Algebraic Equipage for Learning with Errors in Cyclic Division Algebras*

Cong Ling and Andrew Mendelsohn**

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

Abstract. In *Noncommutative Ring Learning With Errors From Cyclic Algebras*, a variant of Learning with Errors from cyclic division algebras, dubbed 'Cyclic LWE', was developed, and security reductions similar to those known for the ring and module case were given, as well as a Regev-style encryption scheme. In this work, we make a number of improvements to that work: namely, we describe methods to increase the number of cryptographically useful division algebras, demonstrate the hardness of CLWE from ideal lattices obtained from non-maximal orders, and study Learning with Rounding in cyclic division algebras.

Keywords: CLWE · Structured LWE · Cyclic Division Algebras

1 Introduction

With the advent of quantum computation[1], new avenues of cryptographic attack have arisen, such as cryptanalysis using the famed 'Shor's Algorithm' to factor integers in polynomial time [36]. The cryptographic community has responded to these developments by searching for quantum-resistant protocols: one of the most prominent of these efforts relies on the hardness of solving lattice-based problems, which appear no easier to solve using quantum than classical algorithms.

One of the most popular of these problems is the Learning with Errors (LWE) problem, which in its simplest form (informally) runs as follows: take a secret vector of integers modulo a prime, $s \in \mathbb{Z}_q^n$, a uniformly random vector $a \leftarrow \mathbb{Z}_q^n$, and an error $e \leftarrow \mathbb{Z}_q$ chosen according to some distribution χ, and output the pair $(a, \langle a, s\rangle + e \bmod q)$. There are two problems to solve: firstly, the *search* LWE problem is to recover s from a number of LWE samples; secondly, the *decision* LWE problem is to decide whether m independent samples are chosen either according the LWE distribution, or uniformly at random, from $\mathbb{Z}_q^n \times \mathbb{Z}_q$. In [32], Regev gave a reduction from approximate GapSVP to decision LWE, guaranteeing it a certain level of hardness, for certain parameters.

The LWE problem was later defined for rings (RLWE) [22] and modules

* This work was supported in part by the Engineering and Physical Sciences Research Council (EPSRC) under Grant Nos. EP/X037010/1 and EP/Y037243/1.

** Corresponding author.

[1] For background, see [23].

(MLWE) [20], amongst a wide range of other algebraic structures such as orders [8] and group rings [10]. In the ring case, the simplest form of an RLWE sample is defined as follows: given a number field K with ring of integers $\mathcal{O}_K$, a prime q, and a secret $s \in \mathcal{O}_{K_q}$, where $\mathcal{O}_{K_q}$ denotes the set of equivalence classes of $\mathcal{O}_K$ modulo q, sample $a \leftarrow \mathcal{O}_{K_q}$ uniformly at random and $e \leftarrow \mathcal{O}_{K_q}$ according to some error distribution, and output $(a, a \cdot s + e) \in \mathcal{O}_{K_q} \times \mathcal{O}_{K_q}$. This, and the other forms of LWE mentioned above, are all forms of *structured* LWE.

To see this, consider the example of $K = \mathbb{Q}[x]/(x^n + 1)$ for power-of-two n, and fixing the usual basis, writing $a = \sum_i a_i x^i$, $s = \sum_i s_i x^i$ and taking a prime q, one can write $a \cdot s + e \bmod q \in \mathcal{O}_{K_q}$ over the integers as

$$\begin{pmatrix} a_0 & -a_{n-1} & \cdots & -a_1 \\ a_1 & a_0 & \dots & -a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & \dots & a_0 \end{pmatrix} \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix} + \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{pmatrix} \bmod q$$

The motivation to design structured forms of LWE arises due to the relative inefficiency of general matrix multiplication, and the large public keys of LWE-based schemes. By choosing particular algebraic structures from which to sample elements for LWE-style instances, one can obtain greater efficiency, albeit often as a tradeoff with the security level of the underlying 'hard problem'. For example, the structure of RLWE transposes the matrix-vector multiplications into polynomial multiplications, which can be computed with greater efficiency. In addition, the structure of such schemes allows one to store fewer bits of information to reconstruct public keys, as will be seen below. Differently structured LWE variants offer differing balances of security and efficiency; particularly desirable would be a scheme with the efficiency of RLWE and the security of MLWE.

In [15], a novel noncommutative LWE construction was created, relying on the structure of cyclic division algebras (CDAs), called 'Cyclic LWE', or CLWE. This work uses the concept of an *order* in an algebra, that is, subrings which are also lattices. Analogously to the commutative ring case, ideals in orders form lattices, and these similarities between orders in CDAs and rings of integers in number fields were used to develop computationally-intractable lattice problems from maximal order ideals, and give a security reduction establishing hardness results for search and decision CLWE from such problems. In addition, a Regev-style encryption scheme was given. Since the the domain over which RLWE is implemented is the maximal order of a number field, RLWE is a special case of CLWE, obtained when the algebra is (trivially) a number field; and a single sample of CLWE is loosely equivalent to multiple correlated MLWE samples.

Our Results In this paper we continue the development of CLWE, that is, LWE from *cyclic division algebras*. Our contributions are four-fold:

1. We discuss the construction of CDAs, focusing on the creation of *non-norm elements*. These elements are fundamental to constructing cryptographically-secure CDAs for CLWE; see [15, Section 3.2] for an attack on CLWE in non-division cyclic algebras. We generalize a theorem from [15] to increase the

number of valid CDAs for CLWE, and give concrete examples of such algebras. In particular, we prove that one can construct CDAs from cyclotomic fields of arbitrary conductor, rather than just prime-power conductor.
2. We discuss obtaining appropriate prime moduli for CLWE. Recall that for RLWE, one chooses a prime completely split in a given number field; for CLWE, one has further constraints on the choice of modulus - we often want the prime to split in an extension also. We provide methods for finding such primes, and give examples of algebras together with appropriate moduli that can be used for CLWE.
3. We analyse the security of CLWE instantiated in suborders of the (so-called) natural order, proving a reduction from problems on ideal lattices, for invertible ideals obtained from such suborders. We then adapt methods from [31] to relax the invertibility condition on the ideals used.
4. We generalize Learning with Rounding (LWR) to cyclic algebras, named Cyclic LWR (CLWR). We adapt the security proof of [6] to hold in this setting, establishing a link between CLWE and CLWR. Our proof holds in the case of power-of-two degree with super-polynomial modulus; the chief difficulty is the analysis of the statistical distance of the relevant distributions. Moving to a Learning with Rounding-based scheme can increase efficiency, since one no longer has to sample an error term.

We present this suite of algebraic results as a step toward taking CLWE from cryptographic theory to reality, allowing greater flexibility of parameter choices for the algebras and orders used, facilitating the further development of CLWE.

Previous Work Cyclic divison algebras have been used extensively in coding theory: they were introduced by Sethuraman et al. [35] and developed by Lahtonen [17] and Oggier [30] (amongst others). The appeal of such an algebraic object was the ability of coding theorists to use them to construct so-called 'perfect codes', exploiting properties of the discriminant and determinant of the algebra, which proved useful when applied to multiple-antenna communication.

Regarding the literature on structured LWE, samples of M/RLWE encode multiple samples of LWE by fixing a $\mathbb{Z}$-basis and viewing ring multiplication as matrix-vector multiplication of the matrices obtained with respect to the fixed basis. In addition to these, polynomial LWE [37], order LWE [8], group ring LWE [10] and others are alternative forms of structuring LWE.

Paper Organisation After preliminaries, in section 3 we discuss non-norm elements, in section 4 prime moduli for CLWE, in section 5 give a reduction from ideals in non-maximal orders, and in section 6 study CLWR.

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 $k = n$.

The above notion can also be generalised to vector spaces over fields. Let V be a finite-dimensional vector space over a number field K with ring of integers $\mathcal{O}_K$. An $\mathcal{O}_K$-*lattice* in V is a subspace $\mathcal{L} \subset V$ such that $\mathcal{L}$ is a finitely-generated $\mathcal{O}_K$-module. Equivalently, $\mathcal{L}$ is a finitely-generated torsion-free $\mathcal{O}_K$-module. $\mathcal{L}$ is *full* if it contains a K-basis of V, so $V = K \cdot \mathcal{L}$. Taking a basis B of V, the $\mathcal{O}_K$-linear span of B is a full lattice.

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 $\mathcal{L}$.

Informally, examples of lattice problems are finding a shortest vector in the lattice (SVP), finding the closest vector to a given point (CVP), deciding whether the shortest vector has size less than one or greater than a parameter β (GapSVP), or outputting n independent sufficiently short vectors (SIVP), when one knows only a certain basis of the lattice. These are believed to be hard and such problems have been used to ground the security of problems that are capable of being used to construct quantum-resistant cryptographic schemes. Such schemes are often based off approximate variants of the above problems; for example, approx-SVP is the problem of finding a lattice vector of norm at most a factor of ξ larger than the shortest vector, for some specified value $\xi > 0$.

Discrete Gaussians For $\mathbb{R}^n$ equipped with (Euclidean) norm $\|\cdot\|$, and $r > 0$, we define the *Gaussian function* $\rho_r : \mathbb{R}^n \to (0, 1]$ by $\rho_r(\boldsymbol{x}) = \exp\left(-\pi \|\boldsymbol{x}\| / r^2\right)$.

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 $D_{\mathcal{L},r}$, defined over a lattice $\mathcal{L}$, outputs $\mathbf{x}$ with probability $\frac{\rho_r(\mathbf{x})}{\rho_r(\mathcal{L})}$ 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 $\rho_{1/r}\left(\mathcal{L}^* / \{\mathbf{0}\}\right) \leq \varepsilon$.

The *statistical distance* between two distributions D, D' over a discrete set S is defined $\Delta(D, D') = \frac{1}{2} \sum_{x \in S} |D(x) - D'(x)|$. We may denote the uniform distribution over S by $U(S)$. The following is a useful lemma:

Lemma 1. *[26, 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, $\rho_r(\mathcal{L} + \boldsymbol{x}) \in \left[\frac{1-\varepsilon}{1+\varepsilon}, 1\right] \cdot \rho_r(\mathcal{L})$.*

Algebraic Number Fields Let K be a number field and $\mathcal{O}_K$ its ring of integers. A Dedekind domain is an integrally closed, Noetherian domain in which

every prime ideal is maximal. In a Dedekind domain every fractional ideal has a unique factorization into prime ideals. Recall $\mathcal{O}_K$ is a Dedekind domain.

Let L be a finite extension of K, $\mathfrak{q}$ a prime ideal of $\mathcal{O}_L$, and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$. We say $\mathfrak{q}$ lies above $\mathfrak{p}$ if $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$. Moreover, $\mathfrak{p}\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$, which is a Dedekind domain, so $\mathfrak{p}\mathcal{O}_L$ has a unique factorization into prime ideals:

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i} = \mathfrak{q}_1^{e_1} ... \mathfrak{q}_g^{e_g}, \tag{1}$$

for $\mathfrak{q}_i \subset \mathcal{O}_L$ prime all lying above $\mathfrak{p}$. We call $e_{\mathfrak{q}_i|\mathfrak{p}} = e_i$ the *ramification index* of $\mathfrak{q}_i$ over $\mathfrak{p}$, and $f_{\mathfrak{q}_i|\mathfrak{p}} = f_i = \left[\mathcal{O}_L/\mathfrak{q}_i : \mathcal{O}_K/\mathfrak{p}\right]$ the *inertial degree* of $\mathfrak{p}$ in $\mathfrak{q}_i$. Now suppose L/K is Galois. Then all the e_i and f_i are equal and $\mathrm{Gal}(L/K)$ acts transitively on the set of primes lying above any fixed prime of $\mathcal{O}_K$, and $\mathcal{O}_L/\mathfrak{q}_i$ and $\mathcal{O}_K/\mathfrak{p}$ are finite fields.

Proposition 1. *The ramification index and inertial degree are multiplicative over towers of number fields; i.e. for ideals $\boldsymbol{Q}/\mathfrak{q}/\boldsymbol{q}$ in $\mathcal{O}_M/\mathcal{O}_L/\mathcal{O}_K$, $e_{\boldsymbol{Q}|\boldsymbol{q}} = e_{\boldsymbol{Q}|\mathfrak{q}} e_{\mathfrak{q}|\boldsymbol{q}}$ and $f_{\boldsymbol{Q}|\boldsymbol{q}} = f_{\boldsymbol{Q}|\mathfrak{q}} f_{\mathfrak{q}|\boldsymbol{q}}$.*

Definition 3. An ideal $\mathfrak{p} \subset \mathcal{O}_K$ *ramifies* in L if $e > 1$, and is *unramified* if $e = 1$. Alternatively, we say that L/K is unramified at $\mathfrak{p}$. If $e = 1$ and $f = 1$, $\mathfrak{p}$ *splits completely*. If $f = g = 1$, then $e = [L : K]$ and $\mathfrak{p}$ is *totally ramified*.

Primes in Cyclotomic Fields Here we consider the ramification of primes p in cyclotomic fields of the form $\mathbb{Q}(\zeta_n)$, for some primitive nth root of unity ζ_n.

Case 1: p does not divide n. Then

Proposition 2. *[25, Proposition 7.7] Let $K = \mathbb{Q}(\zeta_n)$. Let p be a rational prime, $\gcd(p, n) = 1$ and f be the lowest integer such that $p^f \equiv 1$ mod n. Then we have $f = f_{\mathfrak{p}|p}$ for any prime ideal $\mathfrak{p}$ of K lying above p.*

Let p be a prime not dividing n. Then p is unramified in $\mathbb{Q}(\zeta_n)$, since the only ramified primes are those dividing the discriminant, whose prime factors are precisely those of n. This is equivalent to saying that $e = 1$. So $fg = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, where ϕ is the Euler totient function, and one can use the above proposition to find f, and hence g.

Case 2: p divides n. Write $n = p^a \cdot n'$, where $\gcd(p, n') = 1$. Then f is the lowest positive integer such that $p^f \equiv 1 \bmod n'$. Also, $e = \phi(p^a)$, and $g = \phi(n')/f$ ([38]).

We will need Dirichlet's theorem on arithmetic progressions:

Theorem 1. *Let $a, n \in \mathbb{Z}_{\geq 1}$ and $\gcd(a, n) = 1$. Then the natural density of primes p such that $p \equiv a$ mod n in the set of all primes of $\mathbb{Z}$ is $1/\phi(n)$.*

Example: Take q such that p^a is the highest power of p that divides $q-1$. Then $q \equiv 1 \bmod p^a$, so by the theorem there are infinitely many such q.

The following map between fields will be useful:

Definition 4. Let L be a number field of degree n over K. Fix a basis of L/K. Multiplication by an element α of L is a linear map, so has an associated matrix m_α. The *norm* is defined as the map $N_{L/K} : L \to K$, given by $\alpha \mapsto \det(m_\alpha)$. Equivalently, for Galois extensions, $N_{L/K}(\alpha) = \prod_i^n \sigma_i(\alpha)$, where $\sigma_i \in \mathrm{Gal}(L/K)$.

Local Fields We will also need some p-adic theory. For more background information, the interested reader is directed to [34].

Definition 5. A field equipped with a metric is complete if every Cauchy sequence of elements converges. A valuation on a field K is a homomorphism $\nu : K \to \mathbb{R}$ such that $\nu(xy) = \nu(x) + \nu(y)$, $\nu(x) = \infty$ if and only if $x = 0$, and $\nu(x + y) \geq \min(\nu(a), \nu(b))$. If the image of ν is $\mathbb{Z}$ then ν is said to be a *discrete valuation*. If ring R has field of fractions K, and K is equipped with a discrete valuation such that $R = \{x : x \in K \text{ and } \nu(x) \geq 0\}$, then we call R a *discrete valuation ring* (DVR).

DVRs are PIDs and have precisely one proper maximal ideal.

