Learning with Errors from Nonassociative Algebras

Andrew Mendelsohn and Cong Ling

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

Keywords: learning with errors, lattices, post-quantum, public-key encryption

Abstract. We construct a provably-secure structured variant of Learning with Errors (LWE) using nonassociative cyclic division algebras, assuming the hardness of worst-case structured lattice problems, for which we are able to give a full search-to-decision reduction, improving upon the construction of Grover et al. named 'Cyclic Learning with Errors' (CLWE). We are thus able to create structured LWE over cyclic algebras without any restriction on the size of secret spaces, which was required for CLWE as a result of its restricted security proof. We reduce the shortest independent vectors problem in ideal lattices, obtained from ideals in orders of such algebras, to the decision variant of LWE defined for nonassociative CDAs. We believe this variant has greater security and greater freedom with parameter choices than CLWE, and greater asymptotic efficiency of multiplication than module LWE. Our reduction requires new results in the ideal theory of such nonassociative algebras, which may be of independent interest. We then adapt an LPR-like PKE scheme to hold for nonassociative spaces, and discuss the efficiency and security of our construction, showing that it is immune to certain subfield attacks. Finally, we give example parameters to construct algebras for cryptographic use.

1 Introduction

In [1], Ajtai gave a reduction from the 'shortest vector problem' (SVP) on integer lattices to random instances of SVP on a particular class of integer lattices. These reductions were later used to ground the security of a public key encryption (PKE) scheme [2]. Such *worst-case to average-case reductions* have been acclaimed by cryptographers: they imply that if some instance of a problem is 'hard' (i.e. computationally intractable) then with respect to some distribution over problem instances, a randomly selected instance will also be hard to solve.

Similar reductions for other cryptographic problems have subsequently been obtained: in [28] it was shown that an average-case form of the 'small integer solutions' (SIS) problem is at least as hard as a worst-case 'shortest independent vectors problem' (SIVP), and, pertinently for this work, in [39] it was shown that average-case 'learning with errors' (LWE) is at least as hard as worst-case

SIVP.

In more detail, (search) LWE asks a solver to obtain a vector $\mathbf{s} \in \mathbb{Z}_q^n$ of integers modulo q from samples of the form

$$(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$$

Here $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$, e is an 'error' (or 'noise') term and $\mathbf{a}$ is taken uniformly at random over the domain. One can also consider the case of errors taken from a domain which is not discrete. The decision form of the problem is to decide if a collection of samples is taken as above, or is sampled uniformly from the domain.

LWE has subsequently become a centerpiece of lattice-based cryptography. Varied functionalities, from signature schemes (e.g. [22], [11], [12]) to fully homomorphic encryption (e.g. [6], [13], [9], [10]), have been obtained from the LWE assumption. Moreover, in 2022 NIST standardized Crystals-Kyber as their post-quantum KEM of choice, and Crystals-Dilithium as one of two standardized post-quantum signatures [29]. Both schemes are based on structured forms of LWE.

Schemes based on structured forms of LWE, like Kyber, aim to achieve trade-offs between efficiency and security by using algebraic structure (e.g. from rings of integers of number fields or modules over these rings). These structured variants include Ring LWE (RLWE) [24] using rings of integers of number fields, Polynomial LWE [45] using a more general class of polynomial rings, and Module LWE (MLWE) [18] using modules of finite rank over rings of integers, and others.

In [14], a structured form of LWE was introduced, via an object known as a cyclic division algebra (CDA), and called CLWE. This variant generalised RLWE, and aimed to attain a comparable level of security to MLWE while improving on its efficiency. A limitation of CLWE, however, is that while a reduction from worst-case lattice problems to the search CLWE problem was obtained, the reduction from the search to the decision problem only holds for a limited set of secrets. There may thus be choices of secret for CLWE which are in some sense structurally weak, and so no security reduction may be given for them. In this work, we study structured LWE over a closely related family of algebras, for which we obtain a full reduction from worst-case lattice problems. This allows us to totally remove the restriction on the size of the set of secrets which limited CLWE, for well-chosen parameters. We may thus be confident that structured LWE can be created from CDAs with no possibility of structurally weak secrets. This may suggest that the nonassociative generalisation of number fields will prove a more fruitful structure with which to structure LWE than the associative option.

1.1 Contributions

We introduce *NCLWE*, a form of structured LWE obtained by using orders of nonassociative cyclic algebras, rather than orders of associative cyclic algebras as in CLWE. We briefly outline the construction of these algebras (more detail is given in Section 3). In [14], CDAs were built by setting $K = \mathbb{Q}(\zeta_m)$ to be the mth cyclotomic field, and taking a certain finite extension L of degree $[L : K] = d$, with cyclic Galois group generated by an automorphism θ such that a chosen element $\gamma \in \mathcal{O}_K^\times$ is not in the image of the field norm $N_{L/K}(\cdot)$ from L to K. An auxiliary element u satisfying $u^d = \gamma$ and $ux = \theta(x)u$ was defined, and an algebra $\mathcal{A} = L \oplus uL \oplus ... \oplus u^{d-1}L$ constructed. An order (full-rank discrete subring) is then defined: $\Lambda = \mathcal{O}_L \oplus u\mathcal{O}_L \oplus ... \oplus u^{d-1}\mathcal{O}_L$, called the natural order.

In this work we consider the case of $\gamma \in \mathcal{O}_L^\times \setminus \mathcal{O}_K^\times$. As will be seen below, the resulting algebras $\mathcal{A}$ still yield CDAs and Λ is still an order, but multiplication is not associative; for instance, $u(u^{d-1}u) = u\gamma$, but $(uu^{d-1})u = u\theta(\gamma)$. This lack of associativity poses a number of technical problems; mathematically, results on the ideal theory of associative Λ cannot be applied, and cryptographically, the Regev-style cryptosystem of [14] cannot be straightforwardly mirrored for CLWE-style samples defined from nonassociative CDAs.

In this work we overcome both of these obstacles. We begin with a study of multiplicative ideal theory of two-sided ideals in nonassociative natural orders, and obtain

Theorem 6. Let $\Lambda \subset \mathcal{A} = (L/K, \theta, \gamma)$ be the natural order of a nonassociative CDA and $\gamma \in \mathcal{O}_L^\times$. Then multiplication of Λ-ideals $\mathcal{I}$ such that $\mathcal{I} \cap \mathcal{O}_K$ is unramified in $\mathcal{O}_L$ yields ideals, and is commutative and associative.

We use this to give an unrestricted search-to-decision reduction for NCLWE samples, in contrast to the partial reduction for CLWE, for certain moduli. Below, $\Lambda^\vee$ is the dual of Λ.

Theorem 7, informal. Let $\Lambda \subset \mathcal{A} = (L/K, \theta, \gamma)$, $q \geq 2$ such that $q\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{q}_i$, and $\alpha \in (0, 1)$ such that $\alpha q \geq \eta_\varepsilon(\Lambda^\vee)$ for negligible ε. Then there is a probabilistic polynomial-time reduction from search $\text{NCLWE}_{q,s,\Sigma_\alpha,G}$ for s in any pairwise difference set $G \subset \Lambda_q^\vee$ to decision $\text{NCLWE}_{q,\Upsilon_\alpha}$.

When the $\mathfrak{q}_i$ are inert in $\mathcal{O}_L$ and either d is prime or $1, \gamma, \dots, \gamma^{d-1}$ are linearly independent over $\mathcal{O}_K/\mathfrak{q}_i$ for each i, then there is a probabilistic polynomial-time reduction from search $\text{NCLWE}_{q,s,\Sigma_\alpha}$ to decision $\text{NCLWE}_{q,\Upsilon_\alpha}$.

We then obtain a reduction from SIVP on lattices which are embeddings of ideals of Λ in the standard manner of [18],[14], [25], which combined with Theorem 7 yields a reduction from worst-case lattice problems to decision NCLWE.

We then relate NCLWE to cryptography by tweaking the Regev-style scheme of [14] to maintain correctness in spite of the nonassociativity of our algebras, when $d = 2$. We conclude by giving parameter suggestions for CDAs with which to implement our scheme, with a discussion of a subspace attack on structured LWE variants, and with numerical results from the lattice estimator [4] applied to our parameter choices.

As mentioned above, our results introduce a structured form of LWE using cyclic algebras which has a complete security proof. A consequence of this is that we may have greater confidence in NCLWE than CLWE that there are no structurally weak choices of secret, a possibility left open by the security proofs of [14]. We also note that nonassociative rings may be considered the least structured algebraic object used to create ring-based LWE to date (insofar as they lack associativity and commutativity), and it may be considered advantageous to have such unstructured LWE instances so as to hedge against the possibility of algebraic attacks which exploit specific algebraic structures also solving our LWE instances; for instance, attacks against LWE over cyclotomic fields may be unlikely to also apply to LWE over nonassociative algebras.

We note that both CLWE and NCLWE are in fact instance of structured MLWE. This is because one sample of (N)CLWE results in numerous correlated samples of MLWE. It is thus possible that the security of (N)CLWE is close to that of MLWE while allowing for greater asymptotic efficiency than MLWE. We see the exploration of this possibility as an interesting question and we leave quantifying the gap between (N)CLWE and MLWE for future work.

1.2 Prior work

Associative cyclic division algebras were used in coding theory in [41]. Works such as [30], [15] further developed this. Nonassociative CDAs were developed in [46], [19], Steele's thesis [43], and also in [42], [44], [38].

CDAs were used in cryptography to create structured LWE in [14], [25] and for NTRU in [21]. For more on the mathematics of nonassociative rings, see [40].

The usefulness of noncommutative structures for post-quantum cryptography was hinted at by Micciancio and Peikert in the Simons Institute Workshop on the Mathematics of Modern Cryptography [27], where they wrote that lattice-based cryptographic progress had been built on 'approximation problems on point lattices, their specializations to structured lattices arising in algebraic number theory, and, more speculatively, problems from noncommutative algebra.'

2 Preliminaries

2.1 Lattices

A $\mathbb{Z}$-lattice $\mathcal{L}$ is the integer linear span of a set of vectors $\mathbf{b}_i$, $\mathcal{L} = \{\sum_i a_i \mathbf{b}_i : a_i \in \mathbb{Z}\}$. We may write the $\mathbf{b}_i$ as the columns of a matrix B and refer to the lattice $\mathcal{L} = \mathcal{L}(B)$ defined by the span of the columns of B. More generally, if V is a finite-dimensional vector space over a field K and R is a discrete subring of K then an *R-lattice* in V is a subspace $L \subset V$ such that L is a finitely-generated R-module. Equivalently, L is a finitely-generated torsion-free R-module. If $\dim_{\mathbb{Z}}(R) = \dim_{\mathbb{Q}}(V)$, we call R an order. An order is *maximal* if it is maximal with respect to inclusion. An R-lattice L is called *full* if it contains a K-basis of V, so $V = KL$. Fixing a basis B of V, the R-linear span of B is a full lattice. We will be concerned with full lattices in $V = \mathbb{R}^n$.

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

Definition 2. *Let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice and $\| \cdot \|$ be a norm. Then $\lambda_i(\mathcal{L})$ denotes the ith successive minimum of $\mathcal{L}$ with respect to the norm $\| \cdot \|$, that is the minimum length of a set of i linearly independent vectors in $\mathcal{L}$, where the length of a set of vectors $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ is $\max_i (\|\mathbf{x}_i\|)$.*

2.2 Discrete Gaussians

Equip $\mathbb{R}^n$ with the Euclidean norm $\|\cdot\|_2 = \|\cdot\|$, and let $\mathbf{a} \in \mathbb{R}^n$ and $r > 0$. Define the *Gaussian function* by $\rho_{r,\mathbf{a}} : \mathbb{R}^n \to (0, 1], \boldsymbol{x} \mapsto \exp\left(-\pi\|\boldsymbol{x} - \mathbf{a}\|/r^2\right)$. Then the Gaussian distribution D_r is defined by the probability density function $\frac{1}{r}\rho_{r,0}$.

Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be a basis of $\mathbb{R}^n$ and $\mathbf{r} = (r_1, \ldots, r_n) \in \mathbb{R}^n$. An *elliptical* Gaussian distribution $D_{\mathbf{r}}$ over $\mathbb{R}^n$ is obtained by sampling $x_i \leftarrow D_{r_i}$ independently for all $i \neq j$ and outputting $\sum_{i=1}^n x_i \mathbf{b}_i$. If the r_i are all identical, $D_{\mathbf{r}}$ is spherical.

For a lattice $\mathcal{L}$, let $\rho_r(\mathcal{L}) = \sum_{x \in \mathcal{L}} \rho_r(x)$. Then for $x \in \mathcal{L}$, the *discrete* Gaussian distribution $D_{\mathcal{L},r}$ outputs x with probability $\frac{\rho_r(x)}{\rho_r(\mathcal{L})}$.

The *smoothing parameter*, introduced in [28], will be used throughout:

Definition 3. *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 $\rho_{1/r}\left(\mathcal{L}^\vee / \{0\}\right) \leq \varepsilon$.*

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

Lemma 1. *[28, 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, $\rho_r(\mathcal{L} + \boldsymbol{x}) \in \left[\frac{1-\varepsilon}{1+\varepsilon}, 1\right] \cdot \rho_r(\mathcal{L})$*

2.3 Number Fields

An algebraic number field is a field containing $\mathbb{Q}$ with finite index. An example of an algebraic number field is a cyclotomic field, obtained by adjoining a primitive mth root of unity ζ_m to $\mathbb{Q}$ for $\mathbb{Q}(\zeta_m)$, which has degree $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$ where φ is the Euler totient function. Cyclotomic fields are examples of Galois fields. These are characterised by the property that their set of automorphisms has a group structure.

Let L/K be a Galois extension of algebraic number fields. The ring of integers of K is denoted $\mathcal{O}_K$ and is the maximal order of K, and similarly for $\mathcal{O}_L$ and L. Given a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, the ideal $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^g \mathcal{P}_i^e$ factors into a number of powers of prime $\mathcal{O}_L$-ideals $\mathcal{P}_i$. It is a standard result that $efg = [L : K]$, where $f = [\mathcal{O}_L/\mathcal{P}_i : \mathcal{O}_K/\mathfrak{p}]$. If $e = 1$, $\mathfrak{p}$ is called *unramified.* If $g = [L : K]$, $\mathfrak{p}$ *completely splits.* If $f = [L : K]$, $\mathfrak{p}$ is *inert.*

2.4 Lattice Problems

We next define lattice problems used in our reductions for the nonassociative setting outlined below . We parameterise our problems by an algebraic space

A which may be embedded into $\mathbb{R}^n$ for some n, containing an order $A_{\mathbb{Z}}$ over which lattices are defined; for example, $\mathbb{Q}$-SVP$_\xi$ refers to lattice problems over $\mathbb{Z}$-lattices; K-SVP$_\xi$ refers to SVP in an ideal lattice $\mathcal{I}$ of the ring of integers of K; and $\mathcal{A}$-SVP$_\xi$ refers to SVP in an ideal lattice of the natural order of a cyclic algebra $\mathcal{A}$ (definitions below), with respective norms $\|\cdot\|$. Below, $\mathcal{L}$ is an $A_{\mathbb{Z}}$-lattice embedded into $\mathbb{R}^m$.

Definition 4. *For an approximation factor $\xi = \xi(n) \geq 1$, the (approximate) Shortest Vector Problem, A-SVP$_\xi$, is to find an element $a \in \mathcal{L} \setminus 0$ such that $\|a\| \leq \xi \cdot \lambda_1(\mathcal{L})$.*

Definition 5. *The (approximate) Shortest Independent Vectors Problem, A-SIVP$_\xi$, is to find $n := [\mathcal{L} : \mathbb{Z}]$ linearly independent non-zero vectors $\mathbf{x}_1, \ldots, \mathbf{x}_n$ over $\mathbb{Z}$ such that $\max_i (\|\mathbf{x}_i\|) \leq \xi \cdot \lambda_n(\mathcal{L})$, where $\xi \geq 1$.*

Definition 6. *The Discrete Gaussian Sampling problem, denoted A-DGS$_\xi$, is to sample a discrete Gaussian $D_{\mathcal{L},\xi}$, for some parameter $\xi > 0$.*

For A a number field, $d \geq 1$, and $e \in A^d$ let $\|e\|_{2,\infty} = \max_j \sqrt{\sum_{i=0}^{d-1} |\sigma_j(e_i)|^2}$, where the σ_j are the A-embeddings $A \hookrightarrow \mathbb{C}$. We now define the bounded distance decoding (BDD) problems we require.

Definition 7. *Let $\delta < \lambda_1(\mathcal{L})/2$ and ψ be an error distribution. Then the A-BDD$_{\mathcal{L},\delta}$ problem, on input $y = x + e$ for $x \in \mathcal{L}$ and $e \leftarrow \psi$ satisfying $\|e\|_{2,\infty} \leq \delta$, is to compute x.*

Definition 8. *For any $q \geq 2$ the qA-BDD$_{\mathcal{L},d}$ problem is as follows: given an instance of the A-BDD$_{\mathcal{L},\delta}$ problem $y = x + e$ with solution $x \in \mathcal{I}$ and error $e \leftarrow \psi$ satisfying $\|e\|_{2,\infty} \leq \delta$, output $x \bmod q\mathcal{L}$.*

The above two BDD problems are straightforwardly extended to cyclic algebras by considering the error terms as vectors with entries in a number field.

2.5 Learning with Errors

Learning with Errors (LWE) was introduced in [39] by Regev. An LWE sample is constructed by first sampling $\mathbf{a} \leftarrow \mathbb{Z}_q^n$ uniformly at random for some modulus $q \geq 2$ and rank n. One then takes a secret $\mathbf{s} \in \mathbb{Z}_q^n$, samples an error $e \leftarrow \psi$ from an error distribution ψ over $\mathbb{Z}_q$, and outputs

$$(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e \bmod q) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$$

The search problem is to recover $\mathbf{s}$ from polynomially many independent samples, and the decision problem is to decide whether a collection of samples comprises samples taken uniformly random over the domain, or whether they are a collection of independent LWE samples.

One can batch together multiple LWE samples as follows: if there are ℓ LWE samples $(\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s}\rangle + e_i \bmod q)$, one can write

$$(A, A\mathbf{s} + \mathbf{e} \bmod q) \in \mathbb{Z}_q^{\ell \times n} \times \mathbb{Z}_q^n$$

where A has ith row $\mathbf{a}_i$ and the ith entry of $\mathbf{e}$ is e_i. One can take ψ to be an error distribution over a continuous domain, if desired. A reduction from SIVP to the decision LWE problem was given, relating the hardness of LWE to worst-case lattice problems which are currently intractable for well-chosen parameters.

We conclude by observing two issues with LWE: first, that for large values of n, matrix-vector multiplication is not efficient, and second, that storing an LWE sample requires storing $n^2 + n$ values from $\mathbb{Z}_q$, which for large n is a strong requirement. For these reasons and more, variants of LWE have been introduced using algebraic structure to alleviate these concerns, which we explore below.

2.6 Ring LWE

Two works adapted LWE to polynomial rings [45], [24]. The latter of these introduced Ring LWE, using rings of integers of Galois number fields, in particular those of cyclotomic fields $K = \mathbb{Q}(\zeta_m) \cong \mathbb{Q}[x]/\Phi_m(x)$ generated by a primitive mth root of unity (or the roots of the mth cyclotomic polynomial $\Phi_m(x)$). For example, when m is a power of two and $K = \mathbb{Q}[x]/f(x)$ with $f(x) = x^m + 1$, fixing a basis $\{1, x, ..., x^{m-1}\}$, one can write multiplication of polynomials $a = a_0 + a_1 x + ..., s = s_0 + s_1 x + ... \in \mathbb{Z}[x]/f(x)\mathbb{Z}[x]$ as matrix-vector multiplication

$$\operatorname{vec}(a \cdot s) = \begin{pmatrix} a_0 & -a_{m-1} & ... & -a_1 \\ a_1 & a_0 & ... & -a_2 \\ ... & ... & ... & ... \\ a_{m-1} & a_{m-2} & ... & a_0 \end{pmatrix} \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{m-1} \end{pmatrix}$$

In this manner one can replace $As + e$ in LWE samples with polynomial multiplication $a \cdot s + e$ in the ring of integers $\mathcal{O}_K$. Clearly one need only store the m coefficients of a and the m coefficients of $a \cdot s + e$ to store an RLWE key, and fast algorithms exist for polynomial multiplication. Expanding RLWE samples over the integers, one obtains a number of correlated LWE instances.

RLWE was extended to modules of finite rank over number fields, called MLWE [18]. Here one takes $\mathbf{s} \in \mathcal{O}_{K_q}^\ell$, samples $a \leftarrow \mathcal{O}_{K_q}^\ell$ uniformly and $e \leftarrow \psi$ over $\mathcal{O}_{K_q}$ and outputs $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s}\rangle + e \bmod q) \in \mathcal{O}_{K_q}^\ell \times \mathcal{O}_{K_q}$, where $\mathcal{O}_{K_q} = \mathcal{O}_K / q\mathcal{O}_K$ and $\ell > 0$ is the module rank.

