NTRU in Quaternion Algebras of Bounded Discriminant

Cong Ling and Andrew Mendelsohn

Department of EEE, Imperial College London, London, SW7 2AZ, United Kingdom.
andrew.mendelsohn18@imperial.ac.uk
c.ling@imperial.ac.uk

Abstract. The NTRU assumption provides one of the most prominent problems on which to base post-quantum cryptography. Because of the efficiency and security of NTRU-style schemes, structured variants have been proposed, using modules. In this work, we create a structured form of NTRU using lattices obtained from orders in cyclic division algebras of index 2, that is, from quaternion algebras. We present a public-key encryption scheme, and show that its public keys are statistically close to uniform. We then prove IND-CPA security of a variant of our scheme when the discriminant of the quaternion algebra is not too large, assuming the hardness of Learning with Errors in cyclic division algebras.

Keywords: post-quantum cryptography · NTRU · quaternion algebras

1 Introduction

NTRU schemes provide one of the most efficient post-quantum cryptographic frameworks. While attacks such as lattice reduction can be used, known attacks are ineffective against NTRU with well-chosen parameters. This absence of decisive attacks against well-chosen parameters over a long period of time has led NTRU to have a prominent place in the geography of post-quantum cryptography. This is illustrated by two NTRU-based schemes reaching the third round of NIST's post-quantum standardization effort [19], [13]. Moreover, partial security reductions for NTRU have been given in [46], [18], lending further weight to NTRU as a platform for cryptography.

The NTRU problem can be formulated as follows: if f and g are 'short' ring elements, and $h := g \cdot f^{-1}$, find (f, g) from $h \bmod q$, for some modulus $q \in \mathbb{Z}$. Typical choices of rings are polynomial rings of the form $\mathbb{Z}[x]/(x^p - 1)$, $\mathbb{Z}[x]/(x^{2^k} + 1)$, and $\mathbb{Z}[x]/(x^p - x - 1)$ [24], [19], [9]. These enjoy fast algorithms for multiplication and low storage requirements. Moreover, a simple public-key encryption scheme can be based on the hardness of the NTRU problem.

The cryptanalytic history of NTRU is lengthy, beginning with lattice reduction attacks [17] and including meet-in-the-middle attacks [27], hybrid attacks [25], attacks based on decryption failures [26], and subfield attacks [2]. These often exploit particular design choices of specific NTRU schemes (such as a choice of ternary secrets, or an 'overstretched' choice of modulus, or the use

of rings with many subrings), and hence these weak(er) instances or parameters can be avoided by careful design. As a result, after 25 years of cryptanalysis, the NTRU assumption remains a trusted basis for cryptography.

The reliability and speed of NTRU has also prompted work exploring alternatively structured variants of NTRU [15], [16]. Whereas NTRU uses multiplication of elements in polynomial rings, these constructions use operations in modules over polynomial rings, and aim to instantiate efficient and compact NTRU schemes while enabling greater flexibility with parameter choices. However, neither of [15], [16] give a full proof of security: in [16], it is shown that module NTRU public keys are (asymptotically) close to uniform, if the modulus factors into only two prime ideals in the ring - yet the scheme uses primes which completely split in the ring; and the authors of [15] give no such proof.

Our Contributions In this work we study the NTRU problem in the context of quaternion algebras over number fields. In particular, we define NTRU in cyclic division algebras (CDAs) when the ring of scalars (the 'center') of the algebra is a cyclotomic field with power of two conductor. We call this NTRU variant 'CNTRU'. The dimension of these algebras over their center is a square, d^2, and the positive square-root of this dimension, d, is called the index of the algebra. When the index is 1, the CDA is equal to its center, and so in our case is a cyclotomic field; when the index is 2, the CDA is called a quaternion algebra. These quaternion algebras enjoy particularly nice properties (see e.g. [56]) and the proof of our main result on the uniformity of our NTRU public keys appears to fail when $d > 2$. This is because when $d = 2$ and the center is a cyclotomic field of power-of-two conductor, the number of roots of unity in the CDAs used equals the dimension of certain lattices $\mathcal{L}$ concerned, so letting λ_i denote the ith successive minimum of a lattice $\mathcal{L}$, we have $\lambda_1(\mathcal{L}) = \lambda_{[\mathcal{L}:\mathbb{Z}]}(\mathcal{L})$ and can make use of results such as Lemma 3; when $d > 2$, we can no longer apply such lemmas.

The specific algebras in which we consider our NTRU variant are constructed as follows: let m be a prime power, $K = \mathbb{Q}(\zeta_m)$ be a cyclotomic field of conductor m, and $M = \mathbb{Q}(\zeta_{\ell m})$, for some prime ℓ such that $\ell \equiv 1 \bmod m$ and $\ell \not\equiv 1 \bmod pm$ for any prime divisor p of m. Then M/K is cyclic Galois, with Galois group generated by (say) σ. Let L be the intermediate field fixed by σ^2; this can be written explicitly as $L = \mathbb{Q}(\zeta_m, \sqrt{\ell})$ when m is a power of two. Set u to be an element such that $u^2 = \zeta_m$ and $ux = \theta(x)u$ for all $x \in L$, where $\mathrm{Gal}(L/K) = \langle\theta\rangle$. Then $\mathcal{A} = (L/K, \theta, \zeta_m) = L + uL$ is a quaternion algebra. We define $\Lambda := \mathcal{O}_L + u\mathcal{O}_L$ and $\Lambda_q := \Lambda/q\Lambda$ for some prime q. We denote the units of Λ_q by $\Lambda_q^\times$, and the center of Λ by $\mathcal{Z}(\Lambda)$. We then prove, for these quaternion algebras,

Theorem 4. Let $\epsilon > 0$, q be a completely split prime, $p \in \mathcal{Z}(\Lambda_q^\times)$, and $\sigma \geq 4n^{3/2}\sqrt[4]{\ell}\sqrt{2\ln(32nq)}q^{\frac{1}{2}+2\epsilon}$. Let $y_i \in \Lambda_q$ and $z_i = -y_i p^{-1} \bmod q$ for $i = 1, 2$, and $D^\times_{\sigma,z_i}$ denote $D_{\Lambda,\sigma}$ restricted by rejection to $\Lambda_q^\times + z_i$. Then when $d = 2$,

$$\Delta\left(\frac{y_1 + pD^\times_{\sigma,z_1}}{y_2 + pD^\times_{\sigma,z_2}} \bmod q, U\left(\Lambda_q^\times\right)\right) \leq 2^{22n}q^{-8n\epsilon}.$$

To achieve this, we prove a number of new results on q-ary lattices obtained from orders in CDAs (of a particular form). These results can be stated for any $d \geq 1$, but we restrict them to the case of interest, $d = 2$.

We then proceed to study algorithms to encrypt and decrypt messages based on the NTRU problem in these quaternion algebras. We prove that if there is an efficient indistinguishability-under-chosen-plaintext attack (IND-CPA) algorithm for CNTRU, there is an algorithm with non-negligible advantage for decision CLWE [21], a structured form of learning with errors (LWE) in CDAs. The uniformity of CNTRU public keys (over invertible elements) forms a crucial part of the proof of this result. Moreover, this connection is in part a motivation for the particular CDAs we define NTRU over: the existence of a security proof for CLWE in these particular algebras linking SIVP on lattices obtained from ideals of Λ to CLWE allows us to link SIVP and NTRU, too (it should be noted that the reduction from SIVP to CLWE holds for a (slightly) restricted space of secrets). We obtain

Lemma 1. *Let $n \geq 8$ be a power of 2, $d = 2$, $\ell \leq Cn$, and $q \geq 8n$ a prime such that $x^n + 1$ splits completely modulo q. Let $\delta > 0$, $p \in \mathcal{Z}\left(\Lambda_q^\times\right)$ and $\sigma \geq 2n^{3/2}\sqrt[4]{\ell}\sqrt{\ln(32nq)}q^{\frac{1}{2}+2\epsilon}$ satisfy the conditions of Lemma 18 and Theorem 4. If there exists an IND-CPA attack algorithm $\mathcal{A}$ against CNTRU, running in time T with advantage δ, then there exists an algorithm to solve decision-CLWE$^\times_{\text{HNF}}$ that runs in time $T' = T + O(\text{poly}(n))$ with success probability $\delta' = \delta - q^{-\Omega(n)}$.*

Note the condition $\ell \leq Cn$ for a constant C: we impose a bound on ℓ in order to allow for a precise statement on the correctness of the decryption algorithm (see Lemma 18). This is necessary because of the form of L. Consider the square of field element $1+\sqrt{\ell}$; this is an element of small ℓ_2-norm when using $1, \sqrt{\ell}$ as a basis of L/K, but its square, $1+\ell+2\sqrt{\ell}$, may potentially be large indeed, if ℓ is large. This constraint amounts to a bound on the discriminant of the quaternion algebra, which has discriminant which we bound by $(n\sqrt{\ell})^{4n}$ (Lemma 2); when $\ell \leq Cn$, this becomes a function solely in $n = [K : \mathbb{Q}]$.

In practice, we have not found this imposition difficult to satisfy for small values of C. The interested reader is directed to [21, §3.4] and Appendix B of this paper for further discussion on parameter selection.

We also sketch a KEM and a signature scheme based on NTRU in CDAs in the appendix, to give examples of greater functionality from CNTRU.

	Cyclotomic NTRU [57]	ModFalcon [16]	This work
Ambient space	$\mathbb{Q}(\zeta_n)$, any n	$\mathbb{Q}(\zeta_{2^r})^2$	$\mathcal{A} = L \oplus uL$, $L = \mathbb{Q}(\zeta_{2^r}, \sqrt{\ell})$
$\mathbb{Z}$-Dimension	$\varphi(n)$	2^r	2^{r+1}
Recommended q	$q \equiv 1 \bmod n$	$q \equiv 1 \bmod 2^r$	q completely split in L
Provably secure q	$q \equiv 1 \bmod n$	$q \equiv 3 \bmod 8$	q completely split in L

Table 1: Comparison of Cyclotomic NTRU Variants

Previous Work There have been many algebraic variants of NTRU proposed over the years: in CTRU [20], the usual polynomials were replaced with elements

from the ring $\mathbb{F}_2[T][X]/(X^n - 1)$; this was later subjected to a polynomial-time attack in [33], which also introduced NTRU over the Gaussian Integers. This idea was expanded by [41] and [51], which introduced NTRU over the Eisenstein integers (ETRU) and the ring of integers of $\mathbb{Q}(\sqrt{-7})$ (KTRU) respectively. More details on ETRU can be found in [40] and [29]. A version of NTRU using ideal lattices can be found in [30], an attempt to secure CTRU can be found in [4], and an attempt to further secure ETRU can be found in [5].

There have also been more exotic attempts to improve NTRU: some of these include non-commutative variants such as [53], [35], [54], [6]; NTRU over group rings in [58]; non-associative schemes in [34] and [52]; and a variant with different invertibility conditions in [7]. A useful comparison of some of these schemes can be found in [47]. An overview of NTRU can be found in [50].

Despite this flood of NTRU variants, we note that few of them generalise NTRU, in the sense that they do not offer a broader framework from which the traditional form of NTRU can emerge; rather, they simply replace the underlying ring, or make other subtle amendments. Two papers [15], [16] do develop general (module) versions of NTRU; these are compared to the construction featured in this paper below. Finally, we note recent works [10], [46], [18] which provide reductions between various (module) NTRU problems, and also module LWE.

Paper Organization In the next section we state the mathematical background necessary for the rest of the paper. In section 3 we introduce NTRU, in section 4 CDAs, and combine these in section 5. We then begin the mathematical work of the paper: section 6 is dedicated to q-ary lattices obtained from CDAs, section 7 to the CNTRU key generation algorithm, section 8 to proving IND-CPA security of CNTRU (subject to the CLWE assumption). In the appendix we give possible parameters and sketch a KEM and signature scheme.

2 Preliminaries

Lattices An n-dimensional lattice is a discrete additive subgroup of $\mathbb{R}^n$. One can consider a lattice $\mathcal{L}$ to be the set of integer linear combinations of a set of vectors $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_k\}$ that are linearly independent, for some $k \leq n$, written $\mathcal{L}(B) = \left\{\sum_{i=1}^{k} z_i \mathbf{b}_i : z_i \in \mathbb{Z}\right\}$. All lattices in this work will have $k = n$.

Definition 1. Let $\mathcal{L}$ be a lattice, and $\mathbb{R}^n$ be endowed with inner product $\langle \cdot, \cdot \rangle$. Then the set $\mathcal{L}^* = \{v \in \mathbb{R}^n : \langle \mathcal{L}, v \rangle \subset \mathbb{Z}\}$ is called the *dual lattice* of $\mathcal{L}$.

Recall $\lambda_i(\mathcal{L})$, the 'ith successive minimum of $\mathcal{L}$', is the minimum length of a set of i linearly independent vectors in $\mathcal{L}$, where the length of a set of vectors $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ is $\max_i (\|\mathbf{x}_i\|)$, for some norm $\|\cdot\|$.

Discrete Gaussians For vector space $V \subset \mathbb{R}^n$ equipped with (Euclidean) norm $\|\cdot\|$, $\boldsymbol{c} \in V$, and $r > 0$, we define the *Gaussian function* $\rho_{r,\mathbf{c}} : V \to (0, 1]$ by

$\rho_{r,\boldsymbol{c}}(\boldsymbol{x}) = \exp\left(-\pi\|\boldsymbol{x}-\boldsymbol{c}\|/r^2\right)$. If $\boldsymbol{c} = \mathbf{0}$, we write ρ_r.

The spherical Gaussian distribution D_r over $\mathbb{R}^n$ outputs a vector $\mathbf{v}$ with probability proportional to $\rho_r(\mathbf{v})$, and an elliptical Gaussian $D_{\mathbf{r}}$ can be sampled as follows: fix a basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ of $\mathbb{R}^n$, and a vector $\mathbf{r} = (r_1, \ldots, r_n)$. Sample $x_i \leftarrow D_{r_i}$ (independently for $i \neq j$) and output $\sum_{i=1}^n x_i \mathbf{b}_i$.

The discrete Gaussian distribution $D_{\mathcal{L},r,\mathbf{c}}$, defined over a lattice $\mathcal{L}$, outputs $\mathbf{x}$ with probability $\frac{\rho_{r,\boldsymbol{c}}(\mathbf{x})}{\rho_{r,\boldsymbol{c}}(\mathcal{L})}$ for each $\mathbf{x} \in \mathcal{L}$.

The *smoothing parameter*, defined below, will be used throughout this work:

Definition 2. Let $\mathcal{L}$ be a lattice and $\varepsilon > 0$. Then the *smoothing parameter* $\eta_\varepsilon(\mathcal{L})$ of $\mathcal{L}$ is the smallest $r > 0$ such that $\rho_{1/r}\left(\mathcal{L}^* \setminus \{\mathbf{0}\}\right) \leq \varepsilon$.

We will use the following bounds on the smoothing parameter:

Lemma 2. *[44, Lemma 3.5] For any full-rank lattice $\mathcal{L} \subseteq \mathbb{R}^n$ and $\epsilon \in (0,1)$, we have $\eta_\epsilon(\mathcal{L}) \leq \sqrt{\ln(2n(1+1/\epsilon))/\pi} \cdot \frac{1}{\lambda_1^{\infty}(\mathcal{L}^*)}$.*

Lemma 3. *[37, Lemma 3.3] For any full-rank lattice $\mathcal{L} \subseteq \mathbb{R}^n$ and $\epsilon \in (0,1)$, we have $\eta_\epsilon(\mathcal{L}) \leq \sqrt{\ln(2n(1+1/\epsilon))/\pi} \cdot \lambda_n(\mathcal{L})$.*

The *statistical distance* between distributions D, D' over a discrete set S is denoted $\Delta(D, D') = \frac{1}{2}\sum_{x \in S} |D(x) - D'(x)|$. We also need the following lemmas:

Lemma 4. *[37, Lemma 4.1] For a lattice $\mathcal{L}$ over $\mathbb{R}^n, \varepsilon > 0, r \geq \eta_\varepsilon(\mathcal{L})$, and $\boldsymbol{x} \in \mathbb{R}^n$, the statistical distance between $(D_r + \boldsymbol{x}) \bmod \mathcal{L}$ and the uniform distribution modulo $\mathcal{L}$ is bounded above by $\varepsilon/2$. Equivalently, $\rho_r(\mathcal{L} + \boldsymbol{x}) \in \left[\frac{1-\varepsilon}{1+\varepsilon}, 1\right] \cdot \rho_r(\mathcal{L})$*

Lemma 5. *[14, Theorem 1] For any positive definite Σ, vector $\boldsymbol{c}$, lattice coset $A := \Lambda + \mathbf{a} \subset \boldsymbol{c} + \mathrm{span}(\Sigma)$, and injective linear transformation $\mathbf{T}$, we have*

$$\mathbf{T}\left(D_{A,\sqrt{\Sigma},\mathbf{c}}\right) = D_{\mathbf{T}A,\mathbf{T}\sqrt{\Sigma},\mathbf{T}\boldsymbol{c}}.$$

Lemma 6. *[37, Lemma 4.4] For any full-rank lattice $\mathcal{L} \subseteq \mathbb{R}^n$, $\boldsymbol{c} \in \mathbb{R}^n$, $\delta \in (0,1)$ and $\sigma \geq \eta_\delta(\mathcal{L})$, we have $\Pr_{\boldsymbol{b} \leftarrow D_{\mathcal{L},\sigma,\mathbf{c}}}[\|\boldsymbol{b}\| \geq \sigma\sqrt{n}] \leq \frac{1+\delta}{1-\delta}2^{-n}$.*

Number Fields A number field is a finite field-extension of $\mathbb{Q}$. We will be especially interested in cyclotomic fields, $\mathbb{Q}(\zeta_n)$, where ζ_n is such that the smallest integer m such that $\zeta_n^m = 1$ is $m = n$. In this setting the degree $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, where φ is the totient function. We recall that $\varphi(p^r) = p^{r-1}(p-1)$.

A degree-n number field K is Galois over $\mathbb{Q}$ if the set of K-automorphisms fixing $\mathbb{Q}$ pointwise, $\mathrm{Gal}(K/\mathbb{Q})$, forms a group. The automorphisms $\sigma_i \in \mathrm{Gal}(K/\mathbb{Q})$ extend to embeddings $\sigma_i : K \hookrightarrow \mathbb{C}$. Using these embeddings, we embed $K \hookrightarrow \mathbb{C}^n$ via $\sigma_K : x \mapsto (\sigma_1(x), ..., \sigma_n(x))$. Defining a space $H = \{x \in \mathbb{C}^n : x_i = \overline{x_{n-i}} \text{ for } i \in [n]\}$, we have $\sigma_K(K) \subset H$, and $\mathbb{R}^n \cong H$ as an inner product space. Thus the image of any discrete additive subgroup of K under σ_K can be considered a lattice. The map σ_K is called the *canonical embedding*. These definitions

extend straightforwardly to a finite extension of number fields L/K.

