On the Security of Group Ring Learning with Errors

Andrew Mendelsohn[1], Charles Grover[2], and Cong Ling[1]

[1] Department of EEE, Imperial College London, United Kingdom.
andrew.mendelsohn18@imperial.ac.uk, c.ling@imperial.ac.uk
[2] Flare Network, UK.

Abstract. We propose a dimension-reducing transformation on Group Ring Learning with Errors (GRLWE) samples. We exhibit an efficiently computable isomorphism which takes samples defined over the group rings used in the construction of GRLWE to twice as many samples defined over matrix rings, in half the dimension. This is done by composing two maps: the first map is a transformation showing that the group rings used are orders in central simple algebras, and the second map takes the obtained central simple algebra to a matrix ring. When combined with lattice reduction on the resulting matrix samples, this gives an attack on the GRLWE problem. We extend this attack to other groups proposed for cryptographic use by the creators of GRLWE, and display some numerical results quantifying the effects of the transformation, using the 'Lattice Estimator'. We then give a family of groups from which GRLWE-style group rings can be constructed which are immune to our attack, namely the generalized quaternion groups. Finally, we discuss the merits and vulnerabilities of a number of different forms of structured LWE.

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

1 Introduction

The learning with errors (LWE) problem was introduced in [22], and has since become a central object of study in post-quantum cryptography. The problem is to solve systems of 'noisy' linear equations over the integers modulo some prime integer, and the problem can be extended to polynomial rings (RLWE [15], PLWE [25]) and free modules over such rings (MLWE) [12]. These variants on the original problem can in fact be interpreted as higher-dimensional versions of the original LWE problem: taking RLWE as an example, fixing a basis of the polynomial ring in question over $\mathbb{Z}$, samples from problems defined over such rings yield *structured* forms of plain LWE samples.

This line of thinking has motivated numerous and diverse structured LWE variants, including those which generalise MLWE. The importance of MLWE stems from its worst-case to average-case security reduction [12], its greater efficiency than LWE due to its structure, its (conjectured) greater security than

RLWE, and its presence in the standardization process for post-quantum cryptography run by the USA's National Institute of Standards and Technology (NIST). Out of the seven third-round schemes which survived two previous rounds of scrutiny, three (Saber [8], Crystals-Kyber [2], Crystals-Dilithium [9]) were based off LWE-style problems over modules (Saber uses Module Learning with Rounding, the other two MLWE), and Kyber and Dilithium were ultimately selected for standardisation. Thus MLWE has a central place in the landscape of lattice cryptography. Moreover there is a growing body of work exploiting the algebraic structure of the underlying ideal lattice problems RLWE uses to ground its security [7], [17], [21]. In contrast, the higher-rank problems underlying MLWE have so far been unaffected by these lines of attack.

While MLWE is now well-established, the NIST process marks the beginning, not the end, of a paradigm shift to post-quantum cryptography. New variants of LWE beyond RLWE and MLWE warrant further investigation. A branch of this study of particular relevance for this work is that of MLWE variants which have additional algebraic structure. This has often taken the form of algebraic structures which both have a matrix representation over $\mathbb{Z}$ which yields MLWE-style samples, which permits the authors of such works to claim a comparable level of security for their cryptographic schemes as MLWE, and also have a multiplication operation which can be exploited for gains in computational cost over MLWE (comparable to RLWE). These variants also permit the use of longer error correction codes, naturally leading to lower decryption failure rates, a vital consideration for thwarting CCA attacks. The hypothetical advantages of algebraically-structured schemes combining the best of MLWE and RLWE have resulted in a number of proposals of such schemes, which we detail below.

The first such structured MLWE variant was introduced in [18], in which structured LWE samples were defined over the tensor product of number fields, and dubbed 'm-RLWE'. This was subjected to a dimension-reducing attack in [4]. Further discussion of m-RLWE can be found in [19].

A second structured variant was introduced in [6], called group ring LWE (GRLWE). In that work, LWE was defined for elements taken from group rings, where the ring is commutative and the group is dihedral. If interpreted as a generalisation of MLWE via a matrix representation, one GRLWE sample can be seen to be equivalent to two MLWE samples. The authors gave a reduction from lattice problems defined over one-sided group ring ideals to a decision LWE problem, and a PKE scheme. A recent follow-up work [14] provides improved security reductions for the GRLWE problem, and extends them to hold for semidirect product groups.