We also introduce here the dual form of RLWE. Let $\mathrm{Tr}_{K/\mathbb{Q}}(\cdot)$ denote the field trace. We define the codifferent as

$$\mathcal{O}_K^\vee := \{x \in K : \mathrm{Tr}_{K/\mathbb{Q}}(x\mathcal{O}_K) \subset \mathbb{Z}\}.$$

We then define a dual form of RLWE by taking $s \in \mathcal{O}_{K_q}^\vee$, $a \in \mathcal{O}_{K_q}$, and $e \leftarrow \psi$ where ψ samples over $\mathcal{O}_{K_q}$, and outputting $(a, \frac{1}{q}(a \cdot s) + e \bmod \mathcal{O}_K^\vee)$. This can again be straightforwardly turned into a module problem.

Rather than simply taking the coefficients of polynomials to obtain LWE-style problems, one can instead consider the *canonical embedding* of K into $\mathbb{R}^{[K:\mathbb{Q}]}$. If $K/\mathbb{Q}$ is a finite Galois number field and $[K:\mathbb{Q}]=n$, then there exists an α with minimal polynomial $m_\alpha(x)$ such that $K=\mathbb{Q}[x]/(m_\alpha(x))\cong\mathbb{Q}(\alpha)$. Since K is Galois, it has n distinct automorphisms which are defined by their action on α, and the automorphisms each extend to a unique embedding $K\hookrightarrow\mathbb{C}$. If $\sigma_i(K)\subset\mathbb{R}$, for an embedding σ_i, then σ_i is called *real*, and is otherwise called *complex*. There are r_1 real embeddings and r_2 pairs of complex embeddings of K, satisfying $r_1+2r_2=n$. Ordering the real embeddings first, and then the complex embeddings such that $\sigma_{r_1+j}=\overline{\sigma_{r_1+r_2+j}}$ for $1\leq j\leq r_2$, we define

Definition 9. *The canonical embedding $\sigma_K : K\hookrightarrow\mathbb{R}^{r_1}\times\mathbb{C}^{2r_2}$ is defined by*

$$x\mapsto(\sigma_1(x),...,\sigma_n(x)),\ \textit{for } x\in K$$

and $\operatorname{im}\sigma_K\subset H:=\{(x_1,...,x_n)\in\mathbb{R}^{r_1}\times\mathbb{C}^{2r_2} : x_{r_1+r_2+j}=\overline{x_{r_1+j}},1\leq j\leq r_2\}$.

As inner product spaces $H\cong\mathbb{R}^n$. Note $\sigma_K(x)+\sigma_K(y)=\sigma_K(x+y)$, so an algebraic lattice in K has image under σ_K a lattice in $\mathbb{R}^n$, and $\sigma_K(xy)=\sigma_K(x)\star\sigma_K(y)$ where $\star$ denotes entry-wise products of vectors. The norm $\|x\|:=\|\sigma_K(x)\|_2$ can then be defined, and lattice problems with respect to this norm reduced to RLWE.

2.7 Cyclic LWE

In [14], LWE was adapted to the algebraic setting of cyclic division algebras. These are rings which are also vector spaces over a number field, and this LWE variant targeted achieving comparable security to MLWE while attaining a level of efficiency comparable with that of RLWE. The cyclic algebras used are defined by a pair of number fields L,K where L/K is a degree d extension with cyclic Galois group generated by an element θ, and $K:=\mathbb{Q}(\zeta_m)$ is cyclotomic. To form a cyclic algebra, one defines an element u by the properties $u^d=\gamma$ for some $\gamma\in\mathcal{O}_K$, and $ux=\theta(x)u$ for all $x\in L$, and sets

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

This contains a subring which is also a lattice, denoted

$$\Lambda:=\mathcal{O}_L\oplus u\mathcal{O}_L\oplus...\oplus u^{d-1}\mathcal{O}_L$$

and called the natural order. To illustrate multiplication of algebra elements, consider the case $d=2$ and $a=a_0+ua_1$, $s=s_0+us_1$. Then

$$a\cdot s=a_0s_0+\gamma\theta(a_1)s_1+u\left(a_1s_0+\theta(a_0)s_1\right)$$

As in prior LWE variants, a matrix representation ϕ can be obtained by fixing the basis $1,u,...,u^{d-1}$ and computing the multiplication of a generic element

$a = a_0 + ua_0 + ... + u^{d-1}a_{d-1} \in \mathcal{A}$ with an element $s \in \mathcal{A}$ in the basis. This is a linear transformation, so the vector of coefficients of $a \cdot s$ can be written as matrix-vector multiplication:

$$\mathrm{vec}(a \cdot s) = \phi(x)\mathbf{s} = \begin{pmatrix} a_0 & \gamma\theta(a_{d-1}) & \dots & \gamma\theta^{d-1}(a_1) \\ a_1 & \theta(a_0) & \dots & \gamma\theta^{d-1}(a_2) \\ \dots & \dots & \dots & \dots \\ a_{d-1} & \theta(a_{d-2}) & \dots & \theta^{d-1}(a_0) \end{pmatrix} \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{d-1} \end{pmatrix}$$

We can also define a duality via a trace form: set $\mathrm{Tr}(x) := \mathrm{Tr}_{K/\mathbb{Q}} \circ \mathrm{trace}(\phi(x))$, for $x \in \mathcal{A}$. This is a symmetric map, and we define $\Lambda^\vee := \{x \in \mathcal{A} : \mathrm{Tr}(x\Lambda) \subset \mathbb{Z}\}$. An LWE-style distribution was then defined:

Definition 10. *Let L/K be a Galois extension of number fields of dimensions $[L : K] = d$, $[K : \mathbb{Q}] = n$, 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 Λ be the natural order of $\mathcal{A}$, and $\Lambda_q = \Lambda/q\Lambda$. Let $L_\mathbb{R} = L \otimes \mathbb{R}$. 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 $s \in \Lambda_q^\vee$, a sample from the CLWE distribution $\Pi_{q,s,\psi}^C$ is obtained by sampling $a \leftarrow \Lambda_q$ uniformly at random, $e \leftarrow \psi$, and outputting $(a, b) = (a, (a \cdot s)/q + e \bmod \Lambda^\vee) \in \Lambda_q \times \left(\oplus_{i=0}^{d-1} u^i L_\mathbb{R}\right)/\Lambda^\vee$.*

Search and decision problems were defined in the standard way:

Definition 11. *Let Ψ be a family of error distributions over $\bigoplus_{i=0}^{d-1} u^i L_\mathbb{R}$. Then the search CLWE problem, denoted by CLWE $_{q,s,\psi}$, is to recover s from a collection of independent samples from $\Pi_{q,s,\psi}^C$ for arbitrary $s \in \Lambda_q^\vee$ and $\psi \in \Psi$.*

Definition 12. *Let Υ be some distribution on a family of error distributions over $\bigoplus_{i=0}^{d-1} u^i L_\mathbb{R}$ and U_A denote the uniform distribution on $\left(\Lambda_q, \left(\bigoplus_{i=0}^{d-1} u^i L_\mathbb{R}\right)/\Lambda^\vee\right)$. Then, the decision CLWE problem, written $DCLWE_{q,\Upsilon}$, is on input a collection of independent samples from either $\Pi_{q,s,\psi}^C$ 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.*

To see that these definitions do yield structured LWE instances, one can expand them using the map ϕ to obtain equations over $\mathcal{O}_{L_q}$, which can then be expanded over $\mathbb{Z}_q$. Security reductions were also proved. The hardness of the search problem was obtained from ideal SIVP on ideals in Λ, with respect to the family of error distributions comprising Gaussians over $\oplus_{i=0}^{d-1} u^i L_\mathbb{R}$ which have every marginal distribution Gaussian of parameter r_{ij} at most α, denoted Σ_α.

Theorem 1. *[14, Corollary 1] Let $\mathcal{A} = (L/K, \theta, \gamma)$ be a CDA with $|\gamma| = 1$ such that the natural order Λ is maximal, and let $\alpha \in (0, 1)$ and q unramified in L be such that $\alpha q \geq \omega(\sqrt{\log nd^2})$. Then, there is a polynomial-time quantum reduction from $\mathcal{A}$-SIVP$_\xi$ to search CLWE$_{q,s,\Sigma_\alpha}$ for any $\sqrt{8nd^2} \cdot \xi = (\omega(\sqrt{dn})/\alpha)$.*

A restricted search-to-decision reduction was also obtained:

Theorem 2. *Let $K = \mathbb{Q}(\zeta_m)$, Λ be the natural order of a CDA $\mathcal{A} = (L/K, \theta, \gamma)$, $q \in \operatorname{poly}(n)$, and assume that $\alpha q \geq \eta_\varepsilon(\Lambda^\vee)$ for a negligible $\varepsilon = \varepsilon(n)$. Then, there is a probabilistic reduction from search $CLWE_{q,\Sigma_\alpha,G}$ for any pairwise difference set $G \subset \Lambda_q^\vee$ to decision $CLWE_{q,\Upsilon_\alpha}$ which runs in time polynomial in n.*

Above, a pairwise difference set $G \subset \Lambda_q^\vee$ is a set such that the difference of any two elements is invertible. We now discuss the search-to-decision reduction in more detail, and explain why the restriction to such sets was necessary.

We first observe a technical difference between the search-to-decision reductions for CLWE and for RLWE. Both reductions require a Chinese Remainder Theorem (CRT) decomposition modulo q: the reduction for RLWE used a CRT on $\mathcal{O}_K/q\mathcal{O}_K$ to rewrite the quotient as the products of quotients by prime ideals of $\mathcal{O}_K$, whereas the CLWE reduction used a CRT-*style* isomorphism which gives an isomorphism

$$\Lambda/q\Lambda \cong \prod_{i=1}^{g}((\mathcal{O}_L/\mathfrak{q}_i\mathcal{O}_L)/(\mathcal{O}_K/\mathfrak{q}_i), \theta, \gamma)$$

where $q\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{q}_i$, which for primes unramified in $\mathcal{O}_L$ is a direct product of (generalised) cyclic algebras over finite fields $\mathcal{O}_K/\mathfrak{q}_i$. The algebra of the right hand side induced by $\mathfrak{q}_i$ was labelled R_i. However these algebras are not division algebras, but rather each R_i is isomorphic to a matrix ring over a finite field, rather than simply a finite field (which is what is obtained for the corresponding step for RLWE). Let us work through the consequences.

The critical step in the reduction reduces search CLWE 'modulo R_i' to a hybrid distribution. This hybrid distribution is denoted $A^i_{s,\Sigma}$, and is defined over $\Lambda_q \times (\oplus_i u^i L_\mathbb{R})/\Lambda^\vee$ by sampling $(a, b) \leftarrow \Pi^C_{q,s,\Sigma}$ and outputting $(a, b + h/q)$, where $h \in \Lambda_q^\vee$ is uniformly random and independent modulo R_j for all $j \leq i$, and 0 modulo the remaining R_j. Then worst-case decision CLWE modulo R_i, $\text{WDCLWE}^i_{q,\Sigma}$, is, given access to $A^j_{s,\Sigma}$ for arbitrary $s \in \Lambda_q^\vee$, $\Sigma \in \Sigma_\alpha$, and $j \in \{i-1, i\}$, to find j, for $i \in \mathbb{Z}_g$.

The reduction, given a CLWE sample (a, b), guesses s with g and computes

$$(a', b') = (a + v, b + (h + vg)/q) \in \Lambda_q \times (\oplus_i u^i L_\mathbb{R})/\Lambda^\vee,$$

where $v \in \Lambda_q$ is uniformly random $\bmod R_i$ and $0 \bmod R_j$ for $j \neq i$, and $h \in \Lambda_q^\vee$ is uniformly random and independent mod R_j for all $j < i$, and 0 mod the remaining R_j. Observe

$$b' = b + (h + vg)/q = as/q + e + h/q + vg/q = ((a + v)s + h + v(g - s))/q + e.$$

If the guess $g = s$, then (a', b') is a sample from $A^{i-1}_{s,\Sigma}$. However, if $g \neq s$, we do not find that the resulting distribution is $A^i_{s,\Sigma}$ unless $g - s$ is invertible modulo R_i, that is, invertible in some matrix ring over a finite field. To ensure this holds, [14] restricted the secret space for this step of the reduction to a 'pairwise difference set' $G \subset \Lambda_q^\vee$, which under the CRT-style map is a direct product of sets $G_i \subset R_i$, characterised by the property that the difference of any two elements of G_i inverts. Such a set is of size at most $|G_i| \leq q^d$ when $[L : K] = d$, rather than the full secret space of size q^{d^2}. As a result, there is currently no unrestricted reduction from computationally hard lattice problems to decision CLWE. It is the purpose of the present work to circumvent this problem by pivoting to nonassociative algebras.

The CLWE problem was applied to cryptography to design a public key encryption scheme. We also note [21], [25], [20] contributing to the study of CLWE.

3 Nonassociative Cyclic Algebras

We begin by defining nonassociative cyclic algebras. Recall a ring is nonassociative if

$$a(bc) = (ab)c$$

does not always hold, for ring elements a, b, c.

Definition 13. *Let K be a degree n number field and L a cyclic Galois extension of degree d over K. Let θ generate the Galois group of L/K. Let $\gamma \in L$. We call*

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

where u is an auxiliary element subject to $u^d = \gamma$ and to $xu = u\theta(x)$ for all $x \in L$, a cyclic algebra. Fixing the basis $\{1, u, \dots, u^{d-1}\}$, we define multiplication on $u^i x$ and $u^j y$ for $x, y \in L, 0 \leq i, j, < d$ by

$$\left(u^i x\right)\left(u^j y\right) = \begin{cases} u^{i+j}\theta^j(x)y & \text{if } i+j < d \\ u^{i+j-d}\gamma\theta^j(x)y & \text{if } i+j \geq d \end{cases}$$

and extend this linearly to all of $\mathcal{A}$. We denote this algebra by $\mathcal{A} = (L/K, \theta, \gamma)$.

When $\gamma \in L \setminus K$, the above algebra is not associative: observe $(u \cdot u^{d-1}) \cdot u = u^d \cdot u = \gamma u = u\theta(\gamma)$, but $u \cdot (u^{d-1} \cdot u) = u \cdot u^d = u\gamma$. We refer to $\mathcal{A}$ as a *nonassociative cyclic algebra* to emphasise this property. We measure lack of associativity with

Definition 14. *The associator of $\mathcal{A}$ is $[x, y, z] := (xy)z - x(yz)$. The left nucleus is $\mathrm{Nuc}_l(\mathcal{A}) := \{x \in \mathcal{A} : [x, \mathcal{A}, \mathcal{A}] = 0\}$. The middle and right nuclei are defined similarly. The nucleus $\mathcal{N}(\mathcal{A})$ is $\mathcal{N}(\mathcal{A}) := \mathrm{Nuc}_l(\mathcal{A}) \cap \mathrm{Nuc}_m(\mathcal{A}) \cap \mathrm{Nuc}_r(\mathcal{A})$.*

The nuclei are associative subalgebras of $\mathcal{A}$.

Definition 15. *The commuter of $\mathcal{A}$ is $\mathrm{Comm}(\mathcal{A}) = \{x \in \mathcal{A} : xy = yx \text{ for all } y \in \mathcal{A}\}$. The center of $\mathcal{A}$ is $\mathcal{Z}(\mathcal{A}) = \mathrm{Comm}(\mathcal{A}) \cap \mathrm{Nuc}(\mathcal{A})$. An algebra $\mathcal{A}$ is central if $\mathcal{Z}(\mathcal{A}) = K$. An algebra $\mathcal{A}$ is simple if it contains no non-trivial two-sided ideals.*

Proposition 1. *For a nonassociative cyclic algebra $\mathcal{A} = (L/K, \theta, \gamma)$, we have $\mathcal{N}(\mathcal{A}) = L$ and $\mathrm{Comm}(\mathcal{A}) = K$, and $\mathcal{A}$ is a central simple K-algebra.*

Proof. Corollary 3.2.6 and Proposition 3.2.7 from [43]. □

We state a characterisation of the 'division' property of algebras:

Definition 16. *A unital algebra over a field is a division algebra if every non-zero element has a left and a right inverse.*

One can also say an algebra is division if left (and right) multiplication defines a bijective map from the algebra to itself. Thus there are no zero divisors in a division algebra. An algebra element may have distinct left and right inverses. We state a criterion for an associative cyclic algebra to be division, which we emphasize does not apply in the nonassociative case:

Lemma 2. *[3] Let $\mathcal{A} = (L/K, \theta, \gamma)$ be an associative cyclic algebra. Then $\mathcal{A}$ is a division algebra if and only if γ^i is a non-norm element, i.e. $\nexists x \in L : N_{L/K}(x) = \gamma^i$, for $i = 1, ..., [L : K] - 1$.*

Such elements γ as in the above lemma are called 'non-norm elements'. We now state a corresponding result for nonassociative cyclic algebras:

Proposition 2. *Let $\mathcal{A}$ be a nonassociative cyclic algebra of prime degree p. Then $\mathcal{A}$ is a division algebra. If $\mathcal{A}$ has arbitrary degree d and the elements $1, \gamma, ..., \gamma^{d-1}$ are linearly independent over K, then $\mathcal{A}$ is a division algebra. If γ is not contained in any proper subfield of L, $\mathcal{A}$ is a division algebra.*

Proof. Corollary 3.2.11 and Theorem 3.2.10 of [43]. □

The search for non-norm elements, i.e. elements of the ground field K which aren't realisable as the norm of any element of L, is a key part of the construction of associative CDAs. When taken for γ, as we saw above, they ensure the algebra is division. Their importance is paralleled by their rarity, and several, often convoluted, methods have been developed to obtain them (e.g. [25]). However, as shown in the above theorem, it is much easier in the nonassociative case to guarantee a cyclic algebra is division; indeed, in the degree p case it holds automatically.

Example: Let $K = \mathbb{Q}(\zeta_m)$ and $L = \mathbb{Q}(\zeta_{pm})$ where p and m are coprime. Then $\zeta_p \notin K$, and L/K is cyclic and Galois. Then $(L/K, \theta, \zeta_{pm})$ is a nonassociative cyclic division algebra.

Finally, we introduce a mild generalisation of cyclic algebras:

Definition 17. *Let S/R be a finite extension of commutative rings and $G = \langle\theta\rangle$ be a finite cyclic group of order d acting on S with trivial action on R. Let $\gamma \in S$ and u such that $ux = \theta(x)u$ for all $x \in S$ and $u^d = \gamma$. Then we call*

$$\mathcal{A} = (S/R, \theta, \gamma) := \oplus_{i=0}^{d-1} u^i S$$

equipped with multiplication as in Definition 13 a generalised cyclic algebra.

3.1 Matrix Representation

As explained above, one can consider RLWE as a structured form of LWE by fixing a $\mathbb{Z}$-basis of $\mathcal{O}_K$ and writing $a \cdot s$ as $\phi(a)\mathbf{s}$, where $\phi(a)$ is the matrix defined by multiplication by a on the fixed basis and $\mathbf{s}$ is the coefficient vector of s. This yields a number of correlated LWE samples equal to the dimension of the ring. As noted, MLWE and CLWE are also structured forms of LWE. In the case of nonassociative algebras, there is again a matrix representation arising from multiplication on a fixed basis in the nonassociative algebra; however, unlike in associative cases, this defines an embedding into a *vector space* of matrices, rather than a ring, so is not multiplicative. That is, $\phi(as) \neq \phi(a)\phi(s)$. Non-multiplicativity follows from the fact that matrix multiplication is associative; thus there could be no *multiplicative* map from a nonassociative ring into a matrix ring. This additive map is sufficient for our purposes, and will enable us to define a trace map as in the associative case.

The representation is as before: left multiplication by $a = a_0 + ua_1 + \cdots + u^{d-1}a_{d-1}$ on the basis $\{u^i\}$ inside $(L/K, \theta, \gamma)$ yields the following matrix:

$$\phi(a) = \begin{pmatrix} a_0 & \gamma\theta\left(a_{d-1}\right) & \gamma\theta^2\left(a_{d-2}\right) & \cdots & \gamma\theta^{d-1}\left(a_1\right) \\ a_1 & \theta\left(a_0\right) & \gamma\theta^2\left(a_{d-1}\right) & \cdots & \gamma\theta^{d-1}\left(a_2\right) \\ \vdots & \vdots & \vdots & \dots & \vdots \\ a_{d-1} & \theta\left(a_{d-2}\right) & \theta^2\left(a_{d-3}\right) & \cdots & \theta^{d-1}\left(a_0\right) \end{pmatrix}$$

So a sample of nonassociative CLWE defined below yields m correlated MLWE samples from one nonassociative CLWE sample.

3.2 Integral Structures in Nonassociative Algebras

In order to define the lattice problems we will use in our reduction, we need to define orders and ideals in nonassociative algebras. The primary reference for this section is [37]. Set $\mathcal{A} = (L/K, \theta, \gamma)$ with $\gamma \in L \setminus K$ such that $\mathcal{A}$ is a division algebra.