An alternative way to embed a Galois number field into $\mathbb{R}^n$ is to write $K = \mathbb{Q}(\alpha)$ for some element α and writing $x = x_1\alpha + ... + x_n\alpha^n$ for $x \in K, x_i \in \mathbb{Q}$. The element x can then be mapped to $(x_1, ..., x_n) \in \mathbb{R}^n$. This is called the *coefficient embedding* of x, denoted $\text{coeff}(x)$.

Any Galois number field K contains a subring called the ring of integers of the field, which consists of the field elements which are the root of a monic polynomial with integral coefficients. We denote this subring $\mathcal{O}_K$. For any ideal $\mathcal{I}$ of $\mathcal{O}_K$, we define the dual ideal $\mathcal{I}^\vee = \{x \in K : T_{K/\mathbb{Q}}(x\mathcal{I}) \subset \mathbb{Z}\}$. Here $T_{K/\mathbb{Q}}(\cdot) = \sum_{\sigma \in \text{Gal}(K/\mathbb{Q})} \sigma(\cdot)$.

Bases of Real Quadratic Extensions of Cyclotomics We consider an extension L/K, where $K = \mathbb{Q}(\zeta_{2^r})$, $L = K(\sqrt{\ell}) = \mathbb{Q}(\zeta_{2^r}, \sqrt{\ell})$ and $\gcd(2, \ell) = 1$. With $n = [K : \mathbb{Q}]$ and $m = 2^r$, $\varphi(m) = n$. Define the *powerful basis* of $L/\mathbb{Q}$ as

$$\overrightarrow{p} = (1, \zeta_m, ..., \zeta_m^{n-1}, \sqrt{\ell}, \zeta_m\sqrt{\ell}, ..., \zeta_m^{n-1}\sqrt{\ell}).$$

We obtain a matrix from this by applying the canonical embedding to each entry:

$$\sigma_L(\overrightarrow{p}) = (\sigma_L(1), \sigma_L(\zeta_m), ..., \sigma_L(\zeta_m^{n-1}), \sigma_L(\sqrt{\ell}), \sigma_L(\zeta_m\sqrt{\ell}), ..., \sigma_L(\zeta_m^{n-1}\sqrt{\ell})).$$

This is a $2n \times 2n$ matrix. To find the singular values of this matrix, we compute $\sigma_L(\overrightarrow{p})^*\sigma_L(\overrightarrow{p})$. This is diagonal with two blocks: the top left $n \times n$ diagonal entries are all equal to m, and the bottom right $n \times n$ to $m\ell$. The eigenvalues of a diagonal matrix are its non-zero entries, so the singular values of $\sigma_L(\overrightarrow{p})$ are $\sqrt{[L : \mathbb{Q}]}, \sqrt{[L : \mathbb{Q}]\ell}$. Denoting the largest singular value by $s_1(\overrightarrow{p})$ and the smallest by $s_{2n}(\overrightarrow{p})$, we have $s_1(\overrightarrow{p}) = \sqrt{[L : \mathbb{Q}]\ell}$, $s_{2n}(\overrightarrow{p}) = \sqrt{[L : \mathbb{Q}]}$. Since

$$\sigma_L(x) = \sigma_L(\overrightarrow{p}) \cdot \text{coeff}(x),$$

for $x \in L$, we find $\|\sigma_L(x)\| \leq s_1(\overrightarrow{p})\|x\|_{\overrightarrow{p}}$, where $\|\cdot\|_{\overrightarrow{p}}$ is the norm obtained by writing x in the $\overrightarrow{p}$ basis and taking the coefficient embedding. Conversely,

$$\|x\|_{\overrightarrow{p}} \leq \frac{1}{s_{2n}(\overrightarrow{p})}\|\sigma_L(x)\| = \frac{1}{\sqrt{[L : \mathbb{Q}]}}\|\sigma_L(x)\|.$$

The $s_i(\overrightarrow{p})$ can in practice be taken to be polynomial in n, if desired. We will be interested in the above for integral elements $x \in \mathcal{O}_L$, which has powerful basis

$$(1, \zeta_m, ..., \zeta_m^{n-1}, \frac{1+\sqrt{\ell}}{2}, \zeta_m\frac{1+\sqrt{\ell}}{2}, ..., \zeta_m^{n-1}\frac{1+\sqrt{\ell}}{2}),$$

when $\ell \equiv 1 \bmod 4$. Upon computing the singular values of $\sigma(\overrightarrow{p})$, we find that

Proposition 1. *Let $n = 2^{r-1}$, $\ell \equiv 1 \bmod 2^r$ a prime, and $L = \mathbb{Q}(\zeta_{2^r}, \sqrt{\ell})$. Then, using the powerful basis of $\mathcal{O}_L$, we have*

$$s_1(\overrightarrow{p}) = \frac{\sqrt{n}}{2}\sqrt{\ell + 5 + \sqrt{\ell^2 - 6\ell + 25}} \;\&\; s_{2n}(\overrightarrow{p}) = \frac{\sqrt{n}}{2}\sqrt{\ell + 5 - \sqrt{\ell^2 - 6\ell + 25}}$$

Proof. The symmetric matrix $\sigma(\overrightarrow{p})^*\sigma(\overrightarrow{p})$ has a block form: the top left block is $[L:\mathbb{Q}]\cdot I_{2^{r-1}}$, where $I_{2^{r-1}}$ is the $2^{r-1}\times 2^{r-1}$ identity matrix, the lower right block is $2^{r-2}\cdot(\ell+1)$, and the top right and lower left blocks are $2^{r-1}\cdot I_{2^{r-1}}$. The eigenvalues of this matrix are $\lambda_i = 2^{r-2}\cdot\frac{\ell+5\pm\sqrt{\ell^2-6\ell+25}}{2}$. So the singular values are $s_i(\overrightarrow{p}) = \sqrt{2^{r-2}\cdot\frac{\ell+5\pm\sqrt{\ell^2-6\ell+25}}{2}} = \frac{\sqrt{n}}{2}\sqrt{\ell+5\pm\sqrt{\ell^2-6\ell+25}}$. □

If $\overrightarrow{d}$ is the dual of $\overrightarrow{p}$, we obtain $s_1(\overrightarrow{d}) = \frac{1}{s_{2n}(\overrightarrow{p})}$, $s_{2n}(\overrightarrow{d}) = \frac{1}{s_1(\overrightarrow{p})}$. We will use bounds in terms of this 'decoding basis'; in particular, for $x\in\mathcal{O}_L^\vee$,

$$\|x\|_{\overrightarrow{d}} \le \frac{1}{s_{2n}(\overrightarrow{d})}\|\sigma_L(x)\| = \frac{\sqrt{n}}{2}\sqrt{\ell+5+\sqrt{\ell^2-6\ell+25}}\|\sigma_L(x)\|.$$

When ℓ is bounded by some integer multiple of n, say $\ell\le Cn$ for $C\ge 2$, we can use the bound $s_1(\overrightarrow{p}) < 2Cn$, when $n\ge 4$.

Discretisation We will need the following distribution:

Definition 3. [39] Denote by Bern the Bernoulli distribution and let $a\in\mathbb{R}$. The univariate *Reduction distribution* $\mathrm{Red}(a) = \mathrm{Bern}(\lceil a\rceil - a) - (\lceil a\rceil - a)$ is defined

$$\mathrm{Red(a)} := \begin{cases} 1+a-\lceil a\rceil, \text{ with probability } \lceil a\rceil - a,\\ a-\lceil a\rceil, \text{ with probability } 1+a-\lceil a\rceil.\end{cases}$$

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

Definition 4. Let $\mathcal{L}=\mathcal{L}(B)$ be an n-dimensional lattice under the canonical embedding. For $c\in H$, the coordinatewise randomized rounding (CRR) discretisation $\lfloor X\rceil^B_{\mathcal{L}+c}$ of random variable X to $\mathcal{L}+c$ is defined by

$$\lfloor X\rceil^B_{\mathcal{L}+c} = X + B\,\mathrm{Red}\left(B^{-1}(c-X)\right).$$

Extend this to H^d by applying the discretisation in each coordinate. The discretisation variable on H is 0-subgaussian:

Definition 5. For any $\delta\ge 0$, a multivariate random variable $\boldsymbol{X}$ on $\mathbb{R}^n$ (resp. H) is δ-subgaussian with standard parameter $b\ge 0$ if

$$E\left(e^{\langle \boldsymbol{t},X\rangle}\right)\le e^{\delta}e^{\frac{1}{2}b^2\|\boldsymbol{t}\|^2},\quad \text{for all } \boldsymbol{t}\in\mathbb{R}^n \text{ (resp. } \boldsymbol{t}\in H).$$

Extend this to H^d by saying a multivariate random variable $\boldsymbol{Z}$ on H^d is δ-subgaussian with standard parameter $b\ge 0$ if $\boldsymbol{Z}$ is δ-subgaussian with standard parameter $b\ge 0$ in each H-coordinate ($H^d\cong\mathbb{R}^{nd^2}$ as $\mathbb{R}$-vector spaces). Formally,

Definition 6. A multivariate random variable $\boldsymbol{Z}$ on H^d is δ-subgaussian with standard parameter $b \geq 0$ if

$$E\left(e^{\langle \boldsymbol{t}, Z \rangle}\right) \leq e^{\delta} e^{\frac{1}{2} b^2 \|\boldsymbol{t}\|^2}, \quad \text{for all } \boldsymbol{t} \in H^d$$

Definition 7. A random variable $\boldsymbol{Z}$ on $\mathbb{R}^n$ (or H) is noncentral subgaussian with noncentrality $\|E(\boldsymbol{Z})\| \geq 0$ and deviation $d \geq 0$ if the centered random variable $\boldsymbol{Z}_0 = \boldsymbol{Z} - E(\boldsymbol{Z})$ is 0-subgaussian with standard parameter d.

We will need the following lemmas:

Lemma 7. *[38] Suppose that B is a column basis matrix for a lattice in H with largest singular value $s_1(B)$ and $\boldsymbol{Z}$ is an independent noncentral subgaussian random variable with deviation d_Z. The CRR discretisation of $\boldsymbol{Z}$, $\lfloor \boldsymbol{Z} \rceil^B_{\Lambda+c}$ is noncentral subgaussian with noncentrality $\|E(\boldsymbol{Z})\|$ and deviation $\left(d_{\boldsymbol{Z}}^2 + \left(\frac{1}{2}\right)^2 s_1(B)^2\right)^{\frac{1}{2}}$.*

When $L = \mathbb{Q}(\zeta_n, \sqrt{\ell})$ for n a power of two, $\gcd(n, \ell) = 1$, this becomes

Lemma 8. *Suppose that B is a column basis matrix for a lattice in H^d with largest singular value $s_1(B)$ and $\boldsymbol{Z}$ is an independent noncentral subgaussian random variable with deviation d_Z. The CRR discretisation of $\boldsymbol{Z}$ to $\lfloor \boldsymbol{Z} \rceil^B_{\Lambda+c}$ is noncentral subgaussian with noncentrality $\|E(\boldsymbol{Z})\|$ and deviation $\left(d_{\boldsymbol{Z}}^2 + \frac{1}{2} s_1(B)^2\right)^{\frac{1}{2}}$.*

Proof. As in [38, Theorem 2], but with an extra factor of $\sqrt{2}$ from taking the matrix norm of the basis. □

3 NTRU

We begin by defining the problem underlying schemes based on NTRU.

The NTRU Assumption

Definition 8. (NTRU instances) Let $\mathcal{R}$ be a ring and $q \in \mathbb{Z}_{\geq 2}$ a modulus. An instance of NTRU is an element $h \in \mathcal{R}_q$ such that $h \cdot f = g \bmod q\mathcal{R}$ for some pair of non-zero elements $(f, g) \in \mathcal{R}$.

We are interested in the following problem, based off NTRU instances:

Definition 9. (The NTRU problem) Let $\mathcal{R}$ and q be as above, and $\epsilon > 0$. Let $\mathcal{D}$ be a distribution over instances of NTRU. The NTRU problem is, given $h \leftarrow \mathcal{D}$, to find non-zero (f, g) such that $h \cdot f = g \bmod q\mathcal{R}$ and $\|f\|, \|g\| \leq \frac{\sqrt{q}}{\epsilon}$.

The hardness of the NTRU problem varies significantly, depending on ϵ.

Connection to Lattices The solutions over $\mathcal{R}$ to the defining equation $hf \equiv g \bmod q$ form a lattice, denoted

$$\mathcal{L}_{h,q} = \{(x, y) \in \mathcal{R}^2 : hx - y \equiv 0 \bmod q\}.$$

The sum of two solutions to the defining equation is again a solution, and one can also observe that for any $z \in \mathcal{R}$ and $(f, g) \in \mathcal{L}_{h,q}$, $z(f, g)$ satisfies $zhf - zg \equiv z(hf - g) \equiv 0 \bmod q$. Thus $\mathcal{L}_{h,q}$ is a $\mathcal{R}$-module of rank 2, and the NTRU problem can be rephrased as a shortest vector problem in the NTRU lattice $\mathcal{L}_{h,q}$.

Encryption Scheme The NTRU encryption scheme, as in [24], runs as follows:

KeyGen: Let $\mathcal{S}_f$, $\mathcal{S}_g$, $\mathcal{S}_\phi$, and $\mathcal{S}_M$ be sets of polynomials in $\mathcal{R} = \mathbb{Z}[x]/(t(x))$ for some degree-N polynomial $t(x)$. Let $q \gg p \in \mathbb{Z}$ be coprime. Select f from $\mathcal{S}_f$ and g from $\mathcal{S}_g$, such that f is invertible modulo both q and p. Compute $h = g \cdot f^{-1} \bmod q$; this polynomial h is the public key, and (f, g) the private key.
Encryption: Suppose the message is M, taken from $\mathcal{S}_M$. Then to encrypt M, select ϕ from $\mathcal{S}_\phi$ and compute $c = p\phi \cdot h + M \bmod q$. This is the ciphertext.
Decryption: To decrypt c, first compute $a = f \cdot c \bmod q$. Then compute $f^{-1} \cdot a \bmod p$, to recover $M \bmod p$. This decryption holds provided the coefficients of a lie in the correct interval. Otherwise, there is a small chance of *decryption failure*. Parameters can be chosen to eliminate the chance of decryption failure.
Correctness: Observe that

$$a = f \cdot c \bmod q = f \cdot (p\phi \cdot h + M) \bmod q = p\phi \cdot g + f \cdot M \bmod q,$$

so that finally $f^{-1} \cdot a \bmod p = f^{-1} \cdot (p\phi g + f \cdot M) \bmod p = f^{-1} \cdot (fM) \bmod p = M \bmod p$, provided that when we reduce a modulo q (taking the coefficients between $\frac{-q}{2}$ and $\frac{q}{2}$), we obtain simply the polynomial a.

Further Discussion of NTRU There are a variety of parameter choices currently used to instantiate NTRU. In the paper initially proposing the NTRU problem [24], the ring $\mathcal{R} = \mathbb{Z}[x]/\left(x^N - 1\right)$ was used, with N prime (and the authors recommended using Sophie Germain primes). Of the two final round NTRU-based schemes in NIST's post-quantum standardization process, NTRU [13] samples f and g from $\mathbb{Z}[x]/(t(x))$ with $t(x) = \Phi_n(x)$, where n is prime and $\Phi_n(x)$ is the nth cyclotomic polynomial. This is contrasted by NTRU Prime [9], which uses $t(x) = x^p - x - 1$ for some prime p (not to be confused with the modulus of the previous section), such that $\mathbb{Z}_q[x]/(x^p - x - 1)$ is a field.

We also note here that f and g are often chosen to be binary or ternary polynomials (i.e. coefficients are in $\{0, 1\}$, $\{-1, 0, 1\}$ respectively), which increases efficiency, but which has been subjected to meet-in-the-middle attacks [25].

Structured Forms of NTRU Two papers have proposed structured forms of NTRU using modules [15], [16]. The authors construct NTRU modules of the

following form, where $\mathcal{R} = \mathcal{O}_K$ for a number field K:

$$\mathcal{L}_{\mathbf{h},q} = \{(\mathbf{f}, g)^T \in \mathcal{R}^{d+1} : \langle \mathbf{f}, \mathbf{h} \rangle - g \equiv 0 \bmod q\}.$$

Here g is a ring element and $\mathbf{f}$ is an d-dimensional vector over $\mathcal{R}$, and embedding the lattice (via either coefficients or ring embeddings) yields lattices in $\mathbb{R}^{(d+1)n}$, where $\dim_{\mathbb{Z}}(\mathcal{R}) = n$. Multiple samples can be taken and written in the following form, where we have chosen d samples to obtain square matrices for convenience of expression (note squareness of the matrices involved is not required):

$$\mathcal{L}_{\mathbf{h},q} = \{(\mathbf{F}, \mathbf{g})^T \in \mathcal{R}^{d \times (d+1)} : \mathbf{F}\mathbf{h} - \mathbf{g} \equiv \mathbf{0} \bmod q\}.$$

These are more general objects than those considered in this work. However, the authors of [16] are able to prove uniformity of their NTRU public keys only for certain prime moduli, those splitting into two prime ideals in $\mathcal{R}$ (those congruent to 3 modulo 8), which are usually not the primes used in practice - and their recommended parameters are completely split primes and a module rank of 2, over a power-of-two cyclotomic field. They prove:

Theorem 1 (Theorem A.1, [16]). *Let K be a cyclotomic number field of degree d and maximal order R. Let $n \geq m \geq 1$. Let q be a prime integer which factors as $qR = \mathfrak{p}_1\mathfrak{p}_2$, where the $\mathfrak{p}_i$'s have algebraic norm $q^{d/2}$. For $s \geq 2dq^{m/(n+m)+2/(d(n+m))}$, we have:*

$$\Delta\left(\mathcal{E}_s, U\left(R_q^{n \times m}\right)\right) \leq 2^{-\Omega(d)},$$

where $\mathcal{E}_s$ is the distribution of $\mathbf{F}^{-1}\mathbf{G} \bmod q$, for $\mathbf{F}$, $\mathbf{G}$ with entries chosen according to discrete Gaussians.

In contrast, restricting ourselves to more structured modules, we obtain a full proof of uniformity of our public keys, for completely split primes in rank 2. Our modules are obtained from *cyclic division algebras*.

4 Cyclic Division Algebras

In this section we define the cyclic algebras we will use to generalise NTRU.

Definition 10. Let $K/\mathbb{Q}$ be a number field of degree n, and L/K be a Galois extension of degree d with cyclic Galois group, i.e. $\mathrm{Gal}(L/K) = \langle \theta \rangle$ for some automorphism θ. Consider the direct sum

$$\bigoplus_{i=0}^{d-1} u^i L = L \oplus uL \oplus u^2 L \oplus ... \oplus u^{d-1} L,$$

subject to the relations $u^d = \gamma \in \mathcal{O}_K$, and $x \cdot u = u \cdot \theta(x)$, for all $x \in L$.

We denote this direct sum $\mathcal{A} = (L/K, \theta, \gamma)$, which is a *cyclic algebra*.

Definition 11. A cyclic algebra $\mathcal{A} = (L/K, \theta, \gamma)$ is a *division algebra* if for every element $a \in \mathcal{A}$, there exists an inverse element $a^{-1} \in \mathcal{A}$ such that $a \cdot a^{-1} = 1$.