The final relevant structured form of LWE for this work is LWE instantiated in cyclic division algebras (CDAs) [10], referred to as 'CLWE'. In that work, search and decision problems for LWE in CDAs were defined, and security proofs linking the search and decision problems with basic lattice problems given, for certain parameters. This work is immune from the dimension-reducing attack that targeted m-RLWE.

The primary subject of this paper is GRLWE and its security.

1.1 Our Results

The main result of this paper is a dimension-reducing transformation on the GRLWE problem. We show that samples from GRLWE can be invertibly mapped to samples from certain cyclic algebras - though importantly not from CDAs for which the security reductions for CLWE hold. The insecurity of LWE in these algebras allows us to apply a second (invertible) map, which outputs twice the number of samples inputted while halving their dimension. Thus, we can take a GRLWE sample, apply the composition of the two maps, obtain LWE samples in half the original dimension, run lattice attacks on these samples, then invert the mapping to solve the original GRLWE problem.

We then ask whether our method applies to a family of group rings proposed by the authors of [6], and answer affirmatively (subject to a condition on the choice of basis of a pair of number fields). That is, the dimension-reducing transformation applies to a larger *family* of group rings, not just the specific choice originally proposed.

A natural question to ask following these results might be: to what extent is GRLWE dependent on the choice of group over which we instantiate it? We begin to answer this question by identifying the generalised quaternion groups as a family of groups for which the resulting group rings yield GRLWE instances against which our attack fails.

The cryptanalysis developed in this work improves our understanding of structured MLWE variants, which so far have all been defined using particular cases of cyclic algebras over number fields. These variants are of interest both insofar as they spur on cryptographic research relevant to widely-adopted standardised cryptographic schemes, and in their wider cryptographic importance as developments of MLWE. We close with a discussion and comparison of existing structured MLWE variants.

Overview In more detail, the group rings considered are quotients of group rings of the form

$$\mathbb{Z}[D_{2n}] = \left\{ \sum_{g \in D_{2n}} a_g g : a_g \in \mathbb{Z} \right\}$$

by the ideal $(\mathfrak{r}^{n/2}+1)\mathbb{Z}[D_{2n}]$, for power-of-two n and dihedral group defined

$$D_{2n} = \langle \mathfrak{r}, \mathfrak{s} : \mathfrak{r}^n = \mathfrak{e}, \mathfrak{s}^2 = \mathfrak{e}, \mathfrak{s}\mathfrak{r}\mathfrak{s} = \mathfrak{r}^{-1} \rangle$$

with identity element $\mathfrak{e}$. In particular, the quotients have the form

$$R := \mathbb{Z}[D_{2n}]/(\mathfrak{r}^{n/2}+1)\mathbb{Z}[D_{2n}]$$

A GRLWE sample then looks like $(a, a \cdot s + e \bmod q) \in R/qR \times R/qR$. We first prove (Lemma 2) that R can be considered an order Λ in some cyclic algebra $\mathcal{A}$ over a number field K. We note that these algebras are quaternion algebras.

We exploit this structure using a lemma of Reiner, which gives a criterion for

a cyclic algebra to be isomorphic to a matrix ring (Lemma 1) - and this criterion is fulfilled by $\mathcal{A}$. Composing the two isomorphisms thus provides an isomorphism from $\mathcal{A} \cong M_2(K)$.

We next consider the restriction of this isomorphism to R. In particular, since the GRLWE samples are defined over $R_q := R \bmod qR$, we consider the map modulo q from Λ_q to $M_2(\mathcal{O}_{K_q})$, where $\Lambda_q := \Lambda/q\Lambda$. We prove that when q is a prime unramified in the maximal subfield of $\mathcal{A}$, then the map $\Lambda_q \to M_2(\mathcal{O}_{K_q})$ is a bijection (Theorem 3).

We then propose the following attack on GRLWE: take a sample $(a, b) = (a, as+e) \in R_q \times R_q$ and transform it as above to obtain $(A, B) = (A, AS+E) \in M_2(\mathcal{O}_{K_q}) \times M_2(\mathcal{O}_{K_q})$. We show that the first column of the error E is small and so (A, B_1) yields a valid MLWE sample over K, where B_i is the ith column of B. Note that the transform outputs twice as many samples as we started with, in half the dimension of the original samples. Since the hardness of LWE appears to be superlinear in the dimension, running an off-the-shelf lattice attack on the sample (A, B_1) has higher likelihood of obtaining information about S than running such attacks on (a, b), if the size of the error stays (approximately) constant.

