{1}{m})\frac{|T|}{k_{(q,q')}} - (\varepsilon,\varepsilon')$. This gives the first claimed bound on $\lambda_1^\infty(L(a,a'),I_T)$. For $|T| = k_{(q,q')}$, based on our second bound on $n((B,B'),k)$ with $(B,B') = (q^\beta, |q'|^\beta)$, and $n((B,B'),k_{(q,q')}) = (0,0)$, we have:

$$p \leq' (2^{(m+1)(|T|+2n)}, 2^{(m+1)(|T|+4n)}) \times max_{0\leq k<k_{(q,q')}} (q^{n((1-\beta)m-1)(\frac{k}{k_{(q,q')}}-1)}, |q'|^{2n((1-\beta)m-1)(\frac{k}{k_{(q,q')}}-1)}) = (2^{(m+1)(|T|+2n)}, 2^{(m+1)(|T|+4n)}) .(q^{-\frac{n}{k_{(q,q')}}((1-\beta)m-1)}, |q'|^{-\frac{2n}{k_{(q,q')}}((1-\beta)m-1)}),$$

where for any $\beta \leq 1-\frac{1}{m}$, the last equality is satisfied. Using $\beta = 1-\frac{1}{m}-k_{(q,q')}(\varepsilon,\varepsilon')$ gives the second claimed bound on $\lambda_1^\infty(L(a,a'),I_T)$. □

We now give a lower bound on $\lambda_1^\infty((a,a')^\perp(I_T))$ for the distribution of the $\frac{(g,g')}{(f,f')}$ with $k_{(q,q')} = O(1)$.

Lemma 14 (Adapted from [50], Le. 3.3). *Let $n \geq 8$ such that $n+1$ be a prime and $(q,|q'|) \geq' (5,5)$. Assume that $\Phi = x^n + x^{n-1} + ... + x + 1$ splits into $k_{(q,q')}$ distinct irreducible factors modulo (q,q'), each of degree $d_{(q,q')} = \frac{n}{k_{(q,q')}}$. Then, for $m \geq 2$ and $(\varepsilon,\varepsilon') \geq' (0,0)$, we have:*

$$\lambda_1^\infty((a,a')^\perp, I_T) \geq' \begin{cases} (\frac{1}{\sqrt{n}} q^{\frac{1}{m}+(1-\frac{1}{m})\frac{|T|}{k_{(q,q')}}-\varepsilon}, \frac{1}{\sqrt{2n}}|q'|^{\frac{1}{m}+(1-\frac{1}{m})\frac{|T|}{k_{(q,q')}}-\varepsilon'}) \\ \text{for any } 0<|T|\leq k_{(q,q')}, \\ (q^{\frac{1}{m}-k_{(q,q')}.\varepsilon}, |q'|^{\frac{1}{m}-k_{(q,q')}.\varepsilon'}) \\ \text{for } |T|=0. \end{cases}$$

except with probability $\leq' (2^{4n}, 2^{8n})(q^{-\varepsilon mn}, |q'|^{-\varepsilon' 2mn})$ over the uniformly random choice of (a,a') in $(R^\times_{(q,q')})^m$.

Proof. By the proof of Lemma 13, let p denote the probability that $L((a,a')^\perp(I_T))$ contains a non-zero vector (t,t') of infinity norm $<' (B,B')$. By using the union bound, summing the probabilities $p(t,t') = Pr_{(a,a')}[\sum_{i\leq m}(a_i,a'_i)(t_i,t'_i) = (0,0) \bmod (q,q')]$ over all possible values for (t,t') of infinity norm $<' (B,B')$ and $(t_i,t'_i) \in I_T$ for $i=1,...,m$. By CRT, we have $p(t,t') = \prod_{j\leq k_{(q,q')}} p_j(t,t')$, where $p_j(t,t') = Pr_{(a,a')}[\sum_{i\leq m}(a_i,a'_i)(t_i,t'_i) = (0,0) \bmod \Phi_j]$. Let $\Phi_T = \prod_{i\in T}\Phi_i, \Phi_{\bar{T}} = \prod_{i\in\bar{T}}\Phi_i$ and $\Phi_{T'} = gcd((t_1,t'_1),...,(t_m,t'_m),\Phi_{\bar{T}}) = \prod_{i\in T'}\Phi_i$ for some $T' \subseteq \bar{T}$ of cardinality $0 \leq k \leq |\bar{T}|$. For any $j \in T \cup T'$, we have $\sum_{i\leq m}(t_i,t'_i)(a_i,a'_i) = (0,0) \bmod \Phi_j$ regardless of the value of $(a_i,a'_i) \bmod \Phi_j$. For any $j \in \bar{T}\backslash T$, there exists $i \leq m$ such that $(t_i,t'_i) \neq (0,0) \bmod \Phi_j$ so that for any $\{(a_j,a'_j)\}_{j\neq i}$, there is a unique value of $(a_i,a'_i) \bmod \Phi_j$ such that $\sum_{i\leq m}(t_i,t'_i)(a_i,a'_i) = (0,0) \bmod \Phi_j$; so $p_j(t,t') = \frac{(1,1)}{(q,|q'|)^{d_{(q,q')}}-(1,1)}$. Therefore, we have $p(t,t') = \frac{(1,1)}{((q,|q'|)^{d_{(q,q')}}-(1,1))^{|\bar{T}|-k}}$, and:

$$p \leq' \sum_{0\leq k\leq|\bar{T}|} \sum_{\substack{T'\subseteq\bar{T} \\ |T'|=k}} \sum_{\substack{(t,t')\in(R_{(q,q')})^m \\ \forall i,(0,0)<'||(t_i,t'_i)||_\infty<'(B,B') \\ \forall i,\Phi_T.\Phi_{T'}|(t_i,t'_i)}} \frac{(1,1)}{((q,|q'|)^{d_{(q,q')}}-(1,1))^{|\bar{T}-k|}}.$$

For T' with $|T'| = k$, assume $n((B,B'),k)$ denote the number of $(t,t') \in R_{(q,q')}$ such that $||(t,t')||_\infty <' (B,B')$ and $(t,t') = \Phi_T.\Phi_{T'}(t,t')'$ for some $(t,t') \in R_{(q,q')}$ of degree $<' \frac{n(1-(k+|T|)}{k_{(q,q')}})$. Similar to the proof of Lemma 13, we give two upper bounds for $n((B,B'),k)$. At first, with $(B,B') = (\frac{1}{\sqrt{n}}q, \frac{1}{\sqrt{2n}}|q'|)^\beta$, we have $n((B,B'),k) = (0,0)$

for $k \geq \beta.k_{(q,q')} - |T|$, while $n((B,B'),k) \leq' (2^{2n}, 2^{4n})(q^{\beta - \frac{(|T|+k}{k_{(q,q')}})^n}, |q'|^{\beta - \frac{(|T|+k}{k_{(q,q')}})^{2n}})$ for $k < \beta.k_{(q,q')} - |T|$.

The second bound is

$n((B,B'),k) \leq' (2B^{n(1-\frac{|T|+k}{k_{(q,q')}})}, 2B'^{2n(1-\frac{|T|+k}{k_{(q,q')}})})$. By (B,B'), we have:

$$p \leq' (2^{2|\bar{T}|+2n}, 2^{2|\bar{T}|+4n}) \times$$
$$max_{0 \leq k < \beta.k_{(q,q')}} (q^{n(m(\beta - \frac{|T|+k}{k_{(q,q')}}) - \frac{|\bar{T}|-k}{k_{(q,q')}})},$$
$$|q'|^{2n(m(\beta - \frac{|T|+k}{k_{(q,q')}}) - \frac{|\bar{T}|-k}{k_{(q,q')}})}).$$

The exponent in the right hand side is maximized for $k = 0$, and it has the value $(-mn\varepsilon, -2mn\varepsilon')$, when $\beta = \frac{1}{m} + (1 - \frac{1}{m})\frac{|T|}{k_{(q,q')}} - max(\varepsilon, \varepsilon')$. Hence, we have the first claimed bound.

For $|T| = 0$, based on our second bound on $n((B,B'),k)$ with $(B,B') = (q, |q'|)^\beta$, and nothing that $n((B,B'),k_{(q,q')}) = (0,0)$, we have:

$$p \leq' (2^{2|\bar{T}|+n}, 2^{2|\bar{T}|+2n}) \times$$
$$max_{0 \leq k < k_{(q,q')}} (q^{n(1-m\beta)(\frac{k}{k_{(q,q')}} - 1)}, |q'|^{2n(1-m\beta)(\frac{k}{k_{(q,q')}} - 1)})$$
$$= (2^{2|\bar{T}|+n}, 2^{2|\bar{T}|+2n}) \times$$
$$(q^{n(1-m\beta)(1-\frac{1}{k_{(q,q')}})}, |q'|^{2n(1-m\beta)(1-\frac{1}{k_{(q,q')}})}).$$

where the last equality holds for any $\beta \leq \frac{1}{m}$. Using $\beta = \frac{1}{m} - k_{(q,q')}.max(\varepsilon, \varepsilon')$ gives the second claimed bound. □

4.2 Regularity Bounds for Ring $R_{(q,q')}$

In this subsection, we discuss the closness to uniformity of the distribution of $(m+1)$-tuples from $(R^\times_{(q,q')})^m \times R_{(q,q')}$ of the form $((a_1,a'_1),...,(a_m,a'_m), \sum_{i \leq m}(t_i,t'_i)(a_i,a'_i))$, where the (a_i,a'_i)'s are independent and uniformly random in $R^\times_{(q,q')}$, and the (t_i,t'_i)'s are chosen from some distribution on $R_{(q,q')}$ concentrated on elements of small height, component-wise. We use the regularity bound in [50], that is an argument of unstructured generalized knapsacks, based on the "smoothing parameter" of the underlying lattices, even for $m = O(1)$. So we can restrict the (a_i,a'_i)'s to be uniform in $R^\times_{(q,q')}$, and we choose the (t_i,t'_i)'s from a discrete Gaussian distribution. Note that the following results perform coordinate-wise and component-wise, also note that we can obtain a denser lattice for *NTRUEncrypt* by eliminating imaginary part of Eisenstein integers, that is, we have $R_{(q,q')} = \frac{(\mathbb{Z}\times\mathbb{Z})_{(q,q')}[x]}{<x^n + x^{n-1} + ... + x + 1>}$, and each result of this paper is satisfied.