In order to ensure that our algebras are division, we will need to ensure they meet the following condition, known as the *non-norm* condition:

Lemma 9. *[1] Let $\mathcal{A} = (L/K, \theta, \gamma)$ be a CDA. Then $\mathcal{A}$ is a division algebra if and only if γ is a non-norm element, i.e. $\nexists x \in L : N_{L/K}(x) = \gamma$.*

The construction of non-norm elements is therefore crucial in finding division algebras. In [21], much discussion was given to finding such elements - we recap this below, after the following definitions.

In NTRU, polynomials are often sampled from subrings of fields. We now define the corresponding mathematical object within cyclic algebras from which it is suitable to sample elements.

Definition 12. A $\mathbb{Z}$-*order*, $\mathcal{O}$, in $\mathcal{A} = (L/K, \theta, \gamma)$ is a finitely generated $\mathbb{Z}$-module such that $\mathcal{O} \cdot \mathbb{Q} = \mathcal{A}$ and $\mathcal{O}$ is a subring of $\mathcal{A}$ with the same identity element as $\mathcal{A}$. Note $\mathcal{O} \cdot \mathbb{Q} = \{\sum_{i=1}^{m} a_i q_i : a_i \in \mathcal{O}, q_i \in \mathbb{Q}, m \in \mathrm{Z}_{\geq 1}\}$.

Definition 13. Define the *natural order* to be the order of the form

$$\Lambda = \bigoplus_{i=0}^{d-1} u^i \mathcal{O}_L = \mathcal{O}_L \oplus u\mathcal{O}_L \oplus u^2\mathcal{O}_L \oplus ... \oplus u^{d-1}\mathcal{O}_L,$$

where $\mathcal{O}_L$ denotes the ring of integers of L.

Given a prime $q \in \mathbb{Z}$, we can take the quotient of Λ to obtain

$$\begin{aligned}\Lambda_q = \Lambda/q\Lambda &= \bigoplus_{i=0}^{d-1} u^i\big(\mathcal{O}_L/q\mathcal{O}_L\big) \\ &= \mathcal{O}_L/q\mathcal{O}_L \oplus u\big(\mathcal{O}_L/q\mathcal{O}_L\big) \oplus u^2\big(\mathcal{O}_L/q\mathcal{O}_L\big) \oplus ... \oplus u^{d-1}\big(\mathcal{O}_L/q\mathcal{O}_L\big).\end{aligned}$$

When $R = \mathbb{Z}[x]/\Phi_n(x)$, R is the ring of integers of the nth cyclotomic field, say L; then $R_q = \mathcal{O}_L/q\mathcal{O}_L$. So Λ_q can be seen as a tuple of elements of R_q, equipped with a noncommutative multiplication induced by multiplication by u.

Fixing the L-basis of $\mathcal{A}$, $\{u^i\}_{i\geq 0}$, we can express an element as the linear map $\phi(x)$ given by left multiplication on the u^i. For example, if $x = \oplus_{i=0}^{d-1} u^i x_i \in \mathcal{A}$,

$$\phi(x) = \begin{pmatrix} x_0 & \gamma\theta(x_{d-1}) & \dots & \gamma\theta^{d-1}(x_1) \\ x_1 & \theta(x_0) & \dots & \gamma\theta^{d-1}(x_2) \\ \dots & \dots & \dots & \dots \\ x_{d-1} & \theta(x_{d-2}) & \dots & \theta^{d-1}(x_0) \end{pmatrix}.$$

This is called the left regular representation.

If we denote the n embeddings $K \hookrightarrow \mathbb{C}$ by α, we can extend these to embeddings of L (which, in an abuse of notation, we also denote by α). It can be seen that all the nd embeddings of L are obtained from the set $\{\alpha \circ \theta^i\}_{\alpha,i}$. So we may form a vector in $\mathbb{R}^{nd^2}$ from x by concatenating the vectorized images of the $\alpha(\phi(x))$ for all $\alpha \in \mathrm{Emb}(K)$. Then the image of any discrete additive subgroup

of $\mathcal{A}$ is mapped to a lattice in $\mathbb{R}^{nd^2}$. Finally, we define two norms on $\mathcal{A}$: we set $\|x\|_p^p = \sum_{\alpha \in \mathrm{Emb}(K)} \sum_{i,j} |\alpha(\phi(x)_{i,j})|^p$, and $\|x\|_\infty = \max_{\alpha,i,j} |\alpha(\phi(x)_{i,j})|$, where $\phi(x)_{i,j}$ denotes the i,jth entry of $\phi(x)$. We may use $\|\cdot\|$ to denote $\|\cdot\|_2$.

Let $\mathrm{Tr}(\cdot)$ be the map $\mathrm{Tr}(x) = T_{K/\mathbb{Q}} \circ \mathrm{trace}(\phi(x))$, for $x \in \mathcal{A}$. This map is symmetric and additive. The dual of an ideal $\mathcal{I}$ is the set

$$\mathcal{I}^\vee = \{x \in \mathcal{A} : \mathrm{Tr}(x\mathcal{I}) \subset \mathbb{Z}\}.$$

We also define a multiplicative norm on ideals. Let $\mathcal{I}$ be an integral ideal of a maximal order $\mathcal{O}$; then $N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) := |\mathcal{O}/\mathcal{I}|$.

We now outline the construction of CDAs using cyclotomic fields as in [21]. Let $m = p^r$ be a prime power, $K = \mathbb{Q}(\zeta_m)$ and $M = \mathbb{Q}(\zeta_{\ell m})$, for a prime ℓ such that $\ell \equiv 1 \bmod m$ and $\ell \not\equiv 1 \bmod pm$. Then M/K is cyclic Galois, with Galois group generated by (say) θ. Let L be the intermediate field fixed by θ^d. It can be verified that ζ_m is not the norm of any element of L, so $(L/K, \theta, \zeta_m)$ is a division algebra. Moreover, Λ is maximal with respect to inclusion in $\mathcal{A}$. Security reductions for LWE in these algebras were given; here we investigate the properties of NTRU implemented in such an algebra.

In the case $d = 2$, L is the compositum of K and the unique quadratic subfield of $\mathbb{Q}(\zeta_\ell)$, which is $\mathbb{Q}(\sqrt{\ell})$. Thus $L = \mathbb{Q}(\zeta_m, \sqrt{\ell})$ and $\Lambda = \mathcal{O}_L + u\mathcal{O}_L$. We now prove an upper bound on the discriminant of Λ:

Definition 14. $\mathrm{disc}(\Lambda/\mathbb{Z}) := \left\{ \det\left(\mathrm{Tr}\left(x_i x_j\right)\right)_{i,j=1}^{nd^2} \mid (x_1, \ldots, x_{nd^2}) \in \Lambda^{nd^2} \right\}$.

It was proved in [55, Lemma 2.9] that $\mathrm{disc}\left(\Lambda/\mathcal{O}_K\right) = \mathrm{disc}(L/K)^d \gamma^{d(d-1)}$. Since in our case γ is a root of unity, this simplifies to $\mathrm{disc}\left(\Lambda/\mathcal{O}_K\right) = \mathrm{disc}(L/K)^d$.

Proposition 2. *Let $L = \mathbb{Q}(\zeta_{2^r}, \sqrt{\ell})$, $r \geq 2$, $\ell \equiv 1 \bmod 2^r$, and $K = \mathbb{Q}(\zeta_{2^r})$. Then*

$$\mathrm{disc}(\Lambda/\mathbb{Z}) \leq (n\sqrt{l})^{4n}.$$

Proof. Since $u^i\mathcal{O}_L$ and $u^j\mathcal{O}_L$ are orthogonal with respect to the trace form, except when $i + j \equiv 0 \bmod 2$, we have

$$\begin{aligned}\det\left(\mathrm{Tr}\left(u x_k u x_\ell\right)\right)_{k,\ell=1}^{2n} &= \det\left(u^2 \mathrm{Tr}\left(x_k x_\ell\right)\right)_{k,\ell=1}^{2n} = \gamma^{nd} \det\left(\mathrm{Tr}\left(x_k x_\ell\right)\right)_{k,\ell=1}^{2n} \\ &= \det\left(\mathrm{Tr}\left(x_k x_\ell\right)\right)_{k,\ell=1}^{2n} = \mathrm{disc}(L/\mathbb{Q}),\end{aligned}$$

for some $x_i \in \mathcal{O}_L$, since $\gamma = \zeta_n$.

It now suffices to prove that $\mathrm{disc}(L/\mathbb{Q}) \leq (n\sqrt{\ell})^{2n}$. Since L is the compositum of $K = \mathbb{Q}(\zeta_{2^r})$ and $\mathbb{Q}(\sqrt{\ell})$, we can apply a general formula on the discriminants of composita (e.g. [36, ex. 23(c)]) to obtain

$$\mathrm{disc}(L/\mathbb{Q}) = \mathrm{disc}(K/\mathbb{Q})^2 \, \mathrm{disc}(\mathbb{Q}(\sqrt{\ell})/\mathbb{Q})^n.$$

We combine $\mathrm{disc}(K/\mathbb{Q}) \leq n^n$ with $\mathrm{disc}(\mathbb{Q}(\sqrt{\ell})/\mathbb{Q}) = \ell$ for the result. □

Proposition 3. *[8, Proposition 2.5] Let Λ be as above and $\mathcal{I} \subset \Lambda$ be an integral ideal. Then*

$$\mathrm{Vol}(\mathcal{I}) = N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})\sqrt{\mathrm{disc}(\Lambda/\mathbb{Z})}.$$

We will use the following bound on the shortest vector of a Λ-ideal lattice under the canonical embedding, with repect to a p-norm, $\lambda_1^p(\mathcal{L})$:

Proposition 4. *(cf. [45, Lemma 6.1]) Let $\mathcal{I}$ be an ideal of Λ. Then*

$$\lambda_1^p(\mathcal{I}) \leq (nd^2)^{1/p} N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/nd^2}\,\mathrm{disc}(\Lambda/\mathbb{Z})^{1/2nd^2}.$$

Proof. Since $\|x\|_p \leq \left(nd^2\right)^{\frac{1}{p}} \|x\|_\infty$, we bound $\|x\|_\infty$. Recall $\mathcal{A} \hookrightarrow H^d \subset (\mathbb{R}^{r_1} \times \mathbb{C}^{2r_2})^d$, with $r_1 + 2r_2 = nd$. Set $C = \{x \in H^d : \|x\|_\infty \leq 1\}$ and note $Vol(C) = 2^{nd^2}\left(\frac{\pi}{2}\right)^{r_2 d}$. Then if $\beta^{nd^2} > \left(\frac{2}{\pi}\right)^{r_2 d} N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})\sqrt{\mathrm{disc}(\Lambda/\mathbb{Z})}$, we have

$$\begin{aligned}\mathrm{Vol}(\beta C) = \beta^{nd^2}\,\mathrm{Vol}(C) &> \left(\frac{2}{\pi}\right)^{r_2 d} N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})\sqrt{\mathrm{disc}(\Lambda/\mathbb{Z})}2^{nd^2}\left(\frac{\pi}{2}\right)^{r_2 d} \\ &= N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})\sqrt{\mathrm{disc}(\Lambda/\mathbb{Z})}2^{nd^2} = \mathrm{Vol}(\mathcal{I})2^{nd^2}.\end{aligned}$$

By Minkowski's theorem, βC contains a lattice point from $\mathcal{I}$, so $\lambda_1^\infty(\mathcal{I}) \leq \beta$. □

This implies that in the ℓ_2-norm, $\lambda_1(\Lambda) \leq (nd^2)^{1/2}(n\sqrt{\ell})^{1/2} = dn\sqrt[4]{\ell}$.

Proposition 5. *Let $\Lambda \subset \mathcal{A} = (L/K, \theta, \gamma)$ where $|\gamma| = 1$, $[L : K] = d$ and $[K : \mathbb{Q}] = n$. Then, for $x = \oplus_{i=0}^{d-1} u^i x_i \in \Lambda$, $\mathcal{I}$ an ideal of Λ,*

$$\|x\|_p \geq [\mathcal{A} : \mathbb{Q}]^{1/p} \cdot \left(\prod_{0 \leq i < d} |N_{L/\mathbb{Q}}(x_i)|\right)^{1/[\mathcal{A}:\mathbb{Q}]}.$$

When $\mathcal{I} = \mathfrak{J}\Lambda$ for some $\mathcal{O}_K$-ideal $\mathfrak{J}$ and $\bar{\mathcal{I}} := \mathcal{I} \cap \mathcal{O}_L$, then

$$\lambda_1^p(\mathcal{I}) \geq [\mathcal{A} : \mathbb{Q}]^{1/p} \cdot \left|N_{L/\mathbb{Q}}\left(\bar{\mathcal{I}}\right)\right|^{d/[\mathcal{A}:\mathbb{Q}]}, \text{ and } \lambda_1^\infty(\mathcal{I}) \geq \left(N_{L/\mathbb{Q}}(\bar{\mathcal{I}})\right)^{1/nd}.$$

Proof. See Appendix A. □

Mapping Between Bases of $\mathcal{A}$ We will later need to consider mapping between the coefficient embedding of an element and the canonical embedding of the same element, via a linear transformation. Let $d = 2$; then $\mathcal{A}$ embeds into H^2 under the canonical embedding. Now, since $\Lambda = \mathcal{O}_L + u\mathcal{O}_L$, and $\mathcal{O}_L = \mathbb{Z}[\zeta_{2^r}, \frac{1+\sqrt{\ell}}{2}]$, a matrix acting on a vector to map it to a coefficient embedding representation should act on the first and second coordinates $(\sigma_L(\Lambda))_i$, $i = 1, 2$ in the desired way. Thus the required transformation is $V_\Lambda = \begin{pmatrix}\sigma(\overrightarrow{p}) & \mathbf{0} \\ \mathbf{0} & \sigma(\overrightarrow{p})\end{pmatrix}$. Note if $\sigma(\overrightarrow{p})$ is invertible, so is V_Λ. We do similarly

with respect to $\overrightarrow{d}$ and Λ. We can then obtain bounds for norms defined over these bases: for $x \in \Lambda$ with $d = 2$ we obtain

$$\|x\|_{\sigma(\overrightarrow{d})} \leq \sqrt{2} s_1(\overrightarrow{p}) \|x\|.$$

Note that when $d = 1$, $K = L$ and $\mathcal{A} = K$. This is the fact that will enable us to generalise NTRU schemes which sample elements from $\mathbb{Z}[x]/(\Phi_{2^r}(x))$, using algebras of the form $\mathcal{A} = (L/\mathbb{Q}(\zeta_{2^r}), \theta, \zeta_n)$; when $d = 1$, we will recover the familiar families of polynomials in certain spaces, generalising NTRU, ETRU and others. If one uses CDAs over fields K where K is some other popular choice of field for NTRU, one obtains generalisations of those schemes too.

CLWE and its Security Below, we link the hardness of NTRU in CDAs to that of LWE in CDAs. Here we introduce CLWE, and begin by defining a distribution on the error distributions used to establish the hardness of CLWE:

Definition 15. Define the distributions Σ_α as the set of Gaussian distributions Σ over $\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$ with Gaussian marginal distribution in the $(i,j)^{\text{th}}$ coordinate with parameter $r_{i,j} \leq \alpha$. The error distribution Υ_α on the family of error distributions is sampled from by choosing $\Sigma \in \Sigma_\alpha$ and adding it to D_r, where each $r_i := \alpha \left(\left(n \cdot d^2 \right)^{1/4} \cdot \sqrt{y_i} \right)$ for $y_1, \ldots, y_{n \cdot d^2}$ sampled from $\Gamma(2,1)$.

Then the CLWE distribution, and decision CLWE problem, are as follows:

Definition 16. Let L/K be a Galois extension of number fields with $[L : K] = d$ and $[K : \mathbb{Q}] = n$, with $\mathrm{Gal}(L/K)$ cyclic, generated by θ. Let $\mathcal{A} := (L/K, \theta, \gamma)$ be the resulting cyclic K-algebra with element u such that $u^d = \gamma \in \mathcal{O}_K$ and γ satisfying the non-norm condition. Let Λ be the natural order of $\mathcal{A}$. For an error distribution ψ over $\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$, $q \geq 2$, and secret $s \in \Lambda_q^\vee$, a sample from the CLWE distribution $\Pi_{q,s,\psi}$ is obtained by sampling $a \leftarrow \Lambda_q$ uniformly at random, $e \leftarrow \psi$, and outputting $(a, b) = (a, (a \cdot s)/q + e \bmod \Lambda^\vee) \in \left(\Lambda_q, \bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}} \right) / \Lambda^\vee$.

Let Υ be as above and U_Λ the uniform distribution on $\left(\Lambda_q, \left(\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}} \right) / \Lambda^\vee \right)$. Then the decision CLWE problem, $\mathrm{DCLWE}_{q,\Upsilon}$, is on input a collection of independent samples from $\Pi_{q,s,\psi}$ for a random choice of $(s, \psi) \leftarrow U\left(\Lambda_q^\vee\right) \times \Upsilon$ or from U_Λ, to decide which is the case (with non-negligible advantage).

Recall the following security reductions for CLWE, from [21]:

Theorem 2. *Let $\mathcal{A}$ be a cyclic division algebra over a number field L with center K and natural, maximal order Λ with $|\gamma| = 1$. Let $\alpha = \alpha(n) \in (0,1)$ and $q = q(n) \geq 2$, unramified in L, be parameters such that $\alpha \cdot q \geq \omega(\sqrt{\log(nd^2)})$. Then, there is a polynomial-time quantum reduction from $\mathcal{A}$-$SIVP_\xi$ to search $CLWE_{q,\Sigma_\alpha}$ for any $\sqrt{8Nd} \cdot \xi = (\omega(\sqrt{dn})/\alpha)$.*

Theorem 3. *Let Λ be the natural order of a cyclic algebra $\mathcal{A} = (L/K, \theta, \gamma), q \in \mathrm{poly}(n)$, and assume that $\alpha \cdot q \geq \eta_\varepsilon(\Lambda^\vee)$ for a negligible $\varepsilon = \varepsilon(n)$. Then, there is a probabilistic reduction from search $CLWE_{q,\Sigma_\alpha,G}$ for any pairwise different $G \subset \Lambda_q^\vee$ to decision $CLWE_q, \Upsilon_\alpha$ which runs in time polynomial in n.*

These reductions combine to ground the security of decision CLWE on SIVP over ideal lattices in CDAs. Thus if we connect the security of NTRU to that of CLWE, we will have connected the security of NTRU to SIVP. However, we require a particular variant of CLWE to which to reduce NTRU. Here we recall the variant of RLWE used in [48]. Let $s \in R_q$ and ψ be a distribution over R_q. Define $A_s^\times$ as the distribution obtained by sampling $(a, as + e)$ with $(a, e) \leftarrow U(R_q^\times) \times \psi$, where $R_q^\times$ is the set of invertible elements of R_q. When $q = \Omega(n)$, the probability of a uniform element of R_q being invertible is non-negligible, so RLWE is hard even when $A_{s,\psi}$ and $U(R_q \times R_q)$ are replaced by $A^\times_{s,\psi}$ and $U(R_q^\times \times R_q)$ respectively. Denote this variant by RLWE$^\times$.