Recall an $\mathcal{O}_K$-lattice is a finitely generated torsion-free $\mathcal{O}_K$-module. We define the natural order of a nonassociative CDA $(L/K, \theta, \gamma)$ identically as for CLWE: $\Lambda = \bigoplus_{i=0}^{d-1} u^i \mathcal{O}_L$. Then:

Proposition 3. *If $\gamma \in \mathcal{O}_L \setminus \mathcal{O}_K$, Λ is an order of $\mathcal{A} = (L/K, \theta, \gamma)$.*

Proof. Λ is clearly an $\mathcal{O}_K$-module. To see multiplicative closure, we demonstrate the case of $d = 2$. Let $a, b \in \Lambda$ and observe

$$a \cdot b = (a_0 + ua_1) \cdot (b_0 + ub_1) = a_0b_0 + u(\theta(a_0)b_1 + a_1b_0) + \gamma a_1 b_1,$$

which lies in Λ if $\gamma \in \mathcal{O}_L$. So Λ is a subring (this holds for all $d \in \mathbb{Z}_{\geq 1}$) and is discrete by virtue of $\mathcal{O}_L$ being a lattice inside L. □

Note however that if $\gamma \in L \setminus \mathcal{O}_L$, Λ is not multiplicatively closed. We proceed to study ideals in Λ, properties of which we redefine for the nonassociative setting. An 'ideal' will refer to a two-sided ideal (unless specified otherwise).

Definition 18. *A one-sided Λ-ideal $\mathcal{I} \subset \mathcal{A}$ is an additively closed set closed under multiplication from Λ on one side, e.g. $\mathcal{I}$ is a right ideal if $\mathcal{I}\Lambda \subset \mathcal{I}$. A two-sided ideal is closed additively and under multiplication by Λ on both sides.*

Definition 19. *An ideal is maximal if it is not properly contained in any other proper ideal. An ideal is prime if it is a maximal two-sided ideal.*

Definition 20. *The sum and product of two ideals $\mathcal{I}, \mathcal{J}$ are defined as usual; $\mathcal{I}+\mathcal{J} = \{i+j : i \in \mathcal{I}, j \in \mathcal{J}\}$ and $\mathcal{I}\cdot\mathcal{J} = \{\sum_{k=1}^{m} i_k \cdot j_k : i_k \in \mathcal{I}, j_k \in \mathcal{J}, m < \infty\}$. A two-sided ideal $\mathcal{I}$ is fractional if $c\mathcal{I} = \mathcal{J}$ for a two-sided ideal $\mathcal{J}$ and $c \in K$.*

The sum of two fractional ideals can clearly be seen to yield another fractional ideal. The product of two ideals in a nonassociative space less clearly yields another ideal, however. In the following pages we develop an ideal theory that will permit us to prove a security reduction for nonassociative CLWE from nonassociative ideal lattices. We recall and extend a number of results from [37].

Let $q \in \mathbb{Z}$ be a prime. Then $q \in \mathrm{Comm}(\mathcal{A})$ and $q\Lambda$ is a two-sided ideal of Λ. Let $\mathcal{I} \subset \mathcal{O}_K$ be an ideal. Then we have the following product

$$\mathcal{I}\Lambda = \left\{ \sum_i a_i x_i \mid a_i \in \mathcal{I}, x_i \in \Lambda \right\} = \left\{ \sum_{i=0}^{d-1} u^i a_i \mid a_i \in \mathcal{I}\mathcal{O}_L \right\},$$

which is a two-sided ideal of Λ.

Proposition 4. *Let $J \subset \Lambda$ be a two-sided ideal. Then $\mathcal{I} = J \cap \mathcal{O}_L$ is a non-zero ideal of $\mathcal{O}_L$. If $\mathcal{I}$ is an ideal of K, then $\mathcal{I}\Lambda \cap \mathcal{O}_K = \mathcal{I}$.*

Proof. Lemma 5.1 and Remark 5.2 of [37]. □

Proposition 5. *Let $\mathcal{A} = (L/K, \theta, \gamma)$ be a nonassociative CDA with $\gamma \in \mathcal{O}_L^\times \backslash \mathcal{O}_K^\times$ and natural order Λ. Let $\mathcal{I} \subset \Lambda$ be a two-sided ideal. Then $\theta(\mathcal{I} \cap \mathcal{O}_L) = \mathcal{I} \cap \mathcal{O}_L$.*

Proof. Suppose $\theta(\mathcal{I} \cap \mathcal{O}_L) \neq \mathcal{I} \cap \mathcal{O}_L$. So there exists $x \in \mathcal{I} \cap \mathcal{O}_L$ such that $\theta(x) \notin \mathcal{I} \cap \mathcal{O}_L$. As $\mathcal{I}$ is two-sided, $\mathcal{I}u \subset \mathcal{I}$, so $xu = u\theta(x) \in \mathcal{I}$. Moreover, $u^{d-1}\mathcal{I} \subset \mathcal{I}$, so $u^{d-1}(u\theta(x)) = u^d\theta(x) = \gamma\theta(x) \in \mathcal{I}$. Since γ is a unit, $\gamma^{-1}\mathcal{I} \subset \mathcal{I}$, so $\gamma^{-1}(\gamma\theta(x)) = \theta(x) \subset \mathcal{I}$. Finally, $\theta(x) \in \mathcal{O}_L$, so $\theta(x) \in \mathcal{I} \cap \mathcal{O}_L$ - a contradiction. □

This result in fact holds for generalised cyclic algebras when γ is a unit. We now recall that if $\mathcal{I} = \mathfrak{q}_1^{s_1} \cdots \mathfrak{q}_t^{s_t}$ is an ideal of $\mathcal{O}_K$, then we have

$$\mathcal{O}_K/\mathcal{I} = \mathcal{O}_K/\mathfrak{q}_1^{s_1} \cdots \mathfrak{q}_t^{s_t} \cong \mathcal{O}_K/\mathfrak{q}_1^{s_1} \times \cdots \times \mathcal{O}_K/\mathfrak{q}_t^{s_t}$$

and

$$\mathcal{O}_L/\mathcal{I}\mathcal{O}_L = \mathcal{O}_L/\mathfrak{q}_1^{s_1} \cdots \mathfrak{q}_t^{s_t}\mathcal{O}_L \cong \mathcal{O}_L/\mathfrak{q}_t^{s_t}\mathcal{O}_L \times \cdots \times \mathcal{O}_L/\mathfrak{q}_t^{s_t}\mathcal{O}_L.$$

Below is a version of the Chinese remainder theorem (CRT) for Λ:

Theorem 3. *For $\mathcal{I} = \mathfrak{q}_1^{s_1} \cdots \mathfrak{q}_t^{s_t}$ an ideal of $\mathcal{O}_K$, we have*

$$\begin{aligned} \Lambda/\mathcal{I}\Lambda &\cong \left(\left(\mathcal{O}_L/\mathcal{I}\mathcal{O}_L\right) / \left(\mathcal{O}_K/\mathcal{I}\right), \bar{\theta}, \gamma + \mathcal{I}\mathcal{O}_L \right) = \bigoplus_{i=0}^{d-1} u^i \left(\mathcal{O}_L/\mathcal{I}\mathcal{O}_L\right) \\ &\cong \left(\left(\mathcal{O}_L/\mathfrak{q}_1^{s_1}\mathcal{O}_L\right) / \left(\mathcal{O}_K/\mathfrak{q}_1^{s_1}\right), \bar{\theta}, \gamma + \mathfrak{q}_1^{s_1} \right) \times \cdots \\ &\quad \cdots \times \left(\left(\mathcal{O}_L/\mathfrak{q}_t^{s_t}\mathcal{O}_L\right) / \left(\mathcal{O}_K/\mathfrak{q}_t^{s_t}\right), \bar{\theta}, \gamma + \mathfrak{q}_t^{s_t} \right), \end{aligned}$$

where $\bar{\theta}$ is defined by its actions on the quotients $\bar{\theta}\left(x + \mathfrak{q}_i^{s_i}\mathcal{O}_L\right) = \theta(x) + \mathfrak{q}_i^{s_i}\mathcal{O}_L$.

Proof. [37], Theorem 5.3 and Lemma 5.4. □

In an abuse of notation, we may write θ for $\bar{\theta}$. Below, we study quotients $\Lambda/\mathcal{I}\Lambda$ in greater detail.

4 Multiplicative Ideal Theory of Nonassociative Orders

In this section we classify unramified two-sided ideals of natural orders in CDAs of the form $(L/K, \theta, \gamma)$ where $K = \mathbb{Q}(\zeta_m)$ and $\gamma \in \mathcal{O}_L^\times \setminus \mathcal{O}_K^\times$, and use this to prove that multiplication of such ideals is associative and commutative, and that inverses and duals of such ideals can be meaningfully defined. Our strategy to achieve this classification is by induction; we begin by proving, as a base case, that under weak conditions quotient rings of Λ by prime ideals are simple. We then give our induction proof, which essentially claims that two-sided ideals of Λ are twisted direct sums of ideals of $\mathcal{O}_L$. The desired multiplicative properties then follow.

4.1 Unramified Primes: Inert and Split

Recall for fixed prime ideal $\mathfrak{q} \subset \mathcal{O}_K$ we have $[L : K] = e_L f_L g_L$ with g_L the number of primes in the factorization of $\mathfrak{q}\mathcal{O}_L$, e_L the ramification index and f_L the inertial degree. We presently consider cases where $e_L = 1$, so $[L : K] = f_L g_L$. Let $\gamma \in \mathcal{O}_L \setminus \mathcal{O}_K$.

First, suppose $g_L = 1$, so $\mathfrak{q}$ is inert in L. Then $f_L = [L : K] = d$ and $\bar{L} := \mathcal{O}_L/\mathfrak{q}\mathcal{O}_L$ is a cyclic Galois extension of $\bar{K} := \mathcal{O}_K/\mathfrak{q}$ of degree d. Then

Proposition 6. *[37, Theorem 6.1] Let $\mathfrak{q}$ be a prime ideal in $\mathcal{O}_K$ which is inert in $\mathcal{O}_L$, and $\mathfrak{q}\mathcal{O}_L = \mathcal{Q}$, $\mathcal{Q}$ a prime ideal in $\mathcal{O}_L$. Let $\bar{\gamma} = \gamma \bmod \mathfrak{q}$. Then*

$$\Lambda/\mathfrak{q}\Lambda \cong \left((\mathcal{O}_L/\mathfrak{q}\mathcal{O}_L)/(\mathcal{O}_K/\mathfrak{q}), \bar{\sigma}, \bar{\gamma} \right) = (\bar{L}/\bar{K}, \bar{\sigma}, \bar{\gamma})$$

is a nonassociative cyclic algebra of degree d over $\bar{K}$. If d is prime or $1, \bar{\gamma}, ..., \bar{\gamma}^{d-1}$ are linearly independent over $\bar{K}$, then this is a central simple division algebra and the only proper two-sided ideal $\mathcal{J}$ of Λ containing $\mathfrak{q}$ is

$$\mathfrak{q}\Lambda = \bigoplus_{j=0}^{d-1} u^j \mathfrak{q}\mathcal{O}_L.$$

Proof. Note $\gamma \notin \mathfrak{q}$, i.e. $\bar{\gamma} \in (\mathcal{O}_K/\mathfrak{q})^\times$, so $\Lambda/\mathfrak{q}\Lambda \cong ((\mathcal{O}_L/\mathfrak{q}\mathcal{O}_L)/(\mathcal{O}_K/\mathfrak{q}), \bar{\theta}, \bar{\gamma})$ is a degree d nonassociative cyclic algebra over $\mathcal{O}_K/\mathfrak{q}$. By Proposition 2, if d is prime or if $1, \bar{\gamma}, \ldots, \bar{\gamma}^{d-1}$ are linearly independent over $\mathcal{O}_K/\mathfrak{q}$, $\Lambda/\mathfrak{q}\Lambda$ is a division algebra, so any two-sided ideal is trivial. Hence by the correspondence between ideals of Λ containing $\mathfrak{q}\Lambda$ and ideals of $\Lambda/\mathfrak{q}\Lambda$ the only proper two-sided ideal $\mathcal{J}$ of Λ containing $\mathfrak{q}$ is $\mathfrak{q}\Lambda$. □

Next, consider the case when $e_L = 1$ but $g_L > 1$. This is the split case, in which $\mathfrak{q}\mathcal{O}_L = \mathcal{Q}_1 \ldots \mathcal{Q}_{g_L}$. As in the associative setting, it was shown in [37, §7.3] that $\Lambda/\mathfrak{q}\Lambda \cong \left(\left(\bar{L}^{(1)} \times \cdots \times \bar{L}^{(g)}\right)/\bar{K}, \bar{\theta}, \bar{\gamma}\right)$, where $\bar{L}^{(i)} = \mathcal{O}_L/\mathcal{Q}_i$. To prove that this quotient is a simple ring, we first require some definitions.

Definition 21. *Let G be a group. A ring $\mathcal{R}$ is G-graded if there are additive subgroups $\mathcal{R}_g \subset \mathcal{R}$, for $g \in G$, such that $\mathcal{R} = \bigoplus_{g\in G} \mathcal{R}_g$ and $\mathcal{R}_g\mathcal{R}_h \subseteq \mathcal{R}_{g+h}$, for $g, h \in G$. If $\mathcal{R}_g\mathcal{R}_h = \mathcal{R}_{g+h}$, for $g, h \in G$, then $\mathcal{R}$ is strongly G-graded.*

Let $\mathcal{I}$ be an $\mathcal{O}_K$-ideal. Consider $\Lambda/\mathcal{I}\Lambda = \oplus_{i=0}^{d-1} u^i (\mathcal{O}_L/\mathcal{I}\mathcal{O}_L)$. Setting $G = \mathbb{Z}/d\mathbb{Z}$ and $\mathcal{R}_i = u^i\mathcal{O}_L/\mathcal{I}\mathcal{O}_L$, one can see that the $\mathcal{R}_i$ are additive subgroups, and

$$\mathcal{R}_i\mathcal{R}_j = (u^i\mathcal{O}_L/\mathcal{I}\mathcal{O}_L)(u^j\mathcal{O}_L/\mathcal{I}\mathcal{O}_L) = u^{i+j}\theta^j(\mathcal{O}_L/\mathcal{I}\mathcal{O}_L)\mathcal{O}_L/\mathcal{I}\mathcal{O}_L = \mathcal{R}_{i+j}$$

So $\Lambda/\mathcal{I}\Lambda$ is a strongly $\mathbb{Z}/d\mathbb{Z}$-graded ring.

Definition 22. *Let G be a group and $\mathcal{J}$ a two-sided ideal of a ring $\mathcal{R}$. Then $\mathcal{J}$ is G-graded if $\mathcal{J} = \bigoplus_{g\in G} (\mathcal{J} \cap \mathcal{R}_g)$. The ring $\mathcal{R}$ is called G-graded simple if the only G-graded ideals of $\mathcal{R}$ are $\{0\}$ and $\mathcal{R}$.*

We now show $\Lambda/\mathcal{I}\Lambda$ is $\mathbb{Z}/d\mathbb{Z}$-graded simple for certain ideals $\mathcal{I}$.

Lemma 3. *Let $\gamma \in \mathcal{O}_L^\times \setminus \mathcal{O}_K^\times$. Let $\mathcal{I} = \mathfrak{q} \subset \mathcal{O}_K$ be a prime ideal unramified in $\mathcal{O}_L$. Then $\Lambda/\mathcal{I}\Lambda$ is $\mathbb{Z}/d\mathbb{Z}$-graded simple.*

Proof. Equip $\Lambda/\mathcal{I}\Lambda$ with the $\mathbb{Z}/d\mathbb{Z}$ grading as before. We need to show, for any $\mathbb{Z}/d\mathbb{Z}$-graded ideal $\mathcal{J}$, that in fact $\mathcal{J} = \oplus_{i\in\mathbb{Z}/d\mathbb{Z}}\mathcal{J} \cap u^i\mathcal{O}_L/\mathcal{I}\mathcal{O}_L$ is 0 or $\Lambda/\mathcal{I}\Lambda$. Write $\mathcal{I}\mathcal{O}_L = \prod_i \mathcal{Q}_i$. By the correspondence between ideals of Λ containing $\mathcal{I}\Lambda$ and ideals of $\Lambda/\mathcal{I}\Lambda$ and an abuse of notation, write the ideal as $\mathcal{J}/\mathcal{I}\Lambda$. Then $\mathcal{J}/\mathcal{I}\Lambda \cap \prod_i \mathcal{O}_L/\mathcal{Q}_i$ is an ideal of $\prod_i \mathcal{O}_L/\mathcal{Q}_i$, so has the form $\prod_{i\in S}\mathcal{Q}_i/\prod_{i=1}^g \mathcal{Q}_i$ for some $S \subset [g]$. Moreover, by Proposition 5, we must have $\theta(\mathcal{J}/\mathcal{I}\Lambda \cap \prod_i \mathcal{O}_L/\mathcal{Q}_i) = \theta(\prod_{i\in S}\mathcal{Q}_i/\prod_{i=1}^g \mathcal{Q}_i) = \prod_{i\in S}\mathcal{Q}_i/\prod_{i=1}^g \mathcal{Q}_i$. But the Galois action on the primes $\mathcal{Q}_i$ above $\mathfrak{q}$ is transitive, so θ cannot fix any such product except when $S = \{1, ..., g\}$ or $S = \emptyset$. Thus $\mathcal{J}/\mathcal{I}\Lambda \cap \mathcal{O}_L/\mathcal{I}\mathcal{O}_L = \mathcal{J}/\mathcal{I}\Lambda \cap \mathcal{R}_0$ is 0 or $\mathcal{O}_L/\mathcal{I}\mathcal{O}_L$.

Since $\mathcal{J}/\mathcal{I}\Lambda$ is an ideal and γ is invertible, $u^j\mathcal{J}/\mathcal{I}\Lambda = \mathcal{J}/\mathcal{I}\Lambda$, so

$$\begin{aligned}\mathcal{J}/\mathcal{I}\Lambda \cap \mathcal{R}_i &= u^i \cdot \mathcal{J}/\mathcal{I}\Lambda \cap u^i \cdot \mathcal{R}_0 = u^i(\mathcal{J}/\mathcal{I}\Lambda \cap \mathcal{R}_0) \\ &= \begin{cases} 0 & \text{if } \mathcal{J}/\mathcal{I}\Lambda \cap \mathcal{R}_0 = 0 \\ u^i\mathcal{O}_L/\mathcal{I}\mathcal{O}_L & \text{if } \mathcal{J}/\mathcal{I}\Lambda \cap \mathcal{R}_0 = \mathcal{O}_L/\mathcal{I}\mathcal{O}_L. \end{cases}\end{aligned}$$

So either $\mathcal{J}/\mathcal{I}\Lambda$ is $\oplus_{i\in\mathbb{Z}/d\mathbb{Z}}0 = 0$ or $\oplus_{i\in\mathbb{Z}/d\mathbb{Z}}u^i\mathcal{O}_L/\mathcal{I}\mathcal{O}_L = \Lambda/\mathcal{I}\Lambda$. □

A group G is *hypercentral* if every non-trivial factor group of G has a non-trivial center. In particular, any abelian group is hypercentral. We now state

Theorem 4. *[, Theorem 4] If a nonassociative unital ring is graded by a hypercentral group, then the ring is simple if and only if it is graded simple and the center of the ring is a field.*

From the above discussion we can conclude

Proposition 7. *Let $\mathfrak{q}$ be a prime $\mathcal{O}_K$-ideal such that $\mathfrak{q}\mathcal{O}_L = \mathcal{Q}_1 ... \mathcal{Q}_g$ where $\mathcal{Q}_i$ is a prime $\mathcal{O}_L$-ideal, $i = 1, ..., g$. Let $\gamma \in \mathcal{O}_L^\times \setminus \mathcal{O}_K^\times$. Then*

$$\Lambda/\mathfrak{q}\Lambda \cong \left(\left(\bar{L}^{(1)} \times \cdots \times \bar{L}^{(g)}\right)/\bar{K}, \bar{\theta}, \bar{\gamma}\right)$$

is a generalised nonassociative cyclic algebra of degree $d = g$ over $\bar{K}$. The only proper two-sided ideal $\mathcal{J}$ of Λ that contains $\mathfrak{q}$ is

$$\mathcal{J} = \mathfrak{q}\Lambda = \bigoplus_{j=0}^{d-1} u^j \mathfrak{q}\mathcal{O}_L$$

Proof. The first statement is shown in [37, §7.3]. The second follows since 1. $\mathbb{Z}/d\mathbb{Z}$ is hypercentral, 2. the center of $\Lambda/\mathfrak{q}\Lambda$ is a field, and 3. $\Lambda/\mathfrak{q}\Lambda$ is $\mathbb{Z}/d\mathbb{Z}$-graded simple (Lemma 3). Then Theorem 4 implies $\Lambda/\mathfrak{q}\Lambda$ is simple and hence $\mathfrak{q}\Lambda$ is maximal in Λ. □

Although we cannot prove a general result on the factorisation of ideals in nonassociative natural orders, we can prove the following theorem, an analogue of which was given in a concurrent work [26] for associative CDAs; we prove it here for nonassociative CDAs.