Solving (A, B_1) for S_1 does not recover the whole of S, but merely its first column. We surmount this by multiplying a by a primitive nth root of unity ζ_n and show that the image of $(a \cdot \zeta_n, b)$ is a well-defined MLWE instance with secret the image of $\zeta_n^{-1} \cdot s$, which has first column containing the missing coefficients of S. Since the first column of E is small, we may also solve the instance obtained from the image of $(a \cdot \zeta_n, B_1)$ and thus obtain the entire secret matrix S. In both cases, we may invert the transformation, since it is an isomorphism, and piece together the results to obtain the original secret s. Letting $\mathcal{D}_{\Lambda,\alpha}$ denote a discrete Gaussian over Λ of parameter α, our main theorem is

Theorem 4 (informal). *Let $n \geq 2$ be a power of 2 and $\alpha > 0$. Let $L = \mathbb{Q}(\zeta_n)$ be the nth cyclotomic field, $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, $R := \mathbb{Z}[D_{2n}]/\left(\mathfrak{r}^n + 1\right)\mathbb{Z}[D_{2n}]$ and $R_q := \mathbb{Z}[D_{2n}]/\left(\mathfrak{r}^n + 1, q\right)\mathbb{Z}[D_{2n}]$. Let $q \geq 3$ be a prime completely split in $\mathcal{O}_L$ and $s \in R_q$. Then GRLWE over R_q with secret s and error sampled from $\mathcal{D}_{\Lambda,\alpha}$ reduces to solving two MLWE instances over $\mathcal{O}_K$ of rank 2, with modulus q, error sampled from $\mathcal{D}_{\Lambda,\sqrt{2}\alpha}$, and secrets s_i, where $s_1 = \varphi(\zeta_n^{-1} \cdot s)_1$ and $s_2 = \varphi(s)_1$.*

We emphasise that our invertible transformation halves the dimension of the lattice problems it suffices to solve in order to recover the GRLWE secret.

We also show that this attack holds for a proposed generalisation of the GRLWE problem stated in [6]; our attack thus applies to a subset of the group rings considered in the follow-up work [14]. The authors pointed out further group rings for which GRLWE could be defined using groups constructed as follows: let H be a group acting on $\mathbb{Z}/n\mathbb{Z}$. If $|H| = m$ and n a power of two, then $m \mid n/2$ so m is a power of two, and we can define

$$G = \langle \mathfrak{r}, \mathfrak{s} : \mathfrak{r}^n = \mathfrak{e}, \mathfrak{s}^m = \mathfrak{e}, \mathfrak{s}\mathfrak{r}\mathfrak{s}^{-1} = \mathfrak{r}^k \rangle,$$

where $\gcd(k, n) = 1$ and $k^m \equiv 1 \bmod n$; this is a generalised dihedral group. However, our methods also apply to these scenarios: if $R' = \mathbb{Z}[G]/(\mathfrak{r}^{n/2} + 1)\mathbb{Z}[G]$

we show that R' is an order of a cyclic algebra $\mathcal{A}'$ and we obtain a map $R' \to M_m(K)$ for $m \geq 2$ such that $m \mid \frac{n}{2}$. In particular, we prove that $R'_q \to M_m(\mathcal{O}_{K_q})$ is a bijection, subject to a mild condition (Theorem 5). We can then extend our attack to this family of group rings.

We give a table of results using the estimator from [1], demonstrating the approximate loss in security before and after applying our dimension-reducing transformation.

We then proceed to create an integral group ring which appears to be immune to our attack, using the generalized quaternion group, Q_{4n}. We show (Proposition 3) that integral group rings over Q_{4n} of the form $\mathbb{Z}[Q_{4n}]/(\mathfrak{r}^n + 1)\mathbb{Z}[Q_{4n}])$ are in fact isomorphic to natural orders of cyclic *division* algebras (for which CLWE appears hard), and thus our attack fails on them. It is this 'division' property which frustrates our attack - in particular, these CDAs do not satisfy the criterion of the lemma of Reiner mentioned above, so our method, applied to these rings, fails at the second step.