The p-adic valuation: Let $p \in \mathbb{Z}$. Define $\nu_p(x) = r$, for $x = p^r a$ with $a = \frac{b}{c}$ with $\gcd(p, b) = \gcd(p, c) = 1$. Likewise for a Dedekind domain A with field of fractions K and a prime ideal $\mathfrak{p}$, $\nu_\mathfrak{p}(x) := r$, for $(x) = \mathfrak{p}^r \mathbf{b}\mathbf{c}^{-1}$ where $\mathbf{b}, \mathbf{c}$ are fractional ideals coprime to $\mathfrak{p}$. This valuation is discrete. The completion of $\mathbb{Q}$ with respect to ν_p is denoted $\mathbb{Q}_p$ and called the rational field of p-adic numbers.

Definition 6. A *local* field is a field K that is complete with respect to a discrete valuation, and has finite residue field. Denote the ramification index of such a field's unique prime in a finite extension L by $e_{L/K}$.

Thus $\mathbb{Q}_p$ is an example of a local field. We can generate further examples as follows: let K be a number field, and $\mathfrak{q}$ a prime ideal of $\mathcal{O}_K$ lying above q. Denote the completion of K by $\mathfrak{q}$ by $K_\mathfrak{q}$. This is also a local field, and is a finite extension of $\mathbb{Q}_q$. The following gives important properties of such fields:

Proposition 3. *Let K be a local field.*

(i) *$\mathcal{O}_K$ is a discrete valuation ring with a unique proper prime (maximal) ideal.*
(ii) *A generator, π, of the maximal ideal, $\mathfrak{m}$, is called a uniformizer. This element is irreducible.*
(iii) *The group of units of $\mathcal{O}_K$ is denoted $\mathcal{O}_K^\times = U$. The nth unit group is defined $U^n = \{u \in \mathcal{O}_K^\times : u \equiv 1 \ mod\ \mathfrak{m}^n\}$. We have $U/U^n = \left(\mathcal{O}_K/\mathfrak{m}^n\right)^\times$.*

Definition 7. We say an extension of local fields L/K is *tamely* ramified if $char(\bar{K}) \nmid e_{L/K}$, where $\bar{K}$ is the residue field of K.

Proposition 4. *[28, Chapter 2, Proposition 5.3] Let $K_\mathfrak{q}$ be as above. Then we have $K_\mathfrak{q}^\times \cong \mu_{q-1} \times \langle \pi_\mathfrak{q} \rangle \times U_\mathfrak{q}^1$, where μ_{q-1} is a cyclic group of order $q - 1$, $\pi_\mathfrak{q}$ is a uniformizer of $K_\mathfrak{q}$, and $U_\mathfrak{q}^1$ is the first unit group of $K_\mathfrak{q}$.*

Theorem 2 (Hasse Norm Theorem [16]). *Let L/K be a cyclic extension of number fields. A nonzero element of K is a local norm at all primes $\mathfrak{p} \in L$ lying over $p \in K$, for all $p \in K$, if and only if it is a norm of an element in L.*

Theorem 3 (Local Reciprocity Map [13]). *Let $\mathfrak{Q}$ be a prime ideal of $\mathcal{O}_L$ and $\mathfrak{q}$ be a prime ideal of $\mathcal{O}_K$, both lying above q, so $L_{\mathfrak{Q}}/K_{\mathfrak{q}}$ is a finite abelian extension of local fields. Then there is an isomorphism*

$$\Theta : K_{\mathfrak{q}}^{\times}/N_{L_{\mathfrak{Q}}/K_{\mathfrak{q}}}(L_{\mathfrak{Q}}^{\times}) \to \mathrm{Gal}(L_{\mathfrak{Q}}/K_{\mathfrak{q}}).$$

Orders An order $\mathcal{O}$ in a number field K is a subring which is also a lattice. The maximal order (with respect to inclusion) is the ring of integers, $\mathcal{O}_K$. The behaviour of ideals in orders is significantly determined by the *conductor ideal*:

Definition 8. The conductor of an order $\mathcal{O} \subset \mathcal{O}_K$ is defined

$$\mathfrak{c} = \mathfrak{c}_{\mathcal{O}} = \{x \in K : x\mathcal{O}_K \subset \mathcal{O}\}.$$

We need the following lemma on the behaviour of ideals in orders:

Lemma 2. *[11] Let $\mathcal{O}$ be an order in K with conductor $\mathfrak{c}$.*

1. *For each $\mathcal{O}_K$-ideal $\mathfrak{a}$ coprime to $\mathfrak{c}$, $\mathfrak{a} \cap \mathcal{O}$ is an $\mathcal{O}$-ideal coprime to $\mathfrak{c}$ and the natural ring homomorphism $\mathcal{O}/(\mathfrak{a} \cap \mathcal{O}) \to \mathcal{O}_K/\mathfrak{a}$ is an isomorphism.*
2. *For each $\mathcal{O}$-ideal $\mathfrak{b}$ that is coprime to $\mathfrak{c}$, $\mathfrak{b}\mathcal{O}_K$ is an $\mathcal{O}_K$-ideal coprime to $\mathfrak{c}$ and the natural ring homomorphism $\mathcal{O}/\mathfrak{b} \to \mathcal{O}_K/\mathfrak{b}\mathcal{O}_K$ is an isomorphism.*
3. *The nonzero ideals coprime to $\mathfrak{c}$ in $\mathcal{O}_K$ and in $\mathcal{O}$ are in bijection by $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ and $\mathfrak{b} \mapsto \mathfrak{b}\mathcal{O}_K$ and these bijections are multiplicative.*

2.1 Cyclic Division Algebras

Let L/K be a degree d extension of number fields with cyclic Galois group. This means that there is automorphism of L which generates $\mathrm{Gal}(L/K)$ - denote this element of the Galois group by θ. Consider the following direct sum:

$$\mathcal{A} = L \oplus uL \oplus ... \oplus u^{d-1}L,$$

where u is an auxiliary element satisfying 1) $u^d = \gamma$, where $\gamma \in K^{\times}$, and 2) for all $x \in L$, we have $xu = u\theta(x)$. $\mathcal{A}$ is a *cyclic algebra*, and property 2) gives it a non-commutative multiplication operation. To ensure every element of $\mathcal{A}$ has a multiplicative inverse, we require that γ is a *non-norm element*:

Definition 9. An element α of K is *non-norm* (or satisfies the *non-norm condition*) if there does not exist an element $x \in L$ such that $\alpha^i = N_{L/K}(x)$, for $0 < i < [L : K]$. Equivalently, α is non-norm if $\alpha \notin N_{L/K}(N^{\times})$ for all proper intermediate subfields $K \subset N \subset L$ [29].

Proposition 5. *[1, Theorem 11.12, p. 184] The cyclic algebra $\mathcal{A}$ is a division algebra if and only if γ is a non-norm element.*

Then $\mathcal{A}$ is called a *cyclic division algebra* (CDA) with non-norm element γ. We denote this algebra by $\mathcal{A} = (L/K, \theta, \gamma)$. In this scenario, $\mathcal{A}$ is a K-algebra. We note that if γ is a norm, $\mathcal{A}$ is isomorphic to a matrix algebra over K.

(Maximal) Orders Here we discuss integral structures lying within CDAs. The chief references are [33] and [19]. We denote a general cyclic K-algebra by A, and the CDA defined above by $\mathcal{A}$.

Definition 10. An $\mathcal{O}_K$-*order* in A is a full $\mathcal{O}_K$-lattice $\mathcal{O}$ in A which is a subring of A. Thus a $\mathbb{Z}$-*order* $\mathcal{O}$ in an algebra A is a finitely generated $\mathbb{Z}-$module that contains a $\mathbb{Q}-$basis of A, and is also a unital subring of A. If a set is called an order, it is understood to be an $\mathcal{O}_K$-order. Every order in A contains $\mathcal{O}_K$.

In any cyclic K-algebra a maximal order always exists (with respect to inclusion), and every order is contained within a maximal order. We primarily use the following order of $(L/K, \theta, \gamma)$, where $\gamma \in \mathcal{O}_K$, which we call the *natural order*:

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

When γ is a unit, it is possible that the natural order is also maximal, i.e. that Λ is not contained in any other non-trivial order. When $K = \mathbb{Q}(\zeta_n)$ and $\gamma = \zeta_n$, for n a prime power, Λ was shown to be maximal in [15].

Definition 11. Let $\mathcal{L}$ be a full $\mathcal{O}_K$-lattice in A. The *left order* of $\mathcal{L}$ is defined

$$\mathcal{O}_l(\mathcal{L}) = \{a \in A : a\mathcal{L} \subset \mathcal{L}\}.$$

The right order is defined analogously. They are both $\mathcal{O}_K$-orders in A. We note the following properties:

1. If $\mathcal{O}$ is an order, then $\mathcal{O}_l(\mathcal{O}) = \mathcal{O}_r(\mathcal{O}) = \mathcal{O}$.
2. If $\mathcal{L} \subset \mathcal{O}$ for some lattice $\mathcal{L}$ and order $\mathcal{O}$, then $\mathcal{O} \subset \mathcal{O}_l(\mathcal{L})$.

If $\mathcal{I}$ and $\mathcal{J}$ are full $\mathcal{O}_K$-lattices in A, $\mathcal{I}\mathcal{J} = \left\{\sum_{i=1}^{j} x_i y_i : x_i \in \mathcal{I}, y_i \in \mathcal{J}, j \in \mathbb{N}\right\}$ is a full $\mathcal{O}_K$-lattice, and we say $\mathcal{I}\mathcal{J}$ is a *proper* product if $\mathcal{O}_r(\mathcal{I}) = \mathcal{O}_l(\mathcal{J})$.

Ideals in Maximal Orders We will see how the ideal theory of orders changes depending on whether a given order is maximal or not. The theory in the case of maximal orders is much better behaved than for non-maximal orders.

Definition 12. Let $\mathcal{O}$ be an order in A. A *left integral ideal* in $\mathcal{O}$ is an additive subgroup $\mathcal{I}$ such that $\mathcal{O}\mathcal{I} \subset \mathcal{I}$. A *left fractional ideal* is a subset of the form $\lambda\mathcal{I}$, for some left integral ideal $\mathcal{I}$ and $\lambda \in \mathcal{O}_K \setminus \{0\}$. Right ideals may be defined analogously, and an ideal which is both left and right is called *two-sided*. Every integral ideal is a fractional ideal. An ideal in $\mathcal{O}$ may be called an $\mathcal{O}$-ideal.

For any lattice $\mathcal{L}$, $\mathcal{L}$ is a left $\mathcal{O}_l(\mathcal{L})$-ideal and a right $\mathcal{O}_r(\mathcal{L})$-ideal, and the left and right orders of $\mathcal{L}$ are the largest orders satisfying this property. Let $\mathcal{I}$ be a left $\mathcal{O}$-ideal. Then it can be seen that $\mathcal{I}$ is two-sided if and only if $\mathcal{O} \subset \mathcal{O}_r(\mathcal{I})$. When $\mathcal{O}$ is maximal, this is equivalent to $\mathcal{O}_l(\mathcal{I}) = \mathcal{O}_r(\mathcal{I})$. We say an ideal is *full* if it is full as a lattice, and it turns out any ideal in an order of a division algebra is full. Following [19], we denote by $\mathrm{Frac}_2(\mathcal{O})$ the set of full two-sided $\mathcal{O}$-ideals.

The Case of Two-sided Ideals In the following, $\mathcal{I}$ and $\mathcal{J}$ will be full $\mathcal{O}_K$-lattices. Since the product of left $\mathcal{O}$-ideals is a left $\mathcal{O}$-ideal, and since $\mathcal{O}_l(\mathcal{I}\mathcal{J}) \supset \mathcal{O}_l(\mathcal{I})$, $\mathcal{O}_r(\mathcal{I}\mathcal{J}) \supset \mathcal{O}_r(\mathcal{J})$, two-sided ideals are closed under multiplication.

Definition 13. Define the *inverse of* $\mathcal{I}$ to be $\mathcal{I}^{-1} = \{\alpha \in A : \mathcal{I}\alpha\mathcal{I} \subset \mathcal{I}\}$.

Proposition 6. *[33, (22.6), (22.7), (23.3)]* $\mathcal{I}^{-1}$ *is a full* $\mathcal{O}_K$*-lattice in* A*, and*

$$\mathcal{O}_l\left(\mathcal{I}^{-1}\right) \supset \mathcal{O}_r(\mathcal{I}), \quad \mathcal{O}_r\left(\mathcal{I}^{-1}\right) \supset \mathcal{O}_l(\mathcal{I}), \quad \mathcal{I}\mathcal{I}^{-1} \subset \mathcal{O}_l(\mathcal{I}), \text{ and } \mathcal{I}^{-1}\mathcal{I} \subset \mathcal{O}_r(\mathcal{I}).$$

If $\mathcal{I}$ *is a two-sided ideal of a maximal order* $\mathcal{O}$, $\mathcal{I}^{-1}$ *is also an* $\mathcal{O}$*-ideal such that* $\mathcal{I}\mathcal{I}^{-1} = \mathcal{I}^{-1}\mathcal{I} = \mathcal{O}$.

Thus in a maximal order the full two-sided ideals have unique inverses, with identity element being the order itself.

As usual, if $\mathcal{I}, \mathcal{J}$ are $\mathcal{O}$-ideals such that $\mathcal{I} \supset \mathcal{J}$, we say $\mathcal{I}$ *divides* $\mathcal{J}$ and write $\mathcal{I} \mid \mathcal{J}$. If $\mathfrak{P}$ is a two-sided ideal in $\mathcal{O}$, we say $\mathfrak{P}$ is *prime* if $\mathfrak{P} \mid \mathcal{I}\mathcal{J}$ implies $\mathfrak{P} \mid \mathcal{I}$ or $\mathfrak{P} \mid \mathcal{J}$ for any two-sided ideals $\mathcal{I}, \mathcal{J}$. In CDAs the prime ideals perform a similar role as in number fields; we have the following theorem:

Theorem 4. *[33, Theorem 22.10] Suppose* $\mathcal{O}$ *is a maximal* $\mathcal{O}_K$*-order in* A*. Then* $Frac_2(\mathcal{O})$ *is an abelian group with respect to multiplication, and any proper ideal factors into a product of powers of prime ideals in a unique way.*

This theorem does not hold in the non-maximal order case, although ideal multiplication remains commutative. The theorem also does not hold for one-sided ideals: while the product of two one-sided ideals is again a one-sided ideal, the inverse of a one-sided $\mathcal{O}$-ideal is not in general an $\mathcal{O}$-ideal, even if $\mathcal{O}$ is maximal.

Finally, we record an important property of prime ideals of maximal orders of central simple K-algebras:

Proposition 7. *[33, Theorem 32.1] The prime ideals of a maximal order coincide with its maximal two-sided ideals. There is a bijective correspondence between the nonzero prime ideals* $\mathfrak{p} \subset \mathcal{O}_K$ *and the prime ideals* $\mathfrak{P} \subset \mathcal{O}$ *such that* $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$*. Moreover, we have* $\mathfrak{p}\mathcal{O} = \mathfrak{P}^{e_\mathfrak{p}}$ *for some integer* $e_\mathfrak{p} \geq 1$.

The Case of One-Sided Ideals We now develop the one-sided ideal theory. In the following, $\mathcal{I}$ will be a full $\mathcal{O}_K$-lattice. The product of two left $\mathcal{O}$-ideals is again a left $\mathcal{O}$-ideal, and $\mathcal{O}_l(\mathcal{I}\mathcal{J}) \supset \mathcal{O}_l(\mathcal{I})$ and $\mathcal{O}_r(\mathcal{I}\mathcal{J}) \supset \mathcal{O}_r(\mathcal{J})$. So we have closure under multiplication of left (or right) ideals in a fixed order.

The following proposition is a one-sided analogue of Proposition 6.