Theorem 5 (Adapted from [50], Th. 3.1). *Let $n \geq 8$ such that $n+1$ be a prime and $\Phi = x^n + x^{n-1} + ... + x + 1$ splits into $k_{(q,q')}$ irreducible factors modulo prime $(q, |q'|) \geq' (5,5)$. Let $m \geq 2$, $(\varepsilon, \varepsilon') >' (0,0)$, $\delta, \delta' \in (0, 1/2)$ and $(t,t') \hookleftarrow D_{\mathbb{Z}^{3mn},(\sigma,\sigma')}$ component-wise, with $(\sigma,\sigma') \geq' ln((2mn,4mn)(1,1) + \frac{(1,1)}{(\delta,\delta')})/\pi \times min((\sqrt{n},\sqrt{2n}).(q^{\frac{1}{m}+\varepsilon}, |q'|^{\frac{1}{m}+\varepsilon'}), (q^{\frac{1}{m}+k_{(q,q')}\varepsilon}, |q'|^{\frac{1}{m}+k_{(q,q')}\varepsilon'})$. Then for all except a fraction $\leq' (2^{4mn}, 2^{8mn})(q^{-\varepsilon mn}, |q'|^{-\varepsilon' 2mn})$ of $(a,a') \in (R^\times_{(q,q')})^m$, we have $\eta_{(\delta,\delta')}(a,a') \leq'$*

$$\sqrt{ln((2mn,4mn)(1,1) + \frac{(1,1)}{(\delta,\delta')})/\pi} \times$$
$$min((\sqrt{n},\sqrt{2n}) \times$$
$$(q^{\frac{1}{m}+\varepsilon}, |q'|^{\frac{1}{m}+\varepsilon'}), (q^{\frac{1}{m}+k_{(q,q')}\varepsilon}, |q'|^{\frac{1}{m}+k_{(q,q')}\varepsilon'}))$$

and the distance to uniformity of $\sum_{i \leq m}(t_i,t'_i)(a_i,a'_i)$ is $\leq' 2(\delta,\delta')$. As a consequence:

$$\Delta[((a_1,a'_1),...,(a_m,a'_m), \sum_{i \leq m}(t_i,t'_i)(a_i,a'_i)); U((R^\times_{(q,q')})^m \times R_{(q,q')})] \leq'$$
$$2(\delta,\delta') + (2^{4mn}, 2^{8mn})(q^{-\varepsilon mn}, |q'|^{-\varepsilon' 2mn}).$$

Proof. For each $(a,a') \in (R^\times_{(q,q')})^m$, assume $D_{(a,a')}$ denote the distribution of $\sum_{i \leq m}(t_i,t'_i)(a_i,a'_i)$ where (t,t') is sampled from $D_{\mathbb{Z}^{3mn},(\sigma,\sigma')}$ component-wise. We know the above statistical distance is $\frac{(1,1)}{|R^\times_{(q,q')}|^m} \sum_{(a,a') \in (R^\times_{(q,q')})^m} \Delta_{(a,a')}$, where $\Delta_{(a,a')}$ is the distance to uniformity of $D_{(a,a')}$. It is enough to show a uniform bound $\Delta_{(a,a')} \leq' 2(\delta,\delta')$, for all except a fraction $\leq' (2^{4mn}, 2^{8mn})(q^{-\varepsilon mn}, |q'|^{-\varepsilon' 2mn})$ of $(a,a') \in (R^\times_{(q,q')})^m$.

We have the mapping $(t,t') \mapsto \sum_i (t_i,t'_i)(a_i,a'_i)$ that is an isomorphism from the quotient group $\frac{\mathbb{Z}^{3mn}}{(a,a')^\perp}$ to its range. The latter is $R_{(q,q')}$, based on the invertibility of the (a_i,a'_i)'s. Hence, the statistical distance $\Delta_{(a,a')}$ is equal to the distance to uniformity of (t,t') mod $(a,a')^\perp$. Now, we analyze the distance to uniformity of (t,t') mod $(a,a')^\perp(I_T)$ for any $T \subseteq \{1,...,k_{(q,q')}\}$. By Lemma 5, we have $\Delta_{(a,a')} \leq' 2(\delta,\delta')$ if (σ,σ') is greater than the smoothing parameter $\eta_{(\delta,\delta')}((a,a')^\perp(I_T))$ of $(a,a')^\perp(I_T) \subseteq \mathbb{Z}^{3mn}$. We use Lemma 2, to bound $\eta_{(\delta,\delta')}((a,a')^\perp(I_T))$, which reduces the task to bounding the minimum of the dual lattice from below. By Lemma 12, the latter lattice is $\widehat{(a,a')^\perp(I_T)} = \frac{(1,1)}{(q,q')} L((a,a')^*, I_T^*)$, where $(a,a')^* \in (R^\times_{(q,q')})^m$ is in one-to-one correspondence with (a,a'), and the latter issue has been addressed by Lemma 13.

Therefore, by lemmata 2, 5, 12 and 13, we have the following result.

Lemma 15 (Adapted from [50], Le. 3.4). *Let $n \geq 8$ such that $n+1$ be a prime, and $\Phi = x^n + x^{n-1} +$*

... + x + 1 splits into $k_{(q,q')}$ irreducible factors modulo prime $(q, |q'|) \geq' (5,5)$. Let $T \subseteq \{1, ..., k_{(q,q')}\}$, $m \geq 2$, $(\varepsilon, \varepsilon') >' (0,0)$, $\delta, \delta' \in (0, 1/2)$, $(c, c') \in \mathbb{R}^{3mn}$ and $(t, t') \hookleftarrow D_{\mathbb{Z}^{3mn},(\sigma,\sigma'),(c,c')}$, with:

$$(\sigma, \sigma') \geq'$$

$$\begin{cases} \sqrt{(n,2n).ln((2mn,4mn)(1,1) + \frac{(1,1)}{(\delta,\delta')})/\pi} \times \\ (q^{1-(1-\frac{1}{m})(1-\frac{|T|}{k_{(q,q')}})+\varepsilon}, |q'|^{1-(1-\frac{1}{m})(1-\frac{|T|}{k_{(q,q')}})+\varepsilon'}) \\ \text{for any } 0 < |T| \leq k_{(q,q')}, \\ \sqrt{ln((2mn,4mn)(1,1) + \frac{(1,1)}{(\delta,\delta')})/\pi} \times \\ (q^{\frac{1}{m}+k_{(q,q')}.\varepsilon}, |q'|^{\frac{1}{m}+k_{(q,q')}.\varepsilon'}) \\ \text{for } |T| = 0. \end{cases}$$

Then for all except a fraction

$\leq' (2^{4mn}, 2^{8mn})(q^{-\varepsilon mn}, |q'|^{-\varepsilon' 2mn})$ *of* $(a, a') \in (R^{\times}_{(q,q')})^m$, *we have:*

$$\Delta[(t, t') \bmod (a, a')^{\perp}(I_T); U(\frac{R}{(a, a')^{\perp}(I_T)})] \leq' 2(\delta, \delta').$$

So, theorem 5 follows by taking $T = \emptyset$ and $(c, c') = (0, 0)$. □

4.3 Modified Key Generation Algorithm for The *ETRU*

We use our results on modular (q, q')-ary lattices to provide key generation algorithm for the *ETRU* scheme that is shown in Algorithm 1. The generated public keys follow distributions for which Ideal-SVP is given to reduce to R-LWE and R-SIS. The private key polynomials (f, f') and (g, g') are generated by sampling and rejecting so that the output polynomials are invertible modulo (q, q'). We use the same conditions as Stehlé and Steinfeld [50], by choosing a large enough standard deviations (σ, σ') for sampling from discrete Gaussians, so we will assume we have a perfect discrete Gaussian sampler.

We sample (f, f') of the form $(p, p').(f, f') + (1, 1)$ so, it has inverse $(1, 1)$ modulo (p, p'), and it make the decryption computation of *ETRU* more efficient. Note that the rejection condition on (f, f') at Step 1 is equivalent to the condition $((f, f')' \bmod (q, q')) \notin R^{\times}_{(q,q')} - (p, p')^{-1}$, where $(p, p')^{-1}$ is the inverse of (p, p') in $R^{\times}_{(q,q')}$. We show that for some appropriate choice of parameters, the key generation algorithm terminates in expected polynomial time.

Lemma 16 (Adapted from [50], Le. 3.5). *Let $n \geq 8$ such that $n + 1$ be a prime, and $\Phi = x^n + x^{n-1} + ... + x + 1$ splits into $k_{(q,q')}$ irreducible factors modulo prime $(q, |q'|) \geq' (5,5)$. Let $(\sigma, \sigma') \geq' \sqrt{(n, 2n)ln((2n, 4n)(1,1) + \frac{(1,1)}{(\delta,\delta')})/\pi}.(q, |q'|)^{\frac{1}{k_{(q,q')}}}$, for an arbitrary $\delta, \delta' \in (0, 1/2)$. Let $(a, a') \in R$ and $(p, p') \in R^{\times}_{(q,q')}$. Then, $Pr_{(f,f')\hookleftarrow D_{\mathbb{Z}^{3n},(\sigma,\sigma')}}[(p, p').(f, f')' + (a, a') \bmod (q, q') \notin R^{\times}_{(q,q')}] \leq' k_{(q,q')}((q^{\frac{-n}{k_{(q,q')}}}, |q'|^{\frac{-2n}{k_{(q,q')}}}) + 2(\delta, \delta')) \leq' (n, 2n)((q^{-1}, |q'|^{-1}) + 2(\delta, \delta'))$.*

Proof. For any $k \leq k_{(q,q')}$, we aim to bound the probability that $(p, p').(f, f')' + (a, a')$ belongs to $I :=< (q, q'), \Phi_k >$ by $(q^{\frac{-n}{k_{(q,q')}}}, |q'|^{\frac{-2n}{k_{(q,q')}}}) + 2(\delta, \delta')$. By CRT and union bound, we have the result. $N(I) = (q^{\frac{n}{k_{(q,q')}}}, |q'|^{\frac{2n}{k_{(q,q')}}})$, so that $\lambda_1(I) \leq' (\sqrt{n}, \sqrt{2n})(q, q')^{\frac{1}{k_{(q,q')}}}$, by Minkowski's theorem. Since I is an ideal of R, then $\lambda_n(I) = \lambda_1(I)$, and Lemma 2 gives that $(\sigma, \sigma') \geq' \eta_{(\delta,\delta')}(I)$, and Lemma 5 shows that $(f, f') \bmod I$ is within distance $\leq' 2(\delta, \delta')$ to uniformity on $\frac{R}{I}$, so we have $(p, p').(f, f')' + (a, a') = (0, 0) \bmod I$ or $(f, f')' = -\frac{(a,a')}{(p,p')} \bmod I$ with probability $\leq' (q^{\frac{-n}{k_{(q,q')}}}, |q'|^{\frac{-2n}{k_{(q,q')}}}) + 2(\delta, \delta')$. □

Algorithm 1 Modified Key Generation Algorithm For *ETRU*.