These group rings, rather than integral dihedral group rings, appear to provide a more appropriate platform for the use of GRLWE in cryptography since our attack does not apply. We further observe that if one applies the canonical embedding to the image of samples from $\mathbb{Z}[Q_{4n}]/(\mathfrak{r}^n + 1)\mathbb{Z}[Q_{4n}])$, rather than using a coefficient embedding, then the reduction from SIVP to search CLWE applies and a security guarantee for the search problem is obtained. We discuss this further in Section 6, and give some details in the appendices. However, we have not attempted to give a full security proof for decision GRLWE instantiated with Q_{4n}, nor carried out further analysis, and so make no further claims of its security beyond these comments.

The algebras obtained in Proposition 3 are again quaternion algebras, similarly to when $G = D_{2n}$. These quaternion algebras may permit more efficient algorithms for multiplication than the ones used in [10], since their maximal subfield is cyclotomic, whereas those in [10] were finite extensions of cyclotomic fields. We note that one may use the vocabulary of split and non-split quaternion algebras to understand when our attack may succeed (or not), but we do not pursue this link in the current paper.

Finally, we connect the three structured MLWE problems, discussing the attack of [4] on m-RLWE, our attack on GRLWE, and the connection to CLWE.

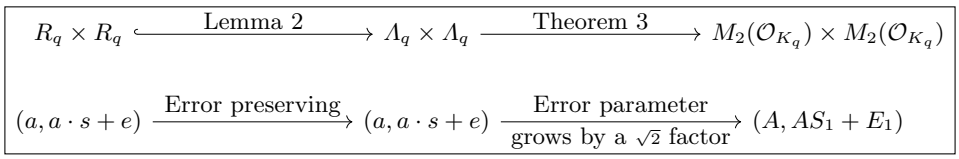

Fig. 1: Transforming a GRLWE sample to an MLWE sample

2 Preliminaries

2.1 Lattices

An n-dimensional lattice is a discrete additive subgroup of $\mathbb{R}^n$. A lattice $\mathcal{L}$ may be given as the set of integer linear combinations of a set of linearly independent vectors $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_k\}$, for some $k \leq n$, written $\mathcal{L}(B) = \left\{\sum_{i=1}^{k} z_i \mathbf{b}_i : z_i \in \mathbb{Z}\right\}$. All lattices below have $k = n$.

The above can be generalised to vector spaces over fields. Let V be a finite-dimensional vector space over a field K and R a discrete subring of K. An *R-lattice* $L \subset V$ is a subspace such that L is a finitely-generated R-module. A lattice L is *full* if it contains a K-basis of V, which implies $V = K \cdot L$. Fixing a basis B of V, the R-linear span of B is a full-rank lattice. We will primarily be interested in the case $V = \mathbb{R}^n$.

Definition 1. *Let $\mathcal{L}$ be a full-rank 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 $\mathcal{L}$.*

The geometry induced by an inner product can be used to define computationally intractable problems on lattices, such as finding the shortest vector in the lattice (SVP), finding the closest vector to a given point (CVP), deciding whether the shortest vector has size less than one or greater than a parameter β (GapSVP), or outputting n independent sufficiently short vectors (SIVP), when one knows only a certain basis of the lattice. For well-chosen parameters these problems are intractable, and have been used to ground the security of certain quantum-resistant cryptographic schemes, such as LWE, discussed below.

2.2 Discrete Gaussians

Equip $\mathbb{R}^n$ with the Euclidean norm $\|\cdot\|_2 = \|\cdot\|$, and let $\mathbf{a} \in \mathbb{R}^n$ and $r > 0$. We define the *Gaussian function* $\rho_{r,\mathbf{a}}$

$$\rho_{r,\mathbf{a}} : \mathbb{R}^n \to (0, 1], \quad \boldsymbol{x} \mapsto \exp\left(-\pi \|\boldsymbol{x} - \mathbf{a}\| / r^2\right)$$

The Gaussian distribution $\mathcal{D}_r$ is defined as having probability density function equal to $\frac{1}{r}\rho_{r,0}$.

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

Let $\mathcal{L}$ be a lattice and define $\rho_r(\mathcal{L}) := \sum_{\mathbf{x} \in \mathcal{L}} \rho_r(\mathbf{x})$. Then the *discrete* Gaussian distribution $\mathcal{D}_{\mathcal{L},r}$ outputs $\mathbf{x} \in \mathcal{L}$ with probability $\frac{\rho_r(\mathbf{x})}{\rho_r(\mathcal{L})}$, for each $\mathbf{x} \in \mathcal{L}$.