It is known that s can be chosen from the same distribution as e without losing security (see [3]). The authors of [48] call the variant of RLWE when the secret and error are both chosen from the error distribution $\text{RLWE}^\times_{\text{HNF}}$. To see this, let algorithm $\mathcal{A}$ be able to solve $\text{RLWE}^\times_{\text{HNF}}$. One can transform samples $((a_i, b_i))_i$ into samples $\left(\left(a_1^{-1}a_i, b_i - a_1^{-1}b_1a_i\right)\right)_i$, where inversion is performed in $R_q^\times$. This transformation maps $A^\times_{s,\psi}$ to $A^\times_{-e_1,\psi}$, and $U\left(R_q^\times \times R_q\right)$ to itself. Note that $b_i - a_1^{-1}b_1a_i = a_is + e_i - a_1^{-1}(a_1s + e_1)a_i = a_is + e_i - a_is - a_1^{-1}e_1a_i = -a_1^{-1}a_ie_1 + e_i$.

We can define CLWE$^\times$ analogously: let $s \in \Lambda_q$, $e \leftarrow \chi$, and $a \leftarrow U(\Lambda_q^\times)$. Output $(a, as + e) \in \Lambda_q^\times \times \oplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$, and call the distribution obtained $A^\times_{q,s,\chi}$. We can take s from the same distribution as the error to obtain $\text{CLWE}^\times_{HNF}$; to see the transformation as in the RLWE case, transform CLWE$^\times$ samples into $\text{CLWE}^\times_{HNF}$ samples via the transformation $(a_i, b_i) \mapsto (a_ia_1^{-1}, b_i - a_ia_1^{-1}b_1)$.

5 NTRU in CDAs

In the following, we follow the method outlined in [24] to implement NTRU in CDAs. After demonstrating that the basic form of NTRU adapts easily to our context, we will go on to discuss the tweaks, improvements, and modifications that have arisen in the literature, and how they can be brought into CDAs. For convenience, we refer to NTRU in a cyclic division algebra as *CNTRU*.

NTRU Instances in CDAs

Definition 17. (CNTRU instances) Let $\mathcal{A} = (L/K, \theta, \gamma)$ be an algebra as constructed above, and Λ the natural order. Let $q \in \mathbb{Z}_{\geq 2}$. An instance of CNTRU is an element $h \in \Lambda_q$ such that $f \cdot h = g \bmod q\Lambda$ for non-zero pair $(f, g) \in \Lambda$.

We define the NTRU problem for CDAs, based off CNTRU instances:

Definition 18. (The CNTRU problem) Let Λ and q be as above, and $\epsilon > 0$. Let $\mathcal{D}$ be a distribution over instances of CNTRU. The CNTRU problem is, given $h \leftarrow \mathcal{D}$, to find non-zero (f, g) such that $f \cdot h = g \bmod q\Lambda$ and $\|f\|, \|g\| \leq \frac{\sqrt{q}}{\epsilon}$.

NTRU Lattices from CDAs We now consider the lattices generated by CNTRU instances. These lattices are a generalization of [16] and [15]'s lattices: take a private key $(f, g) \in \Lambda^2$ and public key $h = f^{-1}g \bmod q\Lambda$. Observe that the pair (f, g) satisfies

$$fh - g = 0 \bmod q\Lambda, \tag{1}$$

so in the same way as NTRU, the set $S = \{(f, g) \in \Lambda^2 : fh - g = 0 \bmod q\Lambda\} \subset \Lambda^2$ is a left Λ-module (i.e. S is additively closed and closed under multiplication from Λ on the left). We note that if we changed our convention and considered

$$\{(f, g) \in \Lambda^2 : hf - g = 0 \bmod q\Lambda\}$$

instead, we could write a generator matrix for this second (right) Λ-module as $\begin{pmatrix} -h & 1 \\ q & 0 \end{pmatrix}$ where the columns generate the module over Λ^2. By fixing a basis $\{u^i\}_i$, we can then rewrite this matrix to obtain one with entries in $\mathcal{O}_L$, $\left(\begin{array}{c|c} -H & I_d \\ \hline qI_d & 0 \end{array}\right)$ where

$$H = \begin{pmatrix} h_0 & \gamma\theta(h_{d-1}) & \gamma\theta^2(h_{d-2}) & \dots & \gamma\theta^{d-1}(h_1) \\ h_1 & \theta(h_0) & \gamma\theta^2(h_{d-1}) & \dots & \gamma\theta^{d-1}(h_2) \\ \dots & \dots & \dots & \dots & \dots \\ h_{d-1} & \theta(h_{d-2}) & \theta^2(h_{d-3}) & \dots & \theta^{d-1}(h_0) \end{pmatrix}.$$

Note that in the module NTRU examples referenced above, the element h defines a vector over a field, so appears in just one column of the corresponding matrix, whereas one sample of CNTRU for $[L : K] = d$ results in $h \bmod q$ defining an NTRU-style matrix with d columns determined by h, as can be seen. This is (loosely) equivalent to d samples of module NTRU.

To make the comparison explicit, recall that module forms of NTRU rely on lattices of the form

$$\mathcal{L}_{\mathbf{h},q} = \{(\mathbf{F}, \mathbf{g}) \in \mathcal{R}^{d\times(d+1)} : \mathbf{Fh} - \mathbf{g} \equiv \mathbf{0} \bmod q\}.$$

In this case, one can see that these $\mathcal{R}$-modules have a similar form to the CNTRU modules defined above as

$$\mathcal{L}_{h,q} = \{(f, g)^T \in \Lambda^2 : fh - g \equiv 0 \bmod q\},$$

when ring multiplication is expanded in matrix-vector form using the regular representation of Λ:

$$\mathcal{L}_{h,q} = \{(\mathbf{f}, \mathbf{g})^T \in \mathcal{O}_L^{2d\times 1} : \phi(f)\mathbf{h} - \mathbf{g} \equiv 0 \bmod q\}.$$

Thus we expect the hardness of NTRU problems in CDAs to lie between that of NTRU over rings and NTRU over modules. Moreover, because of the ring structure of Λ, one could use algorithms such as [11] to follow the analysis of [21] and gain (asymptotic) efficiency over standard forms of module NTRU. Finally, we note that the storage required for a CNTRU private key is much less than the module case (for multiple samples), because of the structure of $\phi(f)$ as compared with that of F, using the above notation. In particular, one only has to store the first column of $\phi(f)$, as opposed to the entire matrix.

NTRU-based PKE To develop encryption based on the CNTRU problem, we proceed as in [24]. Take the following setup: let $\mathcal{A} = (L/K, \theta, \gamma)$ be a CDA, and $\Lambda \subset \mathcal{A}$ the natural order, assumed to be maximal. Let $K = \mathbb{Q}(\zeta_{2^r})$, $[K : \mathbb{Q}] = n$, and $[L : K] = d$. Then $\Lambda = \mathcal{O}_L \oplus u\mathcal{O}_L \oplus ... \oplus u^{d-1}\mathcal{O}_L$. Denote by $\mathcal{S}_f$, $\mathcal{S}_g$, $\mathcal{S}_\phi$, and $\mathcal{S}_M$ sets of elements of Λ. Select $p, q \in \mathbb{Z}$ such that $\gcd(p, q) = 1$ and $p \ll q$.

Key creation: Select f from $\mathcal{S}_f$, and g from $\mathcal{S}_g$. Furthermore, ensure that f has inverses in Λ_q and in Λ_p. Set $(pk, sk) := (h, (f, g))$ where

$$h := f^{-1} \cdot g \bmod q\Lambda.$$

Encryption: Select a message M from $\mathcal{S}_M$ and ϕ from $\mathcal{S}_\phi$. Then use the public key, h, to form the element

$$c := ph \cdot \phi + M \bmod q\Lambda.$$

Decryption: To decrypt c, compute $a := f \cdot c \bmod q\Lambda$, then $f^{-1} \cdot a \bmod p\Lambda$.

Correctness Note that

$$\begin{aligned} a = f \cdot c \bmod q = f \cdot (ph \cdot \phi + M) \bmod q = fph \cdot \phi + f \cdot M \bmod q \\ = pf \cdot (f^{-1} \cdot g) \cdot \phi + f \cdot M \bmod q = pg\phi + f \cdot M \bmod q, \end{aligned}$$

since $f \cdot f^{-1} \equiv 1 \bmod q$. Then

$$\begin{aligned} f^{-1} \cdot a \bmod p = f^{-1}(pg \cdot \phi) + f^{-1}(f \cdot M) = p(f^{-1}g\phi) + (f^{-1} \cdot f) \cdot M \bmod p \\ = (f^{-1} \cdot f) \cdot M \bmod p = M \bmod p. \end{aligned}$$

Remark: This is basically the same as NTRU, but we have to be careful about the order we multiply elements, because of noncommutativity.

Observe that when $d = 1$, we are in the usual set up for NTRU. We could choose the sets $\mathcal{S}_f$, $\mathcal{S}_g$ etc. to be analogous to the ring case, if for example we wanted f and g to be ternary.

Note that the original NTRU scheme doesn't meet the IND-CPA security condition (though [46] gives partial reductions for search and decision NTRU problems). Below we will state an adaptation to the above scheme, and mirror the security guarantee of [48].

6 Results on q-ary Lattices

In this section we prove a regularity lemma on q-ary lattices obtained from the natural order of our family of CDAs.

Uniformity of the NTRU Public Key Distribution We ultimately aim to demonstrate near-uniformity of the CNTRU public key distribution, focusing on the case $d = 2$. Almost all of the argument below holds for arbitrary d, but one step restricts us to $d = 2$; we leave the removal of this restriction as a topic of future research. We prove our result for completely split primes, but note that the proof can be adapted for any prime which is unramified in L.

Let Λ be the natural order of a CDA as above, where $[K : \mathbb{Q}] = n$ and $[L : K] = d$. Let $q \in \mathbb{Z}$ be prime, such that q is unramified in $\mathcal{O}_L$. Then:

Lemma 10. *[43, Proposition 4] Suppose that $\mathcal{I} = \mathfrak{q}$ is a prime in $\mathcal{O}_K$, such that $\mathfrak{q}\mathcal{O}_L = \mathfrak{Q}_1\mathfrak{Q}_2\cdots\mathfrak{Q}_g$ in L, with $\gamma \neq 0 \bmod \mathfrak{q}$. Then the only proper two-sided ideal of Λ containing $\mathcal{I}$ is $\mathcal{I}\Lambda = \oplus_{j=0}^{d-1} u^j \mathfrak{q}\mathcal{O}_L$.*

Since in our case Λ is a maximal order, ideals uniquely factorize into products of prime ideals and prime ideals are maximal. By the above lemma all unramified two-sided ideals of Λ factor into a product of ideals of the form $\mathfrak{q}\Lambda$, where $\mathfrak{q}$ lies in K. Thus any two-sided unramified ideal can be expressed as $\mathcal{I} = \prod_{i\in S} \mathfrak{q}_i\Lambda$, for some indexing set S. In the following, we will consider the ideals lying above $q\Lambda$, where q splits completely L: these have the form $\mathcal{I} = \prod_{i\in S} \mathfrak{q}_i\Lambda$ where $q\mathcal{O}_K = \prod_i^n \mathfrak{q}_i$ and $S \subset \{1, ..., n\}$. We now define the following module lattices:

Definition 19. Let $q \geq 2$ be a prime completely split in $\mathcal{O}_L$. Let $\mathcal{I}$ be an ideal of Λ of the form $\mathcal{I} = \prod_{i\in S} \mathfrak{q}_i\Lambda$ containing $q\Lambda$, and $\mathcal{I}_S$ be an ideal of Λ_q of the form $\mathcal{I}_S = \prod_{i\in S} \mathfrak{q}_i\Lambda/q\Lambda$ for some $S \subset \{1, ..., n\}$. Let $m \geq 2$ and $\boldsymbol{a} = (a_1, ..., a_m) \in \Lambda_q^m$.

$$\boldsymbol{a}^\perp(\mathcal{I}_S) := \{(t_1, ..., t_m) \in \mathcal{I}^m : \sum_i t_i a_i \equiv 0 \bmod q\}, \text{ and}$$

$$L(\boldsymbol{a}, \mathcal{I}_S) := \{(t_1, ..., t_m) \in (\Lambda^\vee)^m : t_i \equiv a_i s \bmod q\mathcal{I}^\vee \text{ for some } s \in \Lambda^\vee, \forall i\}.$$

Lemma 11. *$\boldsymbol{a}^\perp(\mathcal{I}_S) = q(L(\boldsymbol{a}, \mathcal{I}_S))^\vee$, and $L(\boldsymbol{a}, \mathcal{I}_S) = q\left(\boldsymbol{a}^\perp(\mathcal{I}_S)\right)^\vee$.*

Proof. To show $\boldsymbol{a}^\perp(\mathcal{I}_S) \subset q(L(\boldsymbol{a}, \mathcal{I}_S))^\vee$, we show that any $\boldsymbol{t} = (t_1, ..., t_m) \in \boldsymbol{a}^\perp(\mathcal{I}_S)$ has $Tr(\boldsymbol{t} \cdot \boldsymbol{z}) \equiv 0 \bmod q$ for any $\boldsymbol{z} \in L(\boldsymbol{a}, \mathcal{I}_S))^\vee$. Write $z_i = a_i s + qz_i'$, for $s \in \Lambda^\vee$ and $z_i' \in \mathcal{I}^\vee$. Then $Tr(\boldsymbol{t} \cdot \boldsymbol{z}) = Tr(\sum_i t_i z_i) = \sum_i Tr(t_i z_i) = \sum_i Tr(t_i a_i s) + Tr(q \cdot t_i z_i') = Tr(\sum_i (t_i a_i)s) + qTr(t_i z_i') \in q\mathbb{Z}$.

To show the reverse containment, let $x \in L(\boldsymbol{a}, \mathcal{I}_S))^\vee$. We show $\sum_i qx_i a_i \equiv 0 \bmod q$ and $qx_i \in \mathcal{I}$. Note $q \cdot (\mathcal{I}^\vee)^m \in L(\boldsymbol{a}, \mathcal{I}_S))^\vee$. Set v_i to be an element of $L(\boldsymbol{a}, \mathcal{I}_S))^\vee$ with zeroes everywhere except for the ith entry, which is qs' for $s' \in \mathcal{I}^\vee$. Then $Tr(x \cdot v_i) = Tr(q \cdot x_i s') \in \mathbb{Z}$, so $qx_i \in \mathcal{I}$. Moreover, for all $\boldsymbol{t} \in L(\boldsymbol{a}, \mathcal{I}_S))$, we have $Tr(\boldsymbol{x} \cdot \boldsymbol{t}) \in \mathbb{Z}$. Writing $t_i = a_i s + qt_i'$ where $t_i' \in \mathcal{I}^\vee$, we obtain $Tr(\boldsymbol{x} \cdot \boldsymbol{t}) = \sum_i Tr(x_i a_i s + qx_i t_i') = Tr((\sum_i x_i a_i)s) + \sum_i Tr(qx_i t_i') \in \mathbb{Z}$, and hence we have $Tr((\sum_i x_i a_i)s) \in \mathbb{Z}$. So $\sum_i x_i a_i \in \Lambda$, as required. □

We now lower bound the shortest vector in $L(\boldsymbol{a}, \mathcal{I}_S))$, probabilistically. Recall the construction of our algebras: $K = \mathbb{Q}(\zeta_{2^r})$ with $[K : \mathbb{Q}] = n$, $M = \mathbb{Q}(\zeta_{2^r \cdot \ell})$ for a prime ℓ congruent to 1 mod 2^r, and L is intermediate of degree 2 over K.

Lemma 12. *Let $S \subset \{1, ..., n\}$, $m \geq 2$, $d = 2$, and $\epsilon > 0$. Then $\lambda_1^\infty(L(\boldsymbol{a}, \mathcal{I}_S))) \geq B := q^\beta/(n\sqrt{\ell})$, where $\beta = (1 - \frac{|S|}{n})(\frac{3}{4} - \frac{1}{m}) - \epsilon$, except with probability at most $2^{(1+10m)n} q^{-4mn\epsilon}$, where $\boldsymbol{a} \leftarrow U(\Lambda_q^\times)^m$.*

Proof. Set $P = Pr_{\boldsymbol{a} \leftarrow U((\Lambda_q^\times))^m}\left[L(\boldsymbol{a}, \mathcal{I}_S) \text{ contains } \boldsymbol{t} \neq \boldsymbol{0} : \|\boldsymbol{t}\|_\infty < q^\beta/nd\right]$. To bound this, consider $P(\boldsymbol{t}, s) := Pr_{\boldsymbol{a} \leftarrow U((\Lambda_q^\times)^m)}[t_i \equiv a_i s \bmod q\mathcal{I}^\vee, \forall i]$. This, because $\boldsymbol{t} \in (\Lambda^\vee)^m$ lies in $L(\boldsymbol{a}, \mathcal{I}_S)$ iff $t_i \equiv a_i s \bmod q\mathcal{I}^\vee$ for some $s \in \Lambda^\vee$. Since the a_i are sampled independently, we can rewrite this as $P(\boldsymbol{t}, s) = \prod_i^m P_i(t_i, s)$, where $P_i(t_i, s) := Pr_{a_i \leftarrow U(\Lambda_q^\times)}[t_i \equiv a_i s \bmod q\mathcal{I}^\vee]$. So we obtain

$$P \leq \sum_{\substack{\boldsymbol{t} \in (\mathcal{I}^\vee)^m : \\ 0 < \|t_i\|_\infty < B \ \forall i}} \sum_{s \in \Lambda^\vee / q\mathcal{I}^\vee} \prod_i^m P_i(t_i, s).$$

Now, since $\mathcal{I} = \prod_{i \in S} \mathfrak{q}_i \Lambda$, we have $\mathcal{I}^{-1} = \prod_{i \in S} \mathfrak{q}_i^{-1} \Lambda$, and $q\mathcal{I}^\vee = q\mathcal{I}^{-1}\Lambda^\vee = (\prod_{i=1}^n \mathfrak{q}_i \Lambda)(\prod_{i \in S} \mathfrak{q}_i^{-1}\Lambda)\Lambda^\vee = \prod_{i \in S'} \mathfrak{q}_i \Lambda^\vee$, where $S' = \{1, ..., n\} \setminus S$. By the CRT $\mathcal{I}^\vee/q\mathcal{I}^\vee \cong \mathcal{I}^\vee/\mathfrak{q}_{i_1}\Lambda^\vee \times ... \times \mathcal{I}^\vee/\mathfrak{q}_{i_{|S'|}}\Lambda^\vee$, for a subsequence $i_j \in S'$, $j = 1, ..., |S'|$.