Inputs: $n, q \in \mathbb{Z}, q' \in \mathbb{Z}[\zeta_3], p, p' \in R^{\times}_{(q,q')}, (\sigma, \sigma') >' (0,0)$.

Output: A Key Pair $(prk, puk) \in R \times R^{\times}_{(q,q')}$.

1. Sample (f, f') from $D_{\mathbb{Z}^{3n},(\sigma,\sigma')}$
; let $(f, f') = (p, p').(f, f') + (1, 1)$;
if $((f, f') \bmod (q, q')) \notin R^{\times}_{(q,q')}$, resample.
2. Sample (g, g') from $D_{\mathbb{Z}^{3n},(\sigma,\sigma')}$;
if $((g, g') \bmod (q, q')) \notin R^{\times}_{(q,q')}$, resample.
3. Return private key $prk = (f, f')$ and public key $puk = (h, h') = (p, p').(g, g')/(f, f') \in R^{\times}_{(q,q')}$.

Now we show that the generated private key is small.

Lemma 17 (Adapted from [50], Le. 3.6). *Let $n \geq 8$ such that $n + 1$ be a prime, and $\Phi = x^n + x^{n-1} + ... + x + 1$ splits into $k_{(q,q')}$ irreducible factors modulo prime $(q, |q'|) \geq' (8n, 16n)$. Let $(\sigma, \sigma') \geq' (\sqrt{nlnn}, \sqrt{2nln2n})(q, |q'|)^{\frac{1}{k_{(q,q')}}}$. The private key polynomials $(f, f'), (g, g')$ returned by Algorithm 1 satisfy, with probability $\geq' (1,1) - (2^{-n+3}, 2^{-2n+6})$:*

$$||(f, f')|| \leq' (2n, 4n)||(p, p')||(\sigma, \sigma') \text{ and}$$

$$||(g, g')|| \leq' (\sqrt{n}, \sqrt{2n})(\sigma, \sigma').$$

If $deg(p, p') \leq' (1,1)$, then $||(f, f')|| \leq' 4(\sqrt{n}, \sqrt{2n}) \times ||(p, p')||(\sigma, \sigma')$ with probability $\geq' (1,1) - (2^{-n+3}, 2^{-2n+6})$.

Proof. The result follows by combining lemmata 4 and 16. □

In Algorithm 1, $(f, f')'$ and (g, g') are independently sampled from the discrete Gaussian distribution $D_{\mathbb{Z}^{3n}(\sigma,\sigma')}$ restricted to $R^{\times}_{(q,q')} - (p, p')^{-1}$ and $R^{\times}_{(q,q')}$, respectively. We denote by $D^{\times}_{(\sigma,\sigma'),(z,z')}$ the discrete Gaussian $D_{\mathbb{Z}^{3n},(\sigma,\sigma')}$ restricted to $R^{\times}_{(q,q')} + (z, z')$.

We would like to show that the statistical closeness to uniformity of a quotient of two distributions $((z, z') + (p, p').D^{\times}_{(\sigma,\sigma'),(y,y')})$ for $(z, z') \in R_{(q,q')}$ and $(y, y') = -(z, z')(p, p')^{-1} \bmod (q, q')$. This contains the case of $\frac{(g,g')}{(f,f')} \bmod (q, q')$ processed by Algorithm 1. Since $(p, p') \in R^{\times}_{(q,q')}$, multiplication by (p, p') induces a bijection of $R_{(q,q')}$, and thus the statistical closeness to uniformity carries over to the public key $(h, h') = \frac{(p,p').(g,g')}{(f,f')}$. In the following theorem we study two bounds, whose usefulness depends on the number of irreducible factors $k_{(q,q')}$ in the factorization of $x^n + x^{n-1} + ... + x + 1$ modulo (q, q'). As these cyclotomic rings of prime order are large subrings of the orginal *NTRUEncrypt* and *ETRU* rings, we give some results similar to Stehlé and Steinfeld's results ([50], Se. 3) such that the first bound is most useful for large $k_{(q,q')} = \Omega(n)$, while the second bound is better for small $k_{(q,q')} = O(1)$, allowing a smaller (σ, σ') by a factor $\approx (\sqrt{n}, \sqrt{2n})$ versus the first bound.

Theorem 6 (Adapted from [50], Th. 3.2)**.** *Let $n \geq 8$ such that $n + 1$ be a prime, and $\Phi = x^n + x^{n-1} + ... + x + 1$ splits into $k_{(q,q')}$ irreducible factors modulo prime $(q, |q'|) \geq' (5, 5)$. Let $(0, 0) <' (\varepsilon, \varepsilon')' <' (1/3, 1/3)$, $(y_i, y'_i) \in R_{(q,q')}$ and $(z_i, z'_i) = -(y_i, y'_i).(p, p')^{-1}$ mod (q, q') for $i \in \{1, 2\}$. Then:*

$$\Delta[\frac{(y_1, y'_1) + (p, p').D^{\times}_{(\sigma,\sigma'),(z_1,z'_1)}}{(y_2, y'_2) + (p, p').D^{\times}_{(\sigma,\sigma'),(z_2,z'_2)}} \bmod (q, q');$$

$$U(R^{\times}_{(q,q')})] \leq'$$

$$\begin{cases} (2^{10n}, 2^{20n})(q^{\frac{-\lfloor \varepsilon k_{(q,q')} \rfloor}{k_{(q,q')}}.n}, |q'|^{\frac{-\lfloor \varepsilon' k_{(q,q')} \rfloor}{k_{(q,q')}}.2n}) \\ if\ (\sigma, \sigma') \geq' (n, 2n).\sqrt{ln((8n, 16n)(q, |q'|))}\times \\ (q^{1/2+(\varepsilon)'}, |q'|^{1/2+(\varepsilon')'}), \\ \\ (2^{10n}, 2^{20n})(q^{-(\varepsilon)'.n}, |q'|^{-(\varepsilon')'.2n}) \\ if\ (\sigma, \sigma') \geq' \sqrt{(n, 2n).ln((8n, 16n)(q, |q'|))}\times \\ (q^{\frac{1+k_{(q,q')}(\varepsilon)'}{2}}, |q'|^{\frac{1+k_{(q,q')}(\varepsilon')'}{2}}) \\ and\ (q, |q'|) \geq' (n^{\frac{k_{(q,q')}}{1-2k_{(q,q')}(\varepsilon)'}}, 2n^{\frac{k_{(q,q')}}{1-2k_{(q,q')}(\varepsilon')'}}). \end{cases}$$

Proof. For $(a, a') \in R^{\times}_{(q,q')}$, we define $Pr_{(a,a')} = Pr_{(f_1,f'_1),(f_2,f'_2)}[((y_1, y'_1) + (p, p')(f_1, f'_1))/((y_2, y'_2) + (p, p')(f_2, f'_2)) = (a, a')]$, where $(f_i, f'_i) \hookleftarrow D^{\times}_{(\sigma,\sigma'),(z_i,z'_i)}$ for $i \in \{1, 2\}$. We show that $|Pr_{(a,a')} - |R^{\times}_{(q,q')}|^{-1}| \leq' (2^{2n+5}, 2^{4n+10})(q^{-n\lfloor(\varepsilon)'k_{(q,q')}\rfloor/k_{(q,q')}}, |q'|^{-2n\lfloor(\varepsilon')'k_{(q,q')}\rfloor/k_{(q,q')}}).|R^{\times}_{(q,q')}|^{-1} =: (\varepsilon, \varepsilon')$" (resp. $\leq' (2^{6n+4}, 2^{12n+8})(q^{-(\varepsilon)'n}, |q'|^{-(\varepsilon')'2n}).|R^{\times}_{(q,q')}|^{-1})$. This directly gives the claimed bounds. The fraction of $(a, a') \in R^{\times}_{(q,q')}$ such that $|Pr_{(a,a')} - |R^{\times}_{(q,q')}|^{-1}| \leq' (\varepsilon, \varepsilon')$" is equal to the fraction of $(a, a') = ((a_1, a'_1), (a_2, a'_2)) \in (R^{\times}_{(q,q')})^2$ such that $|Pr_{(a,a')} - |R^{\times}_{(q,q')}|^{-1}| \leq' (\varepsilon, \varepsilon')$", where $Pr_{(a,a')} = Pr_{(f_1,f'_1),(f_2,f'_2)}[(a_1, a'_1)(f_1, f'_1) + (a_2, a'_2)(f_2, f'_2) = (a_1, a'_1)(z_1, z'_1) + (a_2, a'_2)(z_2, z'_2)]$, because $(a_1, a'_1)(f_1, f'_1)+(a_2, a'_2)(f_2, f'_2) = (a_1, a'_1)(z_1, z'_1) +(a_2, a'_2)(z_2, z'_2)$ is equivalent to $((y_1, y'_1)+(p, p')(f_1, f'_1))/((y_2, y'_2) + (p, p')(f_2, f'_2)) = -\frac{(a_2,a'_2)}{(a_1,a'_1)}$ in $R^{\times}_{(q,q')}$, and $-\frac{(a_2,a'_2)}{(a_1,a'_1)}$ is uniformly random in $R^{\times}_{(q,q')}$. When $(a, a') \hookleftarrow U((R^{\times}_{(q,q')})^2)$. We have $((f_1, f'_1), (f_2, f'_2)) = ((z_1, z'_1), (z_2, z'_2)) =: (z, z')$ satisfies $(a_1, a'_1)(f_1, f'_1) + (a_2, a'_2)(f_2, f'_2) = (a_1, a'_1)(z_1, z'_1) + (a_2, a'_2)(z_2, z'_2)$, and hence the set of solutions $((f_1, f'_1), (f_2, f'_2)) \in R$ to the latter equation is $(z, z') + (a, a')^{\perp\times}$, where $(a, a')^{\perp\times} = (a, a')^{\perp} \cap (R^{\times}_{(q,q')} + (q, q')\mathbb{Z}^{3n})^2$. Therefore:

$$Pr_{(a,a')} = D_{\mathbb{Z}^{6n},(\sigma,\sigma')}((z, z') + (a, a')^{\perp\times})/$$
$$[D_{\mathbb{Z}^{3n},(\sigma,\sigma')}((z_1, z'_1) + R^{\times}_{(q,q')} + (q, q')\mathbb{Z}^{3n})\times$$
$$D_{\mathbb{Z}^{3n},(\sigma,\sigma')}((z_2, z'_2) + R^{\times}_{(q,q')} + (q, q')\mathbb{Z}^{3n})].$$