We will need a result on summing discrete Gaussians.

Theorem 1. *[3, Theorem 4.13] Let $\Lambda \subseteq \mathbb{Z}^m$ be a full rank lattice and $\sigma \in \mathbb{R}$. For $i = 1, \ldots, k$ let $\mathbf{t}_i \in \mathbb{Z}^m$ and let X_i be mutually independent random variables sampled from $\mathcal{D}_{\Lambda + \mathbf{t}_i, \sigma}$. Let $\mathbf{c} = (c_1, \ldots, c_k) \in \mathbb{Z}^k$, and define*

$$g := \gcd(c_1, \ldots, c_k), \quad \mathbf{t} := \sum_{i=1}^{k} c_i \mathbf{t}_i.$$

Suppose that $\sigma > \|\mathbf{c}\| \cdot \eta_\epsilon(\Lambda)$ *for some negligible* ϵ. *Then* $Z = \sum_{i=1}^{k} c_i X_i$ *is statistically close to* $\mathcal{D}_{g\Lambda+\mathbf{t},\|\mathbf{c}\|\sigma}$.

2.3 Structured LWE

In its simplest form, the LWE distribution can be stated as follows: for a secret $s \in \mathbb{Z}_q^n$, sample a vector $a \leftarrow \mathbb{Z}_q^n$ uniformly at random and noise $e \leftarrow \chi$, where χ is some error distribution over $\mathbb{Z}_q$, and output $(a, \langle a, s\rangle + e)$. The search LWE problem is then to find s, given a collection of such samples. We can view such a collection of samples in terms of matrices, obtaining a sample of the form $(A, As + e)$, where A has columns a_i and e is now an error vector.

Now consider Ring LWE. In this problem, we sample elements not over the integers, but from a polynomial ring instead. Let $R = \mathbb{Z}[x]/f(x)$ be a polynomial ring, and $R_q = R/qR$ for some integer modulus q. For $s \in R_q$, sample $a \leftarrow U(R_q)$ uniformly at random, sample $e \leftarrow \chi$, and output $(a, a \cdot s + e) \in R_q \times R_q$. In the case when $f(x) = x^n + 1$ with n a power of two, fixing a basis of R over $\mathbb{Z}$, we can write multiplication by ring elements in terms of matrix-vector multiplication, obtaining

$$\Phi(a)\mathbf{s} + \mathbf{e},$$

where $\mathbf{s}$ is the vector of coefficients of s, similarly for $\mathbf{e}$, and

$$\Phi(a) = \begin{pmatrix} a_0 & -a_{n-1} & \dots & -a_1 \\ a_1 & a_0 & \dots & -a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & \dots & a_0 \end{pmatrix}.$$

This has the form of an LWE instance with n samples, except the columns are not independently distributed. However, this dependency has not yet been used to solve RLWE.

We can extend this reasoning to the module case, as follows: let $s \in R_q^m$ for some integer m, sample a uniformly at random from R_q^m and $e \leftarrow \chi$ for χ some error distribution over R_q. Then output $(a, \langle a, s\rangle + e) \in R_q^m \times R_q$. One can write a collection of m such samples as $(A, A \cdot s + e)$, where now A is an $m \times m$ matrix with entries in R_q and e is a vector. Thus we have a problem over R_q, which we could extend to a problem over $\mathbb{Z}_q$ if we expand each multiplication of ring elements in the way done above for RLWE. This would result in A being an $mn \times mn$ matrix with integer entries. In this way, it is seen that MLWE is also a structured form of LWE. We now formally define MLWE.

Definition 2. *(MLWE distribution) Let* $d \geq 1$, $K/\mathbb{Q}$ *be an algebraic number field of dimension* $[K : \mathbb{Q}] = n$ *and maximal order* $\mathcal{O}_K$, *and* $\mathcal{O}_{K_q} = \mathcal{O}_K/q\mathcal{O}_K$. *For an error distribution* ψ *over* $K_\mathbb{R} := K \otimes \mathbb{R}$, *an integer modulus* $q \geq 2$, *and a secret* $s \in \left(\mathcal{O}_{K_q}^\vee\right)^d$, *a sample from the MLWE distribution* $\Pi_{n,q,s,\psi,d}^M$ *is obtained by sampling* $a \leftarrow \mathcal{O}_{K_q}^d$ *uniformly at random,* $e \leftarrow \psi$, *and outputting* $(a, b) = \left(a, \frac{1}{q}\langle a, s\rangle + e \bmod \mathcal{O}_K^\vee\right) \in \mathcal{O}_{K_q}^d \times K_\mathbb{R}/\mathcal{O}_K^\vee$.