Theorem 5. *Let $\Lambda \subset \mathcal{A} = (L/K, \theta, \gamma)$ be the natural order of a nonassociative CDA and $\gamma \in \mathcal{O}_L$. Let $\mathcal{I} \subset \Lambda$ be an integral two-sided ideal and $\overline{\mathcal{I}} = \mathcal{I} \cap K$. If the prime factors of $\overline{\mathcal{I}}$ are unramified in L and $\gamma \not\equiv 0 \bmod \overline{\mathcal{I}}$, then $\mathcal{I} = \overline{\mathcal{I}}\Lambda$.*

The proof of the theorem requires a corollary of Propositions 6 and 7:

Corollary 1. *Suppose that $\mathfrak{p}$ is a prime in $\mathcal{O}_K$, such that $\mathfrak{p}$ is unramified in L, with $\gamma \not\equiv 0 \bmod \mathfrak{p}$. Then the only proper two-sided ideal $\mathcal{I}$ of Λ containing $\mathfrak{p}^{-1}$ is $\mathfrak{p}^{-1}\Lambda = \oplus_{i=0}^{d-1} u^i \mathfrak{p}^{-1}\mathcal{O}_L$.*

Proof. If there is a proper ideal $\mathcal{J}$ strictly containing $\mathfrak{p}^{-1}\Lambda$, then $\mathfrak{p}^2\mathcal{J}$ is a proper ideal strictly containing $\mathfrak{p}\Lambda$, which contradicts Propositions 6 and 7. □

We use transfinite induction over a tuple $(e_1, ..., e_n) \in \mathbb{Z}_{\geq 1}^n$, which requires a well-ordering on $\mathbb{Z}_{\geq 1}^n$. Define the following well-ordering: let $(e_1, ..., e_n) \in \mathbb{Z}_{\geq 1}^n$. Given n-tuples $(e_1, ..., e_n), (f_1, ..., f_n)$, we say $(e_1, ..., e_n) > (f_1, ..., f_n) \in \mathbb{Z}_{\geq 1}^n$ if $\prod_1^n p_i^{e_i} > \prod_1^n p_i^{f_i}$, where p_i is the ith prime. For fixed n, the smallest element is $(1, ..., 1)$. Since this is a total order, and since any subset of n-tuples has a smallest element, this is a well-ordering of $\mathbb{Z}_{\geq 1}^n$.

Proof of Theorem 5. Suppose that $\mathcal{I}$ maximally contains a subideal $\mathfrak{J}$ which is unramified in L, that is, $\mathfrak{J}$ is the largest $\mathcal{O}_K$-ideal contained in $\mathcal{I}$. Suppose $\mathfrak{J} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}...\mathfrak{p}_n^{e_n}$, for distinct primes $\mathfrak{p}_i$, and positive integers e_i. We claim that when the largest $\mathcal{O}_K$-ideal of $\mathcal{I}$ has this form, then $\mathcal{I} = \mathfrak{J}\Lambda$.

We want to show that $\mathcal{I} = \mathfrak{p}_1^{e_1}...\mathfrak{p}_n^{e_n}\Lambda$. First, note that $\mathcal{I}$ is contained in a maximal ideal $\mathcal{M}$, which contains some prime ideal $\mathfrak{r}$ of $\mathcal{O}_K$, and so we have $\mathcal{M} = \mathfrak{r}\Lambda$, and $\mathfrak{p}_1^{e_1}...\mathfrak{p}_n^{e_n}\Lambda \subset \mathcal{I} \subsetneq \mathfrak{r}\Lambda$. But $\mathfrak{p}_1^{e_1}...\mathfrak{p}_n^{e_n} \subset \mathfrak{r}$ implies that $\mathfrak{r} = \mathfrak{p}_i$ for some i; without loss of generality suppose $\mathfrak{r} = \mathfrak{p}_1$, and write $\mathfrak{p}_1^{e_1}...\mathfrak{p}_n^{e_n}\Lambda \subset \mathcal{I} \subsetneq \mathfrak{p}_1\Lambda$.

Proceed by double induction on $n \in \mathbb{N}_{\geq 1}$ and $(e_1, ..., e_n) \in \mathbb{Z}_{\geq 1} \times ... \times \mathbb{Z}_{\geq 1}$. The statement is true in the case $n = 1, e_1 = 1$ by Propositions 6 and 7. We first prove the statement for $n = 1$, and use induction on e_1. Suppose the statement holds for $e_1' < e_1$ and suppose $\mathcal{I}$ contains $\mathfrak{p}_1^{e_1}$ and no larger $\mathcal{O}_K$-ideal. Then we have $\mathfrak{p}_1^{e_1}\Lambda \subset \mathcal{I} \subsetneq \mathfrak{p}_1\Lambda$. Then $\mathfrak{p}_1^{-1}\mathcal{I}$ is integral, and the largest $\mathcal{O}_K$-ideal it contains is $\mathfrak{p}_1^{e_1-1}$, so $\mathfrak{p}_1^{-1}\mathcal{I} = \mathfrak{p}_1^{e_1-1}\Lambda$ by hypothesis. Hence $\mathcal{I} = \mathfrak{p}_1^{e_1}\Lambda$, as required.

Next, we show the statement for $(1, ..., 1)$ and any n by inducting on n. Suppose $\mathfrak{J} = \mathfrak{p}_1\mathfrak{p}_2...\mathfrak{p}_n$, for distinct primes $\mathfrak{p}_i$. Note that $\mathcal{I}$ is contained in a maximal ideal $\mathcal{M}$, which contains some prime ideal $\mathfrak{r}$ of $\mathcal{O}_K$, and so we have $\mathcal{M} = \mathfrak{r}\Lambda$, and $\mathfrak{p}_1...\mathfrak{p}_n\Lambda \subset \mathcal{I} \subsetneq \mathfrak{r}\Lambda$. But $\mathfrak{p}_1...\mathfrak{p}_n \subset \mathfrak{r}$ implies that $\mathfrak{r} = \mathfrak{p}_i$ for some i; without loss of generality suppose $\mathfrak{r} = \mathfrak{p}_1$, and write $\mathfrak{p}_1...\mathfrak{p}_n\Lambda \subset \mathcal{I} \subsetneq \mathfrak{p}_1\Lambda$. We now claim that if $\mathfrak{p}_1...\mathfrak{p}_n$ is the largest $\mathcal{O}_K$-ideal in $\mathcal{I}$, then $\mathcal{I} = \mathfrak{p}_1...\mathfrak{p}_n\Lambda$.

We have seen that the $n = 1$ case is true. Proceeding by induction, suppose the statement is true for $n < k$, and consider an integral ideal $\mathcal{I}$ such that $\mathfrak{p}_1...\mathfrak{p}_{k-1}\mathfrak{p}_k$ is the largest $\mathcal{O}_K$-ideal in $\mathcal{I}$. We have $\mathfrak{p}_1...\mathfrak{p}_{k-1}\mathfrak{p}_k\Lambda \subset \mathcal{I} \subsetneq \mathfrak{p}_1\Lambda$. Consider $\mathfrak{p}_1^{-1}\mathcal{I}$; we have $\mathfrak{p}_2...\mathfrak{p}_{k-1}\mathfrak{p}_k\Lambda \subset \mathfrak{p}_1^{-1}\mathcal{I} \subsetneq \Lambda$, so $\mathfrak{p}_1^{-1}\mathcal{I}$ is integral. Then observe that the largest $\mathcal{O}_K$-ideal contained in $\mathfrak{p}_k^{-1}\mathcal{I}$ is $\mathfrak{p}_1...\mathfrak{p}_{k-1}$, so by induction we have $\mathfrak{p}_k^{-1}\mathcal{I} = \mathfrak{p}_1...\mathfrak{p}_{k-1}\Lambda$, and hence $\mathcal{I} = \mathfrak{p}_1...\mathfrak{p}_{k-1}\mathfrak{p}_k\Lambda$, as required.

Now suppose the statement is true for $n < k$ and $(e_1', ..., e_n') = (e_1, ..., e_n) \in \mathbb{Z}_{\geq 1}^n$, and true for $n = k$ and $(e_1', ..., e_k') < (e_1, ..., e_k)$, and consider an ideal $\mathcal{I}$ such that $\mathfrak{p}_1^{e_1}...\mathfrak{p}_{k-1}^{e_{k-1}}\mathfrak{p}_k^{e_k}$ is the largest $\mathcal{O}_K$-ideal in $\mathcal{I}$. Like before, $\mathfrak{p}_1^{e_1}...\mathfrak{p}_{k-1}^{e_{k-1}}\mathfrak{p}_k^{e_k}\Lambda \subset \mathcal{I} \subsetneq \mathfrak{p}_k\Lambda$ (simply relabel the primes for this to hold). Again, $\mathfrak{p}_k^{-1}\mathcal{I}$ is integral, and observe that the largest $\mathcal{O}_K$-ideal contained in $\mathfrak{p}_k^{-1}\mathcal{I}$ is $\mathfrak{p}_1^{e_1}...\mathfrak{p}_k^{e_k-1}$. We split into two cases: $e_k - 1 = 0$, and $e_k - 1 > 0$.

When $e_k - 1 > 0$, we use induction on $(e_1', ..., e_k')$, and since $(e_1, ..., e_k - 1) < (e_1, ..., e_k)$, by hypothesis have $\mathfrak{p}_k^{-1}\mathcal{I} = \mathfrak{p}_1^{e_1}...\mathfrak{p}_k^{e_k-1}\Lambda$. Hence $\mathcal{I} = \mathfrak{p}_1^{e_1}...\mathfrak{p}_{k-1}^{e_{k-1}}\mathfrak{p}_k^{e_k}\Lambda$, as required.

When $e_k - 1 = 0$, the largest $\mathcal{O}_K$-ideal contained in $\mathfrak{p}_k^{-1}\mathcal{I}$ is $\mathfrak{p}_1^{e_1}...\mathfrak{p}_{k-1}^{e_{k-1}}$. We then induct on n, since $n = k - 1 < k$, to obtain $\mathfrak{p}_k^{-1}\mathcal{I} = \mathfrak{p}_1^{e_1}...\mathfrak{p}_{k-1}^{e_{k-1}}\Lambda$ and hence $\mathcal{I} = \mathfrak{p}_1^{e_1}...\mathfrak{p}_{k-1}^{e_{k-1}}\mathfrak{p}_k$, as required. □

When γ is a unit, this fully characterises unramified ideals in the natural order of the CDAs we consider. The following result then follows:

Theorem 6. *Let $\Lambda \subset \mathcal{A} = (L/K, \theta, \gamma)$ be the natural order of a nonassociative CDA and $\gamma \in \mathcal{O}_L^\times$. Then multiplication of Λ-ideals $\mathcal{I}$ such that $\mathcal{I} \cap \mathcal{O}_K$ is unramified in $\mathcal{O}_L$ yields ideals, and is commutative and associative.*

Proof. Let $\mathcal{I}$ and J be two-sided ideals of Λ. Write $\bar{\mathcal{I}} = \mathcal{I} \cap L$. Then $\mathcal{I} = \bar{\mathcal{I}}\Lambda$ and $J = \bar{J}\Lambda$. Then, using that $L = \mathcal{N}(\mathcal{A})$, we have $\mathcal{I}J = (\bar{\mathcal{I}}\Lambda)(\bar{J}\Lambda) = (\bar{\mathcal{I}}(\Lambda\bar{J}))\Lambda = (\bar{\mathcal{I}})\theta(\bar{J})\Lambda))\Lambda = \bar{\mathcal{I}}\bar{J}\Lambda$. It can be seen by a similar argument that $\bar{\mathcal{I}}\bar{J}\Lambda$ is a two-sided ideal of Λ.

Next note that the product of two ideals whose $\mathcal{O}_K$-intersections are ideals unramified in $\mathcal{O}_L$ is an ideal which also has $\mathcal{O}_K$-intersection unramified in $\mathcal{O}_L$, so this set of ideals is closed under taking products.

Moreover, $\mathcal{I}J = (\bar{\mathcal{I}}\Lambda)(\bar{J}\Lambda) = \bar{\mathcal{I}}\bar{J}\Lambda = \bar{J}\bar{\mathcal{I}}\Lambda = (\bar{J}\Lambda)(\bar{\mathcal{I}}\Lambda) = J\mathcal{I}$, so ideal multiplication is commutative.

Finally, let K also be a two-sided Λ-ideal. Then $(\mathcal{I}J)K = (\bar{\mathcal{I}}\bar{J}\Lambda)\bar{K}\Lambda = \bar{\mathcal{I}}\bar{J}\bar{K}\Lambda = \bar{\mathcal{I}}\Lambda(\bar{J}\bar{K}\Lambda) = \mathcal{I}(JK)$. So ideal multiplication is also associative. □

For convenience we will call the two-sided ideals satisfying the condition of the theorem 'unramified ideals of Λ'.

4.2 Inverse Ideals

Let $\mathcal{A} = (L/K, \theta, \gamma)$ with $\gamma \in \mathcal{O}_L^\times \setminus \mathcal{O}_K^\times$, and let $\mathcal{I} = \bar{\mathcal{I}}\Lambda$ be a two-sided unramified ideal of Λ. Then, writing $J = \bar{\mathcal{I}}^{-1}\Lambda$, we have $\mathcal{I} \cdot J = (\bar{\mathcal{I}}\Lambda)(\bar{\mathcal{I}}^{-1}\Lambda) = (\Lambda\bar{\mathcal{I}})(\bar{\mathcal{I}}^{-1}\Lambda) = \Lambda(\bar{\mathcal{I}}(\bar{\mathcal{I}}^{-1}\Lambda)) = \Lambda((\bar{\mathcal{I}}\bar{\mathcal{I}}^{-1})\Lambda) = \Lambda(\mathcal{O}_L\Lambda) = \Lambda$. Motivated by this, we give the following definition:

Definition 23. *Let $\mathcal{A} = (L/K, \theta, \gamma)$ with $\gamma \in \mathcal{O}_L^\times \setminus \mathcal{O}_K^\times$, and let $\mathcal{I} = \bar{\mathcal{I}}\Lambda$ be a two-sided unramified ideal of Λ. Then the inverse of $\mathcal{I}$ is $\mathcal{I}^{-1} := \bar{\mathcal{I}}^{-1}\Lambda$.*

Note all ideals of Λ as in the definition are invertible. Furthermore, observe that $\mathcal{I}^{-1}$ is additively closed, and closed under multiplication on the right from Λ. Moreover, since $\theta(\bar{\mathcal{I}}) = \bar{\mathcal{I}}$ by Proposition 5, we have $\bar{\mathcal{I}}\bar{\mathcal{I}}^{-1} = \mathcal{O}_L$ implies $\theta(\bar{\mathcal{I}})\theta(\bar{\mathcal{I}}^{-1}) = \bar{\mathcal{I}}\theta(\bar{\mathcal{I}}^{-1}) = \mathcal{O}_L$, and hence $\mathcal{O}_L\theta(\bar{\mathcal{I}}^{-1}) = \bar{\mathcal{I}}^{-1}\mathcal{O}_L$. Since $\bar{\mathcal{I}}^{-1}$ is an $\mathcal{O}_L$-ideal, $\theta(\bar{\mathcal{I}}^{-1})$ is also an $\mathcal{O}_L$-ideal, and we obtain $\theta(\bar{\mathcal{I}}^{-1}) = \bar{\mathcal{I}}^{-1}$. So θ fixes $\bar{\mathcal{I}}^{-1}$. Then $\Lambda\mathcal{I}^{-1} = \Lambda(\bar{\mathcal{I}}^{-1}\Lambda) = \Lambda(\Lambda\theta(\bar{\mathcal{I}}^{-1})) = \Lambda(\Lambda\bar{\mathcal{I}}^{-1}) = (\Lambda\Lambda)\bar{\mathcal{I}}^{-1} = \Lambda\bar{\mathcal{I}}^{-1} = \bar{\mathcal{I}}^{-1}\Lambda = \mathcal{I}^{-1}$, and $\mathcal{I}^{-1}$ is closed under multiplication from the left too. So $\mathcal{I}^{-1}$ is a fractional Λ-ideal.

Clearly this means that $(\mathcal{I}^{-1})^{-1} = \mathcal{I}$, so left and right inverse ideals coincide, and hence each unramified ideal has a unique inverse ideal.

4.3 Dual Ideals

When the algebra $\mathcal{A}$ is associative, the *dual lattice* of Λ is defined as

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

where Tr refers to the trace defined $\mathrm{Tr}(a) := \mathrm{Tr}_{K/\mathbb{Q}}(\mathrm{Trace}(\phi(a)))$. Note $\mathrm{Tr}(\cdot)$ is a linear map and non-degenerate, and $\Lambda^\vee$ is additively closed. This is (in the associative scenario) extended to ideals $\mathcal{I}$ of Λ as follows: the *dual* of an ideal is defined as

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

However, when $\mathcal{A}$ is nonassociative the $\mathrm{Tr}(\cdot)$ map is not symmetric (that is, $\mathrm{Tr}(xy) \neq \mathrm{Tr}(yx)$), which causes many familiar results not to hold in the case of nonassociative algebras. This can be seen from the matrix representation: since $\phi : \mathcal{A} \to M_d(L)$ is not a homomorphism of rings but merely of vector spaces, $\phi(xy) \neq \phi(x)\phi(y)$, so in general $\mathrm{Tr}(xy) = T_{K/\mathbb{Q}} \circ \mathrm{Trace}(\phi(xy)) \neq T_{K/\mathbb{Q}} \circ \mathrm{Trace}(\phi(x)\phi(y)) = T_{K/\mathbb{Q}} \circ \mathrm{Trace}(\phi(y)\phi(x)) = \mathrm{Tr}(yx)$. It is hence not clear what the definition of $\mathcal{I}^\vee$ should be for ideals in orders in nonassociative algebras. In the absence of a symmetric trace form, we make the following definition:

Definition 24. *Let Λ be the natural order of cyclic division algebra $\mathcal{A} = (L/K, \theta, \gamma)$, with $\gamma \in \mathcal{O}_L^\times$ and $[L : K] = d$. Let $\mathcal{I}$ be an ideal of Λ and $\bar{\mathcal{I}} = \mathcal{I} \cap L$. Then the dual ideal $\mathcal{I}^\vee$ of $\mathcal{I}$ is defined as*

$$\mathcal{I}^\vee = \bar{\mathcal{I}}^\vee \Lambda$$

Before we prove properties of $\mathcal{I}^\vee$, note that it immediately bears some similarities to the usual notion of the dual ideal of, say, an ideal in the ring of integers in a number field. For integral ideals, we have $\mathcal{I} \subset \Lambda \subset \mathcal{I}^\vee$, and $\mathcal{I}^\vee$ is an $\mathcal{O}_K$-module. Moreover, $(\mathcal{I}^\vee)^\vee = (\bar{\mathcal{I}}^\vee\Lambda)^\vee = (\bar{\mathcal{I}}^\vee\Lambda \cap L)^\vee\Lambda = (\bar{\mathcal{I}}^\vee)^\vee\Lambda = \bar{\mathcal{I}}\Lambda = \mathcal{I}$. Finally, $\mathcal{I}^\vee = \bar{\mathcal{I}}^\vee\Lambda = (\bar{\mathcal{I}}^{-1}\mathcal{O}_L^\vee)\Lambda = (\bar{\mathcal{I}}^{-1}\Lambda)(\mathcal{O}_L^\vee\Lambda) = \mathcal{I}^{-1}\Lambda^\vee$. We now show:

Proposition 8. *Let $\mathcal{I} \subset \Lambda$ be a two-sided integral unramified ideal. Then $\mathcal{I}^\vee$ is a two-sided fractional ideal of Λ.*

Proof. First, note additive closure is immediate since both $\bar{\mathcal{I}}^\vee$ and Λ are additively closed.

Next, since $\bar{\mathcal{I}}^\vee \subset L = \mathcal{N}(\mathcal{A})$ we have that if $x \in \Lambda$, then $\mathcal{I}^\vee x = (\bar{\mathcal{I}}^\vee\Lambda)x = \bar{\mathcal{I}}^\vee(\Lambda x) \subset \bar{\mathcal{I}}^\vee\Lambda = \mathcal{I}^\vee$, so $\mathcal{I}^\vee$ is closed under multiplication from Λ on the right.

To see left multiplication is closed: we have $\theta(\mathcal{I}^\vee) = \theta(\bar{\mathcal{I}}^\vee\Lambda) = \theta(\bar{\mathcal{I}}^\vee)\theta(\Lambda) = \theta(\bar{\mathcal{I}}^\vee)\Lambda$, where θ acts on Λ coefficient-wise, and is the identity on u^i for all i. Letting $x \in \Lambda$, consider $x \cdot \mathcal{I}^\vee = x(\bar{\mathcal{I}}^\vee\Lambda) = (x\bar{\mathcal{I}}^\vee)\Lambda$. In moving elements of $\bar{\mathcal{I}}^\vee$ past x, powers of the automorphism θ are applied to $\bar{\mathcal{I}}^\vee$ (corresponding to the power of u being 'moved past' by the element of $\bar{\mathcal{I}}^\vee$). So if $\theta(\bar{\mathcal{I}}^\vee) = \bar{\mathcal{I}}^\vee$, we would have: $(x\bar{\mathcal{I}}^\vee)\Lambda = (\bar{\mathcal{I}}^\vee x)\Lambda = \bar{\mathcal{I}}^\vee(x\Lambda) \subset \bar{\mathcal{I}}^\vee\Lambda = \mathcal{I}^\vee$, as required.