For any $(t, t') \in (a, a')^{\perp}$ we have $(t_2, t'_2) = -(t_1, t'_1)(a_1, a'_1)/(a_2, a'_2)$, since $-(a_1, a'_1)/(a_2, a'_2) \in R^{\times}_{(q,q')}$, the ring elements (t_1, t'_1) and (t_2, t'_2) must belong to the same ideal I_T of $R_{(q,q')}$ for some $T \subseteq \{1, ..., k_{(q,q')}\}$. So, $(a, a')^{\perp\times} = (a, a')^{\perp} \backslash \cup_{\substack{T\subseteq\{1,...,n\},\\ T\neq\emptyset}} (a, a')^{\perp}(I_T)$. Similarly,

$R^{\times}_{(q,q')} + (q, q')\mathbb{Z}^{3n} = \mathbb{Z}^{3n} \backslash \cup_{\substack{T\subseteq\{1,...,n\},\\ T\neq\emptyset}} (I_T + (q, q')\mathbb{Z}^{3n})$. By inclusion-exclusion principle, we have:

$$D_{\mathbb{Z}^{6n},(\sigma,\sigma')}((z, z') + (a, a')^{\perp\times}) =$$

$$\sum_{T\subseteq\{1,...,n\}} (-1)^{|T|}.D_{\mathbb{Z}^{6n},(\sigma,\sigma')}((z, z') + (a, a')^{\perp}(I_T)), \quad (1)$$

$$\forall i \in \{1, 2\} : D_{\mathbb{Z}^{3n},(\sigma,\sigma')}((z_i, z'_i)+R^{\times}_{(q,q')}+(q, q')\mathbb{Z}^{3n}) =$$

$$\sum_{T\subseteq\{1,...,n\}} (-1)^{|T|}.D_{\mathbb{Z}^{3n},(\sigma,\sigma')}((z_i, z'_i)+I_T+(q, q')\mathbb{Z}^{3n}). \quad (2)$$

Now, we show that except for a fraction $<' (2^{9n}, 2^{18n})(q^{-(\varepsilon)'n}, |q'|^{-(\varepsilon')'2n})$ of $(a, a') \in (R^{\times}_{(q,q')})^2$:

$$D_{\mathbb{Z}^{6n},(\sigma,\sigma')}((z,z')+(a,a')^{\perp\times}) =$$
$$(1,1)+(\delta_0,\delta_0')|R^{\times}_{(q,q')}|(q^{-2n},|q'|^{-4n})),$$
$$\forall i\in\{1,2\}: D_{\mathbb{Z}^{3n},(\sigma,\sigma')}((z_i,z_i')+R^{\times}_{(q,q')}+(q,q')\mathbb{Z}^{3n}) =$$
$$(1,1)+(\delta_i,\delta_i')|R^{\times}_{(q,q')}|(q^{-n},|q'|^{-2n})).$$

where $|(\delta_i,\delta_i')|\leq' (2^{2n+2},2^{4n+4})(q^{-n\lfloor(\varepsilon)'k_{(q,q')}\rfloor/k_{(q,q')}},|q'|^{-2n\lfloor(\varepsilon')'k_{(q,q')}\rfloor/k_{(q,q')}})$ (resp. $|(\delta_i,\delta_i')|\leq' (2^{6n+1},2^{12n+2})(q^{-(\varepsilon)'n},|q'|^{-(\varepsilon')'2n})$) for $i\in\{0,1,2\}$. The bounds on $|Pr_{(a,a')}-|R^{\times}_{(q,q')}|^{-1}|$ follow by a routine computation.

Handling (1). At first, since $(z,z')\in\mathbb{Z}^{6n}$, we have for any $T\subseteq\{1,...,k_{(q,q')}\}$:

$$D_{\mathbb{Z}^{6n},(\sigma,\sigma')}((z,z')+(a,a')^{\perp})(I_T)) =$$
$$\frac{\rho_{(\sigma,\sigma')}((z,z')+(a,a')^{\perp}(I_T))}{\rho_{(\sigma,\sigma')}(\mathbb{Z}^{6n})} =$$
$$\frac{\rho_{(\sigma,\sigma')}((z,z')+(a,a')^{\perp}(I_T))}{\rho_{(\sigma,\sigma')}((z,z')+\mathbb{Z}^{6n})} =$$
$$D_{\mathbb{Z}^{6n},(\sigma,\sigma'),-(z,z')}((a,a')^{\perp}(I_T)).$$

To get our first bound, for the terms of (1) with $|T|\leq' min(\varepsilon,\varepsilon')'k_{(q,q')}$, we apply the first bound of Lemma 15 with $m=2$ and $(\varepsilon,\varepsilon')=(\varepsilon,\varepsilon')'/2$. For $(\delta,\delta'):=(q^{-n(1+\lfloor(\varepsilon)'k_{(q,q')}\rfloor/k_{(q,q')})},|q'|^{-2n(1+\lfloor(\varepsilon')'k_{(q,q')}\rfloor/k_{(q,q')})})$, the assumption of Lemma 15 on (σ,σ') holds. Moreover, we have $det((a,a')^{\perp}(I_T))=(q^{n(1+|T|/k_{(q,q')})},|q'|^{2n(1+|T|/k_{(q,q')})})$: Actually, since $(a,a')\in(R^{\times}_{(q,q')})^2$, there are $(q^{n(1-|T|/k_{(q,q')})},|q'|^{2n(1-|T|/k_{(q,q')})})$ elements of $(a,a')^{\perp}(I_T)$ in $([0,q-1]^{2n},[0,|q'|^2-1]^{4n})$. So, we conclude that $|D_{\mathbb{Z}^{6n},(\sigma,\sigma'),-(z,z')}((a,a')^{\perp}(I_T)-(q^{-n(1+|T|/k_{(q,q')})},|q'|^{-2n(1+|T|/k_{(q,q')})}))|\leq' 2(\delta,\delta')$, for all except a fraction $\leq' (2^{8n},2^{16n})(q^{-(\varepsilon)'n},|q'|^{-(\varepsilon')'2n})$ of $(a,a')\in(R^{\times}_{(q,q')})^2$ (possibly corresponding to a distinct subset of $(R^{\times}_{(q,q')})^2$ for each possible T).

For a term of (1) with $|T|>' max(\varepsilon,\varepsilon')'k_{(q,q')}$, we choose $T'\subseteq T$ with $|T'|=\lfloor max(\varepsilon,\varepsilon')'k_{(q,q')}\rfloor$. Then $(a,a')^{\perp}(I_T)\subseteq(a,a')^{\perp}(I_{T'})$ and hence $D_{\mathbb{Z}^{6n},(\sigma,\sigma'),-(z,z')}((a,a')^{\perp}(I_T))\leq'$

$D_{\mathbb{Z}^{6n},(\sigma,\sigma'),-(z,z')}((a,a')^{\perp}(I_{T'}))$. By T' for small $|T|$, we have $D_{\mathbb{Z}^{6n},(\sigma,\sigma'),-(z,z')}((a,a')^{\perp}(I_T))\leq' 2(\delta,\delta')+(q^{-n(1+\lfloor(\varepsilon)'k_{(q,q')}\rfloor/k_{(q,q')})},|q'|^{-2n(1+\lfloor(\varepsilon')'k_{(q,q')}\rfloor/k_{(q,q')})})$. Finally, we obtain, except possibly for a fraction $\leq' (2^{9n},2^{18n})(q^{-(\varepsilon)'n},|q'|^{-(\varepsilon')'2n})$ of $(a,a')\in(R^{\times}_{(q,q')})^2$:

$$|D_{\mathbb{Z}^{6n},(\sigma,\sigma')}((z,z')+(a,a')^{\perp\times})$$
$$-(\sum_{k=0}^{n}(-1)^k\binom{n}{k}q^{-n-k},\sum_{k=0}^{2}n(-1)^k\binom{2n}{k}|q'|^{-2n-k})|\leq'$$
$$(2^{n+1},2^{2n+2})(\delta,\delta')+(2,2)\times$$
$$(\sum_{\lceil\varepsilon k_{(q,q')}\rceil}^{k_{(q,q')}}\binom{k_{(q,q')}}{k}q^{-n(1+\frac{\lfloor(\varepsilon)'k_{(q,q')}\rfloor}{k_{(q,q')}})},$$
$$\sum_{\lceil\varepsilon' k_{(q,q')}\rceil}^{k_{(q,q')}}\binom{k_{(q,q')}}{k}|q'|^{-2n(1+\frac{\lfloor(\varepsilon')'k_{(q,q')}\rfloor}{k_{(q,q')}})})\leq'$$
$$(2^{n+1},2^{2n+2})((\delta,\delta')+$$
$$(q^{-n(1+\frac{\lfloor(\varepsilon)'k_{(q,q')}\rfloor}{k_{(q,q')}})},|q'|^{-2n(1+\frac{\lfloor(\varepsilon')'k_{(q,q')}\rfloor}{k_{(q,q')}})})).$$

We conclude that $|(\delta_0,\delta_0')|\leq'$

$$\frac{(q^{2n},|q'|^{4n})}{((q^{n/k_{(q,q')}},|q'|^{2n/k_{(q,q')}})-(1,1))^{k_{(q,q')}}}.(2^{n+1},2^{2n+2})((\delta,\delta')+$$
$$(q^{-n(1+\frac{\lfloor(\varepsilon)'k_{(q,q')}\rfloor}{k_{(q,q')}})},|q'|^{-2n(1+\frac{\lfloor(\varepsilon')'k_{(q,q')}\rfloor}{k_{(q,q')}})}))\leq'$$
$$(2^{2n+2},2^{4n+4})(q^{-(\frac{\lfloor(\varepsilon)'k_{(q,q')}\rfloor}{k_{(q,q')}})n},|q'|^{-(\frac{\lfloor(\varepsilon')'k_{(q,q')}\rfloor}{k_{(q,q')}})2n}),$$

as required.