We can now define computational problems from the MLWE distribution. Let Ψ be a family of error distributions over $K_{\mathbb{R}}$.

Definition 3. *(Search MLWE). The search MLWE problem is to find the secret* $s \in \left(\mathcal{O}_{K_q}^{\vee}\right)^d$*, given a collection of samples* $(a_i, b_i) \leftarrow \Pi_{n,q,s,\psi,d}^{M}$*,* $i = 1, ..., m$*, for arbitrary* $s \in \left(\mathcal{O}_{K_q}^{\vee}\right)^d$ *and* $\psi \in \Psi$*.*

We let $\text{MLWE}_{n,q,s,\psi,d,m}$ denote the search problem obtained upon sampling m samples from $\Pi_{n,q,s,\psi,d}^{M}$.

Definition 4. *(Decision MLWE). The decision MLWE problem is to distinguish, with non-negligible advantage, whether a collection of independent samples is taken from the MLWE distribution* $\Pi_{n,q,s,\psi,d}^{M}$ *or is taken uniformly at random over* $\mathcal{O}_{K_q}^{d} \times K_{\mathbb{R}}/\mathcal{O}_K^{\vee}$*.*

We use the same notation as above for the setting when $s \in \mathcal{O}_{K_q}^{d}$ and when our errors are discrete, sampled from discrete Gaussian distributions; context will make plain the setting in which we are working.

2.4 Group Rings

Basic Definitions Let G be a finite group of cardinality n, and S a commutative ring. Then we define the group ring $S[G]$ as

$$S[G] = \left\{ \sum_{i=1}^{n} s_i g_i : s_i \in S, g_i \in G \right\}.$$

This becomes a ring by defining addition and multiplication by

$$\sum_{i=1}^{n} a_i g_i + \sum_{i=1}^{n} b_i g_i = \sum_{i=1}^{n} (a_i + b_i)\, g_i,$$

$$\left(\sum_{i=1}^{n} a_i g_i \right) \left(\sum_{i=1}^{n} b_i g_i \right) = \sum_{l=1}^{n} \left(\sum_{i,j \,:\, g_i g_j = g_l} a_i b_j \right) g_l$$

When $S = \mathbb{Z}$ one can embed $\mathbb{Z}[G] \hookrightarrow \mathbb{R}^n$, under which one-sided ideals yield Euclidean lattices. The authors of [6] use the coefficient embedding and $G = D_{2n}$, the nth dihedral group, for n a power of two; in the following, we will also set n to be be a power of two. For any group ring element $x \in S[G]$, multiplication by x on a fixed basis defines a linear transformation $\Phi(x)$, which is called the regular representation of $S[G]$.

Dihedral Group Rings The dihedral group of order $2n$, denoted by D_{2n}, has cardinality $2n$ and the presentation

$$D_{2n} = \langle \mathfrak{r}, \mathfrak{s} : \mathfrak{r}^n = \mathfrak{e}, \mathfrak{s}^2 = \mathfrak{e}, \mathfrak{s}\mathfrak{r}\mathfrak{s} = \mathfrak{r}^{-1} \rangle.$$

The group ring used in GRLWE [6] is the quotient of a dihedral group ring,

$$R = \mathbb{Z}\left[D_{2n}\right] / \left(\mathfrak{r}^{n/2} + 1\right) \mathbb{Z}\left[D_{2n}\right].$$