We conclude the proof by showing that $\theta(\bar{\mathcal{I}}^\vee) = \bar{\mathcal{I}}^\vee$. Let $\mathfrak{m} \subset \mathcal{O}_L$ be an ideal such that $\theta(\mathfrak{m}) = \mathfrak{m}$, and $x \in \mathfrak{m}^\vee$. We need $\theta(x) \in \mathfrak{m}^\vee$, that is, $T_{L/\mathbb{Q}}(\theta(x)y) \in \mathbb{Z}$ for any $y \in \mathfrak{m}$. Because $\mathrm{Gal}(L/K)$ is cyclic, we can say $T_{L/\mathbb{Q}}(\theta(x)y) = T_{L/\mathbb{Q}}(x\theta^{-1}(y))$; since $\theta(\mathfrak{m}) = \mathfrak{m}$, $\theta^{-1}(y) \in \mathfrak{m}$, and so $T_{L/\mathbb{Q}}(\theta(x)y) = T_{L/\mathbb{Q}}(x\theta^{-1}(y)) \in \mathbb{Z}$. Thus $\theta(x) \in \mathfrak{m}^\vee$, and so $\theta(\mathfrak{m}^\vee) \subset \mathfrak{m}^\vee$. Replacing $\mathfrak{m}$ with $\bar{\mathcal{I}}$, this implies that $\mathcal{I}^\vee$ is a two-sided fractional Λ-ideal. □

Proposition 9. *Let $\gamma \in \mathcal{O}_L^\times$ and $\mathcal{I} \subset \Lambda$ be a two-sided integral unramified ideal. Set $J_\mathcal{I} := \{x \in \mathcal{A} : \mathrm{Tr}(xy) \in \mathbb{Z}$ for all $y \in \mathcal{I}\}$. Then $\mathcal{I}^\vee = J_\mathcal{I}$.*

Proof. We begin by showing $\mathcal{I}^\vee \subset J_{\mathcal{I}}$. We have

$$\begin{aligned}
\mathrm{Tr}(\mathcal{I}^\vee \mathcal{I}) &= \mathrm{Tr}((\bar{\mathcal{I}}^\vee \mathit{\Lambda})(\bar{\mathcal{I}} \mathit{\Lambda})) \\
&= \mathrm{Tr}((\bar{\mathcal{I}}^\vee (\mathit{\Lambda} \bar{\mathcal{I}}))\mathit{\Lambda}) \\
&= \mathrm{Tr}((\bar{\mathcal{I}}^\vee (\theta(\bar{\mathcal{I}})\mathit{\Lambda}))\mathit{\Lambda}) \\
&= \mathrm{Tr}((\bar{\mathcal{I}}^\vee (\bar{\mathcal{I}}\mathit{\Lambda}))\mathit{\Lambda}) \\
&= \mathrm{Tr}((\bar{\mathcal{I}}^\vee \bar{\mathcal{I}})\mathit{\Lambda}).
\end{aligned}$$

Since $\mathrm{Tr}(u^i z_i) = 0$ if $i \neq 0$, we get $\mathrm{Tr}((\bar{\mathcal{I}}^\vee \bar{\mathcal{I}})\mathit{\Lambda}) = T_{L/\mathbb{Q}}((\bar{\mathcal{I}}^\vee \bar{\mathcal{I}})\mathcal{O}_L) = T_{L/\mathbb{Q}}(\bar{\mathcal{I}}^\vee \bar{\mathcal{I}}) \in \mathbb{Z}$, since $\gamma \in \mathcal{O}_L$. So for integral $\mathit{\Lambda}$-ideals, $\mathcal{I}^\vee = \bar{\mathcal{I}}^\vee \mathit{\Lambda}$ satisfies $\mathrm{Tr}(\mathcal{I}^\vee \mathcal{I}) \subset \mathbb{Z}$ and (similarly) $\mathrm{Tr}(\mathcal{I}\mathcal{I}^\vee) \subset \mathbb{Z}$, so $\mathcal{I}^\vee \subset J_{\mathcal{I}}$.

It remains to show that $J_{\mathcal{I}} \subseteq \mathcal{I}^\vee$. Take some $x \in J_{\mathcal{I}}$, and $y \in \mathcal{I}$. Write $x = ab$ with $a \in L$ and $b \in \mathit{\Lambda}$ (this can be done for any algebra element). We want to show that x can be written in the form $a'b'$, where $a' \in \bar{\mathcal{I}}^\vee$ and $b' \in \mathit{\Lambda}$. Thus if $a \in \bar{\mathcal{I}}^\vee$, we will be done.

By definition, $\mathrm{Tr}(x\mathcal{I}) \subset \mathbb{Z}$. This implies that $\mathrm{Tr}(x\bar{\mathcal{I}}) \subset \mathbb{Z}$. Substituting for x, we obtain $\mathrm{Tr}((ab)\bar{\mathcal{I}}) \subset \mathbb{Z}$. We can rearrange to obtain $\mathrm{Tr}((a\bar{\mathcal{I}})b) \subset \mathbb{Z}$. Expanding b into the form $b = \sum_{i=0}^{d-1} u^i b_i$ where the $b_i \in \mathcal{O}_L$ and applying additivity of the trace, we have $\mathrm{Tr}((a\bar{\mathcal{I}})b) = T_{L/\mathbb{Q}}(a\bar{\mathcal{I}}b_0) \subset \mathbb{Z}$. So $ab_0 \in \bar{\mathcal{I}}^\vee$.

Now, note that $u\mathcal{I} \subset \mathcal{I}$. Moreover, up to application by θ and multiplication by γ, we can move any coefficient of $x \in \mathit{\Lambda}$ into the 0th position; if $x = \oplus_{i=0}^{d-1} u^i x_i$, we can place x_j in the 0th position via $xu^{d-j} = \gamma\theta^{d-j}(x_j) + u\gamma\theta^{d-j}(x_{j+1}) + ... + u^{d-1}\theta^{d-j}(x_{j-1})$. Using this trick, one can obtain $\theta^i(a)b_i \in \overline{\mathcal{I}}^\vee$ as follows: $\mathbb{Z} \supset \mathrm{Tr}(x(u^{d-i}\overline{\mathcal{I}})) = \mathrm{Tr}((ab)(u^{d-i}\overline{\mathcal{I}})) = \mathrm{Tr}(((ab)u^{d-i})\overline{\mathcal{I}}) = \mathrm{Tr}((a(bu^{d-i}))\overline{\mathcal{I}}) = T_{L/\mathbb{Q}}(a\gamma\theta^{d-i}(b_i)\overline{\mathcal{I}})$, so $a\theta^{d-i}(b_i) \in \overline{\mathcal{I}}^\vee$, and hence $\theta^i(a)b_i \in \overline{\mathcal{I}}^\vee$. Now observe that $ab = ab_0 + u\theta(a)b_1 + ... + u^{d-1}\theta^{d-1}(a)b_{d-1}$, so $ab \in \oplus_{i=0}^{d-1} u^i \overline{\mathcal{I}}^\vee = \overline{\mathcal{I}}^\vee \mathit{\Lambda}$, as required. □

5 Nonassociative Cyclic Learning with Errors

We begin by defining lattices from ideal lattices in nonassociative algebras. Below $n = [K : \mathbb{Q}]$.

5.1 Ideals as Lattices and the Canonical Embedding

Since an ideal of an order is an additive subgroup of a lattice, it is itself a lattice. We embed order ideals in nonassociative CDAs into $\mathbb{R}^{nd^2}$ using the canonical embedding as above, to obtain lattices in $\mathbb{R}^{nd^2}$. To do this, we consider the matrix representations of order elements, vectorise the columns to obtain vectors with d^2 entries, and apply the canonical embedding of K, which yields a lattice of dimension nd^2. We take norms of algebra elements by taking the sum of the squares of the Frobenius norm of their matrix representation under the presence of K-embeddings; that is, for $x \in \mathcal{A}$ we have $\|x\|^2 = \sum_{i=1}^n \|\alpha_i(\phi(x))\|_F^2$, where $\|\cdot\|_F$ denotes the Frobenius norm and $\alpha_i(\phi(x))$ the application of $\alpha_i \in \mathrm{Emb}(K)$

to the entries of $\phi(x)$. If $|\gamma| = 1$ this norm is submultiplicative, such as when γ is a root of unity.

Recall the family of error distributions used for CLWE:

Definition 25. *Let Σ_α be the set of Gaussian distributions Σ over $\bigoplus_{i=0}^{d-1} u^i L_\mathbb{R}$ with Gaussian marginal distributions of parameters $r_{i,j} \leq \alpha$.*

We use the same distributions mutatis mutandis in the nonassociative setting.

5.2 NCLWE

We now define the nonassociative CLWE (NCLWE) distribution. We superscript the NCLWE distribution (and the lattice problems on ideals in nonassociative orders referred to below) by a 'ν' to distinguish them from associative variants of the problems.

Definition 26. *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 $\theta : L \to L$. Let $\mathcal{A} := (L/K, \theta, \gamma)$ be the resulting nonassociative cyclic algebra with center K and element u satisfying $u^d = \gamma \in \mathcal{O}_L \setminus \mathcal{O}_K$. Let Λ be the natural order of $\mathcal{A}$. For an error distribution ψ over $\bigoplus_{i=0}^{d-1} u^i L_\mathbb{R}$, an integer modulus $q \geq 2$, and a secret $s \in \Lambda_q^\vee$ a sample from the NCLWE distribution $\Pi_{q,s,\psi}^\nu$ is obtained by sampling $a \leftarrow \Lambda_q$ uniformly at random, sampling $e \leftarrow \psi$, and outputting $(a, b) = (a, (a \cdot s)/q + e \bmod \Lambda^\vee) \in \Lambda_q \times \left(\oplus_{i=0}^{d-1} u^i L_\mathbb{R}\right)/\Lambda^\vee$*

From this distribution we give search and decision problems:

Definition 27. *Let Ψ be a family of error distributions over $\bigoplus_{i=0}^{d-1} u^i L_\mathbb{R}$. Let $\Pi_{q,s,\psi}^\nu$ be a NCLWE distribution for parameters $q \geq 2$, $s \in \Lambda_q^\vee$, and error distribution $\psi \in \Psi$. Then, the search NCLWE problem, denoted $SNCLWE_{q,s,\psi}$, is to recover $s \in \Lambda_q^\vee$ from a collection of independent samples from $\Pi_{q,s,\psi}^\nu$.*

Definition 28. *Let Υ be a distribution on a family of error distributions Σ_α over $\bigoplus_{i=0}^{d-1} u^i L_\mathbb{R}$ and U_Λ the uniform distribution on $\Lambda_q \times \left(\bigoplus_{i=0}^{d-1} u^i L_\mathbb{R}\right)/\Lambda^\vee$. Then the decision NCLWE problem, $DNCLWE_{q,\Upsilon}$, is on input a number of independent samples from either $\Pi_{q,s,\psi}^\nu$ for a random choice of $(s, \psi) \leftarrow U\left(\Lambda_q^\vee\right) \times \Upsilon$, or from U_Λ, to decide which with non-negligible advantage.*

6 Search-to-Decision Reduction for NCLWE

Recall the statement of Theorem 3: for $\mathcal{I} = \mathfrak{q}_1^{s_1} ... \mathfrak{q}_t^{s_t} \subset \mathcal{O}_K$ an ideal, we have

$$\begin{aligned}\Lambda/\mathcal{I}\Lambda &\cong \left((\mathcal{O}_L/\mathcal{I}\mathcal{O}_L)/(\mathcal{O}_K/\mathcal{I}), \bar{\theta}, \gamma + \mathcal{I}\mathcal{O}_L\right) = \bigoplus_{i=0}^{d-1} u^i\left(\mathcal{O}_L/\mathcal{I}\mathcal{O}_L\right) \\ &\cong \left((\mathcal{O}_L/\mathfrak{q}_1^{s_1}\mathcal{O}_L)/(\mathcal{O}_K/\mathfrak{q}_1^{s_1}), \bar{\theta}, \bar{\gamma}_1\right) \times ... \times \left((\mathcal{O}_L/\mathfrak{q}_t^{s_t}\mathcal{O}_L)/(\mathcal{O}_K/\mathfrak{q}_t^{s_t}), \bar{\theta}, \bar{\gamma}_t\right)\end{aligned}$$

where $\bar{\gamma}_i = \gamma + \mathfrak{q}_1^{s_1}$. In the following proof, we write this as

$$\Lambda/\mathcal{I}\Lambda \cong R_1 \times \ldots \times R_t.$$

The R_i-NCLWE$_{q,s,\Sigma_\alpha}$ problem is to find the value $s \bmod R_i$ given access to the NCLWE distribution $\Pi^{\nu}_{q,s,\Sigma}$ for some $\Sigma \in \Sigma_\alpha$. We begin the reduction with the following lemma:

Lemma 4. *Let q completely split in $\mathcal{O}_K$ and unramified in $\mathcal{O}_L$, and Σ_α be as in Definition 25. There is a deterministic polynomial time reduction from SNCLWE$_{q,s,\Sigma_\alpha}$ to R_i-NCLWE$_{q,s,\Sigma_\alpha}$.*

Proof. Mutatis mutandis identical to [14, Lemma 13]. □

We now define an intermediate distribution as follows: for $s \in \Lambda_q^\vee$, distribution Σ over $\bigoplus_j u^j L_\mathbb{R}$, and $i \in [n]$, we define a sample from the distribution $\Pi^{\nu\ i}_{q,s,\Sigma}$ over $\Lambda_q \times \left(\bigoplus_{i=0}^{d-1} u^i L_\mathbb{R}\right)/\Lambda^\vee$ by taking $(a, b) \leftarrow \Pi^{\nu}_{q,s,\Sigma}$ and $h \in \Lambda_q^\vee$ which is uniformly random and independent mod $R_j, j \leq i$ and 0 mod $R_j, j > i$, and outputting $(a, b + h/q)$. Set $\Pi^{\nu\ 0}_{q,s,\Sigma} = \Pi^{\nu}_{q,s,\Sigma}$.

Using this distribution we define a worst-case decision problem with respect to one R_i and reduce it to the search problem R_i-NCLWE.

Definition 29. *For $0 < i \leq n$ and family of error distributions Σ_α, the W-D-NCLWE$^i_{q,s,\Sigma_\alpha}$ problem is the problem of finding j given oracle access to $\Pi^{\nu\ j}_{q,s,\Sigma}$ for $j \in \{i-1, i\}$ and valid NCLWE secret and error distribution pair (s, Σ).*

Recall q is a prime which factors in $\mathcal{O}_K$ as $q\mathcal{O}_K = \prod_{i=1}^{g_K} \mathfrak{q}_i$ such that $\mathfrak{q}_i$ is unramified in $\mathcal{O}_L$ for all i, that is $\mathfrak{q}_i\mathcal{O}_L = \prod_{i=1}^{g_L} \mathcal{Q}_i$. In the next step of the reduction, when $g_L > 1$ we restrict the secret space such that the secret is to be chosen from a space G in which the difference of any two elements inverts. These sets were called ‘pairwise difference sets’ in [14], and the decomposition into R_i implies $G \cong G_1 \times \ldots \times G_t$ for $G_i \in R_i$, a fact we use below. The variant of SNCLWE with secrets restricted to such a G is denoted SNCLWE$_{q,s,\Sigma_\alpha,G}$ and similarly for the other distributions already defined. Moreover, the above Lemma 4 holds when the secret is restricted to such sets G. However, when $g_L = 1$, $\mathfrak{q}_i$ is inert in $\mathcal{O}_L$ and by the proof of Proposition 6 R_i is a division algebra. In this case, there is no need to restrict the secret space, since the difference of two distinct elements in a division algebra inverts by definition, and $G_i = R_i$.

Lemma 5. *Let $\gamma \in \mathcal{O}_L^\times \setminus \mathcal{O}_K^\times$, $q\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{q}_i$, and $\bar{K}^{(i)} = \mathcal{O}_K/\mathfrak{q}_i$. Then if $s \in G$ there is a ppt. reduction from R_i-NCLWE$_{q,s,\Sigma_\alpha,G}$ to W-D-NCLWE$^i_{q,s,\Sigma_\alpha}$ for any $0 < i \leq n$.*

When the $\mathfrak{q}_i$ are inert in $\mathcal{O}_L$ for $i = 1, ..., g$ and either $d = [L : K]$ is prime or $1, \bar{\gamma}, \ldots, \bar{\gamma}^{d-1}$ are linearly independent over $\bar{K}^{(i)}$, then for any $s \in R_i$ there is a ppt. reduction from R_i-NCLWE$_{q,s,\Sigma_\alpha}$ to W-D-NCLWE$^i_{q,s,\Sigma_\alpha}$ for any $0 < i \leq n$.

Proof. We will guess the secret s with a value g; we can do this efficiently since there are only $|G_i| \leq q^{d^2} = \mathrm{poly}(n)$ possible values of $s \bmod R_i$, with d considered to be some small constant. To transform $\mathit{\Pi}^{\nu}_{q,s,\mathit{\Sigma}}$ into either $\mathit{\Pi}^{\nu\ i-1}_{q,s,\mathit{\Sigma}}$ if $g = s \bmod R_i$ or $\mathit{\Pi}^{\nu\ i}_{q,s,\mathit{\Sigma}}$ otherwise, for $g \in \mathit{\Lambda}_q^\vee$ we take a sample $(a, b) \leftarrow \mathit{\Pi}^{\nu}_{q,s,\mathit{\Sigma}}$ and set

$$(a', b') := (a + v, b + (h + vg)/q) \in \mathit{\Lambda}_q \times \left(\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}} \right) / \mathit{\Lambda}^\vee,$$

where $v \in \mathit{\Lambda}_q$ is uniformly random mod R_i and 0 mod R_j for $j \neq i$ and $h \in \mathit{\Lambda}_q^\vee$ is uniformly random and independent mod $R_j, j < i$ and 0 on the other R_j. Note $a' \in \mathit{\Lambda}_q$ is uniformly distributed. We now consider the distribution of b'. Conditioning on a fixed a', we have

$$\begin{aligned} b' = b + (h + vg)/q &= (as + h + vg)/q + e \\ &= (a's + h + v(g - s))/q + e, \end{aligned}$$

where $e \sim \mathit{\Sigma}$. Now observe: if $g = s$ mod R_i, then $v(g-s) = 0$ mod R_i, so (a', b') is distributed according to $\prod^{\nu\ i-1}_{q,s,\mathit{\Sigma}}$. However, if $g \neq s$, then $v(g - s)$ is uniformly random mod R_i (since $g - s$ inverts by definition of G) and 0 modulo the other R_j. We then set $h' = h+v(g-s)$ and the distribution of (a', b') is exactly $\mathit{\Pi}^{\nu\ i}_{q,s,\mathit{\Sigma}}$.

The second statement follows since we may choose $G_i = R_i$. □

We now move to obtain a reduction from a worst-case problem to an average-case problem. This section is mutatis mutandis identical to the corresponding section of [14] (and is very similar to that of [24]) and is included for completeness.

Definition 30. *The distribution $\mathit{\Upsilon}_\alpha$ on the set of possible error distributions is defined by choosing an error distribution $\mathit{\Sigma} \leftarrow \mathit{\Sigma}_\alpha$ and adding it to D_r, where $r_i = \alpha((nd^2)^{1/4} \cdot \sqrt{y_i})$ for $y_1, \ldots, y_{nd^2}$ sampled from $\mathit{\Gamma}(2, 1)$.*

Definition 31. *For $i \in [n]$ and distribution $\mathit{\Upsilon}_\alpha$ over possible error distributions, an algorithm solves the DNCLWE$^i_{q,\mathit{\Upsilon}_\alpha}$ problem if with non-negligible probability over $(s, \mathit{\Sigma}) \leftarrow U\left(\mathit{\Lambda}_q^\vee\right) \times \mathit{\Upsilon}_\alpha$ it has a non-negligible difference in acceptance probability on inputs from $\mathit{\Pi}^{\nu\ i}_{q,s,\mathit{\Sigma}}$ and $\prod^{\nu\ i-1}_{q,s,\mathit{\Sigma}}$.*

Lemma 6. *For any $\alpha > 0$ and $i \in [n]$ there is a randomized polynomial-time reduction from W-D-NCLWE$^i_{q,s,\mathit{\Sigma}_\alpha}$ to DNCLWE$^i_{q,\mathit{\Upsilon}_\alpha}$.*

Proof. To sample from $\mathit{\Upsilon}_\alpha$ we sample from $\mathit{\Sigma}_\alpha$ and add an elliptical Gaussian; this is as in [24, Lemma 5.12], and so, replacing each instance of mod $\mathfrak{q}_i R^\vee$ with mod R_i, and R_q with $\mathit{\Lambda}_q$, since associativity isn't used the proof is the same. □

Lemma 7. *Let $\mathit{\Upsilon}_\alpha$ be as above and $s \in \mathit{\Lambda}_q^\vee$. Then given a DNCLWE$_{q,\mathit{\Upsilon}_\alpha}$ oracle $\mathcal{O}$, there exists an efficient algorithm that solves DNCLWE$^i_{q,\mathit{\Upsilon}_\alpha}$ for some $i \in [n]$*

Proof. As in [24, Lemma 5.14] but for replacing the indexing set $\mathbb{Z}_m^*$ by $[n]$. □

We finally obtain:

Theorem 7. *Let Λ be the natural order of a nonassociative CDA $\mathcal{A} = (L/K, \theta, \gamma)$, $\gamma \in \mathcal{O}_L^\times \setminus \mathcal{O}_K^\times$, $d = [L : K]$, $q \geq 2$ such that $q\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{q}_i$ and $\alpha q \geq \eta_\varepsilon(\Lambda^\vee)$ for negligible $\varepsilon = \varepsilon(n)$. Then there is a ppt. reduction from SNCLWE$_{q,s,\Sigma_\alpha,G}$ for any pairwise difference set $G \subset \Lambda_q^\vee$ to DNCLWE$_{q,\Upsilon_\alpha}$.*

When the $\mathfrak{q}_i$ are inert in $\mathcal{O}_L$ and either d is prime or $1, \bar{\gamma}, \ldots, \bar{\gamma}^{d-1}$ are linearly independent over $\bar{K}^{(i)}$, for each i, then there is a ppt. reduction from SNCLWE$_{q,s,\Sigma_\alpha}$ to DNCLWE$_{q,\Upsilon_\alpha}$.