Proposition 8. *$\mathcal{I}^{-1}$ is a full $\mathcal{O}_K$ lattice in A. We have $\mathcal{O}_l\left(\mathcal{I}^{-1}\right) \supset \mathcal{O}_r(\mathcal{I})$, $\mathcal{O}_r\left(\mathcal{I}^{-1}\right) \supset \mathcal{O}_l(\mathcal{I})$, $\mathcal{I}\mathcal{I}^{-1} \subset \mathcal{O}_l(\mathcal{I})$, and $\mathcal{I}^{-1}\mathcal{I} \subset \mathcal{O}_r(\mathcal{I})$.*

Definition 14. Say a lattice $\mathcal{I}$ is *left invertible* if $\mathcal{I}\mathcal{I}^{-1} \subset \mathcal{O}_l(\mathcal{I})$. Right invertibility is defined similarly, and for one-sided ideals one can replace lattice with ideal in the definition. In general, left and right invertibility are not equivalent.

Definition 15. An ideal $\mathcal{I}$ of a maximal order is called *normal*. If $\mathcal{I}$ is normal, $\mathcal{I}$ is integral if it is integral for its left order.

Proposition 9. *[33, §21.2, §22.9] Let $\mathcal{I}$ be a full $\mathcal{O}_K$-lattice in A. Then $\mathcal{O}_l(\mathcal{I})$ is a maximal order if and only if $\mathcal{O}_r(\mathcal{I})$ is. If $\mathcal{I}$ is normal with left order $\mathcal{O}$ and right order $\mathcal{O}'$, then $\mathcal{I}$ is integral as a left $\mathcal{O}$-ideal if and only if it is integral as a right $\mathcal{O}'$-ideal, i.e., $\mathcal{I} \subset \mathcal{O}$ if and only if $\mathcal{O} \subset \mathcal{O}'$.*

Lemma 3. *[33, Theorem 22.15] Let $\mathfrak{m}$ be a maximal left ideal of a maximal order $\mathcal{O}$. Then $\mathfrak{P} = \{\alpha \in \mathcal{O} : \alpha\mathcal{O} \subset \mathfrak{m}\}$ is a prime ideal of $\mathcal{O}$.*

The lemma means that each maximal one-sided ideal $\mathfrak{m}$ of a maximal order has an unique associated prime ideal $\mathfrak{P}$. While the above results are insufficient to form a group on one-sided ideals, one can describe the *Brandt groupoid* instead, which is the set of normal ideals of A with multiplication restricted to proper products (we do not expand on this here). We make the following observations for $\mathcal{I}$ with $\mathcal{O} = \mathcal{O}_l(\mathcal{I})$ and $\mathcal{O}' = \mathcal{O}_r(\mathcal{I})$: if $\mathcal{J} \subset \mathcal{O}$ is two-sided, then $\mathcal{J}\mathcal{I}$ is a right $\mathcal{O}'$-ideal, $\mathcal{I}^{-1}\mathcal{J}$ is a left $\mathcal{O}'$-ideal, and $\mathcal{I}^{-1}\mathcal{J}\mathcal{I}$ is a two-sided $\mathcal{O}'$-ideal.

Quotients of Lattices We now develop useful ideal-theoretic notions for non-maximal orders, generalising lemmas from [31, Section 2] for use in Section 5.

Definition 16. Let $\mathcal{L}, \mathcal{L}' \subset \mathcal{A}$ be lattices. Define the 'lattice quotient'

$$(\mathcal{L} : \mathcal{L}')_l = \{x \in \mathcal{A} : x\mathcal{L}' \subset \mathcal{L}\} \text{ and } (\mathcal{L} : \mathcal{L}')_r = \{x \in \mathcal{A} : \mathcal{L}'x \subset \mathcal{L}\}.$$

Note that $\mathcal{O}_l(\mathcal{L}) = (\mathcal{L} : \mathcal{L})_l$ and $\mathcal{O}_r(\mathcal{L}) = (\mathcal{L} : \mathcal{L})_r$. Observe that the lattice quotient satisfies additive closure. Moreover, $\mathcal{I}\mathcal{L}' \subset \mathcal{L}$ if and only if $\mathcal{I} \subset (\mathcal{L} : \mathcal{L}')_l$, for sets $\mathcal{I} \subset \mathcal{A}$. Finally, we have $(\mathcal{L} : \mathcal{L}')_l(\mathcal{L}' : \mathcal{L}'')_l \subset (\mathcal{L} : \mathcal{L}'')_l$, since $(\mathcal{L} : \mathcal{L}')_l(\mathcal{L}' : \mathcal{L}'')_l\mathcal{L}'' \subset (\mathcal{L} : \mathcal{L}')_l\mathcal{L}' \subset \mathcal{L}$.

Lemma 4. *Let $\mathcal{O}$ be an order, and $\mathcal{I}, \mathcal{I}'$ be fractional two-sided $\mathcal{O}$-ideals such that $\mathcal{I}'$ is invertible. Then $(\mathcal{I} : \mathcal{I}')_l = \mathcal{I}\mathcal{I}'^{-1}$.*

Proof. $\mathcal{I}\mathcal{I}'^{-1}\mathcal{I}' = \mathcal{I} \Rightarrow \mathcal{I}\mathcal{I}'^{-1} \subset (\mathcal{I} : \mathcal{I}')_l$. Then $\mathcal{I} = \mathcal{I}\mathcal{I}'^{-1}\mathcal{I}' \subset (\mathcal{I} : \mathcal{I}')_l\mathcal{I}' \subset \mathcal{I}$. So $(\mathcal{I} : \mathcal{I}')_l \subset \mathcal{I}\mathcal{I}'^{-1}$. Thus $\mathcal{I}\mathcal{I}'^{-1} \subset (\mathcal{I} : \mathcal{I}')_l \subset \mathcal{I}\mathcal{I}'^{-1}$ gives the result. □

Lemma 5. *Let $\mathcal{L}, \mathcal{L}' \subset \mathcal{A}$ be lattices. Then $(\mathcal{L} : \mathcal{L}')_l = (\mathcal{L}'\mathcal{L}^\vee)^\vee$.*

Proof. Let $x \in \mathcal{A}$. We have $x \in (\mathcal{L}'\mathcal{L}^\vee)^\vee \iff \mathrm{Tr}(x\mathcal{L}'\mathcal{L}^\vee) \subset \mathbb{Z} \iff x\mathcal{L}' \subset \mathcal{L}^{\vee\vee} = \mathcal{L} \iff x \in (\mathcal{L} : \mathcal{L}')_l$. □

Lemma 6. *We have $\mathcal{O}_l(\mathcal{L}) \subset \mathcal{O}_l((\mathcal{L} : \mathcal{L}')_l)$ and $\mathcal{O}_l(\mathcal{L}') \subset \mathcal{O}_r((\mathcal{L} : \mathcal{L}')_l)$. Moreover, $(\mathcal{L} : \mathcal{L}')_l$ is a left ideal in $\mathcal{O}_l(\mathcal{L})$ and a right ideal in $\mathcal{O}_l(\mathcal{L}')$.*

Proof. For the latter statements: $\mathcal{O}_l(\mathcal{L})(\mathcal{L} : \mathcal{L}')_l = (\mathcal{L} : \mathcal{L})_l(\mathcal{L} : \mathcal{L}')_l \subset (\mathcal{L} : \mathcal{L}')_l$, and $(\mathcal{L} : \mathcal{L}')_l\mathcal{O}_l(\mathcal{L}') = (\mathcal{L} : \mathcal{L}')_l(\mathcal{L}' : \mathcal{L}')_l \subset (\mathcal{L} : \mathcal{L}')_l$. For the former, note that the previous line implies that $\mathcal{O}_l(\mathcal{L}) \subset \mathcal{O}_l((\mathcal{L} : \mathcal{L}')_l)$ and $\mathcal{O}_l(\mathcal{L}') \subset \mathcal{O}_r((\mathcal{L} : \mathcal{L}')_l)$. □

Lemma 7. *Suppose $\mathcal{L} \subset \mathcal{L}'$ are lattices in $\mathcal{A}$. Then $(\mathcal{L} : \mathcal{L}')_l$ is integral in $\mathcal{O}_l(\mathcal{L})$ and in $\mathcal{O}_l(\mathcal{L}')$.*

Proof. $\mathcal{L} \subset \mathcal{L}' \Rightarrow 1 \in (\mathcal{L}' : \mathcal{L})_l$. Then $(\mathcal{L} : \mathcal{L}')_l \subset (\mathcal{L} : \mathcal{L}')_l(\mathcal{L}' : \mathcal{L})_l \subset (\mathcal{L} : \mathcal{L})_l = \mathcal{O}_l(\mathcal{L})$, and $(\mathcal{L} : \mathcal{L}')_l \subset (\mathcal{L}' : \mathcal{L})_l(\mathcal{L} : \mathcal{L}')_l \subset (\mathcal{L}' : \mathcal{L}')_l = \mathcal{O}_l(\mathcal{L}')$. □

If $\mathcal{O}$ is a non-maximal order contained in $\mathcal{O}'$, then $(\mathcal{O} : \mathcal{O}')_l$ is not an invertible left $\mathcal{O}$-ideal. For suppose there exists a (right) $\mathcal{O}$-ideal $\mathcal{I}$ such that $\mathcal{I}(\mathcal{O} : \mathcal{O}')_l = \mathcal{O}$. Then $\mathcal{O}' = \mathcal{O}\mathcal{O}' = \mathcal{I}(\mathcal{O} : \mathcal{O}')_l\mathcal{O}' = \mathcal{I}(\mathcal{O} : \mathcal{O}')_l = \mathcal{O}$, a contradiction.

Definition 17. The left 'pseudoinverse' of a two-sided $\mathcal{O}$-ideal $\mathcal{I}$ is $(\mathcal{O} : \mathcal{I})_l$.

We record two properties of pseudoinverses: first, if $\mathcal{I}$ is a two-sided ideal of $\mathcal{O}$, $(\mathcal{O} : \mathcal{I})_l$ is a two-sided ideal of $\mathcal{O}$. To see this, note is a left ideal by Lemma 6. Consider $x \in (\mathcal{O} : \mathcal{I})_l$ and $a \in \mathcal{O}$. Then $xa\mathcal{I} \subset x\mathcal{I} \subset \mathcal{O}$.

Second, if $\mathcal{I}$ is a two-sided invertible $\mathcal{O}$-ideal, by Lemma 4 $(\mathcal{O} : \mathcal{I})_l = \mathcal{I}^{-1}$.

Embedding CDAs into $\mathbb{R}^m$ Consider a CDA $\mathcal{A} = (L/K, \theta, \gamma)$ with $[L : K] = d$. 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 $x = \oplus_{i=0}^{d-1} u^i x_i \in \mathcal{A}$,

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

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). Since all the nd embeddings of L are obtained by extending the set of L-automorphisms $\{\alpha \circ \theta^i\}_{\alpha,i}$ to embeddings of L, 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 a lattice in $\mathbb{R}^{nd^2}$. When γ is a unit, this embedding is equivalent to extending the canonical (Minkowski) embedding of L coefficientwise to algebra elements. We then define three 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 $\phi(x)$, and finally we set $\|x\|_{2,\infty} = \max_{\alpha,j} \sqrt{\left(\sum_{i=0}^{d-1} |\alpha \circ \theta^j(x_i)|^2\right)}$. We may denote $\|\cdot\|_2$ by $\|\cdot\|$.

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

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

The codifferent ideal of Λ is $\Lambda^\vee$. We may denote $\Lambda/q\Lambda$ by Λ_q.

The CLWE Problem In [15], LWE was instantiated using the natural order inside a CDA. We first define the following distribution:

Definition 18 (The CLWE Distribution)**.** Let L/K be a Galois extension of number fields of dimension $[L:K]=d$, $[K:\mathbb{Q}]=n$ with cyclic Galois group generated by θ. Let $\mathcal{A}:=(L/K,\theta,\gamma)$ be a cyclic division algebra with element u such that $u^d=\gamma\in\mathcal{O}_K$. Let Λ be the natural order of $\mathcal{A}$. For an error distribution ψ over $\oplus_{i=0}^{d-1}u^iL_{\mathbb{R}}$, integer modulus $q\geq 2$, and a 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 $(a,b)=(a,(a\cdot s)/q+e \bmod \Lambda^\vee)\in\left(\Lambda_q,\oplus_{i=0}^{d-1}u^iL_{\mathbb{R}}/\Lambda^\vee\right)$.

The public value a has matrix representation $\phi(a)$, and to construct this matrix only the first column need be stored by a user. As for RLWE, via the matrix representation one can see that CLWE is a form of structured LWE. We now define search and decision problems, where Ψ is a family of error distributions.:

Definition 19. Let $\Pi_{q,s,\psi}$ be a CLWE distribution for parameters $q\geq 2, s\in\Lambda_q^\vee$, and error distribution $\psi\in\Psi$. The search CLWE problem, denoted $\mathrm{CLWE}_{q,s,\psi}$, is to recover s from a collection of independent samples from $\Pi_{q,s,\psi}$.

Definition 20. Let Υ be a distribution on a family of error distributions over $\bigoplus_{i=0}^{d-1}u^iL_{\mathbb{R}}$ and U_Λ the uniform distribution on $\left(\Lambda_q,\left(\bigoplus_{i=0}^{d-1}u^iL_{\mathbb{R}}\right)/\Lambda^\vee\right)$. The decision CLWE problem, $\mathrm{DCLWE}_{q,\Upsilon}$, is given a collection of independent samples from either $\Pi_{q,s,\psi}$ 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.

3 Non-Norm Elements for General Cyclotomic Fields

In [15], the authors used the work of [27] to construct CDAs containing nth roots of unity for prime-power n. Recall the method runs as follows: let $n=p^r$ for some prime p and $r\in\mathbb{N}$, and set $K=\mathbb{Q}(\zeta_n)$. Let $\ell=1 \bmod n$, $\ell\neq 1 \bmod pn$ be a prime, and set $M=\mathbb{Q}(\zeta_n,\zeta_\ell)=\mathbb{Q}(\zeta_{n\ell})$. One then fixes a subfield of degree d over K inside M by taking the fixed field of σ^d, where d divides n and $\mathrm{Gal}(M/K)=\langle\sigma\rangle$, and the resulting algebra $(L/K,\theta,\zeta_n)$ is division, where $\mathrm{Gal}(L/K)=\langle\theta\rangle$ - that is to say, ζ_n is non-norm. In this section, we extend this method to composite n. The main result of this section is the following theorem:

Theorem 5. *Let $n\in\mathbb{N}_{\geq 2}$. Set $K=\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity. Then there exist infinitely many cyclic Galois extensions L/K of degree n such that ζ_n satisfies the non-norm condition.*

Proof. Write $n=p_1^{e_1}...p_k^{e_k}$, for $p_1,...,p_k$ pairwise coprime. Pick $\ell\in\mathbb{Z}$ prime such that $p_1^{e_1}...p_k^{e_k}\mid\ell-1$, and such that e_i is the highest power of p_i such that this is true, for all i, so we have $\ell-1=p_1^{e_1}...p_k^{e_k}p_{k+1}^{e_{k+1}}...p_r^{e_r}$ for some primes $p_{k+1},...,p_r$ distinct from the p_j for $1\leq j\leq k$, and integers $e_i\geq 1$. By Theorem 1, there are infinitely many such primes q. Note that $\gcd(n,\ell)=1$.