Note in R that $\mathfrak{e} \in D_{2n}$ becomes identified with $1 \in \mathbb{Z}$. We now show that GRLWE samples in the above group ring yield structured LWE samples. Let $a, s,$ and $e \in R$. We can write these elements as degree 1 polynomials in $\mathfrak{s}$ with coefficients being polynomials in $\mathfrak{r}$, for example $a = a_0(\mathfrak{r}) + \mathfrak{s} \cdot a_1(\mathfrak{r})$. If we consider multiplication by a on $\{1, \mathfrak{s}\}$, we have $a \cdot 1 = a$ and $a \cdot \mathfrak{s} = a_0(\mathfrak{r})\mathfrak{s} + \mathfrak{s}a_1(\mathfrak{r})\mathfrak{s} = \overline{a}_1(\mathfrak{r}) + \mathfrak{s}\overline{a}_0(\mathfrak{r})$, where $\bar{\cdot}$ denotes conjugation by $\mathfrak{s}$. Thus we can write $b = a \cdot s + e = A\mathbf{s} + \mathbf{e}$, where

$$A = \begin{pmatrix} a_0(\mathfrak{r}) & \overline{a}_1(\mathfrak{r}) \\ a_1(\mathfrak{r}) & \overline{a}_0(\mathfrak{r}) \end{pmatrix}$$

and $\mathbf{s}$ and $\mathbf{e}$ are the vectors of coefficients of s and e respectively. The $a_i(\mathfrak{r})$ and $\overline{a}_i(\mathfrak{r})$ are elements of the polynomial ring $\mathbb{Z}[\mathfrak{r}]/(\mathfrak{r}^{n/2} + 1)$, which when n is a power of two is exactly the kind of ring used for RLWE. Thus, expanding the entries of b over the integers as done above, we obtain structured LWE samples. Moreover, one can see from the above matrix A that one GRLWE sample yields structured MLWE samples over a rank 2 module.

2.5 Group Ring LWE

Here we define the GRLWE problem(s). As in the previous section, let n be a power of two, and

$$R = \mathbb{Z}\left[D_{2n}\right] / \left(\mathfrak{r}^{n/2} + 1\right) \mathbb{Z}\left[D_{2n}\right].$$

Set

$$R_{\mathbb{R}} = R \otimes_{\mathbb{Z}} \mathbb{R}$$

and let $\mathbb{T} = R_{\mathbb{R}}/R$. Let q be an odd prime. Define

$$R_q = \mathbb{Z}\left[D_{2n}\right] / \left(q, \left(\mathfrak{r}^{n/2} + 1\right) \mathbb{Z}\left[D_{2n}\right]\right) = \mathbb{F}_q\left[D_{2n}\right] / \left(\left(\mathfrak{r}^{n/2} + 1\right) \mathbb{F}_q\left[D_{2n}\right]\right)$$

Let Σ_α be the set of Gaussian distributions on $\mathbb{R}^n$ with Gaussian marginal distributions with parameters $r_{i,j} \leq \alpha$, for all $(i, j) \in \{1, ..., n\}^2$.

Definition 5. *(GRLWE distribution) Let R_q be the ring defined above. For an error distribution ψ over $\mathbb{T}$, an integer modulus $q \geq 2$, and a secret $s \in R_q$, a sample from the GRLWE distribution $\Pi^G_{n,q,s,\psi}$ is obtained by sampling $a \leftarrow R_q$ uniformly at random, $e \leftarrow \psi$, and outputting $(a, b) = (a, (a \cdot s)/q + e \bmod R) \in R_q \times \mathbb{T}$.*

From this distribution we define search and decision problems:

Definition 6. *(Search GRLWE). The search GRLWE problem is to find the secret $s \in R_q$, given a collection of samples $(a_i, b_i) \in R_q \times \mathbb{T}$ taken from $\Pi^G_{n,q,s,\psi}$, for arbitrary $s \in R_q$ and $\psi \in \Sigma_\alpha$.*

Definition 7. *(Decision GRLWE). The decision GRLWE problem is to distinguish, with non-negligible advantage, whether a collection of independent samples is taken from the GRLWE distribution $\Pi^G_{n,q,s,\psi}$ or is taken uniformly at random over $R_q \times \mathbb{T}$.*

These problems can also be defined for discretized errors, in which case a sample has the form $(a, as + e) \in R_q \times R_q$. For clarity of exposition we will work with this form of GRLWE.

Public Key Encryption Scheme The authors of [6] then connected these problems to cryptography, giving a PKE scheme, which runs as follows:

Key Generation: Set $sk := (s, e) \in R_q^2$, with s, e both sampled from the error distribution ψ. Sample $a \leftarrow R_q$ uniformly at random, and set $pk := (a, b) = (a, as/q + e) \in R_q^2$.

Encryption: To encrypt $m \in \{0, 1\}^n$, the authors view the bits of m as coefficients of a polynomial. Then the ciphertext (u, v) is defined

$$(u, v) := (ar/q + e_1, br + e_2 + \lfloor q/2 \rfloor m).$$

where r, e_1, e_2 are sampled from ψ.