For our second bound, for the term of (1) with $|T|=0$, we use the second bound in Lemma 15 with $(\varepsilon,\varepsilon')=(\varepsilon,\varepsilon')'/2$. With $(\delta,\delta'):=(q^{-2n},|q'|^{-4n})$ and by the choice of (σ,σ'), the Lemma 15 assumption on (σ,σ') holds. $|\frac{R}{(a,a')^{\perp}(I_T)}|=det((a,a')^{\perp}(I_T))=(q^n,|q'|^{2n})$ and hence $|D_{\mathbb{Z}^{6n},(\sigma,\sigma'),-(z,z')}((a,a')^{\perp}(I_T))-(q^{-n},|q'|^{-2n})|\leq' 2(\delta,\delta')$, for all except a fraction

$\leq' (2^{8n},2^{16n})(q^{-(\varepsilon)'n},|q'|^{-(\varepsilon')'2n})$ of $(a,a')\in(R^{\times}_{(q,q')})^2$.

For the terms of (1) with $|T|\geq 1$, we cannot choose for $|T|=1$ on $I_{T'}$ with $T'\subseteq T$ and $det((a,a')^{\perp}(I_{T'}))\approx(q^{1+\varepsilon n},|q'|^{1+\varepsilon' 2n})$: This ideal $I_{T'}$ does not exist, as the only possible choice for T' is the empty set, so $det((a,a')^{\perp}(I_{T'}))=(q^n,|q'|^{2n})$, and the latter is too small. Instead, we let $L'=N.\mathbb{Z}^{6n}$, where $N=\lceil(1/4,1/4)(q^{1/2+(\varepsilon)'/2},|q'|^{1/2+(\varepsilon')'/2})\rceil$. Also $detL'=N^{6n}\geq'(2^{-4n},2^{-8n})(q^{1+(\varepsilon)'n},|q'|^{1+(\varepsilon')'2n})$, and since $\lambda_{6n}(L')=N\leq'$

$(1/2,1/2)(q^{1/2+(\varepsilon)'/2},|q'|^{1/2+(\varepsilon')'/2})$, by Lemma 2 with $(\delta,\delta')=(q^{-2n},|q'|^{-4n})$ that $\eta_{(\delta,\delta')}(L')\leq'\sqrt{(n,2n)ln((8n,16n)(q,|q'|))}.(q^{1/2+(\varepsilon)'/2},|q'|^{1/2+(\varepsilon')'/2})$. Therefore, by Lemma 5 and the choice of (σ,σ'), we have $D_{\mathbb{Z}^{6n},(\sigma,\sigma')}(L')\leq'$

$(2^{4n},2^{8n})(q^{-(1+(\varepsilon)')n},|q'|^{-(1+(\varepsilon')')2n})+2(\delta,\delta')$. To use the last bound, we show that for $|T|\geq 1$, we have $D_{\mathbb{Z}^{6n},(\sigma,\sigma')}((z,z')+(a,a')^{\perp}(I_T))\leq' D_{\mathbb{Z}^{6n},(\sigma,\sigma')}(L')$. For this, we use a rounding process $\Phi:\mathbb{Z}^{6n}\to L'$ to map $(z,z')+(a,a')^{\perp}(I_T)$ onto a subset of L' such that:

1. The map Φ is one-to-one on $(z,z')+(a,a')^{\perp}(I_T)$,

2. For each $(v,v')\in\mathbb{Z}^{6n}$, we have $||\Phi(v,v')||\leq'||(v,v')||$.

We know $D_{\mathbb{Z}^{6n},(\sigma,\sigma')}(w,w')\geq' D_{\mathbb{Z}^{6n},(\sigma,\sigma')}(v,v')$

for any $(v,v'),(w,w') \in \mathbb{Z}^{6n}$ with $||(w,w')|| \leq' ||(v,v')||$, by 2 of above $D_{\mathbb{Z}^{6n},(\sigma,\sigma')}(w,w') \geq' D_{\mathbb{Z}^{6n},(\sigma,\sigma')}((z,z')+(a,a')^{\perp}(I_T)) \leq'$

$\sum_{(v,v')\in(z,z')+(a,a')^{\perp}(I_T)}(\Phi(v,v'))$, and by 1, the points $\{\Phi(v,v')\}_{(v,v')\in(z,z')+(a,a')^{\perp}(I_T)}$ are distinct points of L', so that $\sum_{(v,v')\in(z,z')+(a,a')^{\perp}(I_T)}(\Phi(v,v')) \leq' D_{\mathbb{Z}^{6n},(\sigma,\sigma')}(L')$, as required. Now we define Φ and its properties reflected above. For $(v,v') \in \mathbb{Z}^{6n}$, let $\Phi(v,v')$ round each coordinate (v_i,v_i') of (v,v') to the nearest multiple of N which is $\leq' |(v_i,v_i')|$ in absolute value, that is, $\Phi(v,v') = ((v_1,v_1'),...,(v_{6n},v_{6n}'))'$ with $(v_i,v_i')' = \lfloor \frac{|(v_i,v_i')|}{N} \rfloor .N.sign(v_i,v_i')$. Since $|(v_i,v_i')'| \leq' |(v_i,v_i')|$, by 2 is satisfied. To show 1, note that $||\Phi(v,v')-(v,v')||_{\infty} <' N$ for all $(v,v') \in \mathbb{Z}^{6n}$. Suppose Φ is not one-to-one on $(z,z')+(a,a')^{\perp}(I_T)$, then there exist two vectors $(v_1,v_1') \neq (v_2,v_2')$ in $(z,z')+(a,a')^{\perp}(I_T)$ with $\Phi(v,v') = \Phi(v_2,v_2') = (v,v')$. A modification of triangle inequality then gives that $(v_1,v_1')-(v_2,v_2')$ is a non-zero vector of $(a,a')^{\perp}(I_T)$ with $||(v_1,v_1')-(v_2,v_2')|| <' 2N \leq' (q^{1/2+(\varepsilon)'/2},|q'|^{1/2+(\varepsilon)'/2})$. However, by the first bound of Lemma 14 with $m=2$, $|T|=1$, and $(\varepsilon,\varepsilon') = (\varepsilon,\varepsilon')'/2$, we have $\lambda_1^{\infty}((a,a')^{\perp}(I_T)) \geq' (\frac{1}{\sqrt{n}}q^{1/2+(1/2k_{(q,q')})-(\varepsilon)'/2}, \frac{1}{\sqrt{2n}}|q'|^{1/2+(1/2k_{(q,q')})-(\varepsilon')'/2})$, except for a fraction $\leq' (2^{4n},2^{8n})(q^{-(\varepsilon)'n},|q'|^{-(\varepsilon')'2n})$ of $(a,a') \in (R^{\times}_{(q,q')})^2$. By the condition on (q,q') this gives a contradiction, so Φ has property 1, except for a fraction $\leq' (2^{4n},2^{8n})(q^{-(\varepsilon)'n},|q'|^{-(\varepsilon')'2n})$ of $(a,a') \in (R^{\times}_{(q,q')})^2$. As a result, for the terms with $|T| \geq 1$, we have:

$$D_{\mathbb{Z}^{6n},(\sigma,\sigma'),-(z,z')}((a,a')^{\perp}(I_T)) \leq'$$
$$(2^{4n+1},2^{8n+2})(q^{-1+(\varepsilon)'n},|q'|^{-1+(\varepsilon')'2n}).$$

Therefore, we obtain our second bound:

$$|(\delta_0,\delta_0')| \leq' \frac{(q^{2n},|q'|^{4n})}{((q^{n/k_{(q,q')}},|q'|^{2n/k_{(q,q')}})-(1,1))^{k_{(q,q')}}} \times$$
$$(2^{5n+1},2^{10n+2})(q^{-(1+(\varepsilon)'n)},|q'|^{-(1+(\varepsilon')'2n)}) \leq'$$
$$(2^{6n+1},2^{12n+2})(q^{-(\varepsilon)'n},|q'|^{-(\varepsilon')'2n}).$$

Handling (2). For the bounds on (δ_1,δ_1') and (δ_2,δ_2'), let $i \in \{1,2\}$ and the (z_i,z_i') term can be handled like the (z,z') term of (1). For a good bound on $D_{\mathbb{Z}^{3n},(\sigma,\sigma'),-(z_i,z_i')}(I_T+(q,q')\mathbb{Z}^{3n})$, by Lemma 5 this reduces to finding a good bound on the smoothing parameter of the ideal lattice $L_T = I_T+(q,q')\mathbb{Z}^{3n}$. So, we have $L_T = (a,a')^{\perp}(I_T)$ in the special case $m=1$ and $(a_1(x),a_1'(x')) = \prod_{i\in\bar{T}}\Phi_i(x,x')$, where $\bar{T}$ denotes the complement of T. Hence, by Lemma 12, the dual lattice $\widehat{L_T} = \frac{(1,1)}{(q,q')}L(a_1^*,a_1'^*,I_{\bar{T}}^*) = \frac{(1,1)}{(q,q')}L_{\bar{T}'}$ is also a (scaled) ideal lattice, for some $\bar{T}' \subseteq \{1,...,k_{(q,q')}\}$ with $|\bar{T}'| = |\bar{T}|$, and the mapping $(a_1(x),a_1'(x')) \rightarrow (a_1^*(x),a_1'^*(x'))$ induces a bijection on the factors $\Phi_i(x,x')$. Since $detL_{\bar{T}'} = (q^{n|\bar{T}|/k_{(q,q')}},|q'|^{2n|\bar{T}|/k_{(q,q')}})$, by Minkowski's theorem $\lambda_1^{\infty}(L_{\bar{T}'}) \leq' (q,|q'|)^{|\bar{T}|/k_{(q,q')}}$. Also, since $I_T+(q,q')\mathbb{Z}^{3n}$ is an ideal lattice, Lemma 2 gives that:

$$\eta_{(\delta,\delta')}(I_T+(q,q')\mathbb{Z}^{3n}) \leq'$$
$$\frac{(1,1)}{(q,q')}\sqrt{ln((2n,4n)((1,1)+\frac{(1,1)}{(\delta,\delta')}))/\pi}.\lambda_1^{\infty}(L_{\bar{T}'}) \leq'$$
$$\sqrt{(n,2n)ln((4n,8n)(q,|q'|))}(q,|q'|)^{|T|/k_{(q,q')}} \leq' (\sigma,\sigma').$$