Now consider $M = K(\zeta_\ell) = \mathbb{Q}(\zeta_n, \zeta_\ell)$. We have $\mathrm{Gal}(M/K) \cong (\mathbb{Z}/\ell\mathbb{Z})^*$. Let σ be a generator of $\mathrm{Gal}(M/K)$. Then σ^n fixes an extension, denoted L, of degree n over K. We have $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(M/K)/\mathrm{Gal}(M/L)$, which implies that $\mathrm{Gal}(L/K)$ is also cyclic. We will use Theorem 2 to prove the result by localizing at a certain prime ideal. Let the prime ideal $\mathbf{Q}$ lie above $\mathfrak{Q}$ lie above $\mathfrak{q}$ lie above ℓ in the tower of fields $M/L/K/\mathbb{Q}$. Proposition 2 implies that the inertial degree $f_{\mathfrak{q}|\ell} = 1$. This is equivalent to $[\mathcal{O}_K/\mathfrak{q} : \mathbb{F}_\ell] = 1$.

Now, $\ell \mid n\ell$ exactly once, since $\gcd(\ell, n) = 1$. Then $f_{\mathbf{Q}|\ell}$ is the smallest f such that $\ell^f \equiv 1 \bmod n$. But $\ell \equiv 1 \bmod n$, so $f_{\mathbf{Q}|\ell} = 1$. The inertial degree is multiplicative, that is $f_{\mathbf{Q}|\ell} = f_{\mathbf{Q}|\mathfrak{q}} f_{\mathfrak{q}|\ell}$, so $f_{\mathbf{Q}|\mathfrak{q}} = 1$ also. We have found $f_{\mathbf{Q}|\mathfrak{q}}$ by considering the tower $M/K/\mathbb{Q}$; we now consider the tower $M/L/K$, which yields that $f_{\mathbf{Q}|\mathfrak{q}} = f_{\mathbf{Q}|\mathfrak{Q}} f_{\mathfrak{Q}|\mathfrak{q}}$. Hence $f_{\mathbf{Q}|\mathfrak{q}} = 1$ implies $f_{\mathfrak{Q}|\mathfrak{q}} = 1$ also.

Denote the completions of the fields L, K, and $\mathbb{Q}$ by the corresponding valuations by $L_\mathfrak{Q}$, $K_\mathfrak{q}$, and $\mathbb{Q}_\ell$ respectively. Then, since $g = 1$ in extensions of local fields, we combine this with the above discussion on the inertial degrees to conclude that $L_\mathfrak{Q}/K_\mathfrak{q}$ is totally ramified. Further, since the characteristic of the residue field of $K_\mathfrak{q}$ is ℓ, but total ramification of $L_\mathfrak{Q}/K_\mathfrak{q}$ means that the ramification index $e_{L_\mathfrak{Q}/K_\mathfrak{q}} = [L_\mathfrak{Q} : K_\mathfrak{q}] = n$, we obtain that $L_\mathfrak{Q}/K_\mathfrak{q}$ is tamely ramified. Using the local reciprocity map, we obtain $[K_\mathfrak{q}^\times : N_{L_\mathfrak{Q}/K_\mathfrak{q}}(L_\mathfrak{Q}^\times)] = |\mathrm{Gal}(L_\mathfrak{Q}/K_\mathfrak{q})| = [L_\mathfrak{Q} : K_\mathfrak{q}] = n$. Moreover, a standard result of local fields is that for a totally and tamely ramified finite extension of local number fields, $N_{L_\mathfrak{Q}/K_\mathfrak{q}}(L_\mathfrak{Q}^\times)$ contains a uniformizer $\pi_\mathfrak{q}$ of $K_\mathfrak{q}$, as well as $U_\mathfrak{q}^1$ (see [13, page 115]). Pulling together the above in conjunction with the local reciprocity map, we obtain the following commutative diagram:

$$\begin{array}{ccc} \mu_{\ell-1} & \xrightarrow{\quad f \quad} & \mathrm{Gal}(L_\mathfrak{Q}/K_\mathfrak{q}) \\ \Big\downarrow{\scriptstyle h} & \nearrow_{g} & \\ K_\mathfrak{q}^\times & & \end{array} \tag{2}$$

Here g is the homomorphism defined by the local reciprocity map, with kernel $N_{L_\mathfrak{Q}/K_\mathfrak{q}}(L_\mathfrak{Q}^\times)$ and image $\mathrm{Gal}(L_\mathfrak{Q}/K_\mathfrak{q}) \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times ... \times \mathbb{Z}/p_k^{e_k}\mathbb{Z}$, h is the inclusion of $\mu_{\ell-1}$ into $K_\mathfrak{q}^\times \cong \mu_{\ell-1} \times \langle \pi_\mathfrak{q} \rangle \times U_\mathfrak{q}^1$, and f is the natural surjection from the CRT decomposition of $\mu_{\ell-1} \cong \prod_{i=1}^r \mathbb{Z}/p_i^{e_i}\mathbb{Z}$ onto $\mathbb{Z}/p_1^{e_1}\mathbb{Z} \times ... \times \mathbb{Z}/p_k^{e_k}\mathbb{Z}$.

We have $f = g \circ h$, where f, g and h are homomorphisms. Since f maps non-identity elements of order dividing n non-trivially, by commutativity of the diagram g also maps such elements non-trivially, so they are not contained in $\ker(g)$. But by the local reciprocity map, $\ker(g) = N_{L_\mathfrak{Q}/K_\mathfrak{q}}(L_\mathfrak{Q}^\times)$; so $\zeta_n^i \notin N_{L_\mathfrak{Q}/K_\mathfrak{q}}(L_\mathfrak{Q}^\times)$, for $0 < i < p_1^{e_1}...p_k^{e_k}$, as required. The Hasse norm theorem gives the result. □

Corollary 1. *Let $n = p_1^{e_1}...p_k^{e_k}$ and $K = \mathbb{Q}(\zeta_{p_1^{e_1}...p_k^{e_k}})$, where the p_i are pairwise coprime. There exists a cyclic Galois extension E/K of any index d dividing n, such that ζ_n is non-norm in E/K, i.e. ζ_n is not a norm for $0 < i < d$.*

Proof. Mutatis mutandis, identical to [15]. □

These results allow us to create many new CDAs with roots of unity as non-norm elements. We give two examples.

Examples 1. Set $n = 3^2 \cdot 2^6 = 576$. Note $\ell = 577$ is prime, and $\ell - 1 = 576$ is divisible by 576, with neither 27 nor 128 dividing $\ell - 1$. So 577 satisfies the conditions of Theorem 5. Observe $M := \mathbb{Q}(\zeta_n, \zeta_\ell) = \mathbb{Q}(\zeta_{576}, \zeta_{577})$ is an extension of $K := \mathbb{Q}(\zeta_{576})$ of degree 576. Let $\mathrm{Gal}(M/K) = \langle\sigma\rangle$. Then, as in the proof above, $\sigma^n = e$ fixes an extension of degree $n = 576$ over K - in this case the extension is M itself. By the theorem ζ_{576} is a non-norm element in $\mathbb{Q}(\zeta_{576}, \zeta_{577})/\mathbb{Q}(\zeta_{576})$. Apply Corollary 1 to fix a degree 2 cyclic Galois extension of K, denoted E, which is possible since 2 divides 576. This extension also has the property that ζ_{576} is a non-norm element over K. Let $\mathrm{Gal}(E/K)$ be generated by θ. Then the cyclic algebra $(E/K, \theta, \zeta_{576})$ has dimension $2^2 \cdot 192 = 768$ over $\mathbb{Q}$, and is division.

2. Set $n = 3^3 \cdot 2^5 = 864$. Note that $\ell = 16,417$ is prime, $16,416 \equiv 0 \bmod 864$, and neither 81 nor 64 divide $\ell - 1 = 16,416$. So ℓ satisfies the required properties to apply Theorem 5. Observe $M := \mathbb{Q}(\zeta_n, \zeta_\ell) = \mathbb{Q}(\zeta_{864}, \zeta_{16,417})$ is a cyclic extension of $K := \mathbb{Q}(\zeta_{864})$, of degree $16,416$. Let $\mathrm{Gal}(M/K) = \langle\sigma\rangle$. Then, as in the proof above, $\sigma^n = \sigma^{864}$ fixes an extension of degree $n = 864$ over K, denoted L. The theorem indicates that ζ_{864} is a non-norm element in $L/\mathbb{Q}(\zeta_{864})$. We can then apply Corollary 1 to fix a cyclic Galois extension of K of degree 2 over K, since 2 divides $16,416$. This extension also has the property that ζ_{864} is a non-norm element over K. Call this extension E and let $\mathrm{Gal}(E/K) = \langle\theta\rangle$. Then the cyclic algebra $(E/K, \theta, \zeta_{864})$ has dimension $2^2 \cdot 288 = 1152$ over $\mathbb{Q}$, and is division.

Maximality of the Natural Order We note that [15, Theorem 3] states that the natural order in the above prime-power case ($n = p^r$) is maximal. It can be shown with an identical proof that when one takes $n = p_1^{a_1} ... p_l^{a_l}$, as long as ℓ satisfies $\ell \equiv 1 \bmod n$ and $p_i n \nmid \ell - 1$ for $i = 1, ..., l$, the result still holds: note that the ramification of ideals above ℓ in $\mathcal{O}_K$ in $\mathcal{O}_M$ is the same as before (since the inertial degree depends on $\ell \equiv 1 \bmod n$ to equal 1), the ramification index is $\phi(\ell)$, and $g_{M/K} = [M : K]/\phi(\ell) = 1$; this can be summarised by noting that the relevant properties depend on the prime ℓ, and not the degree of K. However, if γ is not a unit, the natural order is not (in general) maximal.

4 Cryptographic Moduli for CDAs from Any Cyclotomics

Here we provide methods to find the primes needed to construct CDAs over cyclotomic fields of composite conductor for CLWE, and give concrete examples. To build algebras meeting the requirements of the previous theorem, we need to find a small degree extension L of $K = \mathbb{Q}(\zeta_n)$ and a non-norm element for L/K. As explained above, this is done by taking a large prime ℓ satisfying certain conditions, taking the compositum of K and $\mathbb{Q}(\zeta_\ell)$, and taking an intermediate extension L of K of desired degree. If chosen well, ζ_n will be a non-norm element.

Recall that ℓ must satisfy two conditions: firstly, that $\ell \equiv 1 \bmod n$, and secondly, that $\ell \not\equiv 1 \bmod p_i \cdot n$, for $i = 1, ..., k$, where p_i is a prime in the prime factorization of $n = p_1^{e_1} ... p_k^{e_k}$. We can find such an ℓ by considering the arithmetic progression $1 + p_1^{e_1} ... p_k^{e_k} + \sum_{i=0}^{m} p_1^{e_1+1} ... p_k^{e_k+1}$, for $m = 0, 1, 2, ...$ Theorem 1 implies there are infinitely many primes in this progression, and for our parameters searching elements in the progression can be done efficiently.

Similarly to RLWE [22][2], the security proof of CLWE holds for primes q completely split in $\mathcal{O}_K$. Moreover, to enable efficient multiplication, it will be convenient to have q also completely split in L. We can use the fact that if q splits completely in M, it splits completely in all subfields. Thus the most naive approach to find a prime that splits completely in L and K is to find a prime that splits completely in $M = \mathbb{Q}(\zeta_{n\ell})$. This is equivalent to $q \equiv 1 \bmod \ell n$.

This approach is limited, however. Since $\ell \equiv 1 \bmod n$, we have $\ell > n$; since $q \equiv 1 \bmod \ell n$, we have $q > \ell n > n^2$. In general, we want $[K : \mathbb{Q}] = \phi(n)$ to be large, and $[L : K]$ small. As we want q not to be too large, this forces n to be small. Moreover, the larger n gets, the smaller ℓ is required to be. For example, take $n = 100$. Then $[K : \mathbb{Q}] = 40$, and, if we can find an appropriate non-norm element, we could take a degree 5 extension of K for an algebra of degree 1000 over $\mathbb{Q}$. 101 is prime, so we can take $\ell = 101$; then we have $q \geq 100 \cdot 101 + 1 = 10101$. Since 10101 is not prime, the next smallest possible option for q is $2\ell n + 1 = 20203$, which is also not prime. The search continues in this manner, with the size of q rapidly growing.

The Quadratic Case We first consider extensions L/K of degree 2, and write L as the compositum of K and a quadratic subfield E of $E' := \mathbb{Q}(\zeta_\ell)$. Since E' is cyclotomic with prime conductor, E is the *unique* quadratic subfield of E'. This can be written explicitly as follows [18, Theorem 9.3]:

$$E = \begin{cases} \mathbb{Q}(\sqrt{\ell}), \text{ if } \ell \equiv 1 \bmod 4 \\ \mathbb{Q}(\sqrt{-\ell}), \text{ if } \ell \equiv 3 \bmod 4. \end{cases}$$

The discriminant of this field, d_E, is also well known, being $d_E = \ell$ if $\ell \equiv 1 \bmod 4$, else $d_E = 4\ell$ if $\ell \equiv 3 \bmod 4$. A final fact is that a prime q splits completely in E if and only if d_E is a quadratic residue modulo q, i.e. there exists $x \in \mathbb{Z}/q\mathbb{Z}$ such that $d_E \equiv x^2 \bmod q$ [28, Proposition 8.5].

A prime q splits in L if and only if q splits in both K and E. Thus to find primes that split in both L and K we search for primes q such that $q \equiv 1 \bmod n$, with d_E becoming a quadratic residue modulo q. Finally, to ensure we can find non-norm elements, we require that $\gcd(n, 2) \neq 1$ (cf. [15, Theorem 10]).

Here we run through an example. Set $n = 320$. With $d = 2$, we obtain a degree 512 algebra. Since $1601 \equiv 1 \bmod 320$ and is prime, we can set $\ell = 1601$. Then $\ell \equiv 1 \bmod 4$, so $d_E = \ell = 1601$. There are many small primes that are congruent to 1 mod 320 and have d_E as a quadratic residue; for example, 4481 suffices. It is prime, and $4481 = 320 \cdot 14 + 1$. Furthermore, we have $1213^2 \equiv 1601$

[2] Subsequent works have allayed this restriction on the modulus.

mod 4481. Below is a table of results for quadratic extensions of $\mathbb{Q}(\zeta_n)$. Listed are n, $[\mathcal{A} : \mathbb{Q}]$, ℓ, example value(s) of q, and 'min log rop'. This last quantity is obtained by running the lattice estimator[3] [2] with similar parameters for the secret, error, and default number of samples as Kyber512, but replacing the lattice dimension and modulus with the corresponding entries of the table. We list the minimum of the base-2 logarithms over the given values of q in the row. The 'meaning' of the rop results is to estimate the number of ring operations required to solve the corresponding LWE instances.

n	$[\mathcal{A} : \mathbb{Q}]$	ℓ	q	min log rop
320	512	1601	4481, 7681, 9601, 13121	120.6
324	432	1621	3889, 6481, 8101, 10369	104.9
352	640	353	3169, 6337, 11617, 13729	151.2
400	640	401	4001, 4801, 14401	150.5
432	576	433	3889, 8209, 12097, 15121	133.8
448	768	449	4481, 8513, 10753	190.6
484	880	1453	3389, 11617, 13553, 15973	215.9
576	768	577	7489, 10369, 13249, 14401	185.0
640	1024	641	7681, 9601, 12161, 13441	265.3
648	864	7129	3889, 6481, 9721, 10369	220.2
864	1152	2593	3457, 10369	316.4

Table 1: The 'Naive' Quadratic Case

The Naive Method for Higher Values of d In this section we address extensions L such that $[L : K] > 2$. Unlike in the quadratic case we cannot, in general, write down explicitly what a low-degree subfield of $\mathbb{Q}(\zeta_\ell)$ is. We return to the naive method explained above, finding $q \equiv 1 \bmod \ell n$. Though cumbersome, one can still obtain some limited results by this method, although the resulting algebras are slightly small since the largest n that can be taken is 141, if one imposes, say, $q < 20000$. A simple method to find appropriate values of ℓ is to fix prime ℓ and set $n = \ell - 1$. Some results are below:

n	d	$[\mathcal{A} : \mathbb{Q}]$	ℓ	q	min log rop
25	5	500	101	5051	130.5
52	6	864	53	8269	225.2
58	6	1008	59	10267	267.0
60	6	720	61	7321	184.0
66	6	720	67	4423	194.4
78	6	936	79	6163	256.0
82	4	640	83	13613	151.3
82	6	1440	83	13613	414.7
138	4	704	139	19183	162.7

Table 2: The 'Naive' Case for $d > 2$

Refined Naive Method There is, however, a refinement on the above method by which we relax the condition that $q \equiv 1 \bmod \ell n$. Again write L as the compositum of K and a subfield E of $E' = \mathbb{Q}(\zeta_\ell)$. Since $\ell > 2$ is prime, the maximal

[3] Commit 564470e.

real subfield $E'^{+} = \mathbb{Q}(\zeta_\ell + \zeta_\ell^{-1})$ of E' has degree $\frac{\ell-1}{2}$ over $\mathbb{Q}$, and Galois group isomorphic to $\mathrm{Gal}(E'/\mathbb{Q})/\{\pm 1\}$. The primes that ramify in E'^{+} are the primes dividing the discriminant of E', which is only ℓ. This makes it easy to select unramified primes. The inertial degree is also well known in the maximal real subfield: it is the smallest integer f such that $q^f \equiv \pm 1 \bmod \ell$. So if E is contained in E'^{+}, we need to find prime q such that $q \equiv \pm 1 \bmod \ell$ and $q \equiv 1 \bmod n$.