7 Hardness of Search NCLWE

We demonstrate the hardness of NCLWE, using the same strategy as [14]. Since the lattices obtained from our algebras can be seen as module lattices (i.e. the lattices are isomorphic to module lattices as $\mathcal{O}_K$-modules), there is a reduction from $\mathcal{A}$-SIVP$_\xi^\nu$ to $\mathcal{A}$-DGS$_\xi^\nu$ [39, Lemma 3.17]. We will need some lemmas.

7.1 Technical Lemmas

The results below are proved for a CDA $\mathcal{A} = (L/K, \theta, \gamma)$ with $\gamma \in \mathcal{O}_L^\times \setminus \mathcal{O}_K^\times$, since they implicitly require the above results on products, inverses, and duals of ideals.

Lemma 8. *Let $\mathcal{I}$ be an unramified ideal of the natural order Λ, and let $\mathcal{J} = q\Lambda$, where $q \in \mathbb{Z}$ is prime and $q\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{q}_i$ is a decomposition into prime ideals. Furthermore, let the $\mathfrak{q}_i$ be unramified in $\mathcal{O}_L$. Assume $\gamma \notin \mathfrak{q}_i$ for each i. Then, there exists an element $t \in \mathcal{I} \cap \mathcal{O}_K$ such that $t \cdot \mathcal{I}^{-1} \subset \Lambda$ is coprime to $\mathcal{J}$, and we can compute such a t efficiently given $\mathcal{I}$ and the prime factorization of $\mathcal{J}$.*

Proof. Denote $\mathcal{I} \cap \mathcal{O}_K$ by $\bar{\mathcal{I}}$, which is an $\mathcal{O}_K$-ideal. We know, by [24], that there exists a $t \in \bar{\mathcal{I}}$ such that $t \cdot \bar{\mathcal{I}}^{-1}$ and $q\Lambda \cap \mathcal{O}_K$ are coprime as $\mathcal{O}_K$-ideals, with $t \in \bar{\mathcal{I}} \setminus \prod_i \mathfrak{q}_i \bar{\mathcal{I}}$. Suppose $t \cdot \mathcal{I}^{-1} + q\Lambda \neq \Lambda$. Then, since they are both two-sided ideals whose sum is a proper ideal, they must be contained in some maximal ideal. By Propositions 6 and 7 above, this maximal ideal must have the form $\mathfrak{q}_i\Lambda$, for some i. Thus $t \cdot \mathcal{I}^{-1} \subset \mathfrak{q}_i\Lambda$ and $t \in \mathfrak{q}_i\mathcal{I}\Lambda \cap \mathcal{O}_K = \mathfrak{q}_i\mathcal{I} \cap \mathcal{O}_K$ (note that the product $\mathfrak{q}_i\mathcal{I}\Lambda$ is well-defined). Since t and $\mathfrak{q}_i$ are central this is a contradiction, and the final equality is a consequence of Proposition 4. □

Lemma 9. *Let $\mathcal{A}$ and q be as in Lemma 8. Let $\mathcal{I} \subset \Lambda$ be unramified and $\mathcal{J} = q\Lambda$, with $t \in \mathcal{I} \cap \mathcal{O}_K$ such that $t \cdot \mathcal{I}^{-1}$ and $q\Lambda$ are coprime as ideals, and let $\mathcal{P}$ be an arbitrary fractional ideal of Λ. Assume $\gamma \notin \mathfrak{q}_i$ for each i. Then the map $\chi_t : \mathcal{A} \to \mathcal{A}, x \mapsto t \cdot x$ induces an $\mathcal{O}_K$-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, we can efficiently compute the inverse.*

Proof. Identical mutatis mutandis to [14, Lemma 7], using $t \in \mathcal{Z}(\mathcal{A})$ and Lemma 8. □

7.2 Reducing Ideal SIVP to Search NCLWE

We now adapt the security proof of [14] to nonassociative CDAs. It proceeds similarly; both our lattices and the lattices of [14] are modules over $\mathcal{O}_K$, so they are module lattices as used in [18]. Thus the results of the latter paper that adapt for CLWE often adapt for NCLWE. Moreover, nonassociativity will not prove a large obstacle in the proofs - the primary result threatened by lack of associativity is Lemma 11, yet we circumnavigate this issue via the centrality of the element t from Lemma 9.

Lemma 10. *For any $q \geq 2$ there is a deterministic polynomial time reduction from $\mathcal{A}$-$BDD^{\nu}_{\mathcal{I},d}$ to $q\mathcal{A}$-$BDD^{\nu}_{\mathcal{I},d}$.*

Proof. Proved in [39, Lemma 3.5], for arbitrary lattices. □

Lemma 11. *There is a probabilistic polynomial time algorithm that given a prime $q \in \mathbb{Z}$, $\alpha \in (0,1)$, unramified fractional Λ-ideal $\mathcal{I}^\vee$, a $q\mathcal{A}$-$BDD^{\nu}_{\mathcal{I}^\vee,\alpha q\omega(\sqrt{\log(nd)})/\sqrt{2nd}r}$ instance $y = x+e$ with $x \in \mathcal{I}^\vee$, $r \geq \sqrt{2}q\eta(\mathcal{I})$, and samples from $D_{\mathcal{I},r'}$ with $r' \geq r$, outputs samples of negligible statistical distance from the NCLWE distribution $\Pi^{\nu}_{q,s,\Sigma}$, where $s = \chi_t\left(x \bmod q\mathcal{I}^\vee\right) \in \Lambda_q^\vee$ and $\Sigma \in \Sigma_\alpha$.*

Proof. The first step of the proof is to compute an element $t \in \mathcal{I}$ such that $\mathcal{I}^{-1} \cdot t$ and $q\Lambda$ are coprime via Lemma 8. We then create a sample according to the NCLWE distribution by taking a Gaussian sample $z \leftarrow D_{\mathcal{I},r'}$ and setting

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

where $e' \leftarrow D_{\alpha/\sqrt{2}}$. Since $r \geq q \cdot \eta(\mathcal{I})$, by Lemma 1 the probability of obtaining any given $z \bmod q\mathcal{I}$ lies in $\left[\frac{1-\varepsilon}{1+\varepsilon}, 1\right] \cdot \beta$ for some $\beta > 0$, so the statistical distance between $z \bmod q\mathcal{I}$ and the uniform distribution is at most 2ε. Since χ_t is a bijection, $a = \chi_t^{-1}(z \bmod q\mathcal{I})$ is at most statistical distance 2ε from being uniformly distributed over Λ_q. Finally, we show that b has the shape $(a \cdot s)/q + e''$, for an error e'' and uniformly random s, conditioned on some fixed value of a. We have

$$b = (z \cdot y)/q + e' = (z \cdot x)/q + (z \cdot e)/q + e' \bmod \Lambda^\vee$$

By construction $z = t \cdot a \bmod \Lambda_q^\vee$. Since $t \in \mathcal{Z}(\mathcal{A})$, we have $(z \cdot x)/q = ((a \cdot t) \cdot x)/q = (a \cdot (t \cdot x))/q = (a \cdot s)/q \bmod \Lambda^\vee$ for $s := \chi_t\left(x \bmod q\mathcal{I}^\vee\right)$. If x is uniform over $\mathcal{I}_q^\vee$, then s is uniformly random over $\Lambda_q^\vee$ since χ_t is bijective. Finally, the analysis of the error proceeds identically to [14, Lemma 10]. □

The above two lemmas reduce BDD to NCLWE. We combine this with a (quantum) proof that given a BDD oracle, we can output a sample from a discrete Gaussian, to recover the iterative step (as in the CLWE reduction). This then implies a reduction from DGS to NCLWE. The quantum step is:

Lemma 12. *There is an efficient quantum algorithm that given any nd^2 dimensional lattice $\mathcal{L} := \sigma_{\mathcal{A}}(\mathcal{I})$ for some ideal $\mathcal{I} \subset \Lambda$, $0 < \delta < \lambda_1 (\mathcal{L}^*) / (2\sqrt{2nd})$, and an oracle that solves $\mathcal{A}$-$BDD^{\nu}_{\mathcal{L}^*,\delta}$ with all but negligible probability, outputs an independent sample from $D_{\mathcal{L},\sqrt{d}\omega(\sqrt{\log(nd)})/\sqrt{2}\delta^*}$.*

Proof. Our lattices are a kind of module lattice (as modules over $\mathcal{O}_K$), so the adaptation of [18] holds in this case too. □

We combine these three results to obtain:

Theorem 8. *Given an oracle that solves $SNCLWE_{q,s,\Sigma_\alpha}$ for $\alpha \in (0,1)$, $q \geq 2$, an unramified ideal $\mathcal{I} \subset \Lambda$, an $r \geq \sqrt{2}q \cdot \eta(\mathcal{I})$ satisfying $r' := r \cdot \omega(\sqrt{\log nd^2})/(\alpha q) > \sqrt{2nd^2}/\lambda_1 (\mathcal{I}^\vee)$, and polynomially many samples from $D_{\mathcal{I},r}$, there exists an efficient quantum algorithm that outputs an independent sample from $D_{\mathcal{I},r'}$.*

Using this theorem, we can obtain:

Theorem 9. *Let $\mathcal{A} = (L/K, \theta, \gamma)$ be a nonassociative CDA, $\gamma \in \mathcal{O}_L^\times \setminus \mathcal{O}_K^\times$, and $|\gamma| = 1$. Let $\alpha = \alpha(n) \in (0,1)$ and $q \geq 2$ unramified in L be parameters such that $\alpha q \geq \omega(1)$. Let $\mathcal{I}$ be an unramified ideal of Λ. Then there is a polynomial-time quantum reduction from $\mathcal{A}$-DGS^{ν}_{ξ} to $SNCLWE_{q,s,\Sigma_\alpha}$ for any $\xi = r\sqrt{d}\omega(\sqrt{\log nd})/\alpha q$, where $r > \sqrt{2}q \cdot \eta_\varepsilon(\mathcal{I})$.*

Proof. We prove the result in the standard iterative manner; for a large value of r, e.g. $r \geq 2^{2N}\lambda_N(\mathcal{I})$, start by sampling classically from $D_{\mathcal{I},r}$. Then apply the above theorem to obtain a polynomial number of samples from $D_{\mathcal{I},r'}$. Iterating this step gives samples from progressively narrower distributions, until we arrive at the desired parameter $s \geq \xi$. □

7.3 On SIVP in Number Fields and Cyclic Division Algebras

Here we comment on SIVP over ideal lattices in number fields, and SIVP over ideal lattices in CDAs. Let $\mathcal{I} = \overline{\mathcal{I}}\Lambda$ be an ideal of Λ. Suppose the prime factors of $\overline{\mathcal{I}}$ are unframified in $\mathcal{O}_L$. Then it is shown in a concurrent (currently unpublished) work [26] that if one solves SIVP in $\overline{\mathcal{I}}\mathcal{O}_L$, one solves SIVP in $\mathcal{I}$. If one solves SIVP in $\overline{\mathcal{I}}\mathcal{O}_L$, one obtains nd short independent vectors in $\overline{\mathcal{I}}\mathcal{O}_L$. Denote these vectors by x_i, $i = 1, ..., nd$. One can then consider these vectors as elements of Λ: $x_i = x_i \cdot (1 + u \cdot 0 + ...u^{d-1} \cdot 0) = x_i \in \Lambda$. Moreover, these vectors clearly belong to $\mathcal{I}$, as do $u^j x_i$, for $j = 0, ..., d-1$ and $i = 1, ..., nd$, when $\gamma \in \mathcal{O}_L^\times$. This gives nd^2 short independent vectors in $\mathcal{I}$, that is, a solution to $\mathcal{I}$-SIVP.

Thus it suffices to solve SIVP in ideal lattices of $\mathcal{O}_L$ rather than in ideal lattices of Λ. However, the SIVP to search NCLWE reduction only gives a lower bound on the security of NCLWE; we expect the hardness of NCLWE to be significantly greater than SIVP in $\mathcal{O}_L$. In the associative setting, the work [26] provides two reductions linking SIVP on ideal lattices and structured module lattices respectively to CLWE. We leave it as future work to see if these reductions extend to NCLWE.

8 NCLWE and Cryptography

Here we give a PKE scheme whose hardness is based on NCLWE. We discuss its efficiency, sample parameters, and security against attacks. Our scheme is given for $d = 2$.

8.1 PKE from Nonassociative LWE

Let $\mathcal{A} := (L/K, \theta, \gamma)$, where $\mathcal{A}$ is a CDA, Σ be an error distribution, and q a prime completely split in $\mathcal{O}_K$, factorising as $q\mathcal{O}_K = \prod_{i=1}^{[K:\mathbb{Q}]} \mathfrak{q}_i$ with prime factors $\mathfrak{q}_i$ inert in $\mathcal{O}_L$. We denote the coefficient vector of $a = a_0 + ua_1 + \ldots + u^{d-1}a_{d-1}$ by $\mathbf{a} = (a_0, a_1, \ldots, a_{d-1})$. Note $\mathcal{O}_L/q\mathcal{O}_L$ has a polynomial-size representation of dimension nd, so in our scheme below we can encode a binary message $\mathbf{m} \in \{0,1\}^{nd^2}$ as an element of Λ_q by sending each block of nd entries of $\mathbf{m}$ to a coefficient of an element of Λ. Recall the Regev-style CLWE-based scheme, similar to the 'LPR' scheme of [24]:

Key generation Generate a CLWE sample $(a, b := a \cdot s + e)$, where $a \in \Lambda_q$ is uniformly random and $e \leftarrow \Sigma$, and output public key (a, b).
Encryption To encrypt $\mathbf{m} \in \{0,1\}^{nd^2}$, sample $t, e_1, e_2 \leftarrow \Sigma$ and output

$$(\mathbf{u}, \mathbf{v}) := \left(\phi(a)^T\mathbf{t} + \mathbf{e}_1, \phi(b)^T\mathbf{t} + \mathbf{e}_2 + \left\lceil \frac{q}{2} \right\rfloor \cdot \mathbf{m}\right)$$

Decryption To decrypt, compute $\mathbf{c} = \mathbf{v} - \phi(s)^T\mathbf{u}$ and recover each coordinate of $\mathbf{m}$ by rounding the entries of $\mathbf{c}$ to 0 or $\left\lceil \frac{q}{2} \right\rfloor$, and output 0 or 1 respectively.

This scheme is not directly applicable to our context, since the matrix representation of nonassociative algebra elements is not multiplicative, i.e. $\phi(a)\phi(s) \neq \phi(as)$. To see this explicitly, let $d = 2$ and $a = a_0 + ua_1$, $s = s_0 + us_1$. Then

$$\phi(a) = \begin{pmatrix} a_0 & \gamma\theta(a_1) \\ a_1 & \theta(a_0) \end{pmatrix} \text{ and } \phi(s) = \begin{pmatrix} s_0 & \gamma\theta(s_1) \\ s_1 & \theta(s_0) \end{pmatrix}.$$

Thus

$$\phi(a)\phi(s) = \begin{pmatrix} a_0s_0 + \gamma\theta(a_1)s_1 & a_0\gamma\theta(s_1) + \gamma\theta(a_1)\theta(s_0) \\ a_1s_0 + \theta(a_0)s_1 & a_1\gamma\theta(s_1) + \theta(a_0)\theta(s_0) \end{pmatrix}.$$

On the other hand, $a \cdot s = a_0s_0 + \gamma\theta(a_1)s_1 + u(a_1s_0 + \theta(a_0)s_1)$, and

$$\phi(as) = \begin{pmatrix} a_0s_0 + \gamma\theta(a_1)s_1 & \gamma\theta(a_1)\theta(s_0) + \gamma a_0\theta(s_1) \\ a_1s_0 + \theta(a_0)s_1 & \theta(a_0)\theta(s_0) + \theta(\gamma)a_1\theta(s_1) \end{pmatrix}.$$

So one can see that

$$\phi(as) - \phi(a)\phi(s) = \begin{pmatrix} 0 & 0 \\ 0 & (\theta(\gamma) - \gamma)a_1\theta(s_1) \end{pmatrix}.$$

Thus when one computes $\mathbf{c} = \mathbf{v} - \phi(s)^T\mathbf{u}$, one is left with

$$\mathbf{c} = \begin{pmatrix} 0 & 0 \\ 0 & (\theta(\gamma) - \gamma)a_1\theta(s_1) \end{pmatrix} \mathbf{t} + \mathbf{e}' + \left\lceil \frac{q}{2} \right\rfloor \mathbf{m}, \tag{1}$$

where $\mathbf{e}'$ is an error term. One could absorb $(\theta(\gamma) - \gamma)a_1\theta(s_1)$ into $\mathbf{e}'$, and if $(\theta(\gamma)-\gamma)a_1\theta(s_1)$ is small proceed as usual; however, $a \in \Lambda_q$ is uniformly random so this has low chance of success. One could encrypt a message with 0 in the lower entry, i.e. $\mathbf{m} = (m \quad 0)^T$, and only run the decryption on the entries of $\mathbf{c}$ for which $\phi(as) - \phi(a)\phi(s) = 0$. However, this restricts the number of bits which can be sent. These observations lead us to the following adapted scheme.

8.2 LPR-Style Cryptosystem

Below the index i runs from 1 to 2. For an n-dimensional vector $\mathbf{v}$ the notation $\tilde{\mathbf{v}}$ denotes the vector $(v_{n-i})_i$, and $\tilde{v}$ denotes an algebra element with vector of coefficients $\tilde{\mathbf{v}}$.

Key generation Generate two NCLWE samples $(a_i, b_i := a_i \cdot s_i + e_i)$, where a_i is sampled uniformly at random, $s_i \in \Lambda_q$ is small, and $e_i \leftarrow \Sigma$, and output public keys (a_i, b_i).
Encryption To encrypt $\mathbf{m} \in \{0,1\}^{2n}$, place the entries of $\mathbf{m}$ as an element m of Λ_q and set $m_1 := m$, $m_2 := \tilde{m}$. Sample $t_i \leftarrow \Lambda_q$, $e_{i,1}, e_{i,2} \leftarrow \Sigma$ and output

$$(\mathbf{u}_i, \mathbf{v}_i) := \left(\phi(a_i)^T\mathbf{t}_i + \mathbf{e}_{i,1}, \phi(b_i)^T\mathbf{t}_i + \mathbf{e}_{i,2} + \left\lfloor \frac{q}{2} \right\rfloor \cdot \mathbf{m}_i\right)$$

Decryption To decrypt, compute $\mathbf{c}_i = \mathbf{v}_i - \phi(s_i)^T\mathbf{u}_i$, and recover half the coordinates of $\mathbf{m}_i$ by rounding the top $\frac{1}{2}[\mathcal{A} : \mathbb{Q}]$ entries of $\mathbf{c}_i$ to 0 or $\left\lfloor \frac{q}{2} \right\rfloor$, and outputting 0 or 1 respectively.

This is IND-CPA secure under NCLWE because the two encryptions (of the m_i) are independent. We now prove this.

Lemma 13. *Let $\mathcal{A} = (L/K, \theta, \gamma)$ be a nonassociative cyclic division algebra with $[L : K] = 2$, where $\gamma \in \mathcal{O}_L^\times$ is a unit. Then*

1. *There exists another cyclic algebra $\mathcal{A}' = \left(L/K, \theta, \theta(\gamma)^{-1}\right)$ with matrix representation $\phi'(\cdot)$ and natural order Λ' such that for any $a \in \mathcal{A}$ there exists $a' \in \Lambda'$ satisfying $\phi(a)^T = \phi'(a')$. Moreover, $\mathcal{A}'$ is a division algebra, and Λ'_q and Λ_q are canonically isomorphic as additive groups.*
2. *If $\theta(\gamma) = \gamma^{-1}$, we may take $\mathcal{A} = \mathcal{A}'$ and there exists $a' \in \Lambda$ satisfying $\phi(a)^T = \phi(a')$.*

Proof. The proof of the first statement is identical to [14, Lemma 19]. For the second statement, recall $\phi(a) = \begin{pmatrix} a_0 & \gamma\theta(a_1) \\ a_1 & \theta(a_0) \end{pmatrix}$ so $\phi(a)^T = \begin{pmatrix} a_0 & a_1 \\ \gamma\theta(a_1) & \theta(a_0) \end{pmatrix}$. Now, set

$$a' := a_0 + u\gamma\theta(a_1)$$

Then $\phi(a') = \begin{pmatrix} a_0 & \gamma\theta(\gamma\theta(a_1)) \\ \gamma\theta(a_1) & \theta(a_0) \end{pmatrix} = \begin{pmatrix} a_0 & a_1 \\ \gamma\theta(a_1) & \theta(a_0) \end{pmatrix}$. Comparison yields the result. □

An example algebra satisfying the second property is $\mathcal{A} = (\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m + \zeta_m^{-1}), \theta, \zeta_m)$, $m > 2$.