for $(\delta,\delta') := (q^{-n/2},|q'|^{-n})$, assuming $|T| \leq k_{(q,q')}/2$. Therefore, for a term of (2) with $|T| \leq k_{(q,q')}/2$, by Lemma 5, we have $|D_{\mathbb{Z}^{3n},(\sigma,\sigma'),-(z_i,z_i')}(I_T+(q,q')\mathbb{Z}^{3n}) - (q^{-n|T|/k_{(q,q')}},|q'|^{-2n|T|/k_{(q,q')}})| \leq' 2(\delta,\delta')$. For a term of (2) with $|T| > k_{(q,q')}/2$, we choose $T' \subseteq T$ with $|T'| = \lfloor k_{(q,q')}/2 \rfloor \geq k_{(q,q')}/3$ for $k_{(q,q')} \geq 2$. By T' for small $|T|$, we have $D_{\mathbb{Z}^{3n},(\sigma,\sigma'),-(z_i,z_i')}(I_T+(q,q')\mathbb{Z}^{3n}) \leq' D_{\mathbb{Z}^{3n},(\sigma,\sigma'),-(z_i,z_i')}(I_{T'}+(q,q')\mathbb{Z}^{3n}) \leq' 2(\delta,\delta') + (q^{-n/3},|q'|^{-2n/3})$. Finally:

$$|D_{\mathbb{Z}^{3n},(\sigma,\sigma')}((z_i,z_i')+R^{\times}_{(q,q')}+(q,q')\mathbb{Z}^{3n})$$
$$-\sum_{k=0}^{k_{(q,q')}}(-1)^k\binom{k_{(q,q')}}{k}(q,|q'|)^{-k}| \leq'$$
$$(2^{n+1},2^{2n+2})(\delta,\delta')$$
$$+(2,2)\sum_{k=\lceil k_{(q,q')}/2\rceil}^{k_{(q,q')}}\binom{k_{(q,q')}}{k}(q^{-n/3},|q'|^{-2n/3}) \leq'$$
$$(2^{n+1},2^{2n+2})((\delta,\delta')+(q^{-n/3},|q'|^{-2n/3})),$$

which leads to the desired bound on (δ_i,δ_i'). □

4.4 A Modified *ETRU* Scheme

In this subsection, we propose the provably secure variant of the *ETRU* scheme. The parameters $n,q,q',p,p',\alpha,\sigma,\sigma'$ are defined as follows. The parameters n,q and q' define the rings R and $R_{(q,q')}$. The parameter $(p,p') \in R^{\times}_{(q,q')}$ defines the plaintext message space as $P = \frac{R}{(p,p')R}$, with $N(p,p') = |P| = (2,2)^{\Omega(n)}$. In our case, we choose $(p,p') = (2,2)$. By reducing modulo the $(px^i,p'x'^i)$, we can write any element of P as $\sum_{0\leq i<n}(\varepsilon_i,\varepsilon_i')(px^i,p'x'^i)$, with $\varepsilon_i \in (-1/2,1/2]$ and $\varepsilon_i' in fundamental domain for p'$. We have $R = \frac{(\mathbb{Z}\times\mathbb{Z}[\zeta_3])[x]}{<x^n+x^{n-1}+...+x+1>}$, then we can assume that any element of P is an element of R with (infinity) norm $\leq' \frac{1}{2}\sqrt{deg(p,p')+(1,1)}.||(p,p')||$. The parameter α is the R-LWE noise distribution parameter, and the parameters σ and σ' are the standard deviation of the discrete Gaussian distribution used in the key generation algorithm. The encryption scheme for *ETRU* is given in Algorithm 2.

Algorithm 2 The Encryption Scheme $ETRU(n, q, q', p, p', \alpha, \sigma, \sigma')$.

1. Key Generation: Use Algorithm 1 and return $prk = (f, f') \in R^{\times}_{(q,q')}$ with $(f, f') = (1, 1) \bmod (p, p')$, and $puk = (h, h') = (p, p').(g, g')/(f, f') \in R^{\times}_{(q,q')}$.

2. Encryption: Given message $(M, M') \in P$, set $s, s', e, e' \leftarrow \bar{\Upsilon}_{\alpha}$ and return ciphertext $(c, c') = (h, h').(s, s') + (p, p').(e, e') + (M, M') \in R_{(q,q')}$.

3. Decryption: Given ciphertext (c, c') and private key (f, f'), compute $(c, c')' = (f, f').(c, c') \in R_{(q,q')}$ and return $(c, c') \bmod (p, p')$.

The following result shows that the decryption algorithm is correct.

Lemma 18 (Adapted from [50], Le. 3.7). *If* $deg(p, p') \leq' 1\omega(n^{0.25}lnn)\alpha||(p, p')||^2(\sigma, \sigma') <' (1, 1)$, *and* $\alpha(q, |q'|) \geq' (n^{0.75}, 2n^{0.75})$, *then the decryption algorithm of ETRU recovers* (M, M') *with probability* $(1 - n^{\omega(1)}, 1 - 2n^{\omega(1)})$ *for each component separately, over the choice of* $s, s', e, e', f, f', g, g'$.

Proof. In the decryption, we have $(c, c')' = (p, p')((g, g')(s, s') + (e, e')(f, f')) + (f, f')(M, M') \bmod (q, q')$. Let $(c, c')" = (p, p')((g, g')(s, s')+(e, e')(f, f')) +(f, f')(M, M')$ computed in R (not modulo (q, q')). If $||(c, c')"||_{\infty} <' (q, |q'|)/2$ then we have $(c, c')' = (c, c')"$ in R and, since $(f, f') = (1, 1) \bmod (p, p')$, $(c, c')' \bmod (p, p') = (c, c')" \bmod (p, p') = (M, M') \bmod (p, p')$, *i.e.*, the decryption algorithm succeds. It thus suffices to give an upper bound on the probability that $||(c, c')"||_{\infty} >' (q, |q'|)/2$. By Lemma 17, both (f, f') and (g, g') with probability $\geq' (1, 1) - (2^{-n+3}, 2^{-2n+6})$ have Euclidean norms $\leq' 4(\sqrt{n}, \sqrt{2n})||(p, p')||(\sigma, \sigma')$ if $deg(p, p') \leq' (1, 1)$. Then $||(p, p')(f, f')||$, $||(p, p')(g, g')|| \leq' 8(\sqrt{n}, \sqrt{2n})||(p, p')||^2(\sigma, \sigma')$, with probability $\geq' (1, 1) - (2^{-n+3}, 2^{-2n+6})$. By Lemma 11, both $(p, p')(f, f')(s, s')$ and $(p, p')(g, g')(e, e')$ have (infinity) norms $\leq' 8\alpha(q, |q'|)\ (n^{0.25}, 2n^{0.25})\omega(lnn) .||(p, p')||^2(\sigma, \sigma')$ with probability $(1 - n^{-\omega(1)}, 1 - 2n^{-\omega(1)})$. Independently:

$$||(f, f')(M, M')||_{\infty} \leq' ||(f, f')(M, M')|| \leq' (\sqrt{n}, \sqrt{2n})||(f, f')||||(M, M')|| \leq' 4(n, 2n)||(p, p')||^2(\sigma, \sigma').$$

Since $\alpha(q, |q'|) \geq' (n^{0.75}, 2n^{0.75})$, we have $||(c, c')"||_{\infty} \leq' 20\alpha(q, |q'|)(n^{0.25}, 2n^{0.25})\omega(lnn).||(p, p')||^2(\sigma, \sigma')$, with probability $(1 - n^{-\omega(1)}, 1 - 2n^{-\omega(1)})$. □

The security of the scheme is obtained by a elementary reduction from the decisional R-LWE$^{\times}_{HNF+}$, using the uniformity of the public key, and invertibility of (p, p').

Lemma 19 (Adapted from [50], Le. 3.8). *Suppose that* $n + 1$ *is a prime such that* $\Phi = x^n + x^{n-1} + ... + x + 1$ *splits into* n *linear factors modulo prime* $(q, |q'|) \geq' (5, 5)$. *Let* $\varepsilon, \varepsilon' \in (0, 1/3)$, $(\delta, \delta') >' (0, 0)$, $(p, p') \in R^{\times}_{(q,q')}$ *and* $(\sigma, \sigma') \geq' (n, 2n)\sqrt{ln((8n, 16n)(q, |q'|))}.(q^{1/2+\varepsilon}, |q'|^{1/2+\varepsilon'})$. *If there exists an IND-CPA attack against ETRU that runs in time* T *and has success probability* $(1/2, 1/2) + (\delta, \delta')$, *then there exists an algorithm solving R-LWE*$^{\times}_{HNF+}$ *with parameters* q, q' *and* α *that runs in time* $T' = T + O(n)$ *and has success probability* $(\delta, \delta')' = (\delta, \delta') - (q, |q'|)^{-\Omega(n)}$.

Proof. Let A be the given IND-CPA attack, B be an algorithm against R-LWE$^{\times}_{HNF+}$ and O be an oracle that samples from either $U(R^{\times}_{(q,q')} \times R_{(q,q')})$ or $A^{\times}_{(s,s'),\psi}$ for some previously chosen $s, s' \hookleftarrow \psi$ and $\psi \hookleftarrow \bar{\Upsilon}_{\alpha}$. Algorithm B first calls O to get a sample $((h, h')', (c, c')')$ from $R^{\times}_{(q,q')} \times R_{(q,q')}$. Then, algorithm B runs A with public key $(h, h') = (p, p').(h, h')' \in R_{(q,q')}$. When A outputs challenge messages $(M_0, M'_0), (M_1, M'_1) \in P$, B picks $b \hookleftarrow U(\{0, 1\})$, computes the challenge ciphertext $(c, c') = (p, p').(c, c')' + (M_b, M'_b) \in R_{(q,q')}$, and returns (c, c') to A. Thus for A guess b' for b, algorithm B outputs 1 if $b' = b$ and 0 otherwise, for each component.

By theorem 6, the public key given to A is within statistical distance $(q, |q'|)^{-\Omega(n)}$ of the public key distribution in the genuine attack. Also, since $(c, c')' = (h, h')(s, s') + (e, e')$ with s, s', e, e' sampled from ψ, (c, c') given to A has exactly the right distribution as in the IND-CPA attack. Overall, if O outputs samples from $A^{\times}_{(s,s'),\psi}$, then A succeeds and B returns 1 with probability $\geq' (1/2, 1/2)+(\delta, \delta')-(q, |q'|)^{-\Omega(n)}$.