We claim that if $P_i(t_i, s) \neq 0$ there exists a subset $S'' \subset S'$ such that t_i and $s \in \prod_{i \in S''} \mathfrak{q}_i \Lambda^\vee$ *and* $t_i, s \notin \mathfrak{q}_j \Lambda^\vee$ for any $j \in S' \setminus S''$. If this weren't the case, there would exist $j \in S'$ such that $s \equiv 0 \bmod \mathfrak{q}_j\Lambda^\vee$ and $t \not\equiv 0 \bmod \mathfrak{q}_j\Lambda^\vee$, or vice versa. But in either scenario $P_i(t_i, s) = 0$, because $a_i \in \Lambda_q^\times$. So such a S'' exists.

If $j \in S''$, $t_i \equiv a_i s \equiv 0 \bmod \mathfrak{q}_j\Lambda^\vee$ for all $a_i \in \Lambda_q^\times$. Alternatively, if $j \in S' \setminus S''$, $t_i \equiv a_i s \not\equiv 0 \bmod \mathfrak{q}_j\Lambda^\vee$, so there is a unique such $a_i \in \Lambda_q^\times$ satisfying the equation. Finally, for $j \in S$, there is no constraint on the a_i. So for a fixed set size $|S''| = d'$, the number of possible $a_i \in \Lambda_q^\times$ satisfying $t_i \equiv a_i s \bmod q\mathcal{I}^\vee$ is

$$\left(\prod_{i=0}^{d-1}(q^d - q^i)\right)^{n-(|S'|-|S''|)} = \left(\prod_{i=0}^{d-1}(q^d - q^i)\right)^{n+d'-|S'|},$$

and so

$$P_i(t_i, s) = \left(\prod_{i=0}^{d-1}(q^d - q^i)\right)^{n+d'-|S'|} / \left(\prod_{i=0}^{d-1}(q^d - q^i)\right)^{n} = \left(\prod_{i=0}^{d-1}(q^d - q^i)\right)^{d'-|S'|},$$

since $\Lambda/\mathfrak{q}_i\Lambda \cong M_d(\mathbb{F}_q)$, so $\Lambda_q \cong \prod_{i=1}^n M_d(\mathbb{F}_q)$ and $|\Lambda_q^\times| = \prod_{i=1}^n |Gl_d(\mathbb{F}_q)|$.

We can now rewrite P as follows, where $\mathfrak{h} = \prod_{i \in S''} \mathfrak{q}_i \Lambda^\vee$:

$$P \leq \sum_{0 \leq d' \leq |S'|} \sum_{\substack{S'' \subset S' \\ |S''| = d'}} \sum_{\substack{\boldsymbol{t} \in (\mathcal{I}^\vee)^m : t_i \in \mathfrak{h} \\ 0 < \|t_i\|_\infty < B \ \forall i}} \sum_{s \in \Lambda^\vee / q\mathcal{I}^\vee \cap \mathfrak{h}} \prod_i^m \left(\prod_{i=0}^{d-1}(q^d - q^i)\right)^{d'-|S'|}.$$

The rest of the analysis divides into two cases, depending on the size of d'. In the first case, we consider $d' \geq \beta n$. Define $N(B, d') := \#\{t \in \mathcal{I}^\vee : \|t\|_\infty < B \text{ and } t \in$

$\mathfrak{h}\}$. Observe that $\|t\|_\infty = \max_{\alpha,i,j} |\alpha((\phi(t))_{i,j})| \geq \lambda_1^\infty(\mathfrak{h}) \geq N_{L/\mathbb{Q}}(\bar{\mathfrak{h}})^{1/nd}$, because $t \in \mathfrak{h}$, where $\bar{\mathfrak{h}} = \mathfrak{h} \cap L$. Observe that $\bar{\mathfrak{h}} = \prod_{i\in S''} \mathfrak{q}_i \Lambda^\vee \cap L = \prod_{i\in S''} \mathfrak{q}_i \mathcal{O}_L^\vee$, so

$$N_{L/\mathbb{Q}}(\bar{\mathfrak{h}})^{1/nd} = N_{L/\mathbb{Q}}(\prod_{i\in S''} \mathfrak{q}_i \mathcal{O}_L^\vee)^{1/nd} = N_{L/\mathbb{Q}}(\prod_{i\in S''} \mathfrak{q}_i \mathcal{O}_L)^{1/nd} N_{L/\mathbb{Q}}(\mathcal{O}_L^\vee)^{1/nd}$$
$$\geq \frac{q^{\frac{dd'}{nd}}}{n\sqrt{\ell}} = \frac{q^{\frac{d'}{n}}}{n\sqrt{\ell}} \geq \frac{q^\beta}{n\sqrt{\ell}} = B,$$

where we used $N_{L/\mathbb{Q}}(\mathcal{O}_L^\vee) = \mathrm{disc}(L)^{-1}$, and the bound $\mathrm{disc}(L) \leq (n^2\ell)^n$ (this bound holds for $d = 2$). Thus $N(B, d') = 0$ if $d' \geq \beta n$.

The second case is $d' < \beta n$. Set $\mathfrak{B}(l, \boldsymbol{c}) = \{\boldsymbol{x} \in H^d : \|\boldsymbol{x} - \boldsymbol{c}\|_\infty < l\}$. One can interpret $N(B, d')$ as the number of points of $\sigma_{\mathcal{A}}(\mathfrak{h})$ in $\mathfrak{B}(B, \mathbf{0})$. Set $\lambda := \lambda_1^\infty(\mathfrak{h})/2$. So $\mathfrak{B}(\lambda, \boldsymbol{v}_2) \cap \mathfrak{B}(\lambda, \boldsymbol{v}_2) = \emptyset$ for any distinct $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathfrak{h}$. Moreover, if $\boldsymbol{v} \in \mathfrak{B}(B, \mathbf{0})$, it holds that $\mathfrak{B}(\lambda, \boldsymbol{v}) \subseteq \mathfrak{B}(B + \lambda, \mathbf{0})$. We can then say that

$$N(B, d') \leq \frac{Vol(\mathfrak{B}(B + \lambda, \mathbf{0}))}{Vol(\mathfrak{B}(B, \lambda, \mathbf{0}))} = \frac{(2(\lambda + B))^{nd^2}}{2\lambda^{nd^2}} = (\frac{B}{\lambda} + 1)^{nd^2}$$
$$\leq \left(\left(\frac{q^\beta}{n\sqrt{s}}\right) / \left(\frac{\lambda_1^\infty(\mathfrak{h})}{2}\right) + 1\right)^{nd^2} \leq (2q^{\beta - \frac{d'}{n}} + 1)^{nd^2} \leq 2^{2nd^2} q^{nd^2\beta - d'd^2}.$$

As we have $\mathfrak{h}/q\mathcal{I}^\vee = \prod_{i\in S''} \mathfrak{q}_i \Lambda^\vee / \prod_{i\in S'} \mathfrak{q}_i \Lambda^\vee \cong \prod_{i\in S''} \mathfrak{q}_i \Lambda / \prod_{i\in S'} \mathfrak{q}_i \Lambda$ $\cong \Lambda / \prod_{i\in S'\setminus S''} \mathfrak{q}_i \Lambda$, then $|\mathfrak{h}/q\mathcal{I}^\vee| = |\Lambda / \prod_{i\in S'\setminus S''} \mathfrak{q}_i \Lambda| = \prod_{i=1}^{|S'\setminus S''|} |M_d(\mathbb{F}_q)| = q^{d^2(|S'| - d')}$. Then

$$P \leq \sum_{0\leq d'\leq \beta n} \sum_{\substack{S''\subset S' \\ |S''| = d'}} \sum_{\substack{\boldsymbol{t}\in (\mathcal{I}^\vee)^m : t_i \in \mathfrak{h} \\ 0 < \|t_i\|_\infty < B\ \forall i}} \sum_{s\in \Lambda^\vee/q\mathcal{I}^\vee \cap \mathfrak{h}} \prod_i^m \left(\prod_{i=0}^{d-1} (q^d - q^i)\right)^{d' - |S'|}$$
$$\leq \max_{d'<\beta n} \frac{q^{d^2(|S'|-d')} N(B, d')^m 2^{|S'|}}{(\prod_{i=0}^{d-1}(q^d - q^i))^{m(|S|-d')}} \leq 2^{n(1+dm+2d^2m)} q^{-d^2nm\epsilon},$$

for $\epsilon = (1 - \frac{|S|}{n})(\frac{d+1}{2d} - \frac{1}{m}) - \beta$, using $|Gl_d(\mathbb{F}_q)| > q^{\frac{d(d+1)}{2}}/2^d$. □

In the above proof we used $\mathrm{disc}(L) \leq (n\sqrt{\ell})^{2n}$, where ℓ is the prime used to construct L. This only holds for our construction of L when $d = 2$. The above result can be proven for more values of d, but because of the restriction in place on a theorem below, we specialise to $d = 2$. We now prove a regularity result.

Lemma 13. *Let q be completely split in L, $d = 2$, $m \geq 2$, $\delta \in (0, 1/2)$, $\epsilon > 0$, $S \subset \{1, ..., n\}$, $\boldsymbol{c} \in \Lambda^m$, and $\boldsymbol{t} \leftarrow D_{\Lambda^m, \sigma, \boldsymbol{c}}$ for $\sigma \geq \frac{n\sqrt{\ell}}{\sqrt{\pi}} \sqrt{\ln(8mn(1 + 1/\delta))} q^{-\beta}$, where $\epsilon = (1 - \frac{|S|}{n})(\frac{3}{4} - \frac{1}{m}) - \beta$. For all but a fraction less than $2^{n(1+10m)} q^{-4nm\epsilon}$ of $\boldsymbol{a} \in (\Lambda_q^\times)^m$,*

$$\Delta\left(\boldsymbol{t} \bmod \boldsymbol{a}^\perp(\mathcal{I}_S), U\left(\Lambda^m / \boldsymbol{a}^\perp(\mathcal{I}_S)\right)\right) \leq 2\delta.$$

Proof. A direct combination of Lemmas 2, 4, 11, and 12. □

7 An NTRU Key Generation Algorithm

In [48] and [49], the authors published work improving the hardness guarantees of NTRU. They tweak the original version of NTRU, adding an error term that allows them to demonstrate IND-CPA security, assuming the hardness of a variant of RLWE. Here we adapt their work to our setting, following [57].

The Revised CNTRU Scheme Recall D_σ samples over $L_{\mathbb{R}}^2$ to enable us to sample elements of $\Lambda \otimes_{\mathbb{Q}} \mathbb{R}$, and $p \in \Lambda_q^\times$. We will sample the elements s, e from the same distribution, $\chi = \lfloor D_{\xi q} \rceil_{\Lambda^\vee}$, where $\lfloor \cdot \rceil_{\Lambda^\vee}$ is the CRR discretisation, $\xi = \alpha \left(\frac{2nk}{\log(4nk)} \right)^{\frac{1}{4}}$, $\alpha q \geq \omega(\sqrt{\log 4n})$, and $k = O(1)$.

KeyGen: Sample $f' \leftarrow D_{\Lambda,\sigma}$ and let $f = p \cdot f' + 1$; if $f \bmod q \notin \Lambda_q^\times$, resample. Sample $g \leftarrow D_{\Lambda,\sigma}$; if $g \bmod q \notin \Lambda_q^\times$, resample.
Return secret key $sk = (f, g)$ and public key $pk = h = f^{-1}pg \in \Lambda_q^\times$.
Encryption: Given $m \in \Lambda_p^\vee$, sample $s, e \leftarrow \chi$ and return $c = hs + pe + m \in \Lambda_q^\vee$.
Decryption: Given ciphertext c and secret key f, compute $c' = f \cdot c \in \Lambda_q^\vee$ and return $c' \bmod p$.
Correctness: $c' = fc = f(hs + pe + m) = fhs + fpe + fm = pgs + fpe + fm$. If the coefficients of $pgs + fpe + fm$ are small enough, reduction modulo q leaves the coefficients unchanged, and $c' \bmod p = m \bmod p$.

Recall that in an order of a CDA, if p is a central element, reduction by p works as usual; if $p \notin \mathcal{Z}(\Lambda)$, then we understand $(p) = \Lambda p \Lambda$.

We want to prove that if there is an IND-CPA attack on CNTRU, then a variant of CLWE can be broken. The following holds for the algebras used in CLWE, namely when $K = \mathbb{Q}(\zeta_{2^r})$, $n = [K : \mathbb{Q}]$ and L is a finite cyclic extension of K of degree 2. We now show there is a high probability of selecting an appropriate value f for the public key.

Lemma 14. *[21, Lemma 17] For a fixed d, the proportion of invertible elements of $M_d(\mathbb{F}_q)$ is at least $(1 - \frac{1}{q})^d$.*

Lemma 15. *Let $d = 2$, $0 < \epsilon < \frac{1}{2}$, $r \geq 2n\sqrt[4]{l}\sqrt{\frac{\ln 8n(1+1/\epsilon)}{\pi}} \cdot q^{\frac{1}{n}}$, $p \in \Lambda_q^\times$, $D_{\Lambda,r}$ a discrete Gaussian sampling Λ and $q \in \mathbb{Z}$ a prime that splits completely in K, i.e. $q\mathcal{O}_K = \prod_{i=1}^{[K:\mathbb{Q}]} \mathfrak{p}_i$. Then $\Pr_{f' \leftarrow D_r}[(pf' + 1 \bmod q\Lambda) \notin \Lambda_q^\times] \leq n \left(\frac{2}{q} - \frac{1}{q^2} + 2\epsilon \right)$.*

Proof. We bound $\Pr_{f' \leftarrow D_r}[(pf' + 1 \bmod \mathfrak{p}_i\Lambda) \notin \Lambda/\mathfrak{p}_i\Lambda^\times]$. Since r is sufficiently large, $pf' + 1 \bmod \mathfrak{p}_i\Lambda$ is statistically close to the uniform distribution. Thus the probability that $pf' + 1$ is not invertible in $\Lambda/\mathfrak{p}_i\Lambda$ is 1 minus the proportion of invertible elements in $\Lambda/\mathfrak{p}_i\Lambda \cong M_d(\mathbb{F}_q)$ plus 2ϵ. Note $M_d(\mathbb{F}_q)$ has size $|M_d(\mathbb{F}_q)| = q^{d^2}$ and the set of invertible elements in R_i has size $|GL_d(q)| = \prod_{i=0}^{d-1} \left(q^d - q^i \right)$. By Lemma 14, this proportion is at least $(1 - \frac{1}{q})^d$, so with $d = 2$ we lower bound the probability with $1 - (1 - \frac{1}{q})^2$. The CRT and a union bound implies the result.

Regarding r, since when $d = 2$ and K is a cyclotomic field with power of 2 conductor, the number of roots of unity in Λ is equal to $[\mathcal{A} : \mathbb{Q}]$ and hence since $\mathfrak{p}_i\Lambda$ is a Λ-ideal, $\lambda_{nd^2}(\mathfrak{p}_i\Lambda) = \lambda_1(\mathfrak{p}_i\Lambda)$. We then apply Lemma 3 and compute $\eta_\epsilon(\mathfrak{p}_i\Lambda) \leq \sqrt{\ln(2nd^2(1+1/\epsilon))/\pi} \cdot \lambda_{nd^2}(\mathfrak{p}_i\Lambda) = \sqrt{\ln(2nd^2(1+1/\epsilon))/\pi} \cdot \lambda_1(\mathfrak{p}_i\Lambda) \leq \sqrt{\ln(2nd^2(1+1/\epsilon))/\pi} \cdot 2n\sqrt[4]{l}q^{1/n} = \sqrt{\ln(8n(1+1/\epsilon))/\pi} \cdot 2n\sqrt[4]{l}q^{1/n}$. □

If $q \geq n+1$, then $(1-\frac{1}{q})^{nd} \geq \left((1-\frac{1}{n+1})^n\right)^d \geq e^{-d}$ and the proportion of invertible elements in Λ_q is non-negligible. We now show that with high likelihood the elements f and g used to construct the public key will not be too large.

Lemma 16. *Let $n \geq 8$ be a power of 2 such that x^n+1 splits completely modulo $q \geq 8n$. Let $\mathcal{A} = (L/K, \theta, \gamma)$ with $K = \mathbb{Q}(\zeta_n)$, $[L : K] = 2$, $\delta > 0$, and $\sigma \geq 2n\sqrt[4]{l}\sqrt{\frac{2\ln(24n)}{\pi}} \cdot q^{1/n}$. The secret key polynomials f, g returned by the cyclic-NTRU algorithm satisfy, with probability $\geq 1 - 2^{4-4n}$,*

$$\|f\| \leq \sqrt{2}(1 + \sigma\|p\|_\infty\sqrt{2n}) \text{ and } \|g\| \leq 2\sigma\sqrt{n}.$$

Proof. When $d = 2$, $\lambda_{nd^2}(\Lambda) = \lambda_1(\Lambda) \leq d\sqrt{n} \cdot (\mathrm{disc}(\Lambda))^{\frac{1}{2nd^2}} \leq 2n\sqrt[4]{l}$. If we set $\delta = \frac{1}{3n-1}$, then Lemma 3 implies $\eta_\delta(\Lambda) \leq \sqrt{\frac{2\ln(24n)}{\pi}} \cdot 2n\sqrt[4]{l}$. We can then use Lemma 6 to obtain $\Pr_{x \leftarrow D_{\Lambda,\sigma}}(\|x\| \geq d\sqrt{n}\sigma) \leq \frac{3n}{3n-2}2^{-nd^2}$. Then

$$\begin{aligned}
\Pr_{g \leftarrow D_{\Lambda,\sigma}}\left(\|g\| \geq d\sqrt{n}\sigma \mid g \in \Lambda_q^\times\right) &= \frac{\Pr_{g \leftarrow D_{\Lambda,\sigma}}\left(\|g\| \geq d\sqrt{n}\sigma \text{ and } g \in \Lambda_q^\times\right)}{\Pr_{g \leftarrow D_{\Lambda,\sigma}}\left(g \in \Lambda_q^\times\right)} \\
&\leq \frac{\Pr_{g \leftarrow D_{\Lambda,\sigma}}(\|g\| \geq d\sqrt{n}\sigma)}{\Pr_{g \leftarrow D_{\Lambda,\sigma}}\left(g \in \Lambda_q^\times\right)} \\
&\leq \frac{3n}{3n-2} \cdot 2^{-4n} \cdot \left(1/1 - n\left(\frac{2}{q} - \frac{1}{q^2} + 2\epsilon\right)\right) \\
&\leq 2^{-4n} \cdot 16 \leq 2^{4-4n}.
\end{aligned}$$

This applies to both f' and g, so we have $\|f'\|, \|g\| \leq 2\sqrt{n}\sigma$ with probability at least $1 - 2^{4-4n}$. Finally, observe $\|f\| = \|pf' + 1\| \leq \|pf'\| + \|1\| \leq \|p\|_\infty\|f'\| + \sqrt{2} \leq \|p\|_\infty\sigma 2\sqrt{n} + \sqrt{2} = \sqrt{2}(1 + \sigma\|p\|_\infty\sqrt{2n})$ with probability $\geq 1 - 2^{4-4n}$. □

We now show near-uniformity of the required distribution, to ensure our NTRU public keys are statistically close to the uniform distribution over $\Lambda_q^\times$.