We say a scheme is IND-CPA secure if any probabilistic polynomial time (ppt.) adversary has only negligible advantage in the PubK experiment:

Definition 32. *([17]) Let $\Pi = (Gen, Enc, Dec)$ be a PKE scheme, and $\mathcal{A}$ be an adversary. Say Π is indistinguishable under chosen-plaintext attack if a ppt. adversary in the following experiment* $\mathrm{PubK}_{\mathcal{A},\Pi}(n)$ *has negligible advantage:*

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

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

We now prove our scheme is IND-CPA secure, assuming NCLWE is intractable.

Lemma 14. *Let $\mathcal{A} = (L/K, \theta, \gamma)$ be a nonassociative cyclic division algebra with $[L : K] = 2$, where γ is a unit and $\theta(\gamma) = \gamma^{-1}$. Then the above scheme is correct if*

$$\left\| \boldsymbol{e}_3 + \left\lceil \frac{q}{2} \right\rfloor \cdot \mathbf{m} - \begin{pmatrix} s_0 & s_1 \\ 0 & 0 \end{pmatrix} \boldsymbol{e}_1 - \begin{pmatrix} 0 & 0 \\ \theta(s_0) & \theta(s_1) \end{pmatrix} \boldsymbol{e}_2 \right\|_\infty \leq \left\lceil \frac{q}{4} \right\rfloor$$

and is IND-CPA secure, assuming the hardness of NCLWE.

Proof. The correctness condition follows from the computation of Section 8.1.

For IND-CPA security, the adversary receives public key (a_1, b_1, a_2, b_2). Under the NCLWE assumption, this four-tuple is indistinguishable from uniformly random (i.e. distinguishable with at most negligible advantage). Note the pairs (a_1, b_1) and (a_2, b_2) are independent. We may thus replace b_1, b_2 by uniformly random elements b_1', b_2' and proceed with the experiment. The adversary then receives an encryption of m_b of the form $(\mathbf{u}_1, \mathbf{v}_1, \mathbf{u}_2, \mathbf{v}_2)$, for $b \in \{0,1\}$. Since the four-tuple $(\mathbf{u}_1, \mathbf{v}_1 - \left\lfloor \frac{q}{2} \right\rfloor m, \mathbf{u}_2, \mathbf{v}_2 - \left\lfloor \frac{q}{2} \right\rfloor \tilde{m})$ is a tuple of valid independent NCLWE samples in $\mathcal{A}'$ (by Lemma 13), we have that $(\mathbf{u}_1, \mathbf{v}_1 - \left\lfloor \frac{q}{2} \right\rfloor m, \mathbf{u}_2, \mathbf{v}_2 - \left\lfloor \frac{q}{2} \right\rfloor \tilde{m})$ is indistinguishable from a uniformly random four-tuple (with at most negligible advantage) under the NCLWE assumption. We then obtain that $(\mathbf{u}_1, \mathbf{v}_1, \mathbf{u}_2, \mathbf{v}_2)$ is also close to uniform, and we conclude that the adversary has at most negligible advantage. □

We close this section with a remark. The above scheme encrypts a message of dimension nd^2 by performing two independent Regev-style encryptions. While this scheme is IND-CPA secure, it is of course less efficient than only needing to perform one Regev-style encryption. By inspecting Equation (1), one can see that if a_1 and s_1 are both small elements, they may be absorbed into the error term and rounded away. Thus, making the assumption that NCLWE samples of the form $(a, b) = (a_0 + ua_1, (a_0 + ua_1) \cdot (s_0 + us_1) + (e_0 + ue_1))$ provide intractable instances of LWE when a_1 and s_1 have bounded magnitudes, one could obtain IND-CPA security of a PKE scheme which only requires one round of Regev-style encryption. Since we could not prove such intractability for these instances, we make no such claim but leave it as an open problem.

8.3 Operational Complexity

An algorithm was given in [14] to compute the complexity of the multiplication $\phi(a)\mathbf{s}$, where a and s are algebra elements in an associative CDA and q is unramified in K. The complexity of this algorithm was estimated at $O\left(N \log N/d^2\right) + \tilde{O}\left(Nd^{\omega-2}\right)$, where ω is the exponent of matrix multiplication and $N = nd^2$. This is an improvement over that coming from module elements in the same dimension. We note that such an algorithm also applies to the nonassociative case, because the algorithm relies on the CDAs being quotients of skew polynomial rings, as are the algebras of this work [37]. In this section we provide exposition of our algorithm.

Our multiplication algorithm uses the CRT-style map of (3) to decompose the problem of multiplying elements of Λ_q into a number of more tractable multiplications, when q has 'good' ramification properties. We do this by viewing our algebras as quotients of skew polynomial rings, and so via the CRT we may apply the algorithm of [33][1]. We may then invert the CRT to obtain the result of the multiplication. We study the complexity of this algorithm and compare it to the corresponding complexity of other algebraically structured LWE instances. Below, $\omega \in [2, 2.373]$ denotes the exponent of matrix multiplication.

Background on Skew Polynomial Rings Let R be a commutative ring with $1 \in R$, and let θ be an endomorphism of R. Then we may define a noncommutative ring of polynomials in an indeterminate u with coefficients in R, by defining addition coefficientwise and defining multiplication of polynomials in the standard manner, subject to the condition

$$ux = \theta(x)u \text{ for all } x \in R$$

We denote the ring of such polynomials by $R[u, \theta]$, known as a skew polynomial ring, and note $R[u, \theta] = \{\sum_{i=0}^{n} u^i x_i : x_i \in R, n < \infty\}$. We remark that one may define left division by an element $b \in R[u, \theta]$, since for all $a \in R[u, \theta]$, there exists a unique pair $k, r \in R[u, \theta]$ such that $a = bk + r$ with $\deg(r) < d$ [31]. We will

[1] We also note the earlier version [34].

take $R = \mathbb{F}$ to be a field from now on, and θ an automorphism.

Let $\mathbb{F}^\theta$ be the fixed field of θ, defined $\mathbb{F}^\theta = \{x \in \mathbb{F} : \theta(x) = x\}$. Suppose θ has order d. Then $\mathbb{F}^\theta[u^d]$ is the largest commutative subring of $\mathbb{F}[u, \theta]$. The elements of this subring are called *central* and generate two-sided ideals of $\mathbb{F}[u, \theta]$. The quotients of $\mathbb{F}[u, \theta]$ by ideals generated by central elements are associative rings. If, however, we consider the quotient of $\mathbb{F}[u, \theta]$ by monic elements of the form $f(u)$ with coefficients not in $\mathbb{F}^\theta$, we may obtain a nonassociative ring on the set of polynomials of degree less than d [37] by defining multiplication of a and b as

$$a \cdot b = ab \bmod f(u) \tag{2}$$

where 'mod' means we perform left division and take the remainder. We let $\mathbb{F}_{q^m}[u, \theta]_{<d}$ denote the set of skew polynomials of degree less than d.

We now focus on quotients of $\mathbb{F}[u, \theta]$ by $(u^d - \gamma)\mathbb{F}[u, \theta]$ for $\gamma \in \mathbb{F}$ such that $\theta(\gamma) \neq \gamma$. As stated above, from this we obtain a nonassociative ring. In the following, we assume that we have choices of d and γ which obtain nonassociative division algebras as in [37], and we thus have $(\mathbb{F}/\mathbb{F}^\theta, \theta, \gamma) \cong \mathbb{F}[u, \theta]/(u^d - \gamma)\mathbb{F}[u, \theta]$ [35, 36, 7]. Thus quotients of skew polynomial rings yield nonassociative cyclic algebras.

For more on skew polynomials, see [31] or [16, Chapter 8].

Quotients of Natural Orders We now let $q \in \mathbb{Z}$ be a prime completely split into factors $\mathfrak{q}_i$ in $\mathcal{O}_K$ which are inert in $\mathcal{O}_L$. Write this as $q\mathcal{O}_K = \prod_{i=1}^{[K:\mathbb{Q}]} \mathfrak{q}_i$, as a product of prime ideals. We then recall the CRT-style isomorphism

$$\Lambda_q \cong \prod_{i=1}^{[K:\mathbb{Q}]} \left(\left(\mathcal{O}_L / \mathfrak{q}_i \mathcal{O}_L \right) / \left(\mathcal{O}_K / \mathfrak{q}_i \right), \overline{\theta}_i, \overline{\gamma}_i \right) \tag{3}$$

We may thus use this isomorphism to reduce our problem in Λ_q to problems in the factors $\left(\left(\mathcal{O}_L / \mathfrak{q}_i \mathcal{O}_L \right) / \left(\mathcal{O}_K / \mathfrak{q}_i \right), \overline{\theta}_i, \overline{\gamma}_i \right)$ on the right hand side of (3) for each i, where $\overline{\gamma}_i = \gamma \bmod \mathfrak{q}_i \mathcal{O}_L$ and $\overline{\theta}_i$ is the action of θ modulo $\mathfrak{q}_i$, which are generalised cyclic algebras. Since we assumed the $\mathfrak{q}_i$ are inert in $\mathcal{O}_L$, $\mathfrak{q}_i \mathcal{O}_L$ is a prime ideal, say $\mathcal{Q}_i$, and we find $\mathcal{O}_L / \mathfrak{q}_i \mathcal{O}_L = \mathcal{O}_L / \mathcal{Q}_i \cong \mathbb{F}_{q^{[L:K]}}$, while $\mathcal{O}_K / \mathfrak{q}_i \cong \mathbb{F}_q$. This gives us

$$\left(\left(\mathcal{O}_L / \mathfrak{q}_i \mathcal{O}_L \right) / \left(\mathcal{O}_K / \mathfrak{q}_i \right), \overline{\theta}_i, \overline{\gamma}_i \right) \cong (\mathbb{F}_{q^{[L:K]}} / \mathbb{F}_q, \overline{\theta}_i, \overline{\gamma}_i), \tag{4}$$

So we in fact have cyclic algebras over finite fields on the right hand side (not generalised cyclic algebras). These cyclic algebras may then be interpreted as quotients of skew polynomial rings $\mathbb{F}_{q^{[L:K]}}[u, \overline{\theta}_i]$ by an ideal generated by $u^d - \overline{\gamma}_i$, as described above.

We close this section with a discussion of the complexity of the CRT-style map of (3), when K is a cyclotomic field. We follow [14, Appendix F]. The isomorphism sends

$$\sum_{j=0}^{d-1} u^j x_j \to \bigotimes_{i=1}^{n} \sum_{j=0}^{d-1} u^j \left(x_j \mod \mathfrak{q}_i \mathcal{O}_L \right)$$

Thus the CRT-style map sends each u^j-coefficient to its mod $\mathfrak{q}_i\mathcal{O}_L$ 'parts' via the standard CRT for number fields. The result of [14, Appendix F5] was that when the $\mathfrak{q}_i$ are inert in $\mathcal{O}_L$, this decomposition can be performed in time $O(nd^2 \log n)$. The method for performing this relies on the following observation: since the quotient $\mathcal{O}_L/\mathfrak{q}_i\mathcal{O}_L$ is a vector space over $\mathcal{O}_K/\mathfrak{q}_i$, we can decompose an arbitrary $\mathcal{O}_{K_q}$ basis $\ell_1, \ldots, \ell_d$ of $\mathcal{O}_{L_q}$ into $[K : \mathbb{Q}]$ bases $\ell_j = (\ell_{1,j}, \ldots, \ell_{n,j})$ such that each $\ell_{i,1}, \ldots, \ell_{i,d}$ (of $\mathfrak{q}_i\mathcal{O}_L$ parts) is a basis of the vector space basis over $\mathcal{O}_K/\mathfrak{q}_i$.

Now take any integral $\mathcal{O}_K$-basis $\ell_1, \ldots, \ell_d$ of $\mathcal{O}_L$. Compute and store the $\ell_j \bmod \mathfrak{q}_i\mathcal{O}_L$, for each i and j. The CRT-style map then splits each of the u^i-coefficients of an element of Λ_q into its mod $\mathfrak{q}_i\mathcal{O}_L$ parts. We store elements of $\mathcal{O}_{L_q}$ as $\mathcal{O}_K$-combinations of the chosen basis, that is as $\ell = \sum_{j=1}^{d} \ell_j k_j$ for $k_j \in \mathcal{O}_{K_q}$. We may then split $\ell \in \mathcal{O}_{L_q}$ into its $\mathcal{O}_L/\mathfrak{q}_i$ parts in time $O(d \cdot n \log n)$, since

$$\sum_{j=1}^{d} \ell_j k_j \bmod \mathfrak{q}_i\mathcal{O}_L = \sum_{j=1}^{d} (\ell_j \bmod \mathfrak{q}_i\mathcal{O}_L) \cdot (k_j \bmod \mathfrak{q}_i\mathcal{O}_L)$$

where the $k_j \bmod \mathfrak{q}_i$ may be computed in time $O(n \log n)$ by the standard cyclotomic field CRT and the $\ell_j \bmod \mathfrak{q}_i \bmod \mathcal{O}_L$ were precomputed. Since we have d u^i-coefficients, we obtain a complexity of $O(nd^2 \log n)$.

To invert the CRT-style map after performing computations in its range, we must rewrite the resulting elements (of whatever computations have been performed) in our chosen basis of the decomposition step. Since $\mathcal{O}_L \bmod \mathfrak{q}_i\mathcal{O}_L$ is a d-dimensional vector space over $\mathcal{O}_K/\mathfrak{q}_i$, we may precompute a suitable change of basis matrix over $\mathcal{O}_K/\mathfrak{q}_i$ in time $\tilde{O}\left(d^\omega\right)$. Since we have to do this for the of n rings, which each have d coordinates, the total complexity of this is $\tilde{O}\left(nd^{\omega+1}\right)$.

Thus the complexity of decomposing and inverting via the CRT-style map is

$$O(nd^2 \log n) + \tilde{O}\left(nd^{\omega+1}\right)$$

The Puchinger-Wachter-Zeh (PW-Z) Algorithm In [34, 33] the authors give an algorithm for performing multiplication in skew polynomial rings over finite fields. We omit the details of their algorithm for brevity; it may be found in [33, Algorithm 1][2]. Below we use the algorithm as a black-box, and require only a statement on its complexity:

Theorem 10. *[33, Theorem 7] Let $a, b \in \mathbb{F}_{q^m}[u, \theta]_{\leq s}, s^* := \lceil \sqrt{s+1} \rceil$. Then $c = a \cdot b$ can be calculated in $O\left(s^{\frac{3}{2}}\right)$ field operations, plus the cost of multiplying an $s^* \times s^*$ with an $s^* \times (s + s^*)$ matrix, using [33, Algorithm 1].*

The authors give a more precise estimate of the asymptotic complexity of their algorithm; let $\mathcal{M}_{q^m}(s)$ denote the complexity of multiplying two skew polynomials from $\mathbb{F}_{q^m}[u, \theta]_{\leq s}$, and ω denote the exponent of matrix multiplication.

[2] Cf. [34, Algorithm 2].

Corollary 2. *[33, Corollary 8] One has*

$$\mathcal{M}_{q^m}(s) \in O\left(s^* \cdot (s^*)^{\omega}\right) \subseteq O\left(s^{\frac{\omega+1}{2}}\right)$$

We now combine a number of the above observations. Suppose we have two elements a, b of $\left(\left(\mathcal{O}_L/\mathfrak{q}_i\mathcal{O}_L\right) / \left(\mathcal{O}_K/\mathfrak{q}_i\right), \overline{\theta}_i, \overline{\gamma}_i\right)$. This is isomorphic to $(\mathbb{F}_{q^{[L:K]}}/\mathbb{F}_q, \overline{\theta}_i, \overline{\gamma}_i)$, which in turn can be realised as the quotient $\mathbb{F}_{q^{[L:K]}}[u, \overline{\theta}_i]/(u^d - \overline{\gamma}_i)\mathbb{F}_{q^{[L:K]}}$. There is a natural inclusion map

$$\iota : \mathbb{F}_{q^{[L:K]}}[u, \overline{\theta}_i]/(u^d - \overline{\gamma}_i)\mathbb{F}_{q^{[L:K]}}[u, \overline{\theta}_i] \hookrightarrow \mathbb{F}_{q^{[L:K]}}[u, \overline{\theta}_i]$$

which takes an element of $\mathbb{F}_{q^{[L:K]}}[u, \overline{\theta}_i]/(u^d - \overline{\gamma}_i)\mathbb{F}_{q^{[L:K]}}[u, \overline{\theta}_i]$ and simply drops the quotient ring structure. This allows us to run algorithms for skew polynomial rings on elements obtained from quotients of natural orders in nonassociative cyclic algebras. We use this remark below as the center of our algorithm.

Applying the above to our setting, so taking $s = d-1$ and using Corollary 2, we find that the complexity of the PW-Z algorithm applied to each ring mod $\mathfrak{q}_i$ is $O\left((d-1)^{\frac{\omega+1}{2}}\right)$. For simplicity we will upper bound this by $O\left(d^{\frac{\omega+1}{2}}\right)$. Since we must perform this n times, we have a final complexity of $O\left(nd^{\frac{\omega+1}{2}}\right)$.

The authors go on to to prove that their multiplication algorithm implies a division algorithm for skew polynomials of complexity $\tilde{O}(s^{\min\left(\frac{\omega+1}{2}, 1.635\right)})$ for skew polynomials of degree at most s [33, Corollary 10]. With $s = d-1$ as above, this becomes $\tilde{O}\left((d-1)^{\min\left(\frac{\omega+1}{2}, 1.635\right)}\right)$. Since this is less (ignoring log factors) than the complexity of multiplication, we ignore this complexity below, beyond factoring in this log factor into our analysis.

Our Algorithm We now outline our algorithm. Our method consists of applying the CRT-style map to our algebra elements a, b to obtain $a, b \in \left(\left(\mathcal{O}_L/\mathfrak{q}_i\mathcal{O}_{\underline{L}}\right) / \left(\mathcal{O}_K/\mathfrak{q}_i\right), \overline{\theta}_i, \overline{\gamma}_i\right)$, for $i = 1, ..., [K : \mathbb{Q}]$. We then map these images to $\iota(a), \iota(b) \in \mathbb{F}_{q^{[L:K]}}[u, \overline{\theta}_i]$ as at the end of the previous section, for each i, and apply the Puchinger-Wachter-Zeh (PW-Z) algorithm to these images. Taking the output of the PW-Z algorithm and running left division with respect to $(u^d - \overline{\gamma}_i)\mathbb{F}_{q^{[L:K]}}[u, \overline{\theta}_i]$ yields an element of the nonassociative ring described at the beginning of this discussion, which is isomorphic to $\left(\left(\mathcal{O}_L/\mathfrak{q}_i\mathcal{O}_L\right) / \left(\mathcal{O}_K/\mathfrak{q}_i\right), \overline{\theta}_i, \overline{\gamma}_i\right)$. We then invert the tuple of products in these latter CDAs under the CRT-style map to obtain our product in Λ_q. A step-by-step description may be found in Algorithm 1.

Since the bottlenecks of our algorithm are computing the CRT and performing multiplication, we estimate a final complexity of

$$O(nd^2 \log n) + \tilde{O}\left(nd^{\omega+1}\right) + \tilde{O}\left(nd^{\frac{\omega+1}{2}}\right) = O(nd^2 \log n) + \tilde{O}\left(nd^{\omega+1}\right)$$

The complexity of our algorithm is essentially the same as that of [14, Appendix F], except we replace its use of the algorithm of [8] with the PW-Z algorithm. This is because we cannot apply the algorithm of [8] to our skew polynomial

```
Algorithm 1: Fast multiplication of elements of $\Lambda_q$
  Input: Two elements $a, b$ of $\Lambda_q$
  Output: The product $a \cdot b \in \Lambda_q$
  Compute the images of $a, b$ under the CRT-style map of (3) in
    $\left(\left(\mathcal{O}_L/\mathfrak{q}_i\mathcal{O}_L\right)/\left(\mathcal{O}_K/\mathfrak{q}_i\right), \overline{\theta}_i, \overline{\gamma}_i\right)$, for each $i$.
  Compute isomorphisms $\mathcal{O}_L/\mathfrak{q}_i\mathcal{O}_L \cong \mathbb{F}_{q^{[L:K]}}$ and $\mathcal{O}_K/\mathfrak{q}_i \cong \mathbb{F}_q$, for each $i$.
  Compute $\iota(a), \iota(b) \in \mathbb{F}_{q^{[L:K]}}[u, \overline{\theta}_i]$, for each $i$.
  Compute $\iota(a)\iota(b) \in \mathbb{F}_{q^{[L:K]}}[u, \overline{\theta}_i]$ via the PW-Z algorithm, for each $i$.
  Compute $\iota(a) \cdot \iota(b) = \iota(a)\iota(b) \mod u^d - \overline{\gamma}_i \in \mathbb{F}_{q^{[L:K]}}[u, \overline{\theta}_i]/(u^d - \overline{\gamma}_i)\mathbb{F}_{q^{[L:K]}}[u, \overline{\theta}_i]$,
    for each $i$.
  Compute the image of $\iota(a) \cdot \iota(b) \in \mathbb{F}_{q^{[L:K]}}[u, \overline{\theta}_i]/(u^d - \overline{\gamma}_i)\mathbb{F}_{q^{[L:K]}}[u, \overline{\theta}_i]$ in
    $\left(\left(\mathcal{O}_L/\mathfrak{q}_i\mathcal{O}_L\right)/\left(\mathcal{O}_K/\mathfrak{q}_i\right), \overline{\theta}_i, \overline{\gamma}_i\right)$, for each $i$.
  Return the inverse of the CRT-style map in $\Lambda_q$ on the resulting tuple.
```

rings, since it requires γ to fulfill certain conditions which are not met when $\gamma \in \mathcal{O}_L \setminus \mathcal{O}_K$.