Moreover, if O outputs samples from $U(R^{\times}_{(q,q')} \times R_{(q,q')})$ and since $(p, p') \in R^{\times}_{(q,q')}$, then $(p, p')(c, c')'$ and (c, c') are uniformly random in $R_{(q,q')}$ and independent of b. Therefore, B outputs 1 with probability $1/2$ for each component. The claimed advantage of B now follows. □

Overall, by combining lemmata 18 and 19 with theorem 4 our main result is obtained:

Theorem 7. *Suppose* $n + 1$ *is a prime such that* $\Phi = x^n + x^{n-1} + ... + x + 1$ *splits into* n *linear factors*

modulo prime $(q, q') = (Poly(n), Poly(n))$ *such that* $(q^{1/2-\varepsilon}, |q'|^{1/2-\varepsilon'}) = \omega(n^{2.25} ln^2 n)||(p, p')||^2$, *with* $(\varepsilon, \varepsilon') = (\omega(1/n), \omega(1/n))$ *and* $(\varepsilon, \varepsilon') <' (1/3, 1/3)$ *and* $(p, p') \in R^{\times}_{(q,q')}$ *with* $deg(p, p') \leq' (1, 1)$. *Let* $(\sigma, \sigma') = (n, 2n)\sqrt{ln((8n, 16n)(q, |q'|))}.(q^{1/2+\varepsilon}, |q'|^{1/2+\varepsilon'})$ *and* $\alpha^{-1} = \omega(n^{0.25} lnn)||(p, p')||^2(\sigma, \sigma')$. *If there exists an IND-CPA attack against ETRU which runs in time* $Poly(n)$ *and has success probability* $1/2+1/Poly(n)$ *for each component, then there exists a* $Poly(n)$*-time quantum algorithm for* γ*-Ideal-SVP with* $\gamma = \omega(n^{2.75} ln^{2.5} n)||(p, p')||^2(q^{1/2+\varepsilon}, |q'|^{1/2+\varepsilon'})$. *Also, the decryption algorithm succeds with probability* $(1 - n^{-\omega(1)}, 1 - 2n^{-\omega(1)})$ *for each component separately.*

5 Conclusions and Open Problems

In this paper the structure of all generated polynomial rings of quotient over direct product of Dedekind domains $\mathbb{Z}$ and $\mathbb{Z}[\zeta_3]$ were described, in which ζ_3 is complex cube root of unity. It shown that if the private key polynomials of the *ETRU* are selected from direct product of some Dedekind domains using discrete Gaussians, then the public key, is statistically indistinguishable from uniform over its range. futhermore the security of this scheme is based on the hardness of the R-SIS and R-LWE problems by their extensions. In this paper we studied the sequence of rings $R_{(q,q')} := \frac{(\mathbb{Z}\times\mathbb{Z}[\zeta_3])_{(q,q')}[x]}{\Phi=<(1,1)x^n+(1,1)x^{n-1}+\ldots+(1,1)x+(1,1)>}$ for provably secure encryption scheme. We can now introduce some open problems. Some interesting challenges are modification and generalization of *group and ring signatures*, *identity-based schemes*, *homomorphic encryption*, *zero-knowledge proofs*, and *identification protocols* over direct product of rings and extended ideal lattices. Also an interesting choice could be another cyclotomic rings for *ETRU*, one might then be able to show that the hardness carries over to *ETRU* rings. From lattice-based cryptographic primitives for direct product of Dedekind domain polynomials, both fast Fourier transform (FFT) and discrete Gaussian sampling are of main ingredients in provably secure lattice-based cryptography. Therefore, implementation of FFT with different degrees and typical parameter sets, as well as discrete Gaussian sampling algorithm are remaining interesting challenges.

References

[1] J. Hoffstein, J. Pipher, , and J. H. Silverman. NTRU: a new high speed public key cryptosystem. In *presented at the rump session of Crypto'96*, 1996.

[2] J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: a ring based public key cryptosystem. In *International Algorithmic Number Theory Symposium*, pages 267–288. Springer, Berlin, Heidelberg, 1998. ISBN 978-3-540-64657-0. doi:10.1007/BFb0054868.

[3] IEEE Standard Specifications for Public-Key Cryptography. *IEEE Std 1363-2000*, pages 1–228, Aug 2000. doi:10.1109/IEEESTD.2000.92292.

[4] Ray A. Perlner and D. A. Cooper. Quantum resistant public key cryptography: a survey. In *Proceedings of the 8th Symposium on Identity and Trust on the Internet*, pages 85–93. ACM, 2009. ISBN 978-1-60558-474-4. doi:10.1145/1527017.1527028.

[5] J. Hoffstein, J. P., and J. H. Silverman. NSS: An NTRU Lattice-Based Signature Scheme. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 211–228. Springer, Berlin, Heidelberg, 2001. ISBN 978-3-540-42070-5. doi:10.1007/3-540-44987-6_14.

[6] M. Szydlo. Hypercubic Lattice Reduction and Analysis of GGH and NTRU Signatures. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 433–448. Springer, Berlin, Heidelberg, 2003. ISBN 978-3-540-14039-9. doi:10.1007/3-540-39200-9_27.

[7] S. Min, G. Yamamoto, and K. Kim. Weak property of malleability in NTRUSign. In *Australasian Conference on Information Security and Privacy*, pages 379–390. Springer, Berlin, Heidelberg, 2004. ISBN 978-3-540-27800-9. doi:10.1007/978-3-540-27800-9_33.

[8] P. Q. Nguyen and O. Regev. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. *Journal of Cryptology*, 22(2):139–160, 2009. ISSN 0933-2790. doi:10.1007/s00145-008-9031-0.

[9] V. Lyubashevsky and D. Micciancio. Generalized compact knapsacks are collision resistant. In *International Colloquium on Automata, Languages, and Programming*, pages 144–155. Springer, Berlin, Heidelberg, 2006. ISBN 978-3-540-35907-4. doi:10.1007/11787006_13.

[10] C. Peikert and A. Rosen. Lattices that admit logarithmic worst-case to average-case connection factors. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 478–487. ACM, 2007. ISBN 978-1-59593-631-8. doi:10.1145/1250790.1250860.

[11] C. Peikert and A. Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In *Theory of Cryptography Conference*, pages 145–166. Springer, Berlin, Heidelberg, 2006. ISBN 978-3-540-32731-8. doi:10.1007/11681878_8.

[12] V. Lyubashevsky, D. Micciancio, C. Peikert, and

A. Rosen. SWIFFT: a modest proposal for FFT hashing. In *International Workshop on Fast Software Encryption*, pages 54–72. Springer, Berlin, Heidelberg, 2008. ISBN 978-3-540-71038-7. doi:10.1007/978-3-540-71039-4_4.

[13] V. Lyubashevskyand C. Peikert and O. Regev. On ideal lattices and learning with errors over rings. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 1–23. Springer, Berlin, Heidelberg, 2010. ISBN 978-3-642-13189-9. doi:10.1007/978-3-642-13190-5_1.

[14] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6), 2009. doi:10.1145/1568318.1568324.

[15] D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa. Efficient public key encryption based on ideal lattices. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 617–635. Springer, Berlin, Heidelberg, 2009. ISBN 978-3-642-10365-0. doi:10.1007/978-3-642-10366-7_36.

[16] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 197–206. ACM, 2008. ISBN 978-1-60558-047-0. doi:10.1145/1374376.1374407.

[17] V. Lyubashevsky. Fiat-shamir with aborts: Applications to lattice and factoring-based signatures. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 598–616. Springer, Berlin, Heidelberg, 2009. ISBN 978-3-642-10365-0. doi:10.1007/978-3-642-10366-7_35.

[18] P.L Cayrel, R. Lindner, M. Rückert, and R. Silva. A lattice-based threshold ring signature scheme. In *International Conference on Cryptology and Information Security in Latin America*, pages 255–272. Springer, Berlin, Heidelberg, 2010. ISBN 978-3-642-14711-1. doi:10.1007/978-3-642-14712-8_16.

[19] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert. Bonsai trees, or how to delegate a lattice basis. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 523–552. Springer, Berlin, Heidelberg, 2010. ISBN 978-3-642-13189-9. doi:10.1007/978-3-642-13190-5_27.

[20] C. Gentry. Toward basing fully homomorphic encryption on worst-case hardness. In *Annual Cryptology Conference*, pages 116–137. Springer, Berlin, Heidelberg, 2010. ISBN 978-3-642-14622-0. doi:10.1007/978-3-642-14623-7_7.

[21] C. Gentry and S. Halevi. Fully homomorphic encryption without squashing using depth-3 arithmetic circuits. In *IEEE 52nd Annual Symposium on Foundations of Computer Science*, pages 107–109. IEEE, 2011. ISBN 978-1-4577-1843-4. doi:10.1109/FOCS.2011.94.

[22] V. Vaikuntanathan Z. Brakerski, C. Gentry. Fully homomorphic encryption without bootstrapping. *Cryptology ePrint Archive*, 18, 2011.

[23] V. Lyubashevsky. Lattice-based identification schemes secure under active attacks. In *International Workshop on Public Key Cryptography*, pages 162–179. Springer, Berlin, Heidelberg, 2008. ISBN 978-3-540-78439-5. doi:10.1007/978-3-540-78440-1_10.

[24] A. Kawachi, K. Tanaka, and K. Xagawa. Concurrently secure identification schemes and ad hoc anonymous identification schemes based on the worst-case hardness of lattice problems. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 372–389. Springer, Berlin, Heidelberg, 2008. ISBN 978-3-540-89254-0. doi:10.1007/978-3-540-89255-7_23.

[25] C. Peikert and V. Vaikuntanathan. Noninteractive statistical zero-knowledge proofs for lattice problems. In *Annual International Cryptology Conference*, pages 536–553. Springer, Berlin, Heidelberg, 2008. ISBN 978-3-540-85173-8. doi:10.1007/978-3-540-85174-5_30.

[26] Philippe Gaborit, Julien Ohler, and Patrick Solé. CTRU, a polynomial analogue of NTRU. Technical Report RR-4621, INRIA, November 2002. URL `https://hal.inria.fr/inria-00071964`.

[27] M. Coglianese and B.M. Goi. MaTRU: A New NTRU-Based Cryptosystem. In *International Conference on Cryptology in India*, pages 232–243. Springer, Berlin, Heidelberg, 2005. ISBN 978-3-540-30805-8. doi:10.1007/11596219_19.