Theorem 4. *Let $\epsilon > 0$, q be a completely split prime, $p \in \mathcal{Z}(\Lambda_q^\times)$, and $\sigma \geq 4n^{3/2}\sqrt[4]{\ell}\sqrt{2\ln(32nq)}q^{\frac{1}{2}+2\epsilon}$. Let $y_i \in \Lambda_q$ and $z_i = -y_ip^{-1} \bmod q$ for $i = 1, 2$, and $D^\times_{\sigma,z_i}$ denote $D_{\Lambda,\sigma}$ restricted by rejection to $\Lambda_q^\times + z_i$. Then when $d = 2$,*

$$\Delta\left(\frac{y_1 + pD^\times_{\sigma,z_1}}{y_2 + pD^\times_{\sigma,z_2}} \bmod q, U\left(\Lambda_q^\times\right)\right) \leq 2^{22n}q^{-8n\epsilon}.$$

Proof. Let $P_a := Pr_{f_i \leftarrow D^{\times}_{\sigma,z_i}, i=1,2}\left[(y_1 + pf_1) \cdot (y_2 + pf_2)^{-1} = a\right]$, where $a \in \Lambda_q^{\times}$. We aim to show that $|P_a - \frac{1}{|\Lambda_q^{\times}|}| < \epsilon'$, for some small $\epsilon' > 0$, except for an exponentially small fraction of the $a \in \Lambda_q^{\times}$.

Let $\boldsymbol{a} = (a_1, a_2) \leftarrow U((\Lambda_q^{\times})^2)$. When $z_i = -p^{-1}y_i \bmod q$, $(y_1 + pf_1) \cdot (y_2 + pf_2)^{-1} = -a_1^{-1}a_2 \bmod q$ is equivalent to $a_1f_1 + a_2f_2 = p^{-1}(-a_1y_1 - a_2y_2) \bmod q$, and so to $a_1f_1 + a_2f_2 = a_1z_1 + a_2z_2 \bmod q$. Since $-a_1^{-1}a_2 \in \Lambda_q^{\times}$ is uniform,

$$P_{-a_1^{-1}a2} = P_{\boldsymbol{a}} := Pr_{f_i \leftarrow D^{\times}_{\sigma,z_i}, i=1,2}[a_1f_1 + a_2f_2 = a_1z_1 + a_2z_2 \bmod q],$$

if $\boldsymbol{a} \in (\Lambda_q^{\times})^2$. One can see that the set of solutions to $a_1f_1 + a_2f_2 = a_1z_1 + a_2z_2 \bmod q$ in Λ, taken from $D^{\times}_{\sigma,z_i}$, $i = 1, 2$, is $\boldsymbol{z} + \boldsymbol{a}^{\perp\times}$, where $\boldsymbol{a}^{\perp\times} = \boldsymbol{a}^{\perp} \cap (\Lambda_q^{\times} \cap q\Lambda)^2$, and $\boldsymbol{a}^{\perp} = \boldsymbol{a}^{\perp}(\Lambda_q)$. We can then write

$$P_{\boldsymbol{a}} = \frac{D_{\Lambda^2,\sigma}(\boldsymbol{z} + \boldsymbol{a}^{\perp\times})}{D_{\Lambda,\sigma}(z_1 + \Lambda_q^{\times} + q\Lambda) \cdot D_{\Lambda,\sigma}(z_2 + \Lambda_q^{\times} + q\Lambda)}.$$

Now, let $\boldsymbol{t} \in \boldsymbol{a}^{\perp}$. Then $t_1a_1 + t_2 + a_2 \equiv 0 \bmod q$ implies that $t_2 = -t_1\frac{a_1}{a_2}$ and the t_i lie in a shared ideal of Λ_q. Denote this ideal by $\mathcal{I}_S$. Then

$$\boldsymbol{a}^{\perp\times} = \boldsymbol{a}^{\perp} \setminus \cup_{S \subset \{1,\ldots,n\}} \boldsymbol{a}^{\perp}(\mathcal{I}_S) \text{ and } \Lambda_q^{\times} + q\Lambda = \Lambda \setminus \cup_{S \subset \{1,\ldots,n\} \setminus \emptyset}(\mathcal{I}_S + q\Lambda).$$

Applying an inclusion-exclusion argument, we get two expressions to analyse:

$$D_{\Lambda^2,\sigma}(\boldsymbol{z} + \boldsymbol{a}^{\perp\times}) = \sum_{S \subset \{1,\ldots,n\}} (-1)^{|S|} D_{\Lambda^2,\sigma}(\boldsymbol{z} + \boldsymbol{a}^{\perp}(\mathcal{I}_S)), \text{ and} \tag{2}$$

$$D_{\Lambda,\sigma}(z_i + \Lambda_q^{\times} + q\Lambda) = \sum_{S \subset \{1,\ldots,n\}} (-1)^{|S|} D_{\Lambda,\sigma}(z_i + \mathcal{I}_S + q\Lambda). \tag{3}$$

We deal with (2) first, with two cases. If $|S| \leq \epsilon n$, use Lemma 13 with $m = 2$ and $\delta = q^{-nd^2 - \lfloor \epsilon n \rfloor d^2}$. Note that $q\Lambda^2 \subset \boldsymbol{a}^{\perp}(\mathcal{I}_S) \subset \Lambda^2$, so $|\Lambda^2/\boldsymbol{a}^{\perp}(\mathcal{I}_S)| = q^{d^2(n-|S|)}$. Then for all except a fraction less than $2^{n(1+4d^2+2d)}q^{-2d^2n\epsilon}$ of $\boldsymbol{a} \in (\Lambda_q^{\times})^2$,

$$\left| D_{\Lambda^2,\sigma}(\boldsymbol{z} + \boldsymbol{a}^{\perp}(\mathcal{I}_S)) - \frac{q^{d^2(n-|S|)}}{q^{2nd^2}} \right| = \left| D_{\Lambda^2,\sigma}(\boldsymbol{z} + \boldsymbol{a}^{\perp}(\mathcal{I}_S)) - q^{-nd^2 - d^2|S|} \right| \leq 2\delta.$$

In the second case, when $|S| > \epsilon n$, one can choose a subset $S'' \subset S'$ such that $|S''| = \lfloor \epsilon n \rfloor$. Then $\boldsymbol{a}^{\perp}(\mathcal{I}_S) \subset \boldsymbol{a}^{\perp}(\mathcal{I}_{S'})$, so $D_{\Lambda^2,\sigma}(\boldsymbol{z} + \boldsymbol{a}^{\perp}(\mathcal{I}_S)) \leq D_{\Lambda^2,\sigma}(\boldsymbol{z} +$

$\boldsymbol{a}^\perp(\mathcal{I}_{S'})$), so $D_{\Lambda^2,\sigma}(\boldsymbol{z}+\boldsymbol{a}^\perp(\mathcal{I}_S)) \le 2\delta + q^{-nd^2-d^2\lfloor \epsilon n\rfloor}$. We can now say that

$$\begin{aligned}
&\left| D_{\Lambda^2,\sigma}(\boldsymbol{z}+\boldsymbol{a}^{\perp\times}) - 2^{n(d-1)}\frac{|\Lambda_q^\times|}{|\Lambda_q|^2}\right| \\
&\le \left| \sum_{S\subset\{1,\dots,n\}} (-1)^{|S|} D_{\Lambda^2,\sigma}(\boldsymbol{z}+\boldsymbol{a}^\perp(\mathcal{I}_S)) - 2^{n(d-1)}\left(\frac{(q^{d^2}-1)^n}{2^{n(d-1)}q^{2nd^2}}\right)\right| \\
&\le \left| \sum_{S\subset\{1,\dots,n\}} (-1)^{|S|} D_{\Lambda^2,\sigma}(\boldsymbol{z}+\boldsymbol{a}^\perp(\mathcal{I}_S)) - \frac{(q^{d^2}-1)^n}{q^{2nd^2}}\right| \\
&\le \left| \sum_{S\subset\{1,\dots,n\}} (-1)^{|S|} D_{\Lambda^2,\sigma}(\boldsymbol{z}+\boldsymbol{a}^\perp(\mathcal{I}_S)) - \sum_{k=0}^{n}(-1)^k\binom{n}{k}q^{d^2(-n-k)}\right| \\
&\le \left| \sum_{S\subset\{1,\dots,n\}} (-1)^{|S|} D_{\Lambda^2,\sigma}(\boldsymbol{z}+\boldsymbol{a}^\perp(\mathcal{I}_S)) - \sum_{S\subset\{1,\dots,n\}}^{n}(-1)^{|S|}q^{-d^2(n+|S|)}\right| \\
&\le \left| \sum_{S\subset\{1,\dots,n\}} (-1)^{|S|}\left(D_{\Lambda^2,\sigma}(\boldsymbol{z}+\boldsymbol{a}^\perp(\mathcal{I}_S)) - q^{-d^2(n+|S|)}\right)\right| \\
&\le 2^n(2\delta + 2q^{-d^2(n+\lfloor\epsilon n\rfloor)}) \le 2^{n+1}(\delta + q^{-d^2(n+\lfloor\epsilon n\rfloor)}),
\end{aligned}$$

except for a fraction of $\boldsymbol{a}\in(\Lambda_q^\times)^2$ less than $2^{n(2+2d+4d^2)}q^{-2d^2n\epsilon}$. Writing

$$D_{\Lambda^2,\sigma}(\boldsymbol{z}+\boldsymbol{a}^{\perp\times}) = (1+\delta_0)2^{n(d-1)}\frac{|\Lambda_q^\times|}{|\Lambda_q|^2},$$

we find that $|\delta_0| \le \frac{|\Lambda_q|^2}{|\Lambda_q^\times|}2^{-n(d-1)}2^{n+1}(\delta + q^{-d^2(n+\lfloor\epsilon n\rfloor)})$
$\le 2^{nd}q^{nd^2}2^{-n(d-1)}2^{n+1}(\delta + q^{-d^2(n+\lfloor\epsilon n\rfloor)}) = 2^{2n+2}q^{-d^2\lfloor\epsilon n\rfloor}$.

Moving on to (3), begin by observing that

$$\det(\mathcal{I}_S + q\Lambda) = N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})\sqrt{\operatorname{disc}(\Lambda)} = q^{|S|}\sqrt{\operatorname{disc}(\Lambda)}.$$

Moreover, $\lambda_{nd}(\mathcal{I}_S+q\Lambda) = \lambda_1(\mathcal{I}_S+q\Lambda) \le d\sqrt{n}\cdot\det(\mathcal{I}_S+q\Lambda)^{1/nd^2} = d\sqrt{n}\cdot q^{|S|/nd^2}\operatorname{disc}(\Lambda)^{1/2nd^2}$. When $d=2$ and n is a power of two, we in fact have $\lambda_{nd^2}(\mathcal{I}_S+q\Lambda) \le d\sqrt{n}\cdot q^{|S|/nd^2}\operatorname{disc}(\Lambda)^{1/2nd^2}$. Since $\operatorname{disc}(\Lambda/\mathbb{Z}) \le (n\sqrt{\ell})^{4n}$, we obtain $\lambda_{nd^2}(\mathcal{I}_S+q\Lambda) \le d\sqrt{n}q^{|S|/nd^2}\sqrt{n}\sqrt[4]{\ell} = nd\sqrt[4]{\ell}q^{|S|/nd^2}$. Then Lemma 3 implies that $\eta_\delta(\mathcal{I}_S+q\Lambda) \le \sqrt{\ln(2nd^2(1+1/\delta))/\pi}\lambda_{nd^2}(\mathcal{I}_S+q\Lambda)$, so we find $\eta_\delta(\mathcal{I}_S+q\Lambda) \le \sqrt{\ln(2nd^2(1+1/\delta))/\pi}nd\sqrt[4]{\ell}q^{|S|/nd^2}$. Since σ is larger than this quantity for $|S| \le n/2$ and $\delta = q^{-nd^2/2}$, we can apply Lemma 4 to obtain $|D_{\Lambda,\sigma}(z_i+\mathcal{I}_S+q\Lambda) - \frac{1}{|\Lambda/\mathcal{I}|}| = |D_{\Lambda,\sigma}(z_i+\mathcal{I}_S+q\Lambda) - \frac{1}{q^{d^2|S|}}| \le 2\delta$. If $|S| > n/2$, we can pick a subset $S'\subset S$ such that $|S'| \le n/2$, and then $D_{\Lambda,\sigma}(z_i+\mathcal{I}_S+q\Lambda) \le D_{\Lambda,\sigma}(z_i+\mathcal{I}_{S'}+q\Lambda) \le 2\delta + q^{-nd^2/2}$. We now justify a claim, before proceeding with the rest of the proof:

Claim. For $d \geq 2$ and $q \geq 5$, we have $\prod_{i=1}^{d}(q^i - 1) \geq (q^{\frac{d(d+1)}{2}} - 1)/2^{\frac{d-1}{2}}$.

To see this, induct on d. When $d = 2$, the claim simplifies to the statement $(q-1)(q^2-1) > (q^3-1)/\sqrt{2}$, which is true iff the polynomial $(\sqrt{2}-1)q^3 - \sqrt{2}q^2 - \sqrt{2}q + (1+\sqrt{2}) > 0$, which is true when $q \geq 5$. Suppose the claim is true for $d = k-1 \geq 2$, and consider $\prod_{i=1}^{k}(q^i - 1)$. By induction, $\prod_{i=1}^{k-1}(q^i - 1) \geq (q^{\frac{k(k-1)}{2}} - 1)/2^{\frac{k-2}{2}}$, and we can write

$$\prod_{i=1}^{k}(q^i - 1) \geq (q^{\frac{k(k-1)}{2}} - 1)(q^k - 1)/2^{\frac{k-2}{2}} = (q^{\frac{k(k+1)}{2}} - q^{\frac{k(k-1)}{2}} - q^k + 1)/2^{\frac{k-2}{2}}.$$

Then the claim is true if

$$(q^{\frac{k(k+1)}{2}} - q^{\frac{k(k-1)}{2}} - q^k + 1)/2^{\frac{k-2}{2}} > (q^{\frac{k(k+1)}{2}} - 1)/2^{\frac{k-1}{2}},$$

i.e $(\sqrt{2}-1)q^{\frac{k(k+1)}{2}} - \sqrt{2}q^{\frac{k(k-1)}{2}} - \sqrt{2}q^k + \sqrt{2} + 1 > 0$, which holds if $q \geq 5$, $k \geq 2$.

The claim implies that $2^{\frac{n(d-1)}{2}}|\Lambda_q^\times|/(q^{d^2}-1)^n > 1$, for appropriate d and q, which we will use below. Resuming the proof, we have

$$\begin{aligned}
&\left| D_{\Lambda,\sigma}(z_i + \Lambda_q^\times + q\Lambda) - 2^{\frac{n(d-1)}{2}}\frac{|\Lambda_q^\times|}{|\Lambda_q|} \right| \\
&\leq \left| \sum_{S \subset \{1,\ldots,n\}} (-1)^{|S|} D_{\Lambda,\sigma}(z_i + \mathcal{I}_S + q\Lambda) - \frac{(q^{d^2}-1)^n}{q^{nd^2}} \right| \\
&= \left| \sum_{S \subset \{1,\ldots,n\}} (-1)^{|S|} D_{\Lambda,\sigma}(z_i + \mathcal{I}_S + q\Lambda) - \sum_{k=0}^{n} (-1)^k \binom{n}{k} q^{-d^2 k} \right| \\
&= \left| \sum_{S \subset \{1,\ldots,n\}} (-1)^{|S|} D_{\Lambda,\sigma}(z_i + \mathcal{I}_S + q\Lambda) - \sum_{S \subset \{1,\ldots,n\}} (-1)^{|S|} q^{-d^2|S|} \right| \\
&= \left| \sum_{S \subset \{1,\ldots,n\}} (-1)^{|S|} \left(D_{\Lambda,\sigma}(z_i + \mathcal{I}_S + q\Lambda) - q^{-d^2|S|} \right) \right| \\
&\leq 2^n(2\delta + 2q^{-nd^2/2}) = 2^{n+1}(\delta + q^{-nd^2/2});
\end{aligned}$$

writing $D_{\Lambda,\sigma}(z_i + \Lambda_q^\times + q\Lambda) = (1+\delta_i)2^{\frac{n(d-1)}{2}}\frac{|\Lambda_q^\times|}{|\Lambda_q|}$, for $\epsilon < \frac{1}{2}$ we get the required bounds on the δ_i since $|\delta_i| \leq 2^{\frac{-n(d-1)}{2}}\frac{|\Lambda_q|}{|\Lambda_q^\times|}2^{n+1}(\delta + q^{-nd^2/2}) \leq 2^{\frac{n(d+3)}{2}+2}q^{-nd^2/2}$.

Finally, we obtain that since $P_{\boldsymbol{a}} = \frac{D_{\Lambda^2,\sigma}(\boldsymbol{z}+\boldsymbol{a}^{\perp\times})}{D_{\Lambda,\sigma}(z_1+\Lambda_q^\times+q\Lambda)\cdot D_{\Lambda,\sigma}(z_2+\Lambda_q^\times+q\Lambda)}$,

$$\begin{aligned}\left|P_{\boldsymbol{a}} - \frac{1}{|\Lambda_q^\times|}\right| &= \left|\frac{D_{\Lambda^2,\sigma}(\boldsymbol{z}+\boldsymbol{a}^{\perp\times})}{D_{\Lambda,\sigma}(z_1+\Lambda_q^\times+q\Lambda)\cdot D_{\Lambda,\sigma}(z_2+\Lambda_q^\times+q\Lambda)} - \frac{1}{|\Lambda_q^\times|}\right| \\ &= \left|\frac{(1+\delta_0)2^{n(d-1)}\frac{|\Lambda_q^\times|}{|\Lambda_q|^2}}{(1+\delta_1)2^{\frac{n(d-1)}{2}}\frac{|\Lambda_q^\times|}{|\Lambda_q|}(1+\delta_2)2^{\frac{n(d-1)}{2}}\frac{|\Lambda_q^\times|}{|\Lambda_q|}} - \frac{1}{|\Lambda_q^\times|}\right| \\ &= \left|\frac{(1+\delta_0)}{(1+\delta_1)(1+\delta_2)|\Lambda_q^\times|} - \frac{1}{|\Lambda_q^\times|}\right|,\end{aligned}$$

and since the δ_i tend to 0, we obtain the result. □

8 A Provably Secure NTRU-based Scheme

In this section we provide a proof of IND-CPA security, subject to the hardness of LWE in CDAs, for the revised CNTRU scheme. Recall the definition of IND-CPA security:

Definition 20. [31] Let Π = (Gen, Enc, Dec) be a PKE scheme, and $\mathcal{A}$ be an adversary. Say Π is *indistinguishable under chosen-plaintext attack* if a ppt. adversary in the following experiment $\mathrm{PubK}_{\mathcal{A},\Pi}(n)$ has negligible advantage:

1. Gen is run to obtain keys (pk, sk).
2. Adversary $\mathcal{A}$ is given pk, and outputs a pair of equal-length messages m_0, m_1 in the message space.
3. A uniform bit $b \in \{0,1\}$ is chosen, and then a ciphertext $c \leftarrow \mathrm{Enc}_{pk}(m_b)$ is computed and given to $\mathcal{A}$. We call c the challenge ciphertext.
4. $\mathcal{A}$ outputs a bit b'. The output of the experiment is 1 if $b' = b$, and 0 otherwise. If $b' = b$ we say that $\mathcal{A}$ succeeds.