Comparison Between Algebraic Structures In this section we fix the total dimension of the ambient algebraic structure as an integer N, and compare the complexities of multiplication in such spaces in such dimensions. We follow [14, Section 5.3] in the comparison of these alternatives via the study of the product As over $\mathbb{Z}_q$, equipped with various structures.

1. The ring case: here $N = n$ and we may write As over $\mathbb{Z}_q$ as multiplication of ring elements via the left regular representation $a \cdot s$ in $\mathbb{Z}_q[X]/\left(X^N + 1\right)$. Via CRT analysis in dimension N described in [23], the complexity of this multiplication is dominated by the CRT map, which has time complexity $O(N \log N)$, but includes a coordinatewise multiplication step which requires time $O(N)$.
2. The module case: here the module rank is d, $N = nd$, and $\mathbf{A}$ is a $d \times d$ matrix over $\mathbb{Z}_q[X]/\left(X^N + 1\right)$. One can compute As by applying the CRT coordinatewise in dimension n on A and s. This requires $d^2 + d$ applications of the CRT, for a total asymptotic complexity of $O\left(d^2 n \log n\right) = O(Nd \log(N/d))$. There is again a coordinatewise multiplication step requiring time $O(Nd)$.
3. The associative cyclic algebra case: here $N = nd^2$ and A is the matrix obtained from the left regular representation $\phi(a)$ of an element $a \in \Lambda_q$. In [14], the complexity of the multiplication $\phi(a) \cdot \mathrm{vec}(s)$ was estimated as $O\left(N \log\left(N/d^2\right)\right) + \tilde{O}\left(Nd^{\omega-1}\right)$ in the case where q is inert in L [14, Appendix F5]. Here the second term comes from the skew polynomial multiplication algorithm of [8], and the first from the CRT map.
4. The nonassociative cyclic algebra case: again we have $N = nd^2$ and A is the matrix obtained from the left regular representation $\phi(a)$ of an element $a \in \Lambda_q$. We estimated our complexity as $O(nd^2 \log n) + \tilde{O}\left(nd^{\omega+1}\right) = O(N \log N/d^2) + \tilde{O}\left(Nd^{\omega-1}\right)$, which is identical to the associative case. Note

that this is not surprising: multiplying two elements does not require associativity.

8.4 Concrete Algebras for NCLWE

Here we detail a variety of methods to construct nonassociative CDAs from cyclotomic fields (and their subfields). We pay particular attention to cases when $[\mathcal{A} : \mathbb{Q}] = 3 \cdot 2^r$ for some r, since [14] could not give such constructions.

A method to construct nonassociative CDAs was given above: let $K = \mathbb{Q}(\zeta_m)$ and $L = \mathbb{Q}(\zeta_{pm})$ with $\gcd(p, m) = 1$. Then $\zeta_{pm} \notin K$ and L/K is cyclic, so since ζ_{pm} does not lie in a proper subfield of L, by Proposition 2 the algebra $(L/K, \theta, \zeta_{pm})$ is a nonassociative CDA. Since $[L : K] = p - 1$, when $p = 3$ we have an appropriate degree algebra for the above PKE scheme. Note we can let $\gamma = \zeta_{pm}^k$ for any k such that $\gcd(pm, k) = 1$, since these are primitive pmth roots of unity, and no primitive pmth root of unity lies in a proper subfield. Moreover, for prime power $m = q^r$ we can create extensions by setting p to be a power of q; that is, p and m do not need to be coprime, but need to be chosen such that L/K is cyclic. Below is a table of parameters for possible algebras:

m	p	$[K : \mathbb{Q}]$	$[L : K]$	$[\mathcal{A} : \mathbb{Q}]$
128	5	64	4	1024
256	3,4	128	2	512
256	5	128	4	2048
512	3,4	256	2	1024
243	3,4	162	2	648
243	5	162	4	2592
125	3,4	100	2	400
125	5	100	4	1600
625	3,4	500	2	2000
343	3,4	294	2	1176

Table 1: Even Low-degree Nonassociative Algebras

Alternatively, let $L = \mathbb{Q}(\zeta_{pm}) = \mathbb{Q}(\zeta_{3^r \cdot 2^k})$, $K = \mathbb{Q}(\zeta_{3^{r-1} \cdot 2^k})$. Then $[L : \mathbb{Q}] = \phi(3^r \cdot 2^k) = 3^{r-1} \cdot 2^k$, $[K : \mathbb{Q}] = \phi(3^{r-1} \cdot 2^k) = 3^{r-2}2^k$, and $[L : K] = 3$. Note L/K is cyclic, so $\mathcal{A} = (L/K, \theta, \zeta_{3^r \cdot 2^k})$ is a nonassociative CDA. Below is a table of parameters for possible algebras:

m	K	p	L	$[K : \mathbb{Q}]$	$[\mathcal{A} : \mathbb{Q}]$
64	$\mathbb{Q}(\zeta_{192})$	9	$\mathbb{Q}(\zeta_{576})$	64	576
64	$\mathbb{Q}(\zeta_{576})$	27	$\mathbb{Q}(\zeta_{1728})$	192	1728
128	$\mathbb{Q}(\zeta_{384})$	9	$\mathbb{Q}(\zeta_{1152})$	128	1152
128	$\mathbb{Q}(\zeta_{1152})$	27	$\mathbb{Q}(\zeta_{3456})$	384	3456
256	$\mathbb{Q}(\zeta_{768})$	9	$\mathbb{Q}(\zeta_{2304})$	256	2304

Table 2: Cubic-degree Nonassociative Algebras

Now, consider the case when K is strictly contained within a cyclotomic field. The simplest example of this is $\mathcal{A} = (\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m + \zeta_m^{-1}), \theta, \zeta_m)$, $m > 2$. For examples with $[\mathcal{A} : \mathbb{Q}]$ divisible only by powers of 2 and 3, proceed as follows: set $v = 2^k$, $w = 9$, $\mathbb{Q}(\zeta_{vw})^+ = \mathbb{Q}(\zeta_{vw} + \zeta_{vw}^{-1})$. Then $\mathcal{A} = (L/K, \theta, \gamma) = (\mathbb{Q}(\zeta_{vw})/\mathbb{Q}(\zeta_{vw})^+, \theta, \zeta_{vw})$ has dimension $[L : \mathbb{Q}][L : K] = 2\phi(v)\phi(w) = 2^k \cdot 6 = 2^{k+1}3$. This creates a cyclic division algebra which has degree divisible by only one power of 3. We can also create algebras with degree divisible by higher powers of 3. Below is a table of parameters for possible algebras:

v	w	L	$[L : \mathbb{Q}]$	$[\mathcal{A} : \mathbb{Q}]$
64	27	$\mathbb{Q}(\zeta_{1728})$	576	1152
128	9	$\mathbb{Q}(\zeta_{1152})$	384	768
128	27	$\mathbb{Q}(\zeta_{3456})$	1152	2304
256	9	$\mathbb{Q}(\zeta_{2304})$	768	1536
512	9	$\mathbb{Q}(\zeta_{4608})$	1536	3072

Table 3: Nonassociative Algebras Over Maximal Real Subfields

Another way of constructing algebras with similar sizes to those above is as follows. Let $p = 7$ and $m = 2^r$. Setting $L = \mathbb{Q}(\zeta_{7 \cdot 2^r})$ and $K = \mathbb{Q}(\zeta_{2^r}, \sqrt{-7})$, $[L : K]$ is cyclic as $\mathbb{Q}(\sqrt{-7})$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_7)$, and we have $[L : K] = 3$, $[K : \mathbb{Q}] = 2^r$, so $[\mathcal{A} : \mathbb{Q}] = 9 \cdot 2^r$.

Finally, we give a construction where $|\gamma| \neq 1$. This leads to some distortion of the error in the proof of Lemma 11, but aside from this does not lead to significant complications. Let $K = \mathbb{Q}(\zeta_{p^k})$, where $(p, 7) = 1$, and $L = \mathbb{Q}(\zeta_{p^k}, \zeta_7 + \zeta_7^{-1})$. Then $[L : K] = 3$ and $\mathcal{A} = (L/K, \theta, \zeta_7 + \zeta_7^{-1})$ is a CDA of degree $9(p-1)p^{k-1}$ over $\mathbb{Q}$. In particular, we can construct a degree three extension where $p = 2$, and K has power of two degree. Below is a table of parameters for such algebras.

p^k	$[L : \mathbb{Q}]$	$[\mathcal{A} : \mathbb{Q}]$
128	192	576
256	384	1152
512	768	2304
243	243	729
125	300	900

Table 4: Nonassociative Algebras of Cubic Degree over Prime-power Cyclotomic Fields

8.5 Attacking NCLWE

Subfield Attacks A form of structured LWE named multivariate LWE (mLWE) [32] was attacked in [5]. The attack found a homomorphism from the mLWE sample domain into a subfield, where mLWE is defined over the tensor product of number fields. If a mLWE sample is defined over $\mathbb{Z}_q[x]/(x^{2^{r_1}}+1) \otimes \mathbb{Z}_q[x]/(x^{2^{r_2}}+1)$, $1 < r_2 \leq r_1$, then one can map a sample of dimension $r_1 r_2$ to r_2 samples of dimension r_1 (see [5] for details). We argue that NCLWE is immune to this attack for the same reason as is CLWE. Let $\mathcal{A} = (L/K, \theta, \gamma)$ be a nonassociative CDA. Suppose there exists a homomorphism $\chi : \mathcal{A} \to L$. The restriction of χ to L is an automorphism of L, so χ must satisfy $\chi(u) \cdot \chi(\ell) = \chi(u\ell) = \chi(\theta(\ell)u) = \chi(u) \cdot \chi(\theta(\ell))$ for any $\ell \in L$. However, this implies χ is not injective on L, and thus there is no homomorphism to a maximal (or any other) subfield. So our construction is immune from this dimension-reducing attack.

Plain Lattice Attacks Here we provide results from the lattice estimator of the cost of attacking out constructions, using plain lattice attacks. Here the attacks are run by ignoring the algebraic structure of the underlying lattice problems. This cost estimate is obtained by using the lattice estimator[3] [4] with similar parameters for the secret and error as Kyber512, but using lattice dimensions from examples in the previous section. We allow the estimator as many samples as the dimension of the corresponding lattice problem. We use a value of q completely split in L. The 'meaning' of the rop results in the final column is to give a rough idea of the number of ring operations required to solve the corresponding LWE instances, and is thus a measure of security. We list the minimum base-2 logarithms of these rop values over all attacks costed by the estimator.

$[\mathcal{A} : \mathbb{Q}]$	q	min log rop
512	7681	127.5
576	7489	143.7
648	2917	182.9
768	3457	209.9
900	7001	228.5
1024	7681	258.9
1152	3457	319.9
1176	8233	297.5
1536	18433	364.5

Table 5: Cost of Plain Lattice Attacks

References

[1] M. Ajtai. "Generating Hard Instances of Lattice Problems". In: *Electron. Colloquium Comput. Complex.* TR96 (1996). DOI: 10.1145/237814.237838.

[2] Miklós Ajtai and Cynthia Dwork. "A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence". In: *29th ACM STOC.* ACM Press, May 1997, pp. 284–293. DOI: 10.1145/258533.258604.

[3] Commit 564470e.

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

[4] 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.

[5] C. Bootland, W. Castryck, and F. Vercauteren. "On the security of the multivariate ring learning with errors problem". In: *ANTS XIV*. Auckland, New Zealand: MSP, 2020. DOI: 10.2140/obs.2020.4.57.

[6] Z. Brakerski and V. Vaikuntanathan. "Efficient Fully Homomorphic Encryption from (Standard) LWE". In: *FOCS 2011*. 2011, pp. 97–106. DOI: 10.1109/FOCS.2011.12.

[7] C. Brown and S. Pumplun. "How a nonassociative algebra reflects the properties of a skew polynomial". In: *Glasgow Mathematical Journal* 63.1 (2021), pp. 6–26. DOI: 10.1017/S0017089519000478.

[8] X. Caruso and J. Le Borgne. "Fast Multiplication for Skew Polynomials". In: *ISSAC 2017*. Assoc. for Computing Machinery, 2017, pp. 77–84. DOI: 10.1145/3087604.3087617.

[9] J. H. Cheon, A. Kim, M. Kim, and Y. Song. "Homomorphic Encryption for Arithmetic of Approximate Numbers". In: *ASIACRYPT 2017*. Ed. by T. Takagi and T. Peyrin. Vol. 10624. LNCS. Springer International Publishing, 2017, pp. 409–437. DOI: 10.1007/978-3-319-70694-8_15.

[10] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. "TFHE: Fast Fully Homomorphic Encryption Over the Torus". In: *J. Cryptol.* 33 (2019), pp. 34 –91. DOI: 10.1007/s00145-019-09319-x.

[11] L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky. "Lattice Signatures and Bimodal Gaussians". In: *CRYPTO 2013*. Ed. by R. Canetti and J. A. Garay. Vol. 8042. LNCS. Springer Berlin Heidelberg, 2013, pp. 40–56. DOI: 10.1007/978-3-642-40041-4_3.

[12] L. Ducas, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehle. *CRYSTALS-Dilithium: Digital Signatures from Module Lattices*. 2017. URL: https://pq-crystals.org/dilithium/index.shtml.

[13] Craig Gentry, Amit Sahai, and Brent Waters. "Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based". In: *CRYPTO 2013, Part I*. Ed. by Ran Canetti and Juan A. Garay. Vol. 8042. LNCS. Springer, Heidelberg, Aug. 2013, pp. 75–92. DOI: 10.1007/978-3-642-40041-4_5.

[14] C. Grover, A. Mendelsohn, C. Ling, and R. Vehkalahti. "Non-commutative Ring Learning with Errors from Cyclic Algebras". In: *J. Cryptol.* 35.3 (July 2022), p. 22. DOI: 10.1007/s00145-022-09430-6.

[15] 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.

[16] W.C. Huffman, J.L. Kim, and P. Solé. *Concise Encyclopedia of Coding Theory*. CRC Press, 2021. ISBN: 9781138551992.

[17] J. Katz and Y. Lindell. *Introduction to Modern Cryptography, Second Edition.* Chapman & Hall/CRC Cryptography and Network Security Series. Taylor & Francis, 2014. ISBN: 9781466570269.

[18] 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. DOI: 10.1007/s10623-014-9938-4.

[19] H. J. Lee and W. C. Waterhouse. "Maximal orders in nonassociative quaternion algebras". In: *Journal of Algebra* 146.2 (1992), pp. 441–453. DOI: 10.1016/0021-8693(92)90077-Y.

[20] C. Ling and A. Mendelsohn. "Middle-Products of Skew Polynomials and Learning with Errors". In: *IMACC 2023.* Ed. by E. A. Quaglia. Vol. 14421. LNCS. Springer, 2024, pp. 199–219. DOI: 10.1007/978-3-031-47818-5_11.

[21] C. Ling and A. Mendelsohn. "NTRU In Quaternion Algebras Of Bounded Discriminant". In: *PQCrypto 2023.* Vol. 14154. LNCS. Springer-Verlag, 2023, pp. 256–290. DOI: 10.1007/978-3-031-40003-2_10.

[22] V. Lyubashevsky. "Lattice Signatures without Trapdoors". In: *EUROCRYPT 2012.* Ed. by D. Pointcheval and T. Johansson. Vol. 7237. LNCS. Springer Berlin Heidelberg, 2012, pp. 738–755. DOI: 10.1007/978-3-642-29011-4_43.

[23] V. Lyubashevsky, C. Peikert, and O. Regev. "A Toolkit for Ring-LWE Cryptography". In: *EUROCRYPT 2013.* Ed. by T. Johansson and P. Q. Nguyen. Vol. 7881. LNCS. Springer Berlin Heidelberg, 2013, pp. 35–54. DOI: 10.1007/978-3-642-38348-9_3.

[24] V. Lyubashevsky, C. Peikert, and O. Regev. "On Ideal Lattices and Learning with Errors over Rings". In: *J. ACM* 60.6 (2013). DOI: 10.1145/2535925.

[25] A. Mendelsohn and C. Ling. "Fractional non-norm elements for division algebras, and an application to Cyclic Learning with Errors". In: *Adv. Math. Commun.* (2023). DOI: 10.3934/amc.2023043.

[26] A Mendelsohn and C Ling. *On the Hardness of Cryptographic Problems from Cyclic Algebras.* To appear.

[27] D. Miccancio and C. Peikert. *The Mathematics of Modern Cryptography Workshop.* https://simons.berkeley.edu/workshops/mathematics-modern-cryptography. July 2015.

[28] D. Micciancio and O. Regev. "Worst-case to average-case reductions based on Gaussian measures". In: *FOCS 2004.* Vol. 37. SIAM J. Comput. 2004, pp. 372–381. DOI: 10.1137/S0097539705447360.

[29] NIST. *Post-Quantum Cryptography: Selected Algorithms 2022.* https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022. Dec. 2022.

[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. DOI: 10.3934/amc.2013.7.441.

[31] O. Ore. "Theory of Non-Commutative Polynomials". In: *Annals of Mathematics* 34.3 (1933), pp. 480–508. URL: www.jstor.org/stable/1968173.

[32] A. Pedrouzo-Ulloa, J. R. Troncoso-Pastoriza, and F. Pérez-González. "On Ideal Lattices over the Tensor Product of Number Fields and Ring Learning with Errors over Multivariate Rings". In: *CoRR* abs/1607.05244 (2016). eprint: 1607.05244. URL: http://arxiv.org/abs/1607.05244.

[33] S. Puchinger and A. Wachter-Zeh. "Fast operations on linearized polynomials and their applications in coding theory". In: *Journal of Symbolic Computation* 89 (2018), pp. 194–215. DOI: 10.1016/j.jsc.2017.11.012.

[34] S. Puchinger and A. Wachter-Zeh. "Sub-quadratic decoding of Gabidulin codes". In: *2016 IEEE International Symposium on Information Theory (ISIT)*. 2016, pp. 2554–2558. DOI: 10.1109/ISIT.2016.7541760.

[35] S. Pumplün. "How to obtain lattices from (f, σ, δ)-codes via a generalization of Construction A". In: *Appl. Algebra Eng. Commun. Comput.* 29 (2016), pp. 313–333. DOI: 10.1007/s00200-017-0344-9.

[36] S. Pumplün. "Finite nonassociative algebras obtained from skew polynomials and possible applications to $(f,\ \sigma,\ \delta)$-codes". In: *Adv. Math. Commun.* 11.3 (2017), pp. 615–634. DOI: 10.3934/amc.2017046.

[37] S. Pumplün. "Quotients of orders in algebras obtained from skew polynomials with applications to coding theory". In: *Communications in Algebra* 46.11 (2018), pp. 5053–5072. DOI: 10.1080/00927872.2018.1461882.

[38] S. Pumplün and T. Unger. "Space-time block codes from nonassociative division algebras". In: *Adv. Math. Commun.* 5.3 (2011), pp. 449–471. DOI: 10.3934/amc.2011.5.449.

[39] O. Regev. "On lattices, learning with errors, random linear codes, and cryptography". In: *J. of the ACM* 56 (6 2009). DOI: 10.1145/1568318.

[40] R. Schafer. *An Introduction to Nonassociative Algebras*. Benediction Classics, 2010. ISBN: 1849025908.

[41] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar. "Full-diversity, high-rate space-time block codes from division algebras". In: *IEEE Trans. Inf. Theory* 49.10 (2003), pp. 2596–2616. DOI: 10.1109/TIT.2003.817831.

[42] A. Steele. "Nonassociative cyclic algebras". In: *Israel Journal of Mathematics* 200 (June 2014). DOI: 10.1007/s11856-014-0021-7.

[43] A. Steele. "Some new classes of division algebras and potential applications to space-time block coding". PhD thesis. Univeristy of Nottingham, 2014. URL: https://eprints.nottingham.ac.uk/13934/.

[44] A. Steele, S. Pumplün, and F. Oggier. "MIDO space-time codes from associative and nonassociative cyclic algebras". In: *2012 IEEE Information Theory Workshop*. Sept. 2012, pp. 192–196. DOI: 10.1109/ITW.2012.6404655.

[45] Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. "Efficient Public Key Encryption Based on Ideal Lattices". In: *ASIACRYPT 2009*. Ed. by Mitsuru Matsui. Vol. 5912. LNCS. Springer, Heidelberg, Dec. 2009, pp. 617–635. DOI: 10.1007/978-3-642-10366-7_36.

[46] W. C. Waterhouse. “Nonassociative quarternion algebras”. In: *Algebras, Groups, Geometries* 4.3 (1987), pp. 365–378.