So which subfields are contained in E'^{+}? Since $\mathrm{Gal}(E'/\mathbb{Q})$ is cyclic and $\mathrm{Gal}(E'/E'^{+})$ is one of its subgroups, $\mathrm{Gal}(E'/E'^{+})$ is cyclic, so the quotient of the two groups is cyclic and isomorphic to $\mathrm{Gal}(E'^{+}/\mathbb{Q})$, of order $\frac{\ell-1}{2}$. The subgroups of a cyclic group $\mathbb{Z}/m\mathbb{Z}$ correspond to divisors d of m, and there is a single subgroup of order d for each divisor. Hence in $\mathrm{Gal}(E'^{+}/\mathbb{Q})$ there is a subgroup for each divisor of $\frac{\ell-1}{2}$, and by the Galois correspondence there is a unique Galois subfield of E'^{+} with degree over $\mathbb{Q}$ equal to that divisor. Since this is also a subfield of E', this subfield is also the unique subfield of the given degree in E'. Note also that any Galois extension of $\mathbb{Q}$ is either totally real or totally imaginary, so odd-degree subfields of $\mathbb{Q}(\zeta_\ell)$ are totally real.

In light of this, our approach is as follows: we look for small values of n, so that we can find small values of ℓ, and hence find a value of q in the appropriate range. We will also look for values of ℓ such that our desired values of $d = [L : K]$ divide $\frac{\ell-1}{2}$, so that E will be totally real and we can apply this 'refined naive method' in our hunt for q. A final constraint to note is that we must have $\gcd(n, d) \geq 2$, else we will not have ζ_n be a non-norm element.

Here we run through the previous example again. We have $n = 100$, $[K : \mathbb{Q}] = 40$, and want a degree 5 extension of K to obtain an algebra of degree 1000 over $\mathbb{Q}$. Since 101 is prime, we can take $\ell = 101$. This time, instead of requiring $q \equiv 1 \bmod \ell n$, we need $q \equiv \pm 1 \bmod \ell$ and $q \equiv 1 \bmod n$. Note that $5 \mid \frac{101-1}{2} = 50$, so a subfield of degree 5 of the maximal totally real subfield exists. One finds that 10301 satisfies both of these conditions: $10301 = 100 \cdot 103 + 1$, and $10301 = 101 \cdot 102 - 1$. Furthermore, 10301 is of the appropriate size; where the naive method failed, the tweaked version yielded a small prime.

Below is a table, Table 3, giving examples of valid primes using this method. Listed are n, the degree $d = [L : K]$, $[\mathcal{A} : \mathbb{Q}]$, and possible values for ℓ and q.

n	d	$[\mathcal{A} : \mathbb{Q}]$	ℓ	q	min log rop
32	5	400	97	18913	91.8
45	5	600	181	16651	138.4
70	5	600	71	9941	145.9
70	7	1176	71	9941	326.3
90	5	600	2791	5581	155.2
100	5	1000	101	10301	264.1
102	3	288	103	10711	72.1
130	5	1200	131	17291	318.7

Table 3: The Refined 'Naive' Case for $d > 2$

Completely Splitting Primes in Subfields of Cyclotomics We now consider primes in subextensions of higher degree. The results in Tables 4 and 5 are based off the following theorem:

Theorem 6. *[24, Theorem 30] Let ℓ be a prime, $E' = \mathbb{Q}(\zeta_\ell)$, and denote its unique subfield of degree d over $\mathbb{Q}$ by E'_d. Let q be a prime coprime to ℓ. Then q splits completely in E'_d if and only if q is a dth power modulo ℓ.*

This allows us to generalize the method of the quadratic case to larger degree subfields of E'. As examples, we list results for cubic and quartic extensions of K: we list, in addition to the previous values, an x for which $q \equiv x^d \bmod \ell$. We illustrate the quartic case with extensions of $\mathbb{Q}(\zeta_{128})$, which yields $[\mathcal{A} : \mathbb{Q}] = 1024$.

n	$[\mathcal{A} : \mathbb{Q}]$	ℓ	x	q	min log rop
111	648	4441	2152	12211	155.1
171	972	6841	2112	3079	291.8
183	1080	8053	1422	7321	301.1
201	1188	4423	2246	4021	363.9
360	864	2521	461	6121	232.3

Table 4: The Cubic Case

n	ℓ	x	q	min log rop
128	2689	275	3329	304.8
128	641	147	3457	303.8
128	3457	780	4481	295.7
128	12161	10957	4993	292.3
128	4481	571	6529	287.8

Table 5: The Quartic Case

5 Hardness of CLWE from Ideal Lattices in Suborders

In this section we define LWE in suborders of Λ, and obtain a security reduction analogous to the maximal order case. In order for this proof to hold, we initally restrict our ideals to those coprime to the ideal generated in a suborder of Λ by the conductor ideal of an $\mathcal{O}_K$-suborder of $\mathcal{O}_L$, as described below. Similarly to CLWE, one step of the reduction requires a restricted secret space.

Constructing Non-Maximal Orders Here we construct families of non-maximal orders in $\mathcal{A} = (L/K, \theta, \gamma)$ where $K = \mathbb{Q}(\zeta_n)$, L is constructed as in [15], and $\gamma = \zeta_n$. We do this as follows: let $\mathcal{O}' \subsetneq \mathcal{O}_L$ be an order in L. Define

$$\mathcal{O} := \bigoplus_{i=0}^{d-1} u^i \mathcal{O}' = \mathcal{O}' \oplus u\mathcal{O}' \oplus ... \oplus u^{d-1}\mathcal{O}'.$$

This is an additively closed subset of Λ. Since $\mathcal{O}'$ is multiplicatively closed and $\gamma \in \mathcal{O}'$, we conclude that $\mathcal{O}$ is a subring of Λ, and so discrete. Since $\mathcal{O}' \cdot \mathbb{Q} = L$, we have $\mathcal{O} \cdot \mathbb{Q} = \mathcal{A}$. Thus we have

Proposition 10. *Let $\mathcal{A}$ and $\mathcal{O}$ be as above. Then $\mathcal{O}$ is a suborder of $\mathcal{A}$.*

Ideal Lattice Problems in Non-maximal Orders As shown above, when an order is maximal it has a 'nice' ideal theory closely related to the ideals of $\mathcal{O}_K$. When an order is not maximal, many of these properties (e.g. two-sided ideals forming an abelian group) may be lost. However, we can still define the standard lattice problems on lattices obtained from embeddings of these ideals.

Definition 21. Let $\mathcal{A}$ be a cyclic algebra, let $\mathcal{I}$ be ideal of an order $\mathcal{O}$, and let $0 < \delta < \lambda_1(\mathcal{I})/2$. Then the $\mathcal{A}$-BDD$_{\mathcal{O},\mathcal{I},\delta}$ problem, on input $y = x + e$ for $x \in \mathcal{I}$ and $e \in \bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$ satisfying $\|e\|_{2,\infty} \leq \delta$, is to compute x.

Definition 22. For any $q \geq 2$, the $q\mathcal{A}$-BDD$_{\mathcal{O},\mathcal{I},d}$ problem is as follows: given an instance of the $\mathcal{A}$-BDD$_{\mathcal{O},\mathcal{I},\delta}$ problem $y = x + e$ with solution $x \in \mathcal{I}$ and error $e \in \bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$ satisfying $\|e\|_{2,\infty} \leq \delta$, output $x \bmod q\mathcal{I}$.

Lemma 8. *For any $q \geq 2$ and order ideal $\mathcal{I}$, there is a deterministic polynomial time reduction from $\mathcal{A}$-BDD$_{\mathcal{O},\mathcal{I},\delta}$ to $q\mathcal{A}$-BDD$_{\mathcal{O},\mathcal{I},\delta}$*

Proof. Adapted from [32, Lemma 3.5], which is lattice preserving. □

Cyclic Order LWE We call CLWE over a possibly non-maximal order Cyclic Order LWE, COLWE. We define the COLWE distribution analogously to CLWE:

Definition 23. Let L/K be a Galois extension of number fields of dimension $[L : K] = d$ with cyclic Galois group generated by θ. Let $\mathcal{A} := (L/K, \theta, \gamma)$ be the resulting cyclic algebra with center K and invariant u with $u^d = \gamma \in \mathcal{O}_K$. Let $\mathcal{O} \subset \Lambda$ be a non-maximal order of $\mathcal{A}$. For an error distribution ψ over $\oplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$, an integer modulus $q \geq 2$, and a secret $s \in \mathcal{O}_q^\vee$, a sample from the COLWE distribution $\Pi_{\mathcal{O},q,s,\psi}$ is obtained by sampling $a \leftarrow \mathcal{O}_q$ uniformly at random, $e \leftarrow \psi$, and outputting $(a, b) = (a, (a \cdot s)/q + e \bmod \mathcal{O}^\vee) \in \mathcal{O}_q \times (\oplus_{i=0}^{d-1} u^i L_{\mathbb{R}})/\mathcal{O}^\vee$.

Definition 24. Let Ψ be a family of error distributions over $\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$. The search COLWE problem, denoted by COLWE$_{\mathcal{O},q,s,\psi}$, is to recover s from a collection of independent samples from $\Pi_{\mathcal{O},q,s,\psi}$ for any $s \in \mathcal{O}_q^\vee$ and $\psi \in \Psi$.

Definition 25. Let Υ be a distribution on a family of error distributions over $\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$. Let $U_{\mathcal{O}}$ denote the uniform distribution on $\left(\mathcal{O}_q, \left(\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}\right)/\mathcal{O}^\vee\right)$. Then, the decision COLWE problem, DCOLWE$_{\mathcal{O},q,\Upsilon}$, is given a collection of independent samples from either $\Pi_{q,s,\psi}$ for a random choice of $(s, \psi) \leftarrow U\left(\mathcal{O}_q^\vee\right) \times \Upsilon$ or from $U_{\mathcal{O}}$, decide which is the case with non-negligible advantage.

Security Reductions A proof of the hardness of search COLWE from BDD over ideals in non-maximal orders requires one to restrict to invertible ideals (as is done for group ring LWE and for OLWE). We note in passing that a proof of the hardness of search COLWE from BDD over one-sided ideals in non-maximal orders is also plausible, possibly requiring further restrictions to the valid ideals.

The Technical Lemmas We adapt the method of [8]. Let $\mathrm{ass}_{\mathcal{O}}(\mathcal{I}) = \{\mathfrak{p}_i : \mathcal{I} \subset \mathfrak{p}_i\}$ be the *associated primes* of the ideal $\mathcal{I}$, where the $\mathfrak{p}_i$ are prime ideals of $\mathcal{O}$.

Lemma 9. *Let $\mathcal{I}$ be an invertible ideal of non-maximal order $\mathcal{O}$ and $\mathcal{J}$ be an integral ideal of $\mathcal{O}$. Then there exists a $t \in \mathcal{I} \cap \mathcal{O}_K$ such that the ideal $t \cdot \mathcal{I}^{-1} \subset \mathcal{O}$ is coprime to $\mathcal{J}$, and we can compute such a t efficiently given $\mathcal{I}$ and $\mathrm{ass}_{\mathcal{O}}(\mathcal{J})$.*

Proof. Let $\{\mathfrak{p}_1, ..., \mathfrak{p}_r\} = \mathrm{ass}_{\mathcal{O}}(J)$ and $t \in (\mathcal{I} \setminus \bigcup_i \mathfrak{p}_i\mathcal{I}) \cap \mathcal{O}_K$. Suppose $t \cdot \mathcal{I}^{-1} + \mathcal{J} \neq \mathcal{O}$. So $t \cdot \mathcal{I}^{-1} + \mathcal{J} \subset \mathcal{M}$ for maximal ideal $\mathcal{M} \subset \mathcal{O}$. Maximal ideals are prime, so $t \cdot \mathcal{I}^{-1}$ lies in an associated prime of $\mathcal{J}$. This implies $t \in \mathfrak{p}_i\mathcal{I}$ for some $\mathfrak{p}_i \in \mathrm{ass}_{\mathcal{O}}(\mathcal{J})$, a contradiction. To construct such a t, take an $\mathcal{O}_K$ element in $\mathcal{I} \setminus \mathfrak{p}_i\mathcal{I}$ for all i, and compute the preimage under the CRT (see [33, §22.3]). □

Lemma 10. *Let $\mathcal{O}$ be as above. Let $\mathcal{I}, \mathcal{J}$ be ideals of $\mathcal{O}$, with $\mathcal{I}$ invertible, and $t \in \mathcal{I} \cap \mathcal{O}_K$ chosen such that $t \cdot \mathcal{I}^{-1}$ and $\mathcal{J}$ are coprime as ideals, and let $\mathcal{P}$ be an arbitrary fractional ideal of $\mathcal{O}$. Then, the function $\chi_t : \mathcal{A} \to \mathcal{A}$ defined as $\chi_t(x) = t \cdot x$ induces a module isomorphism from $\mathcal{P}/\mathcal{J} \cdot \mathcal{P} \to \mathcal{I} \cdot \mathcal{P}/\mathcal{I} \cdot \mathcal{J} \cdot \mathcal{P}$. Furthermore, if $\mathcal{J} = \langle q \rangle$ for an unramified prime $q \in \mathbb{Z}$ we can efficiently compute the inverse.*

Proof. The standard argument which relies on coprimality of the ideals. □

Hardness of the Search Problem from Invertible Ideals We first state a lemma from [15], which enables the quantum step of the proof to hold:

Lemma 11. *There is an efficient quantum algorithm that given any nd^2 dimensional lattice $\mathcal{L} := \sigma_{\mathcal{A}}(\mathcal{I})$ for some ideal $\mathcal{I} \subset \mathcal{O}$, $0 < \delta < \lambda_1(\mathcal{L}^*)/(2\sqrt{2nd})$, and an oracle that solves $\mathcal{A}$-$BDD_{\mathcal{O},\mathcal{L}^*,\delta}$ with all but negligible probability, outputs an independent sample from $D_{\mathcal{L},\sqrt{d}\omega(\sqrt{\log(nd)})/\sqrt{2}\delta}$.*

We now prove an important lemma:

Lemma 12. *Let $\mathcal{A} = (L/K, \theta, \gamma)$ be a CDA constructed as above, and $\mathcal{O} \subset \Lambda$ be a non-maximal order. There is a ppt. algorithm that given an unramified prime $q \geq 2$, an invertible fractional $\mathcal{O}$-ideal $\mathcal{I}^\vee$, a $q\mathcal{A}$-$BDD_{\mathcal{O},\mathcal{I}^\vee,\alpha q \cdot \omega(\sqrt{\log(nd)})/\sqrt{2nd} \cdot r}$ instance $y = x + e$, a parameter $r \geq \sqrt{2}q \cdot \eta(\mathcal{I})$, and $D_{\mathcal{I},r'}$ samples with $r' \geq r$, outputs samples within negligible statistical distance of the COLWE distribution $\Pi_{\mathcal{O},q,s,\Sigma}$ for a secret $s = \chi_t(x \bmod q\mathcal{I}^\vee) \in \mathcal{O}_q^\vee$, where χ_t is as in Lemma 9 and Σ is an error distribution such that if $|\gamma| = 1$ the resulting error e'' has Gaussian marginal distribution in its i, j^{th} coordinate with parameter $r_{i,j} \leq \alpha$.*

Proof. First compute $t \in \mathcal{I}$ such that $\mathcal{I}^{-1} \cdot t$ and $q\mathcal{O}$ are coprime using the Lemma 9. We now create a sample from the COLWE distribution as follows: sample $z \leftarrow D_{\mathcal{I},r'}$, $e' \leftarrow D_{\alpha/\sqrt{2}}$, and compute a pair

$$(a, b) = \left(\chi_t^{-1}(z \bmod q\mathcal{I}), (z \cdot y)/q + e' \bmod \mathcal{O}^\vee\right) \in \mathcal{O}_q \times \bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}/\mathcal{O}^\vee$$

We show that (a, b) is within negligible statistical distance of the COLWE distribution and s is uniformly random. First, note that $r \geq q \cdot \eta(\mathcal{I})$ so Lemma 1 implies the statistical distance between $z \bmod q\mathcal{I}$ and the uniform distribution is at most 2ε. As χ_t is bijective, $a = \chi_t^{-1}(z \bmod q\mathcal{I})$ is statistical distance 2ε of the uniform distribution over $\mathcal{O}_q$, as required. We now show that $b = a \cdot s/q + e''$, for an error e'' and uniform s, conditioned on some fixed a. We have

$$\begin{aligned} b &= (z \cdot y)/q + e' \bmod \mathcal{O}^\vee \\ &= (z \cdot x)/q + (z \cdot e)/q + e' \bmod \mathcal{O}^\vee, \end{aligned}$$

so since $z = t \cdot a \bmod \mathcal{O}_q^\vee$ and t lies in the center of $\mathcal{A}$ it follows that $(z \cdot x)/q = (a \cdot t \cdot x)/q = (a \cdot s)/q \bmod \mathcal{O}^\vee$ for $s := \chi_t(x \bmod q\mathcal{I}^\vee)$ (this only holds for invertible ideals). Hence s is uniformly random over $\mathcal{O}_q^\vee$, if x is uniform over $\mathcal{I}^\vee$, since χ_t is a bijection. The analysis of the error is as in [15, Lemma 11]. □

Combining Lemma 12 and Lemma 11, we arrive at the following:

Theorem 7. *Given a COLWE$_{\mathcal{O},q,\Sigma_\alpha}$ oracle for input $\alpha \in (0,1)$, $q \in \mathbb{Z}_{\geq 2}$, an ideal $\mathcal{I} \subset \mathcal{O}$, $r \geq \sqrt{2}q \cdot \eta(\mathcal{I})$ satisfying $r' = r \cdot \omega(\sqrt{\log N})/(\alpha q) > \sqrt{2N}/\lambda_1(\mathcal{I}^\vee)$, and polynomially many samples from the discrete Gaussian $D_{\mathcal{I},r}$ there exists an efficient quantum algorithm that outputs an independent sample from $D_{\mathcal{I},r'}$.*

Corollary 2. *Let $\mathcal{A}, \mathcal{O}, \alpha$ and q be as above. Then there is a polynomial-time quantum reduction from $\mathcal{A}$-SIVP$_\xi$ to COLWE$_{\mathcal{O},q,\Sigma_\alpha}$ when $\sqrt{8Nd}\xi = \omega(\sqrt{dn})/\alpha$.*

Search to Decision Reduction Here we adapt the standard search-to-decision reduction for structured LWE. Consider the following CRT-style decomposition:

Lemma 13. *[30] Let Λ be the natural order of a cyclic division algebra $\mathcal{A} = (L/K, \theta, \gamma)$ with $\gamma \in \mathcal{O}_K$ and let $\mathcal{I}$ be an ideal of $\mathcal{O}_K$ which splits completely as $\mathcal{I} = \mathfrak{q}_1 \dots \mathfrak{q}_n$ as an ideal of $\mathcal{O}_K$. Then, we have the isomorphism*

$$\Lambda/\mathcal{I}\Lambda \cong \mathcal{R}_1 \times \ldots \times \mathcal{R}_n$$

where $\mathcal{R}_i = \bigoplus_{j=0}^{d-1} u^j (\mathcal{O}_L/\mathfrak{q}_i\mathcal{O}_L)$ is the ring subject to relations $(\ell + \mathfrak{q}_i\mathcal{O}_L)\, u = u\,(\theta(\ell) + \mathfrak{q}_i\mathcal{O}_L)$ and $u^d = \gamma + \mathfrak{q}_i$.

When γ is a unit, $\Lambda^\vee = \bigoplus_i u^i \mathcal{O}_L^\vee$. The above lemma is also valid when each instance of $\mathcal{O}_L$ and Λ is replaced by its respective dual. For the following we will assume γ is a unit. In this case, as a consequence of Wedderburn's theorem, each $\mathcal{R}_i$ is isomorphic to the matrix ring $M_d(\mathbb{F}_q)$.

In order to obtain a search to decision reduction for LWE in suborders of Λ, we need to obtain a decomposition similar to that stated in the above lemma. Here we restrict our proof to a large class of suborders and prime moduli as follows, in order to guarantee such a decomposition.

Let $\mathcal{A} = (L/K, \theta, \zeta_n)$ be a CDA constructed as usual, and let $\mathcal{O}' \subset \mathcal{O}_L$ and $\mathcal{O} = \oplus_{i=0}^{d-1} u^i \mathcal{O}'$ be as above. Denote the conductor ideal of $\mathcal{O}'$ by $\mathfrak{c}$. Then

Proposition 11. *Let $\mathcal{A} = (L/K, \theta, \zeta_n)$, Λ, $\mathcal{O}' \subset \mathcal{O}_L$, and $\mathcal{O} = \oplus_{i=0}^{d-1} u^i \mathcal{O}'$ be as above. Let q be an integer prime, either completely split in K and inert in L/K, or completely split in L. If $\gcd(q\mathcal{O}', \mathfrak{c}) = 1$, then $\mathcal{O}/q\mathcal{O} \cong \Lambda/q\Lambda$.*

Proof. We have

$$\begin{aligned}\mathcal{O}/q\mathcal{O} &= (\oplus_{i=0}^{d-1} u^i \mathcal{O}')/q(\oplus_{i=0}^{d-1} u^i \mathcal{O}') \cong \oplus_{i=0}^{d-1} u^i \mathcal{O}'/q\mathcal{O}' \\ &\cong \oplus_{i=0}^{d-1} u^i \mathcal{O}_L/q\mathcal{O}_L \cong \Lambda/q\Lambda,\end{aligned}$$

where the second isomorphism follows from Lemma 2. □

This result means that we can use a decomposition of $\mathcal{O}/q\mathcal{O}$ into the direct product of matrix rings, provided that q is coprime to $\mathfrak{c}$, which we assume. The rest of the reduction is then identical to that of [15], and we obtain

Theorem 8. *Let $\mathcal{O} \subset \Lambda$ be a suborder of the natural order of a CDA $\mathcal{A} = (L/K, \theta, \zeta_n)$ as above, $q \in \mathrm{poly}(n)$ completely split in K such that $\gcd(q\mathcal{O}', \mathfrak{c}) = 1$, and $\alpha q \geq \eta_\varepsilon(\Lambda^\vee)$ for a negligible $\varepsilon = \varepsilon(n)$. Then there is a ppt. reduction from $COLWE_{\mathcal{O},q,\Sigma_\alpha,G}$ for any pairwise difference set $G \subset \Lambda_q^\vee$ to $DCOLWE_{\mathcal{O},q,\Upsilon_\alpha}$.*

Above, a pairwise difference set G is a set $G = \prod_{i=1}^n G_i$ where each G_i is such that $g \neq h \in G_i$ implies $g - h$ is invertible. G is of size $|G| \leq q^{nd}$. We are currently unable to avoid this restriction. For more on this restriction, see [15].

COLWE Hardness from Other Ideals The reduction from ideal lattice problems to search COLWE above used invertible ideals of suborders. Here we weaken this restriction, using analogous methods to [31]. We begin with:

Lemma 14. *Let $\mathcal{O} \subset \mathcal{A}$ be an order, $\mathcal{Q}$ and $\mathcal{I}$ be two-sided $\mathcal{O}$-ideals, and suppose that $(\mathcal{O} : \mathcal{I})_l (\mathcal{I} : \mathcal{O})_l + \mathcal{Q} = \mathcal{O}$. Then there exists $t \in (\mathcal{I} : \mathcal{O})_l \cap \mathcal{O}_K$ such that $(\mathcal{O} : \mathcal{I})_l t + \mathcal{Q} = \mathcal{O}$, and such a t can be found in polynomial time given $\mathcal{O}, \mathcal{I}$, and the associated $\mathcal{O}$-primes of $\mathcal{Q}$.*

Proof. Let $\{\mathfrak{p}_1, ..., \mathfrak{p}_r\} = \mathrm{ass}_{\mathcal{O}}(\mathcal{Q})$. Let $t \in ((\mathcal{I} : \mathcal{O})_l \setminus \cup_{i=1}^r \mathfrak{p}_i (\mathcal{I} : \mathcal{O})_l) \cap \mathcal{O}_K$. Then

$$(\mathcal{O} : \mathcal{I})_l t + \mathcal{Q} \subset (\mathcal{O} : \mathcal{I})_l (\mathcal{I} : \mathcal{O})_l + \mathcal{Q} = \mathcal{O}.$$

Suppose the containment is strict. Then $(\mathcal{O} : \mathcal{I})_l t + \mathcal{Q} \subset \mathfrak{m}$ for some maximal left ideal $\mathfrak{m}$ of $\mathcal{O}$. Since $\mathcal{Q}$ is two-sided, $\mathcal{Q} \subset \mathfrak{m}$ implies that the associated two-sided prime ideal of $\mathfrak{m}$ is one of the $\mathfrak{p}_i$. We thus have $(\mathcal{O} : \mathcal{I})_l t \subset \mathfrak{m}_i$. Recall that $(\mathcal{O} : \mathcal{I})_l$ is two-sided when $\mathcal{I}$ is two-sided; thus in fact $(\mathcal{O} : \mathcal{I})_l t \subset \mathfrak{p}_i$ also. Then

$$\mathcal{O}t = ((\mathcal{O} : \mathcal{I})_l (\mathcal{I} : \mathcal{O})_l + \mathcal{Q})t \subset (\mathcal{O} : \mathcal{I})_l (\mathcal{I} : \mathcal{O})_l t + \mathcal{Q}t.$$

Since $t \in \mathcal{O}_K$, it commutes with other algebra elements, so we have

$$\begin{aligned} \mathcal{O}t &\subset (\mathcal{O} : \mathcal{I})_l t (\mathcal{I} : \mathcal{O})_l + \mathcal{Q}t \\ &\subset \mathfrak{p}_i (\mathcal{I} : \mathcal{O})_l + \mathfrak{p}_i (\mathcal{I} : \mathcal{O})_l \\ &= \mathfrak{p}_i (\mathcal{I} : \mathcal{O})_l , \end{aligned}$$

which is a contradiction.

Finally, we show there exists such a t, that is, $((\mathcal{I} : \mathcal{O})_l \setminus \cup_{i=1}^r \mathfrak{p}_i (\mathcal{I} : \mathcal{O})_l) \cap \mathcal{O}_K$ is non-empty. It suffices by the CRT to show that $((\mathcal{I} : \mathcal{O})_l \setminus \mathfrak{p}_i (\mathcal{I} : \mathcal{O})_l) \cap \mathbb{Z}$ is non-empty for any i. Note that $(\mathcal{I} : \mathcal{O})_l = \mathcal{I}$, and recall that any ideal of $\mathcal{O}$ has finite index. Then the smallest non-zero integer contained in $\mathcal{I}$ is $|\mathcal{O}/\mathcal{I}|$, and that in $\mathfrak{p}_i\mathcal{I}$ is $|\mathcal{O}/\mathfrak{p}_i\mathcal{I}|$; but since $\mathfrak{p}_i$ is a proper prime ideal, we have $|\mathcal{O}/\mathcal{I}| < |\mathcal{O}/\mathfrak{p}_i\mathcal{I}|$, so we have $|\mathcal{O}/\mathcal{I}| \in ((\mathcal{I} : \mathcal{O})_l \setminus \mathfrak{p}_i (\mathcal{I} : \mathcal{O})_l) \cap \mathbb{Z}$. □

Lemma 15. *Let $\mathcal{O} \subset \mathcal{A}$ be an order, $\mathcal{Q}$ and $\mathcal{I}$ be $\mathcal{O}$-ideals, $\mathcal{J}$ be a fractional $\mathcal{O}$-ideal, and $t \in (\mathcal{I} : \mathcal{O})_l \cap \mathcal{O}_K$ such that $(\mathcal{O} : \mathcal{I})_l t + \mathcal{Q} = \mathcal{O}$. Then the map $\chi_t : \mathcal{A} \to \mathcal{A}, u \mapsto t \cdot u$ induces an $\mathcal{O}$-module isomorphism from $\mathcal{J}/\mathcal{J}\mathcal{Q}$ to $\mathcal{I}\mathcal{J}/\mathcal{I}\mathcal{J}\mathcal{Q}$.*

Proof. We follow [31, Lemma 2.14]. Consider the function $f : \mathcal{J} \to \mathcal{I}\mathcal{J} \bmod \mathcal{I}\mathcal{J}\mathcal{Q}$ induced by multiplication by t. It is clearly an $\mathcal{O}$-module homomorphism. The kernel of f contains $\mathcal{J}\mathcal{Q}$, because $t \in (\mathcal{I} : \mathcal{O}) = \mathcal{I}$. We now show $\ker f = \mathcal{J}\mathcal{Q}$.

Suppose $tu \in \mathcal{I}\mathcal{J}\mathcal{Q}$ for some $u \in \mathcal{J}$. Then $(\mathcal{O} : \mathcal{I})_l tu \subset (\mathcal{O} : \mathcal{I})_l \mathcal{I}\mathcal{J}\mathcal{Q} \subset \mathcal{J}\mathcal{Q}$. Because $(\mathcal{O} : \mathcal{I})_l t + \mathcal{Q} = \mathcal{O}$, we find $u \in \mathcal{O}u = ((\mathcal{O} : \mathcal{I})_l t + \mathcal{Q})\, u \subset \mathcal{J}\mathcal{Q} + \mathcal{Q}\mathcal{J} \subset \mathcal{J}\mathcal{Q}$, as desired. Thus $f \bmod \mathcal{J}\mathcal{Q}$ is injective.