That is, $\Pr[\mathrm{PubK}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathrm{neg}(n)$.

Security Analysis We first obtain a bound on the infinity norm of a discretised Gaussian sample under the canonical embedding with the following lemma:

Lemma 17. *Assume that* $\xi = \alpha\left(\frac{ndk}{\log(nd^2k)}\right)^{\frac{1}{4}}, \chi = \lfloor D_{\xi q}\rceil_{\Lambda^\vee}, \alpha q \geq \omega(\sqrt{\log nd^2})$ *and* $k = O(1)$. *Set* $\delta = \omega\left(\sqrt{nd\log nd^2}\cdot\alpha^2q^2\right)$ *and* B *the decoding basis of* $\Lambda^\vee$. *Then for any* $\boldsymbol{t} \in H^d$, $\Pr_{x\leftarrow\chi}\left(|\langle \boldsymbol{t}, \boldsymbol{x}\rangle| > \delta\|\boldsymbol{t}\|^2\right) \leq (nd^2)^{-\omega(\sqrt{nd\log nd^2})\|\mathbf{t}\|^2}$.

Proof. A Gaussian random variable $\boldsymbol{x} \leftarrow D_{q\xi}$ of mean $\mathbf{0}$ and standard deviation $\frac{q\xi}{\sqrt{2\pi}}$ has a noncentral subgaussian discretisation $\lfloor \boldsymbol{x}\rceil$ with noncentrality 0 and deviation $\left(\frac{q^2\xi^2}{2\pi} + \frac{1}{2}s_1(B)^2\right)^{\frac{1}{2}}$ by Lemma 8. The definition of subgaussian gives

$$E\left(e^{\langle \boldsymbol{t}, \lfloor x\rceil\rangle}\right) \leq e^{\frac{1}{2}\left(\frac{q^2\xi^2}{2\pi} + \frac{1}{2}s_1(B)^2\right)\|\boldsymbol{t}\|^2},$$

for any $\boldsymbol{t} \in H^d$. A Chernoff bound then implies

$$\begin{aligned}\Pr\left(|\langle \boldsymbol{t}, \lfloor x \rceil \rangle| > \delta \|\boldsymbol{t}\|^2\right) &= \Pr\left(e^{|\langle \boldsymbol{t}, \lfloor x \rceil \rangle|} > e^{\delta \|\boldsymbol{t}\|^2}\right) \\ &\leq 2e^{\frac{1}{2}\left(\frac{q^2\xi^2}{2\pi} + \frac{1}{2}s_1(B)^2\right)\|\boldsymbol{t}\|^2 - \delta\|\boldsymbol{t}\|^2}.\end{aligned}$$

$s_1(B) \leq 1$, so $\frac{1}{2}\left(\frac{q^2\xi^2}{2\pi} + \frac{1}{2}s_1(B)^2\right)\|\boldsymbol{t}\|^2 = \Omega\left(\alpha^2 q^2 \sqrt{nd}\log(nd^2)^{-\frac{1}{2}} \cdot \|\boldsymbol{t}\|^2\right)$. Thus

$$\Pr\left(|\langle \boldsymbol{t}, \lfloor \boldsymbol{x} \rceil \rangle| > \delta \|\boldsymbol{t}\|^2\right) \leq (nd^2)^{-\omega(\sqrt{nd\log nd^2})\|\boldsymbol{t}\|^2}. \qquad \square$$

The above lemma gives an estimate for $\|\boldsymbol{x}\|_\infty$ with $\boldsymbol{x} \leftarrow \chi = \lfloor D_{q\cdot\xi} \rceil$:

$$Pr_{e \leftarrow \lceil \chi \rfloor}\left(\|e\|_\infty > \delta\right) \leq (nd^2)^{-\delta}, \tag{4}$$

where $\delta = \omega(\sqrt{nd\log nd^2}\alpha^2 q^2)$ and $\alpha q \geq \omega(\sqrt{\log nd^2})$. In the following, we make our assumption that $\ell \leq Cn$ for some constant $C \geq 2$; in this case, when C_1 and C_2 are bounds such that $\|\cdot\|^c \leq C_1\|\cdot\|$ and $\|\cdot\| \leq C_2\|\cdot\|^c$, we have $C_1 = \sqrt{2}s_1(\overrightarrow{p}) < 2\sqrt{2}Cn$, so $C_1 = O(n)$, and $C_2 = \sqrt{2}s_1(\overrightarrow{d}) < 1$.

Lemma 18. *Let $n \geq 8$ be a power of 2, $q \geq 8n$ split completely in L, $\ell \leq Cn$, $\sigma \geq 2n\sqrt[4]{l}\sqrt{\frac{2\ln(24n)}{\pi}}q^{1/n}$. The decryption algorithm outputs m with probability $1 - (4n)^{-\omega(\sqrt{2n\log 4n})}$ over s, e, f, g if $\omega\left(2\sqrt{2}n^2\sqrt{\log 4n}\alpha^2 q^2\right)\sigma\|p\|_\infty^2 \leq q/2$.*

Proof. Notice that $f \cdot h \cdot s = p \cdot g \cdot s \bmod q\Lambda^\vee$, we have $fc = pgs + pfe + fm \bmod q\Lambda^\vee \in \Lambda^\vee$. If $\|pgs + pfe + fm\|_\infty^c < \frac{q}{2}$, then we have fc has the representation of the form $pgs + pfe + fm$ in $\Lambda_q^\vee$. Hence, we have $m = (fc \bmod q\Lambda^\vee) \bmod p\Lambda^\vee$. It thus suffices to upper bound the probability that $\|pgs + pfe + fm\|_\infty^c \geq \frac{q}{2}$.

Note that $\|fc\|_\infty^c \leq \|fc\|^c \leq C_1\|fc\| = C_1\|pgs + pfe + fm\| \leq C_1(\|pgs\| + \|pfe\| + \|fm\|)$. By the choice of σ and Lemma 16, with probability larger than $1 - 2^{4-nd^2}$, $\|f\| \leq \sqrt{d}(1 + \sigma\|p\|_\infty\sqrt{nd})$ and $\|g\| \leq \sqrt{n}d\sigma$. Combining with (4),

$$\begin{aligned}\|pfe\| + \|pgs\| &\leq \sqrt{d}(1 + \sigma\|p\|_\infty\sqrt{nd})\|p\|_\infty\|e\|_\infty + \sqrt{n}d\sigma\|p\|_\infty\|s\|_\infty \\ &\leq 2\sigma\sqrt{n}d\|p\|_\infty^2\|e\|_\infty + \sqrt{n}d\sigma\|p\|_\infty\|s\|_\infty \leq \omega(nd^{3/2}\sqrt{\log nd^2}\alpha^2 q^2)\sigma\|p\|_\infty^2\end{aligned}$$

with probability $1-(nd^2)^{-\omega(\sqrt{nd\log nd^2})}$. Since $m \in \Lambda^\vee/p\Lambda^\vee$, by reducing modulo the $p\sigma(\vec{d})_i$, write $m = \sum_{i=1}^{nd^2}\varepsilon_i p\sigma(\vec{d})_i$ with $\varepsilon_i \in \left(-\frac{1}{2}, \frac{1}{2}\right]$. We have

$$\|m\| = \left\|\sum_{i=1}^{nd^2}\varepsilon_i p\sigma(\vec{d})_i\right\| \leq \|p\|_\infty\left\|\sum_{i=1}^{nd^2}\varepsilon_i\sigma(\vec{d})_i\right\| \leq \|p\|_\infty\frac{\sqrt{n}d}{2}C_2,$$

so $\|fm\| \leq \|f\|\|m\| \leq \sqrt{d}(1 + \sigma\|p\|_\infty\sqrt{nd}) \cdot \|p\|_\infty\frac{\sqrt{n}d}{2}C_2 \leq 2\sigma\sqrt{n}d\|p\|_\infty \cdot \|p\|_\infty\frac{\sqrt{n}d}{2}C_2 \leq nd^2\sigma\|p\|_\infty^2 C_2$ with probability $\geq 1 - 2^{4-n}$. All together, we have

$$\begin{aligned}\|fc\|_\infty^c &\leq C_1\left(\omega(nd^{3/2}\sqrt{\log nd^2}\alpha^2 q^2)\sigma\|p\|_\infty^2 + nd^2\sigma\|p\|_\infty^2 C_2\right) \\ &\leq \omega\left(n^2 d^{3/2}\sqrt{\log nd^2} \cdot \alpha^2 q^2\right)\sigma\|p\|_\infty^2\end{aligned}$$

with probability $1-(nd^2)^{-\omega(\sqrt{nd\log nd^2})}$, since $C_2 \leq 1$ and $C_1 = O(n)$. □

We now attempt a proof of IND-CPA security. Recall the CLWE variant we will use: let $s, e \leftarrow \chi$, and $a \leftarrow U(\Lambda_q^\times)$. Here χ is the CRR discretisation of the usual CLWE distribution to $\Lambda_q^\vee$; [21] gave a reduction from CLWE to this variant. Output $(a, as+e) \in \Lambda_q^\times \times \Lambda_q^\vee$, and call this distribution $A^\times_{q,s,\chi}$. Define the usual search and decision problems over this distribution to obtain $\mathrm{CLWE}^\times_{HNF}$.

Lemma 19. *Let $n \geq 8$ be a power of 2, $d = 2$, $\ell \leq Cn$, and $q \geq 8n$ a prime such that x^n+1 splits completely modulo q. Let $\delta > 0$, $p \in \mathcal{Z}\left(\Lambda_q^\times\right)$ and $\sigma \geq 2n^{3/2}\sqrt[4]{\ell}\sqrt{\ln(32nq)}q^{\frac{1}{2}+2\epsilon}$ satisfy the conditions of Lemma 18 and Theorem 4. If there exists an IND-CPA attack algorithm $\mathcal{A}$ against CNTRU, running in time T with advantage δ, then there exists an algorithm to solve decision-CLWE$^\times_{\mathrm{HNF}}$ that runs in time $T' = T + O(\mathrm{poly}(n))$ with success probability $\delta' = \delta - q^{-\Omega(n)}$.*

Note that if $p \in \mathbb{Z}_q^\times$, the algorithm runs in time $T' = T + O(n)$.

Proof. The proof runs similarly to [48, Lemma 13], [57, Lemma 16]. We use the attack algorithm against CNTRU to construct an algorithm $\mathcal{B}$ with non-negligible advantage against $\mathrm{CLWE}^\times_{HNF}$. Write $\mathcal{O}$ for an oracle that samples from one of $U(\Lambda_q^\times \times \Lambda_q^\vee)$ and $A^\times_{s,\chi}$ for some previously chosen $s \leftarrow \chi$. $\mathcal{B}$ begins by obtaining a sample $(h', c') \in \Lambda_q^\times \times \Lambda_q^\vee$ via $\mathcal{O}$. The idea is that $\mathcal{B}$ uses $\mathcal{A}$ with public key $h = p \cdot h' \in \Lambda_q$ to guess the bit b in the IND-CPA experiment. As part of the IND-CPA experiment, $\mathcal{A}$ outputs messages $m_0, m_1 \in \Lambda_p^\vee$. $\mathcal{B}$ then samples $b \leftarrow U(\{0,1\})$, computes ciphertext $c = p \cdot c' + m_b$, and sends c to $\mathcal{A}$. Finally, $\mathcal{A}$ submits a value b' for b, and if $b' = b$, $\mathcal{B}$ outputs 1. Else, $\mathcal{B}$ outputs 0.

Since h' is uniformly random in $\Lambda_q^\times$ and p is invertible mod q, so is h, and so the public key given to $\mathcal{A}$ is of statistical distance at most $q^{-\Omega(n)}$ from the correct distribution for the attack algorithm, by Theorem 4. Additionally, since $c' = h \cdot s + e$ with $s, e \leftarrow \chi$, c has the desired distribution for the IND-CPA attack algorithm. In conclusion, if $\mathcal{O}$ outputs samples from $A^\times_{s,\chi}$, then $\mathcal{A}$, and hence $\mathcal{B}$, returns 1 with probability $\geq 1/2 + \delta - q^{-\Omega(n)}$. If $\mathcal{O}$ outputs uniform samples from $U(\Lambda_q^\times \times \Lambda_q^\vee)$, then c is uniformly random in $\Lambda_q^\vee$ since $p \in \Lambda_q^\times$, and is independent of b. Thus $\mathcal{B}$ outputs 1 with probability $1/2$, as desired. □

If $K = \mathbb{Q}(\zeta_{2^r})$, $2^{r-1} = n \geq 8$, $L = \mathbb{Q}(\zeta_{2^r}, \sqrt{\ell})$ for prime $\ell : \ell \equiv 1 \bmod 2^r$, $\ell \leq Cn$ for some $C \geq 2$, $q \geq 8n$ a prime q split completely in L, $\alpha \in (0,1)$: $\alpha q \geq \omega(\sqrt{\log 4n})$, $\xi = \alpha\left(\frac{2nk}{\log(4nk)}\right)^{\frac{1}{4}}$ with $k = O(1)$, $\epsilon \in \left(0, \frac{1}{2}\right)$, $p \in \Lambda_q^\times$, $\sigma \geq 2n^{3/2}\sqrt[4]{\ell}\sqrt{\ln(32nq)}q^{\frac{1}{2}+2\epsilon}$ and $\omega\left(2\sqrt{2}n^2\sqrt{\log 4n}\alpha^2q^2\right)\sigma\|p\|_\infty^2 \leq q/2$, the security reduction to CLWE from ideal lattice problems holds, and CNTRU connects with SIVP (note that the CLWE reduction is valid for a restricted secret space).

9 Conclusion

In this work we have defined a general form of NTRU, and shown that for certain parameters the NTRU instances obtained are indistinguishable from samples

chosen uniformly at random. We have given the cryptographic application of a public-key encryption scheme, and shown that an IND-CPA attack on the PKE scheme implies an efficient attack on decision CLWE. Along the way we have proved new results on q-ary lattices obtained from natural orders of CDAs.

Future work includes selecting parameters for the signature scheme and the KEM and implementing these schemes. Further cryptanalysis is required to better understand the security of CNTRU. It would also be desirable to see if one could lift the constraint '$d = 2$', and obtain results for higher degrees. As explained in the introduction, the methods of this work are constrained to degree-two extensions of power-of-two cyclotomic fields, and we do not currently know how to remove this restriction.

A Proofs

Proof of Proposition 5. We have

$$\begin{aligned}
\|x\|_p^p &= \sum_{\alpha\in\mathrm{Emb}(K)}\sum_{1\le i,j<d}|\alpha((\phi(x))_{i,j})|^p \ge d^2\sum_{\alpha\in\mathrm{Emb}(K)}\left(\prod_{i,j}|\alpha((\phi(x))_{i,j})|^p\right)^{1/d^2}\\
&\ge d^2[K:\mathbb{Q}]\left(\prod_{\alpha\in\mathrm{Emb}(K)}\left(\prod_{0\le i<d}|\alpha(N_{L/K}(x_i))|^p\right)^{1/d^2}\right)^{1/[K:\mathbb{Q}]}\\
&= [\mathcal{A}:\mathbb{Q}]\left(\prod_{0\le i<d}|N_{L/\mathbb{Q}}(x_i)|\right)^{p/[\mathcal{A}:\mathbb{Q}]}, \text{ and if } x\in\mathcal{I},\\
\|x\|_p^p &\ge [\mathcal{A}:\mathbb{Q}]\left(\prod_{0\le i<d}|N_{L/\mathbb{Q}}(x_i)|\right)^{p/[\mathcal{A}:\mathbb{Q}]} = [\mathcal{A}:\mathbb{Q}]\left|N_{L/\mathbb{Q}}\left(\prod_{0\le i<d}x_i\right)\right|^{p/[\mathcal{A}:\mathbb{Q}]}
\end{aligned}$$

By assumption, the coefficients x_i lie in the ideal $\mathfrak{J}\mathcal{O}_L$. Thus $x_i \in \bar{\mathcal{I}} := \mathcal{I}\cap\mathcal{O}_L$ for $i = 0,...,d-1$, and so $\prod_{0\le i<d}x_i \in \bar{\mathcal{I}}^d$, and hence $\|x\|_p^p \ge [\mathcal{A}:\mathbb{Q}]\cdot\left|N_{L/\mathbb{Q}}\left(\bar{\mathcal{I}}\right)\right|^{dp/[\mathcal{A}:\mathbb{Q}]}$. Finally, to see $\lambda_1^\infty(\mathcal{I}) \ge \left(N_{L/\mathbb{Q}}(\bar{\mathcal{I}})\right)^{1/nd}$,
$\|x\|_\infty = \sup_{i,j,\alpha}|\alpha(\phi(x)_{i,j})| \ge \prod_{i,j,\alpha}|\alpha((\phi(x))_{i,j})|^{1/nd^2} = N_{L/\mathbb{Q}}(\prod_{0\le i<d}x_i)^{1/nd^2}$. □

B Choosing Parameters and Number Fields

In this section, we give a brief overview of some parameters choices for NTRU, focusing on n and q, before giving possible parameters for CDAs. We note that many suggested parameters (including ours) are not chosen according to security proofs, but rather take into account considerations such as speed and efficiency. We note the analysis of [12], and [32] for LWE, and welcome similar analysis for provably secure NTRU variants and CNTRU.

Parameters for NTRU in Previous Works NTRU [24] uses convolution rings $\mathbb{Z}[x]/(x^N - 1)$ with N prime, which are not ring of integers of algebraic number fields. This is the same as in [23], [28]; since CDAs are constructed from fields, the parameters used here do not adapt straightforwardly to our setting. This situation is mirrored in the NTRU finalist in NIST's post-quantum standardisation process, [13]. The authors use the rings $\mathbb{Q}(x)/(x-1)\Phi_n(x)$ with prime n, which are not fields. In this case, the polynomials '$\Phi_n(x)$' are cyclotomic, hence $x^n - 1 = (x-1)\Phi_n(x)$; and $(x-1)\Phi_n(x)$ is plainly not irreducible.

However, the authors of [48], [49] replace $x^n - 1$ by $x^n + 1$, for power-of-two n. These are the $2n$th cyclotomic polynomials, which are amenable to generalisation by CDAs. Since n is a power of two, natural choices are $n = 512$ or $n = 1024$. They also recommend $p = 3$ or $p = 2$. As for q, if $\alpha q > n^{0.75}$, the decryption algorithm recovers m with probability $1 - n^{\omega(1)}$. For the security proof to hold, one needs $q \equiv 1 \bmod 2n$. So in the context of CDAs, one could choose $n = 256$, $q = 7681$, or $n = 512$, $q = 12289$, if working with the same framework as [49].

Falcon [19] uses $n = 512$ for NIST Level I, and $n = 1024$ for NIST Level V, where n is the degree of the cyclotomic ring. They use $q = 12289$. ModFalcon [16] uses a rank two module over a power of two cyclotomic of degree 512, and also sets $q = 12289$. In contrast, ModNTRU [15] uses a rank three module over a power of two cyclotomic of degree 512, but uses $q = 2^{19}$, instead of prime q.