[28] N. Vats. NNRU, a Noncommutative Analogue of NTRU. *arXiv preprint arXiv:0902.1891*, 2009.

[29] R. Kouzmenko. *Generalizations of the NTRU Cryptosystem*. PhD thesis, Master's thesis, Polytechnique Montreal, Canada, 2005.

[30] K. Jarvis and M. Nevins. ETRU: NTRU over the Eisenstein Integers. *Designs Codes and Cryptography*, 47(1), 2013. doi:10.1007/s10623-013-9850-3.

[31] M. EHSAN, Z. ALI, and M. ATEFEH. QTRU: Quaternionic Version of the NTRU Public-Key Cryptosystems. *The ISC International Journal of Information Security*, 3(1):29–42, 2011. doi:10.22042/isecure.2015.3.1.3.

[32] A. H. Karbasi and R. E. Atani. ILTRU: An NTRU-Like Public Key Cryptosystem Over Ideal Lattices. *IACR Cryptology ePrint Archive*, 2015:

549, 2015. doi:cr.org/2015/549.

[33] A.H. Karbasi and R.E. Atani. A Survey on Lattice-based Cryptography. *Biannual Journal for Cyberspace Security (Monadi AFTA)*, 3(1): 3–14, 2015.

[34] A.H. Karbasi and R.E. Atani. PSTRU: A provably secure variant of NTRUEncrypt over extended ideal lattices. In *The 2nd National Industrial Mathematics Conference, Tabriz, Iran*, 2015.

[35] B. Rajabi and Z. Eslami. A CCA2-Secure Incomparable Public Key Encryption Scheme. *Journal of Computing and Security*, 3(1):3–12, 2016. ISSN 2322-4460.

[36] J. Alizadeh and M. R. Aref. JHAE: A Novel Permutation-Based Authenticated Encryption Mode Based on the Hash Mode JH. *Journal of Computing and Security*, 2(1):3–20, 2015. ISSN 2322-4460.

[37] S. Khodambashi and A. Zakerolhosseini. A Weak Blind Signature Based on Quantum Key Distribution. *Journal of Computing and Security*, 1(3): 179–186, 2014. ISSN 2322-4460.

[38] M. Ajtai. Generating hard instances of lattice problems (extended abstrat). In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 99–108. ACM, 1996. ISBN 0-89791-785-5. doi:10.1145/237814.237838.

[39] R. Lindner and C. Peikert. Better key sizes (and attacks) for LWE-based encryption. In *Cryptographers' Track at the RSA Conference*, pages 319–339. Springer, Berlin, Heidelberg, 2011. ISBN 978-3-642-19073-5. doi:10.1007/978-3-642-19074-2_21.

[40] D. Micciancio and C. Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 700–718. Springer, Berlin, Heidelberg, 2012. ISBN 978-3-642-29010-7. doi:10.1007/978-3-642-29011-4_41.

[41] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert. Bonsai trees, or how to delegate a lattice basis. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 523–552. Springer, Berlin, Heidelberg, 2010. ISBN 978-3-642-13189-9. doi:10.1007/978-3-642-13190-5_27.

[42] S. Agrawal, D. Boneh, and X. Boyen. Efficient lattice (H)IBE in the standard model. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 553–572. Springer, Berlin, Heidelberg, 2010. ISBN 978-3-642-13189-9. doi:10.1007/978-3-642-13190-5_28.

[43] S. Agrawal, D. Boneh, and X. Boyen. Lattice basis delegation in fixed dimension and shorter ciphertext hierarchical IBE. In *Annual Cryptology Conference*, pages 98–115. Springer, Berlin, Heidelberg, 2010. ISBN 978-3-642-14622-0. doi:10.1007/978-3-642-14623-7_6.

[44] Z. Brakerski and V. Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In *Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*, pages 97–106. IEEE, 2011. ISBN 978-0-7695-4571-4. doi:10.1109/FOCS.2011.12.

[45] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, pages 309–325. Springer, Berlin, Heidelberg, 2012. ISBN 978-1-4503-1115-1. doi:10.1145/2090236.2090262.

[46] X. Boyen. lattice mixing and vanishing trapdoors: A framework for fully secure short signatures and more. In *International Workshop on Public Key Cryptography*, pages 499–517. Springer, Berlin, Heidelberg, 2010. ISBN 978-3-642-13012-0. doi:10.1007/978-3-642-13013-7_29.

[47] V. Lyubashevsky. Lattice signatures without trapdoors. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 738–755. Springer, Berlin, Heidelberg, 2012. ISBN 978-3-642-29010-7. doi:10.1007/978-3-642-29011-4_43.

[48] O. Regev. The learning with errors problem. `http://www.cs.tau.ac.il/~odedr/`, Date Accessed: 2010.

[49] M. EHSAN, Z. ALI, and M. ATEFEH. Generalized compact knapsacks,cyclic lattices, and efficient one-way functions. *computational complexity*, 16(4):365–411, 2007. doi:10.1007/s00037-007-0234-9.

[50] D. Stehlé and R. Steinfeld. Making NTRUEncrypt and NTRUSign as secure as standard worst-case problems over ideal lattices. In *Proceedings of the 30th Annual international conference on Theory and applications of cryptographic techniques: advances in cryptology*, pages 27–47. ACM, 2011. ISBN 978-3-642-20464-7.

[51] K. Jarvis. *NTRU over the Eisenstein integers*. PhD thesis, University of Ottawa, 2011.

[52] C. Peikert. An efficient and parallel gaussian sampler for lattices. In *Annual Cryptology Conference*, pages 80–97. Springer, Berlin, Heidelberg, 2010. ISBN 978-3-642-14622-0. doi:10.1007/978-3-642-14623-7_5.

[53] L. Ducas and P. Q. Nguyen. Faster gaussian lattice sampling using lazy floating-point arithmetic. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 415–432. Springer, Berlin, Heidelberg,

2012. ISBN 978-3-642-34960-7. doi:10.1007/978-3-642-34961-4_26.

[54] N. H. Graham, J. H. Silverman, A. Singer, and W. Whyte. NAEP: Provable security in the presence of decryption failures. *International Association for Cryptologic Research*, 2003, 2003.

[55] R. Steinfeld, S. Ling, J. Pieprzyk, C. Tartary, and H. Wang. NTRUCCA: How to Strengthen NTRUEncrypt to Chosen-Ciphertext Security in the Standard Model. In *International Workshop on Public Key Cryptography*, pages 353–371. Springer, Berlin, Heidelberg, 2012. ISBN 978-3-642-30056-1. doi:10.1007/978-3-642-30057-8_21.

[56] A. L. Alt, E. Tromer, and V. 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*, pages 1219–1234. ACM, 2012. ISBN 978-1-4503-1245-5. doi:10.1145/2213977.2214086.

[57] P. Garrett. Abstract Algebra. Technical report, University of Minnesota, 2007. URL `http://www-users.math.umn.edu/~garrett/m/algebra/notes/Whole.pdf`.

[58] D. Micciancio and O. Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM Journal on Computing*, 37(1): 267–302, 2007. doi:10.1137/S0097539705447360.

[59] H. Cohen. *Advanced topics in computational number theory*. Springer, 2000.

[60] C. Fieker and D. Stehlé. Short bases of lattices over number fields. In *International Algorithmic Number Theory Symposium*, pages 157–173. Springer, Berlin, Heidelberg, 2010. ISBN 978-3-642-14517-9. doi:10.1007/978-3-642-14518-6_15.

[61] A. K. Lenstra, H. W. LenstraJr, and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982. ISSN 0025-5831. doi:10.1007/BF01457454.

[62] C. P. Schnorr. A hierarchy of polynomial lattice basis reduction algorithms. *Theoretical Computer Science*, 53(2):201–224, 1987. ISSN 0025-5831. doi:10.1016/0304-3975(87)90064-8.

[63] D. Micciancio and P. Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on voronoi cell computations. *SIAM Journal on Computing*, 17(3):351–358, 2010. doi:10.1145/1806689.1806739.

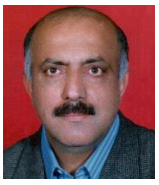
[64] B. Applebaum, D. Cash, C. Peikert, and A. Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In *Annual International Cryptology Conference*, pages 595–618. Springer, Berlin, Heidelberg, 2009. ISBN 978-3-642-03355-1. doi:10.1007/978-3-642-03356-8_35.

[65] V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. *Journal of the ACM (JACM)*, 60(6):43, 2013.

[66] V. Lyubashevsky, C. Peikert, and O. Regev. A toolkit for Ring-LWE cryptography. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 35–54. Springer, Berlin, Heidelberg, 2013. ISBN 978-3-642-38347-2. doi:10.1007/978-3-642-38348-9_3.

[67] L. Ducas and A. Durmus. Ring-LWE in polynomial rings. In *International Workshop on Public Key Cryptography*, pages 34–51. Springer, Berlin, Heidelberg, 2012. ISBN 978-3-642-30056-1. doi:10.1007/978-3-642-30057-8_3.

Reza Ebrahimi Atani studied Electronics Engineering at the University of Guilan, Rasht, Iran and got his B.S. degree in 2002. He followed his masters and Ph.D. studies at Iran University of Science & Technology (IUST) in Tehran, and received Ph.D. degree in 2010. He is now holding an associated professor position in the Department of Computer Engineering at the University of Guilan. His research interests focuses on design and implementation of cryptographic algorithms and protocols as well as their applications to computer and network security and mobile communications. He is a member of IEEE and IACR.



Shahabaddin Ebrahimi Atani got his B.S. and M.S. in Mathematics. In 1996, he graduated from a Ph.D. program of Mathematical Science Department in University of Manchester, England. He is now a professor at faculty of Mathematical Sciences of the University of Guilan. His research interests include Rings and Semi-ring theory and Pullback of Rings.

Amir Hassani Karbasi studied his BSc in Applied Mathematics at the University of Tabriz in Tabriz, Iran. He received his BSc degree in 2010. He received his MSc in Computer Networks in 2013 from University of Guilan. He received his Ph.D. in 2018 from University of Guilan (Elite Entrance Students to Ph.D.) and has worked on "Design and security analysis of lattice-based cryptographic structures". Now, He is a part-time faculty member at some Universities and information security specialist at some companies. His main research interests include lattice-based cryptography, digital signatures, network security, blockchain, cryptocurrencies, rings and semi-ring theory and Pullback of Rings.