We now construct a preimage for any $v \in \mathcal{I}\mathcal{J}$. Since $(\mathcal{O} : \mathcal{I})_l t + \mathcal{Q} = \mathcal{O}$ by assumption, we can find some $c \in (\mathcal{O} : \mathcal{I})_l t$ such that $c = 1 \bmod \mathcal{Q}$. Set $a = cv \in (\mathcal{O} : \mathcal{I})_l t\mathcal{I}\mathcal{J} \subset t\mathcal{J}$. Then $a - v = (c-1)v \in \mathcal{I}\mathcal{J}\mathcal{Q}$. Now set $w = a \cdot t^{-1} \in \mathcal{J}$, so $\chi_t(w) = a = v \bmod \mathcal{I}\mathcal{J}\mathcal{Q}$, and $w \bmod \mathcal{J}\mathcal{Q}$ is the preimage of $v \bmod \mathcal{I}\mathcal{J}\mathcal{Q}$. □

Lemma 16. *Let $\mathcal{O} \subset \Lambda$ be a non-maximal order, and $\mathcal{I}$ be a two-sided $\mathcal{O}$-ideal such that $\mathcal{O}_l(\mathcal{I}) = \mathcal{O}$. Then there is a ppt. algorithm that on input a prime $q \geq 2$, a $q\mathcal{A}$-$BDD_{\mathcal{O},\mathcal{I},\alpha q \cdot \omega(\sqrt{log(nd)})/\sqrt{2nd}r}$ instance $y = x + e$ with $x \in \mathcal{I}^\vee$, $r \geq \sqrt{2}q \cdot \eta(\mathcal{I})$, and samples from $D_{\mathcal{I},r}$ outputs samples that are within negligible statistical distance of the COLWE distribution $\Pi_{\mathcal{O},q,s,\Sigma}$ where $s = \chi_t(x \bmod q\mathcal{I}^\vee) \in \mathcal{O}_q^\vee$, χ_t is as in Lemma 15, and Σ is an error distribution as in Lemma 12.*

Proof. The proof is similar to that of Lemma 12. By Lemma 14, compute a $t \in (\mathcal{I} : \mathcal{O})_l \cap \mathcal{O}_K$ to obtain χ_t. Sample $z \leftarrow D_{\mathcal{I},r}$ and create the COLWE sample

$$(a, b) := \left(\chi_t^{-1}(z \bmod q\mathcal{I}), (z \cdot y)/q + e' \bmod \mathcal{O}_l(\mathcal{I})^\vee\right) \in \left(\mathcal{O}_q \times \left(\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}\right) / \mathcal{O}_l(\mathcal{I})^\vee\right)$$

where $e' \leftarrow D_{\alpha/\sqrt{2}}$. As before, these samples are within negligible statistical distance of the CLWE distribution and s is uniformly random. We have that $a \in \mathcal{O}_q$ is statistically close to uniform since $r \geq q \cdot \eta(\mathcal{I})$ and ${\chi_t}^{-1}$ is a bijection.

As for b, we show that it has the shape $(a \cdot s)/q + e''$ for an error e'' of the specified distribution, and uniformly random s. Observe that

$$\begin{aligned} b &:= (z \cdot y)/q + e' \bmod \mathcal{O}_l(\mathcal{I})^\vee \\ &= (z \cdot x)/q + (z \cdot e)/q + e' \bmod \mathcal{O}_l(\mathcal{I})^\vee. \end{aligned}$$

We now use χ_t with $\mathcal{J} = \mathcal{I}^\vee$, and obtain (by Lemma 5)

$$\chi_t : \mathcal{I}^\vee/\mathcal{I}^\vee q \to \mathcal{I}\mathcal{I}^\vee/\mathcal{I}\mathcal{I}^\vee q = (\mathcal{I} : \mathcal{I})_l^\vee/(\mathcal{I} : \mathcal{I})_l^\vee q = \mathcal{O}_l(\mathcal{I})^\vee/\mathcal{O}_l(\mathcal{I})^\vee q$$

Thus, since $z = t \cdot a \bmod \mathcal{O}_q^\vee$, setting $s = t \cdot x$, if s is uniformly distributed over $\mathcal{I}_q^\vee$, it is uniformly distributed over $\mathcal{O}_l(\mathcal{I})_q^\vee = \mathcal{O}_q^\vee$.

The distribution of the error can be analysed as in [15, Lemma 11]. □

6 Cyclic Learning with Rounding

In this section we extend Learning with Rounding to samples taken from the natural order of a CDA. We begin with the definition of the rounding function.

Definition 26. Let $q > p \in \mathbb{Z}_{\geq 2}$. Set $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$. Define the function $\lfloor \cdot \rceil_p : \mathbb{Z}_q \to \mathbb{Z}_p$ by $\lfloor x \rceil_p = \lfloor \frac{p}{q} \cdot x \rceil \bmod p$, for all $x \in \mathbb{Z}_q$. We extend this to vectors component-wise, and to the ring case coefficient-wise, i.e. for $a = a_0 + a_1 x + ... + a_{n-1}x^{n-1} \in R_q$, a polynomial ring with coefficients in $\mathbb{Z}_q$, we have

$$\lfloor a \rceil_p = \left\lfloor \frac{p}{q} \cdot a_0 \right\rceil + \left\lfloor \frac{p}{q} \cdot a_1 \right\rceil x + ... + \left\lfloor \frac{p}{q} \cdot a_{n-1} \right\rceil x^{n-1} \in R_p.$$

Learning with Rounding This function is then used to deterministically generate errors, as opposed to probabilistically sampling vectors or polynomials from an error distribution and adding this noise to a lattice point. We state the standard decision problems in the plain and module cases.

Definition 27. Let $s \in \mathbb{Z}_q^n$. Given uniformly random $a \leftarrow \mathbb{Z}_q^n$, output a $\mathrm{LWR}_{q,p}$ sample $(a, \lfloor \langle a \cdot s \rangle \rceil_p) \in \mathbb{Z}_q^n \times \mathbb{Z}_p$. Then the *decision*-$\mathrm{LWR}_{q,p}$ problem is: given m independent $\mathrm{LWR}_{q,p}$ samples, distinguish them with non-negligible probability from m samples $(a, u) \leftarrow U\left(\mathbb{Z}_q^n \times \mathbb{Z}_p\right)$.

Definition 28. (MLWR) Let $s \in R_q^n$ and $A \leftarrow U\left(R_q^{n \times d}\right)$. Output $(A, \lfloor A^t s \rceil_p) \in R_q^{n \times d} \times R_p^d$. The *decision* MLWR problem is: given m independent MLWR samples, distinguish them with non-negligible probability from m samples $(A, u) \leftarrow U(R_q^{n \times d} \times R_p^d)$.

To ensure that $\lfloor \langle a \cdot s \rangle \rceil_p$ is uniformly distributed, one takes p such that $p \nmid q$.

Cyclic Learning with Rounding Here we extend the function $\lfloor \cdot \rceil_p$ to the natural order as follows: let $a \in \Lambda_q$, with $a = a_0 + ua_1 + ... + u^{d-1}a_{d-1}$, with every $a_i \in \mathcal{O}_L/q\mathcal{O}_L$, so we can write $a_i = a_{i,0} + a_{i,1}x + ... + a_{i,nd-1}x^{nd-1}$ with $a_{i,j} \in \mathbb{Z}_q$ for $j = 0, ..., nd-1$. Then we apply $\lfloor \cdot \rceil_p$ to a coefficient-wise.

Definition 29. Let $s \in \Lambda_q$ and $q >> p$. A $\mathrm{CLWR}_{q,p,s}$ sample is sampled by taking $a \leftarrow U(\Lambda_q)$ and outputting $(a, \lfloor a \cdot s \rceil_p) \in \Lambda_q \times \Lambda_p$. Then the *decision* CLWR ($\mathrm{DCLWR}_{q,p,s}$) problem is: given m independent $\mathrm{CLWR}_{q,p,s}$ samples, distinguish them with non-negligible probability from m samples $(a, u) \leftarrow U(\Lambda_q \times \Lambda_p)$.

The Hardness of LWR There have been numerous attempts to obtain reductions from LWE to ensure the hardness of LWR. In [6], LWR was introduced, extended to rings (RLWR) and a proof given bounding the hardness of LWR by LWE. The proof relies on the distribution of the error being bounded, as stated in Definition 30, and on the modulus q being super-polynomial.

In [3], a proof is given for MLWR. Other papers giving reductions for LWR and its variants include [4], [7], [9], and [21].

The Hardness of CLWR We adapt work done in [6], which shows that decision-LWR is at least as hard as decision-LWE, to cyclic algebras. This is

done by applying the triangle inequality to the probability that an adversary can distinguish between samples obtained from various 'games'. Our proof too needs super-polynomial q. After preliminary definitions, we define five games.

Definition 30. [6, §3.1] A probability distribution χ over $\mathbb{Z}$ is *B-bounded* if $\Pr_{x\leftarrow\chi}[|x| > B] \leq \mathrm{neg}(n)$. A distribution χ over a ring R is B-bounded if the marginal distribution of every coefficient (with respect to a fixed basis) of $x \leftarrow \chi$ is B-bounded. A distribution χ over Λ is B-bounded if the marginal distribution of every coefficient (with respect to the basis $\{u^i\}$) of $x \leftarrow \chi$ is B-bounded.

We extend this to the natural order as follows: a distribution over the natural order is B-bounded if the marginal distribution of every coefficient, with respect to the power basis $\{u^i\}$, is B-bounded, in the sense given above.

Definition 31. [6, §2.1] The distinguishing advantage of an adversary $\mathcal{A}$ for games H_0, H_1 is $\mathrm{Adv}_{H_0,H_1}(\mathcal{A}) := |\Pr[\mathcal{A} \text{ accepts in } H_0] - \Pr[\mathcal{A} \text{ accepts in } H_1]|$.

The variant of CLWE we use below is called the 'primal' form in [14], which we denote $\mathrm{CLWE}_{q,s,\chi}$ and has a reduction from standard CLWE defined over $\Lambda^\vee$.

Let $f_B = b_0 + ub_1 + ... + u^{d-1}b_{d-1} \in \Lambda_q$ be such that each $b_i \in \mathcal{O}_{L_q}$ is B-bounded. Then if, for fixed b, $\lfloor b + f_B \rceil_p \neq \lfloor b \rceil_p$, we call this a *bad* event (denoted BAD below). We now define the following distinguishing games (as in [6]):

Game 0: Choose $s \in \Lambda_q$ and generate a number of CLWR samples upon the request of the attacker. The attacker must distinguish these from the same number of samples taken uniformly at random from $\Lambda_q \times \Lambda_p$.
Game 1: Choose $s \in \Lambda_q$. Upon the request of the attacker, generate $(a, b) = (a, a \cdot s + e) \in \Lambda_q \times \Lambda_q$ as in $\mathrm{CLWE}_{q,s,\chi}$, and output $(a, \lfloor b \rceil_p) \in \Lambda_q \times \Lambda_p$. In Game 1, if we encounter a bad event, we abort the game.
Game 2: Upon the request of the attacker, take $(a, b) \leftarrow U(\Lambda_q \times \Lambda_q)$ and output $(a, \lfloor b \rceil_p) \in \Lambda_q \times \Lambda_p$. If we encounter a bad event, we abort the game.
Game 3: Upon the request of the attacker, choose $(a, b) \leftarrow U(\Lambda_q \times \Lambda_q)$ and output $(a, \lfloor b \rceil_p) \in \Lambda_q \times \Lambda_p$ (note there is no condition on bad events occuring).
Game 4: Upon the request of the attacker, choose $(a, b) \leftarrow U(\Lambda_q \times \Lambda_p)$ and output this to the attacker.

Lemma 17. *Let $(a, b) \leftarrow U(\Lambda_q \times \Lambda_q)$ and denote Game i by G_i. Then* $\Pr[\mathit{BAD} \text{ occurs on } b \text{ in } G_2] \leq (2B+1) \cdot p \cdot nd^2/q$.

Proof. For the case of plain LWR, that is $b \in \mathbb{Z}_q$, by [6] we have

$$\Pr[\text{BAD occurs on } b \text{ in } G_2] \leq (2B+1) \cdot p/q. \qquad \square$$

Lemma 18. *Let $K/\mathbb{Q}$ be a cyclotomic field of power-of-2 degree, and L/K a cyclic Galois extension of power-of-2 degree. Then the statistical distance $\Delta\left(U\left(\Lambda_q^n \times \Lambda_p\right), U\left(\Lambda_q^n\right) \times \lfloor U\left(\Lambda_q\right) \rceil_p\right) \leq \mathrm{neg}(n)$ for some q exponential in p, n.*

In our cases, the quantities $|\Lambda_p|$, $|\Lambda_q|$ will always be powers of p and q respectively. We usually take q split completely in K, in which case $|\Lambda_q| = q^{nd^2}$.

Proof. See appendix. □

Theorem 9. *Let χ be an efficiently sampleable B-bounded distribution over Λ and $q \geq pBd^2 \cdot n^{\omega(1)}$ such that $\Delta = \mathrm{neg}(n)$. For any distribution over $s \in \Lambda_q$, $DCLWR_{q,p,s}$ is at least as hard as $DCLWE_{q,s,\chi}$ for the same distribution over s.*

Proof. By Lemmas 17, 18, the same as [6, Theorem 3.2] mutatis mutandis. □

Thus one could replace the sampled errors of CLWE with errors introduced by deterministic rounding (for specific parameters) with a certain level of confidence in the security of such a procedure. We note the popularity of rounding-based schemes [12],[5], and leave open the development of CLWR-based schemes.

References

[1] A.A. Albert. *Structure of Algebras*. AMS colloquium publications v. 24. American Mathematical Society, 1939. ISBN: 9780821810248.

[2] M. Albrecht, R. Player, and S. Scott. "On the concrete hardness of Learning with Errors". In: *Journal of Mathematical Cryptology* 9.3 (2015), pp. 169–203. DOI: doi:10.1515/jmc-2015-0016.

[3] J. Alperin-Sheriff and D. Apon. *Dimension-Preserving Reductions from LWE to LWR*. Cryptology ePrint Archive, Report 2016/589. https://eprint.iacr.org/2016/589. 2016.

[4] J. Alwen, S. Krenn, K. Pietrzak, and D. Wichs. "Learning with Rounding, Revisited". In: *CRYPTO 2013*. Ed. by R. Canetti and J. A. Garay. Vol. 8042. LNCS. Springer Berlin Heidelberg, 2013, pp. 57–74. DOI: 10.1007/978-3-642-40041-4_4.

[5] R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé. *CRYSTALS-Kyber*. CRYSTALS Cryptographic Suite for Algebraic Lattices. https://pq-crystals.org/kyber/data/kyber-specification-round3-20210804.pdf. 2021.

[6] A. Banerjee, C. Peikert, and A. Rosen. "Pseudorandom Functions and Lattices". In: *EUROCRYPT 2012*. Ed. by D. Pointcheval and T. Johansson. Vol. 7237. LNCS. Springer Berlin Heidelberg, pp. 719–737. DOI: 10.1007/978-3-642-29011-4_42.

[7] A. Bogdanov, S. Guo, D. Masny, S. Richelson, and A. Rosen. "On the Hardness of Learning with Rounding over Small Modulus". In: *TCC 2016*. Ed. by T. Kushilevitz E. & Malkin. Vol. 9562. LNCS. Springer Berlin Heidelberg, 2016, pp. 209–224. DOI: 10.1007/978-3-662-49096-9_9.

[8] M. Bolboceanu, Z. Brakerski, R. Perlman, and D. Sharma. "Order-LWE and the Hardness of Ring-LWE with Entropic Secrets". In: *ASIACRYPT 2019*. Vol. 11922. LNCS. Springer International, 2019, pp. 91–120. DOI: doi.org/10.1007/978-3-030-34621-8_4.

[9] L. Chen, Z. Zhang, and Z. Zhang. "On the Hardness of the Computational Ring-LWR Problem and Its Applications". In: *ASIACRYPT 2018*. Springer International, 2018. DOI: 10.1007/978-3-030-03326-2_15.

[10] Q. Cheng, J. Zhang, and J. Zhuang. "LWE from non-commutative group rings". In: *Designs, Codes and Cryptography* 90.1 (Jan. 2022), pp. 239–263. DOI: 10.1007/s10623-021-00973-6.

[11] K. Conrad. *The Conductor Ideal of an Order*. 2018. URL: https://kconrad.math.uconn.edu/blurbs/gradnumthy/conductor.pdf.