Parameters for NTRU in CDAs We follow the module NTRU instances in using power of two cyclotomics. Although there has been some concern raised over the large number of subfields and automorphisms attached to these objects [42], there has not yet been an efficient attack against the NTRU problem exploiting these features (for non-'overstretched' parameters). We recommend using algebras of dimension approximately 1000 over $\mathbb{Q}$. Following the construction detailed above: $\mathcal{A} = (L/\mathbb{Q}(\zeta_n), \theta, \zeta_n)$ with $K \subset L \subset M = \mathbb{Q}(\zeta_{\ell n})$ for $\ell \equiv 1 \bmod n$, $\ell \not\equiv 1 \bmod pn$ for any prime $p \mid n$. Take q to be a prime completely split in L, not too large to avoid attacks exploiting 'overstretched' parameters. Example parameters might be $n = 1024$, $d = 2$, $\ell = 12289$, and $q = 13313$.

As for choosing the sets $\mathcal{S}_f$ and so on, one can take these to be binary or ternary with set weights for efficiency, as some other NTRU schemes do, if desired. We leave the precise analysis of choices of such sets as future work.

C Sketched Cryptographic Functionality

KEM Here we outline an CNTRU-based KEM. We follow the structure of the KEM in [13] closely. Denote the CNTRU key generation, encryption, and decryption algorithms by KeyGen, Encrypt, and Decrypt respectively.

KeyGen_{KEM}
1. $(pk', sk') = (h, (f, g, h)) \leftarrow \text{KeyGen(seed)}$
2. $s \leftarrow_{\$} \{0,1\}^{nd^2}$
3. return $(pk, sk) = (pk', (sk', s)) = (h, (f, g, h, s))$

Below, $H_1(\cdot)$ and $H_2(\cdot)$ are hash functions. Correctness is straightforward.

Encapsulate(h)
1. $(r, m) \leftarrow \mathcal{L}_r \times \mathcal{L}_m$
2. $c \leftarrow \text{Encrypt}(h, (r, m))$
3. $k_1 \leftarrow H_1(r, m)$
4. return (c, k_1)

Decapsulate($(f, g, h, s), c$)
1. $(r, m) \leftarrow \text{Decrypt}(sk, c)$
2. $k_1 \leftarrow H_1(r, m)$, $k_2 \leftarrow H_2(s, c)$
3. if $(r, m) \neq \perp$ return k_1
4. else return k_2

Signatures We now give a signature scheme for CNTRU, based on pqNTRUSign [22]. Below are the key generation, signing, and verification algorithms. As usual, we fix coprime integers p and q with $q \gg p$. In [22], ternary polynomials are used, though we note this is not essential for the correctness of the scheme. Let $\mathcal{T}$ denote elements of Λ with ternary coefficients, i.e. $\mathcal{T} = \{f = \oplus_{i=0}^{d-1} u^i f_i \in \Lambda : f_i \text{ is ternary}\}$. Moreover, let $\mathcal{R} = \{h = \oplus_{i=0}^{d-1} u^i h_i : \|h_i\|_\infty \leq q/2, i = 0, ..., d-1\}$ and $\mathcal{S} = \{g = \oplus_{i=0}^{d-1} g_i \in \Lambda : \|g_i\|_\infty \leq p/2, i = 0, ..., d-1\}$.

KeyGen_{Sign}
1. $F \leftarrow \mathcal{T}$ and set $f = pF$.
2. If $f \notin \Lambda_q^\times$, resample F.
3. $g \leftarrow \mathcal{S}$.
4. If $g \notin \Lambda_q^\times$, resample g.
5. $h := f^{-1} g \bmod q$.
6. $(pk, sk) = (h, (f, g))$.

Like pqNTRUSign, we require a function H which takes a public key h and a message μ to be signed, and outputs a pair of elements with bounded norm, that is $H : \mathcal{R} \times \{0,1\}^* \to \mathcal{S} \times \mathcal{S}$. The values B_s and B_t are bounds that can be changed to vary the security level and efficiency of the protocol.

Sign(μ): input $(pk, sk, \mu) = (h, (f, g), \mu)$
1. $(s_p, t_p) = H(h, \mu)$.
2. $r \leftarrow \Lambda : \|r\|_\infty \leq \left\lfloor \frac{q}{2p} + \frac{1}{2} \right\rfloor$, $i = 0, ..., d-1$.
3. $(s_0, t_0) := (s_p + pr, s_0 h \bmod q)$.
4. $a := (t_p - t_0) g^{-1} \bmod p$.
5. If $\|af\|_\infty > B_s$ or $\|ag\|_\infty > B_t$ or $\|s\|_\infty > \frac{q}{2} - B_s$ or $\|t\|_\infty > \frac{q}{2} - B_t$, restart.
6. $(s, t) := (s_0, t_0) + (af, ag)$.
7. Output $\sigma = (s, t, \mu)$.

The signing algorithm is nearly identical to that of pqNTRUSign. We do, however, have to be careful about how we multiply a and f, g. For correctness to hold, we use the pair (af, ag) in our algorithm, whereas in [22] one can use (fa, ga) or (af, ag). This is because the NTRU lattice is an $\mathcal{O}_L$-bimodule in the commutative case, whereas CNTRU lattices are only left Λ-modules.

Verify(σ): input $(h, \sigma) = (h, (s, t, \mu))$
1. $(s_p, t_p) \leftarrow H(h, \mu)$.
2. Check $(s_p, t_p) \equiv (s, t) \bmod p$.
3. Check $t \equiv sh \bmod q$.
4. Check $\|s\|_\infty \leq \frac{q}{2} - B_s$ and $\|t\|_\infty \leq \frac{q}{2} - B_t$.
5. If all checks succeed, output *Valid*.

It is straightforward to show correctness for this scheme, for well chosen B_s, B_t.

We do not analyse the above schemes in detail; we include them to demonstrate that such functionality is obtainable from NTRU in noncommutative rings.

References

1. Albert, A.: Structure of Algebras, AMS colloquium publications, vol. 24. American Mathematical Society (1939)
2. Albrecht, M., Bai, S., Ducas, L.: A subfield lattice attack on overstretched NTRU assumptions. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9814, pp. 153–178. Springer Berlin Heidelberg (2016). https://doi.org/10.1007/978-3-662-53018-4$_6$
3. Applebaum, B., Cash, D., Peikert, C., Sahai, A.: Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 595–618. Springer Berlin Heidelberg (2009). https://doi.org/10.1007/978-3-642-03356-8$_3$5
4. Atani, R., Atani, S., Karbasi, A.: NETRU: A noncommutative and secure variant of CTRU cryptosystem. ISC Int. J. Inf. Sec. **10**, 45–53 (2018)
5. Atani, R., Atani, S., Karbasi, A.: A provably secure variant of ETRU based on extended ideal lattices over direct product of dedekind domains. JCS **5**, 13–34 (2018). https://doi.org/10.22108/jcs.2018.106856.0
6. Bagheri, K., Sadeghi, M.R., Panario, D.: A non-commutative cryptosystem based on quaternion algebras. Designs, Codes and Cryptography **86**(10), 2345–2377 (2018). https://doi.org/10.1007/s10623-017-0451-4
7. Banks, W., Shparlinski, I.: A variant of NTRU with non-invertible polynomials. In: Menezes, A., Sarkar, P. (eds.) INDOCRYPT 2002. LNCS, vol. 2551 (2002). https://doi.org/10.1007/3-540-36231-2$_6$
8. Bayer-Fluckiger, E., Cerri, J.P., Chaubert, J.: Euclidean minima and central division algebras. International Journal of Number Theory **05**(07), 1155–1168 (2009). https://doi.org/10.1142/S1793042109002614
9. Bernstein, D., Chuengsatiansup, C., Lange, T., van Vredendaal, C.: NTRU prime: Reducing attack surface at low cost. In: Adams, C., Camenisch, J. (eds.) SAC 2017. LNCS, vol. 10719, pp. 235–260. Springer International (2017)
10. Boudgoust, K., Jeudy, C., Roux-Langlois, A., Wen, A.: Entropic hardness of module-LWE from module-NTRU. In: Isobe, T., Sarkar, S. (eds.) INDOCRYPT 2022. LNCS, vol. 13774, pp. 78–99. Springer International Publishing (2022)
11. Caruso, X., Borgne, J.L.: Fast multiplication for skew polynomials. In: ISSAC 2017. p. 77–84. Association for Computing Machinery (2017). https://doi.org/10.1145/3087604.3087617
12. Chatterjee, S., Koblitz, N., Menezes, A., Sarkar, P.: Another look at tightness II: Practical issues in cryptography. In: Phan, R.C.W., Yung, M. (eds.) Mycrypt 2016. LNCS, vol. 10311, pp. 21–55. Springer International Publishing (2017)

13. Chen, C., Danba, O., Hoffstein, J., Hülsing, A., Rijneveld, J., Schanck, J.M., Schwabe, P., Whyte, W., Zhang, Z.: NTRU: Algorithm specifications and supporting documentation (2019), ntru.org/f/ntru-20190330.pdf
14. Chen, Y., Genise, N., Mukherjee, P.: Approximate trapdoors for lattices and smaller hash-and-sign signatures. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019. LNCS, vol. 11923, pp. 3–32. Springer International Publishing (2019). https://doi.org/10.1007/978-3-030-34618-8$_1$
15. Cheon, J.H., Kim, D., Kim, T., Son, Y.: A new trapdoor over module-NTRU lattice and its application to id-based encryption. Cryptol. ePrint Archive, Rpt. 2019/1468 (2019), https://eprint.iacr.org/2019/1468
16. Chuengsatiansup, C., Prest, T., Stehlé, D., Wallet, A., Xagawa, K.: Modfalcon: Compact signatures based on module-NTRU lattices. In: ASIA CCS 2020. p. 853–866. Assoc. for Computing Machinery (2020). https://doi.org/10.1145/3320269.3384758
17. Coppersmith, D., Shamir, A.: Lattice attacks on NTRU. In: EUROCRYPT 1997. LNCS, vol. 1233, pp. 52–61. Springer Berlin Heidelberg (1997)
18. Felderhoff, J., Pellet-Mary, A., Stehlé, D.: On module unique-SVP and NTRU. In: Agrawal, S., Lin, D. (eds.) ASIACRYPT 2022. LNCS, vol. 13793, pp. 709–740. Springer Nature Switzerland (2022). https://doi.org/10.1007/978-3-031-22969-5$_2$4
19. Fouque, P.A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., Zhang, Z.: Falcon: Fast-fourier lattice-based compact signatures over NTRU, https://falcon-sign.info/falcon.pdf
20. Gaborit, P., Ohler, J., Solé, P.: CTRU, a polynomial analogue of NTRU. Tech. Rep. RR-4621, INRIA (2002), https://inria.hal.science/inria-00071964
21. Grover, C., Mendelsohn, A., Ling, C., Vehkalahti, R.: Non-commutative ring learning with errors from cyclic algebras. J. of Cryptology **35**(3), 22 (2022). https://doi.org/10.1007/s00145-022-09430-6
22. Hoffstein, J., Pipher, J., Schanck, J.M., Silverman, J.H., Whyte, W.: Transcript secure signatures based on modular lattices. In: Mosca, M. (ed.) PQCrypto 2014. LNCS, vol. 8772, pp. 142–159. Springer International Publishing (2014)
23. Hoffstein, J., Pipher, J., Schanck, J.M., Silverman, J.H., Whyte, W., Zhang, Z.: Choosing parameters for NTRUEncrypt. In: Handschuh, H. (ed.) CT-RSA 2017. LNCS, vol. 10159, pp. 3–18. Springer International Publishing (2017)
24. Hoffstein, J., Pipher, J., Silverman, J.: NTRU: A ring-based public key cryptosystem. In: ANTS 1998. LNCS, vol. 1423, p. 267–288. Springer (1998)
25. Howgrave-Graham, N.: A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 150–169. Springer Berlin Heidelberg (2007). https://doi.org/10.1007/978-3-540-74143-5$_9$
26. Howgrave-Graham, N., Nguyen, P.Q., Pointcheval, D., Proos, J., Silverman, J.H., Singer, A., Whyte, W.: The impact of decryption failures on the security of NTRU encryption. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 226–246. Springer Heidelberg (2003). https://doi.org/10.1007/978-3-540-45146-4$_1$4
27. Howgrave-Graham, N., Silverman, J., Whyte, W.: A meet-in-the-middle attack on an NTRU private key. Tech. rep., NTRU Cryptosystems (07 2003)
28. Howgrave-Graham, N., Silverman, J.H., Whyte, W.: Choosing parameter sets for NTRUEncrypt with NAEP and SVES-3. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 118–135. Springer Heidelberg (2005). https://doi.org/10.1007/978-3-540-30574-3$_1$0
29. Jarvis, K.: NTRU over the Eisenstein Integers. Master's thesis (2011), https://ruor.uottawa.ca/handle/10393/19862

30. Karbasi, A.H., Atani, R.: ILTRU: An NTRU-like public key cryptosystem over ideal lattices. Cryptol. ePrint Arch. p. 549 (2015)
31. Katz, J., Lindell, Y.: Introduction to Modern Cryptography, Second Edition. Chapman & Hall/CRC, Taylor & Francis (2014)
32. Koblitz, N., Samajder, S., Sarkar, P., Singha, S.: Concrete analysis of approximate ideal-SIVP to decision ring-LWE reduction. Advances in Mathematics of Communications (2022). https://doi.org/10.3934/amc.2022082
33. Kouzmenko, R.: Generalizations of the NTRU cryptosystem. Ph.D. thesis (2005)
34. Malekian, E., Zakerolhosseini, A.: OTRU: A non-associative and high speed public key cryptosystem. In: CADS 15. pp. 83–90 (2010). https://doi.org/10.1109/CADS.2010.5623536
35. Malekian, E., Zakerolhosseini, A., Mashatan, A.: QTRU: quaternionic version of the NTRU public-key cryptosystem. ISC Int. J. of Information Security **3**, 29–42 (2011). https://doi.org/10.22042/isecure.2015.3.1.3
36. Marcus, D.: Number Fields. Universitext, Springer-Verlag (1977)
37. Micciancio, D., Regev, O.: Worst-case to average-case reductions based on Gaussian measures. In: FOCS 2004. SIAM J. Comput., vol. 37, pp. 372–381 (2004). https://doi.org/10.1109/FOCS.2004.72
38. Murphy, S., Player, R.: δ-subgaussian random variables in cryptography. In: Jang-Jaccard, J., Guo, F. (eds.) ACISP 2019. LNCS, vol. 11547, pp. 251–268. Springer International Publishing (2019). https://doi.org/10.1007/978-3-030-21548-4$_1$4
39. Murphy, S., Player, R.: Discretisation and product distributions in Ring-LWE. J. of Mathematical Cryptology **15**(1), 45–59 (2021). https://doi.org/doi:10.1515/jmc-2020-0073
40. Nevins, M., Jarvis, K.: ETRU: NTRU over the Eisenstein integers. Designs, Codes and Cryptography **74**, 219–242 (2013). https://doi.org/https://doi.org/10.1007/s10623-013-9850-3
41. Nevins, M., KarimianPour, C., Miri, A.: NTRU in rings beyond $\mathbb{Z}$. Designs, Codes and Cryptography **56**, 65–78 (2009). https://doi.org/https://doi.org/10.1007/s10623-009-9342-7
42. NTRU Prime Risk-Management Team: Risks of lattice KEMs (2021), `https://ntruprime.cr.yp.to/warnings.html`
43. Oggier, F., Sethuraman, B.A.: Quotients of orders in cyclic algebras and space-time codes. AMC **7**(4), 441–461 (2013). https://doi.org/10.3934/amc.2013.7.441
44. Peikert, C.: Limits on the hardness of lattice problems in ℓ_p norms. In: CCC 07. pp. 333–346 (2007). https://doi.org/10.1109/CCC.2007.12
45. Peikert, C., Rosen, A.: Lattices that admit logarithmic worst-case to average-case connection factors. In: STOC '07. p. 478–487. Association for Computing Machinery (2007). https://doi.org/10.1145/1250790.1250860
46. Pellet-Mary, A., Stehlé, D.: On the hardness of the NTRU problem. In: Tibouchi, M., Wang, H. (eds.) ASIACRYPT 2021. LNCS, vol. 13090, pp. 3–35. Springer (2021)
47. Singh, S., Padhye, S.: Generalisations of NTRU cryptosystem. SCN **9**(18), 6315–6334 (2016). https://doi.org/https://doi.org/10.1002/sec.1693
48. Stehlé, D., Steinfeld, R.: Making NTRU as secure as worst-case problems over ideal lattices. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 27–47. Springer Heidelberg (2011). https://doi.org/10.1007/978-3-642-20465-4$_4$
49. Stehlé, D., Steinfeld, R.: Making NTRUEncrypt and NTRUSign as secure as standard worst-case problems over ideal lattices. Cryptology ePrint Archive (2013), `https://eprint.iacr.org/2013/004`

50. Steinfeld, R.: NTRU cryptosystem: Recent developments and emerging mathematical problems in finite polynomial rings. In: Niederreiter, H., Ostafe, A., Panario, D., Winterhof, A. (eds.) Algebraic Curves and Finite Fields, pp. 179–212. De Gruyter (2014). https://doi.org/doi:10.1515/9783110317916.179
51. Thakur, K., Tripathi, B.: KTRU: NTRU over the Kleinian integers. J. of International Academy of Physical Sciences **20**(03), 177–183 (2016)
52. Thakur, K., Tripathi, B.P.: STRU: A non alternative and multidimensional public key cryptosystem. GJPAM **13**, 1447–1464 (2017), `http://www.ripublication.com/Volume/gjpamv13n5.htm`
53. Truman, K.: Analysis and Extension of Non-Commutative NTRU. Ph.D. thesis (2007), `https://drum.lib.umd.edu/handle/1903/7344`
54. Vats, N.: NNRU, a noncommutative analogue of NTRU. CoRR **abs/0902.1891** (2009), `http://arxiv.org/abs/0902.1891`
55. Vehkalahti, R., Hollanti, C., Lahtonen, J., Ranto, K.: On the densest mimo lattices from cyclic division algebras. IEEE Trans. Inf. Theory **55**(8), 3751–3780 (2009). https://doi.org/10.1109/TIT.2009.2023713
56. Voight, J.: Quaternion Algebras. Graduate Texts in Mathematics, Springer International Publishing (2021)
57. Wang, Y., Wang, M.: Provably secure NTRUEncrypt over any cyclotomic field. In: Cid, C., Jr., M.J.J. (eds.) SAC 2018. LNCS, vol. 11349, pp. 391–417. Springer (2018). https://doi.org/10.1007/978-3-030-10970-$7_1$8
58. Yasuda, T., Anada, H., Sakurai, K.: Application of NTRU using group rings to partial decryption technique. In: Yung, M., Zhang, J., Yang, Z. (eds.) INTRUST 2015. LNCS, vol. 9565, pp. 203–213. Springer (2016). https://doi.org/10.1007/978-3-319-31550-$8_1$3