[12] J-P. D'Anvers, A. Karmakar, S. Sinha Roy, and F. Vercauteren. "Saber: Module-LWR Based Key Exchange, CPA-Secure Encryption and CCA-Secure KEM". In: *AFRICACRYPT 2018*. Ed. by A. Joux, A. Nitaj, and T. Rachidi. Vol. 10831. LNCS. Springer International, 2018, pp. 282–305. DOI: doi.org/10.1007/978-3-319-89339-6_16.

[13] I.B. Fesenko and S.V. Vostokov. *Local Fields and Their Extensions*. Transl. Math. Monogr. Amer. Math. Soc., 2002. ISBN: 978-0821832592.

[14] C. Grover. "LWE over cyclic algebras: a novel structure for lattice cryptography". PhD thesis. Imperial College London, June 2020. URL: https://spiral.imperial.ac.uk/handle/10044/1/97982.

[15] C. Grover, A. Mendelsohn, C. Ling, and R. Vehkalahti. "Non-commutative Ring Learning with Errors from Cyclic Algebras". In: *J. Cryptol.* 35 (July 2022). DOI: 10.1007/s00145-022-09430-6.

[16] H. Hasse. *Beweis eines Satzes und Wiederlegung einer Vermutung über das allgemeine Normenrestsymbol*. German. 1931, pp. 64–69. URL: https://www.digizeitschriften.de/id/252457811_1931|log1.

[17] C. Hollanti, J. Lahtonen, and H.-F. Lu. "Maximal Orders in the Design of Dense Space-Time Lattice Codes". In: *IEEE Transactions on Information Theory* 54.10 (2008), pp. 4493–4510. DOI: 10.1109/TIT.2008.928998.

[18] G. Janusz. *Algebraic Number Fields*. Amer. Math. Soc., 1995. ISBN: 9780821872437.

[19] M. Kimball. *Quaternion Algebras in Number Theory*. 2017. URL: http://www2.math.ou.edu/~kmartin/quaint.

[20] A. Langlois and D. Stehlé. "Worst-case to average-case reductions for module lattices". In: *Designs, Codes and Cryptography* 75.3 (June 2015), pp. 565–599. ISSN: 1573-7586. DOI: 10.1007/s10623-014-9938-4.

[21] F.-H. Liu and Z. Wang. "Rounding in the Rings". In: *CRYPTO 2020*. Ed. by D. Micciancio and T. Ristenpart. Vol. 12171. LNCS. Springer International, 2020, pp. 296–326. DOI: 10.1007/978-3-030-56880-1_11.

[22] V. Lyubashevsky, C. Peikert, and O. Regev. "On Ideal Lattices and Learning with Errors over Rings". In: *EUROCRYPT 2010*. Ed. by H. Gilbert. Vol. 6110. LNCS. Springer Berlin Heidelberg, 2010, pp. 1–23. DOI: 10.1007/978-3-642-13190-5_1.

[23] Y. I. Manin. "Classical computing, quantum computing, and Shor's factoring algorithm". In: *Séminaire Bourbaki* 41 (1998-1999), pp. 375–404. URL: http://eudml.org/doc/110265.

[24] D. Marcus. *Number Fields*. Universitext. Springer-Verlag, 1977. ISBN: 9783319902326.

[25] A. B. Meli. *Cyclotomic Extensions and Quadratic Reciprocity*. 2013. URL: http://math.uchicago.edu/~may/REU2013/REUPapers/Meli.pdf.

[26] D. Micciancio and O. Regev. "Worst-case to average-case reductions based on Gaussian measures". In: *FOCS '04*. 2004. DOI: 10.1109/FOCS.2004.72.

[27] J. Lahtonen N. Markin G. McGuire. "Construction of Multiblock Space–Time Codes From Division Algebras With Roots of Unity as Nonnorm Elements". In: *IEEE Trans. Inf. Theory* 54.11 (2008), pp. 5231–5235.
[28] J. Neukirch. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2010. ISBN: 9783642084737.
[29] F. Oggier and G. Berhuy. *An Introduction to Central Simple Algebras and Their Applications to Wireless Communication*. AMS Mathematical Surveys and Monographs. AMS, 2013. ISBN: 978-0-8218-4937-8.
[30] F. Oggier and B. A. Sethuraman. "Quotients of orders in cyclic algebras and space-time codes". In: *Adv. Math. Commun.* 7.4 (2013), pp. 441–461.
[31] C. Peikert and Z. Pepin. "Algebraically Structured LWE, Revisited". In: *TCC 2019*. Vol. 11891. LNCS. Springer International, 2019, pp. 1–23. DOI: 10.1007/978-3-030-36030-6_1.
[32] O. Regev. "On lattices, learning with errors, random linear codes, and cryptography". In: *Journal of the ACM* 56 (2009). DOI: 10.1145/1568318.
[33] I. Reiner. *Maximal Orders*. London Mathematical Society Monographs. Oxford University Press, 2003. ISBN: 9780198526735.
[34] J.P. Serre. *Local Fields*. Trans. by M.J. Greenberg. Graduate Texts in Mathematics. Springer New York, 2013. ISBN: 9781475756739.
[35] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar. "Full-diversity, high-rate space-time block codes from division algebras". In: *IEEE Transactions on Information Theory* 49.10 (2003), pp. 2596–2616.
[36] P. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *FOCS 1994*. IEEE Comp. Soc. Press, 1994, pp. 124–134.
[37] D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa. "Efficient Public Key Encryption Based on Ideal Lattices". In: *ASIACRYPT 2009*. Ed. by M. Matsui. Vol. 5912. LNCS. Springer Berlin Heidelberg, 2009, pp. 617–635. DOI: 10.1007/978-3-642-10366-7_36.
[38] L. C. Washington. *Introduction to Cyclotomic Fields*. Graduate Texts in Mathematics. Springer New York, 2012. ISBN: 9781461219347.

A Proof of Lemma 18

Consider $P(\lfloor \mathcal{O}_{K_q} \rceil_p = x)$. Coefficients are rounded independently, so $P(\lfloor a \rceil_p = x) = \prod_{i=0}^{n-1} P(\lfloor a_i \rceil_p = x_i)$, for $a \in \mathcal{O}_{K_q}$ with $\mathbb{Z}_q$-coefficients a_i and x x_i. Since $P(\lfloor a_i \rceil_p = x_i) \in \{\frac{y}{q}, \frac{y+1}{q}\}$, $P(\lfloor a \rceil_p = x) \in \{\frac{y^n}{q^n}, \frac{y^{n-1}(y+1)}{q^n}, ..., \frac{y(y+1)^{n-1}}{q^n}, \frac{(y+1)^n}{q^n}\}$. Let $q = py + r$ with r minimal. The statistical distance is then

$$\Delta = \frac{1}{2}\Big[r^n \left|\frac{1}{p^n} - \frac{(y+1)^n}{q^n}\right| + \binom{n}{1} r^{n-1}(p-r)\left|\frac{1}{p^n} - \frac{y(y+1)^{n-1}}{q^n}\right| + ... \\ + \binom{n}{n-1} r(p-r)^{n-1}\left|\frac{1}{p^n} - \frac{y^{n-1}(y+1)}{q^n}\right| + (p-r)^n \left|\frac{1}{p^n} - \frac{y^n}{q^n}\right|\Big]$$

We pair the first and last terms, and consider inner terms one by one. For the outer terms $\frac{1}{2}\left[r^n\left|\frac{1}{p^n}-\frac{(y+1)^n}{q^n}\right|+(p-r)^n\left|\frac{1}{p^n}-\frac{y^n}{q^n}\right|\right]$ $(*)$, note

$$(p-r)^n\left|\frac{1}{p^n}-\frac{y^n}{q^n}\right| = \left|\frac{(p-r)^n}{p^n}-\frac{(p-r)^n y^n}{q^n}\right| = \left|(1-\frac{r}{p})^n-\frac{(py-ry)^n}{q^n}\right|$$
$$= \left|(1-\frac{r}{p})^n-\frac{(q-r(y+1))^n}{q^n}\right| = \left|(1-\frac{r}{p})^n-\left(1-\frac{r(y+1)}{q}\right)^n\right|.$$

Since n is a power of two this is a difference of two squares. Factoring it as a product of a sum and difference, the difference is also a difference of two squares. We iterate this to factor out $|\frac{r(y+1)}{q}-\frac{r}{p}|$, which is bounded by $\frac{p}{q}$ by [6]. Formally,

$$\left|(1-\frac{r}{p})^n-(1-\frac{r(y+1)}{q})^n\right| = \left|\frac{r(y+1)}{q}-\frac{r}{p}\right|\cdot\left|1-\frac{r}{p}+1-\frac{r(y+1)}{q}\right|$$
$$\cdot\left|(1-\frac{r}{p})^2+(1-\frac{r(y+1)}{q})^2\right|\cdot\ldots\cdot\left|(1-\frac{r}{p})^{n/2}+\left(1-\frac{r(y+1)}{q}\right)^{n/2}\right|.$$

We can do similarly for $r^n\left|\frac{1}{p^n}-\frac{(y+1)^n}{q^n}\right|$; we have, factorising,

$$r^n\left|\frac{1}{p^n}-\frac{(y+1)^n}{q^n}\right| = \left|\frac{r^n}{p^n}-\frac{r^n(y+1)^n}{q^n}\right| = \left|\left(\frac{r}{p}\right)^n-\left(\frac{r(y+1)}{q}\right)^n\right|$$
$$= \left|\frac{r}{p}-\frac{r(y+1)}{q}\right|\cdot\left|\frac{r}{p}+\frac{r(y+1)}{q}\right|\cdot\ldots\cdot\left|\left(\frac{r}{p}\right)^{n/2}+\left(\frac{r(y+1)}{q}\right)^{n/2}\right|$$

Combining these, we find that the sum of the outer terms

$$(*) = \frac{1}{2}\Big[\left|\frac{r}{p}-\frac{r(y+1)}{q}\right|\cdot\left|\frac{r}{p}+\frac{r(y+1)}{q}\right|\cdot\ldots\cdot\left|(\frac{r}{p})^{n/2}+(\frac{r(y+1)}{q})^{n/2}\right|+$$
$$\left|\frac{r(y+1)}{q}-\frac{r}{p}\right|\cdot\left|1-\frac{r}{p}+1-\frac{r(y+1)}{q}\right|\cdot\ldots\cdot\left|(1-\frac{r}{p})^{n/2}+(1-\frac{r(y+1)}{q})^{n/2}\right|\Big].$$

We remove the previously mentioned factor:

$$(*) = \frac{1}{2}\Big[\left|\frac{r}{p}-\frac{r(y+1)}{q}\right|\cdot\Big[\left|\frac{r}{p}+\frac{r(y+1)}{q}\right|\cdot\ldots\cdot\left|(\frac{r}{p})^{n/2}+(\frac{r(y+1)}{q})^{n/2}\right|$$
$$+\left|1-\frac{r}{p}+1-\frac{r(y+1)}{q}\right|\cdot\ldots\cdot\left|(1-\frac{r}{p})^{n/2}+(1-\frac{r(y+1)}{q})^{n/2}\right|\Big]\Big]$$
$$\leq \frac{p}{2q}\Big[\left|\frac{r}{p}+\frac{r(y+1)}{q}\right|\cdot\ldots\cdot\left|(\frac{r}{p})^{n/2}+(\frac{r(y+1)}{q})^{n/2}\right|$$
$$+\left|1-\frac{r}{p}+1-\frac{r(y+1)}{q}\right|\cdot\ldots\cdot\left|(1-\frac{r}{p})^{n/2}+(1-\frac{r(y+1)}{q})^{n/2}\right|\Big].$$

A term inside the large brackets has equal powers of q on the numerator and denominator. Multiplying the bracket by $\frac{p}{q}$, it has as a polynomial in q degree -1, as required. For inner terms of the statistical distance, the ith term is

$\frac{1}{2}\binom{n}{i} r^{n-i}(p-r)^i \left|\frac{1}{p^n} - \frac{y^i(y+1)^{n-i}}{q^n}\right|$. Since n is even, so is $\binom{n}{i}$. We can write

$$r^{n-i}(p-r)^i\left|\frac{1}{p^n} - \frac{y^i(y+1)^{n-i}}{q^n}\right| = \left|\frac{r^{n-i}(p-r)^i}{p^n} - \frac{r^{n-i}(p-r)^i y^i(y+1)^{n-i}}{q^n}\right|$$
$$= \left|\frac{r^{n-i}(p-r)^i q^n - p^n(q-r(y+1))^i(r(y+1))^{n-i}}{p^n q^n}\right|, \text{ and since}$$
$$p^n(q-r(y+1))^i(r(y+1))^{n-i} = (pq-pr(y+1))^i(pr(y+1))^{n-i}$$
$$= (pq-r(py+p))^i(r(py+p))^{n-i} = (pq-r(q-r+p))^i(r(q-r+p))^{n-i}$$
$$= (pq-rq-r^2+rp))^i(rq-r^2+rp))^{n-i} = ((q+r)(p-r))^i(rq+r(p-r))^{n-i}$$

we find that the q^n term has coefficient $(p-r)^i r^{n-i}$. Hence the numerator of $\frac{r^{n-i}(p-r)^i q^n - p^n(q-r(y+1))^i(r(y+1))^{n-i}}{p^n q^n}$ has q-degree $n-1$, and the denominator q-degree n, as required. Putting the above together, we find

$$\begin{aligned}\Delta &= \frac{1}{2}\Big[r^n\left|\frac{1}{p^n} - \frac{(y+1)^n}{q^n}\right| + \binom{n}{1} r^{n-1}(p-r)\left|\frac{1}{p^n} - \frac{y(y+1)^{n-1}}{q^n}\right| + ... \\ &+ \binom{n}{n-1} r(p-r)^{n-1}\left|\frac{1}{p^n} - \frac{y^{n-1}(y+1)}{q^n}\right| + (p-r)^n\left|\frac{1}{p^n} - \frac{y^n}{q^n}\right|\Big] \\ &= \frac{1}{2}\Big[r^n\left|\frac{1}{p^n} - \frac{(y+1)^n}{q^n}\right| + (p-r)^n\left|\frac{1}{p^n} - \frac{y^n}{q^n}\right| + \\ &nr^{n-1}(p-r)\left|\frac{1}{p^n} - \frac{y(y+1)^{n-1}}{q^n}\right| + ... + nr(p-r)^{n-1}\left|\frac{1}{p^n} - \frac{y^{n-1}(y+1)}{q^n}\right|\Big]\end{aligned}$$

$$\begin{aligned}&\leq \frac{p}{2q}\Bigg[\left|\frac{r}{p} + \frac{r(y+1)}{q}\right| \cdot ... \cdot \left|\left(\frac{r}{p}\right)^{n/2} + \left(\frac{r(y+1)}{q}\right)^{n/2}\right| + \\ &\left|1 - \frac{r}{p} + 1 - \frac{r(y+1)}{q}\right| \cdot ... \cdot \left|\left(1-\frac{r}{p}\right)^{n/2} + \left(1 - \frac{r(y+1)}{q}\right)^{n/2}\right|\Bigg] \\ &+ \frac{1}{2}\sum_{i=1}^{n-1}\binom{n}{i}\left|\frac{r^{n-i}(p-r)^i q^n - p^n(q-r(y+1))^i(r(y+1))^{n-i}}{p^n q^n}\right|,\end{aligned}$$

and so by the previous analysis there exists some q' exponentially large in p and n such that for all $q \geq q'$, the considered statistical distance is negligible.

We now find $P(\lfloor \Lambda_q \rceil_p = x)$. This is the same as above, since the coefficients are rounded independently: namely, since by assumption $[\Lambda : \mathbb{Q}] = 2^r$ for some r, we have $P(\lfloor a \rceil_p = x) = \prod_{i=0}^{nd^2-1} P(\lfloor a_i \rceil_p = x_i)$ for any $a \in \Lambda_q$ with coefficients a_i. To find the statistical distance, the argument then proceeds identically.