Decryption: To decrypt (u, v), compute $v - su$, to obtain

$$v - su = br + e_2 + \lfloor q/2 \rfloor m - s(ar/q + e_1) = (er - se_1 + e_2) + \lfloor q/2 \rfloor m.$$

If $er - se_1 + e_2$ has small coefficients, one can round to obtain m.

2.6 Cyclic Algebras

Let L/K be a degree d extension of number fields with cyclic Galois group. This means that the automorphisms of L which fix every element of K form a group which is generated by a single element - denote this element of the Galois group by θ. Consider the following direct sum:

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

where u is an auxiliary element satisfying the properties $1)$ $u^d = \gamma$, where $\gamma \in K$, and $2)$ for all $x \in L$, we have $xu = u\theta(x)$. The direct sum is a unital algebra, and property $2)$ yields a non-commutative multiplication operation. To illustrate the

multiplication of elements of a cyclic algebra, suppose $d = 2$, $y = y_0 + uy_1$, and $z = z_0 + uz_1 \in \mathcal{A}$. Then

$$y \cdot z = (y_0 + uy_1)(z_0 + uz_1) = y_0 z_0 + \gamma\theta(y_1)z_1 + u\left(y_1 z_0 + \theta(y_0)z_1\right)$$

A cyclic algebra over a number field K is a central simple algebra over K: here the center Z of an algebra is the set of elements which commute with all other algebra elements, that is $Z(\mathcal{A}) := \{x \in \mathcal{A} : xy = yx \text{ for all } y \in \mathcal{A}\}$. We then say a K-algebra $\mathcal{A}$ is central if $Z(\mathcal{A}) = K$. We say an algebra is simple if it has no nontrivial two-sided ideals. A (not necessarily commutative) ring is called a division ring if every non-zero element has a multiplicative inverse; one can ensure every element of $\mathcal{A}$ has a multiplicative inverse by requiring that γ is a *non-norm* element:

Definition 8. *Let $N_{L/K}(\cdot)$ denote the field norm from L to K. An element α of K satisfies the non-norm condition if there does not exist an element $x \in L$ such that $\alpha^i = N_{L/K}(x)$, for any $0 < i < [L : K]$.*

Then there is the following result:

Proposition 1. *[20] The algebra $\mathcal{A}$ is a division algebra if and only if γ is a non-norm element.*

Then with non-norm element γ, $\mathcal{A}$ is called a *cyclic division algebra* (CDA). We denote this algebra by $\mathcal{A} = (L/K, \theta, \gamma)$ and restrict to the case when $\gamma \in \mathcal{O}_K$.

Cyclic algebras contain subrings called *orders*. These are defined as subrings which are also full-rank lattices. A *maximal* order in $\mathcal{A}$ is an order not properly contained within any other order of the algebra, and such orders have convenient ideal structures. For example, when $[L : K] = 1$, we have $\mathcal{A} = K$ and the maximal order is the ring of integers $\mathcal{O}_K$, fractional ideals of which form an abelian group, and uniquely factor into products of prime ideals. Such properties hold for maximal orders in CDAs for $[L : K] > 1$ also. A useful algebra order is the *natural order*, denoted Λ, defined

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

Whether or not this order is maximal depends on the construction of the algebra $\mathcal{A}$ within which it lies.

If we fix the basis $\{u^i\}_{i \geq 0}$ of $\mathcal{A}$ over L, left multiplication by an element $a = a_0 + ua_1 + ... + u^{d-1}a_{d-1} \in \mathcal{A} = (L/K, \theta, \gamma)$ can be represented as a matrix $\Phi(a) \in M_d(L)$ as follows:

$$\Phi(a) = \begin{pmatrix} a_0 & \gamma\theta\left(a_{d-1}\right) & \gamma\theta^2\left(a_{d-2}\right) & \cdots & \gamma\theta^{d-1}\left(a_1\right) \\ a_1 & \theta\left(a_0\right) & \gamma\theta^2\left(a_{d-1}\right) & \cdots & \gamma\theta^{d-1}\left(a_2\right) \\ a_2 & \theta\left(a_1\right) & \theta^2\left(a_0\right) & \cdots & \gamma\theta^{d-1}\left(a_3\right) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{d-1} & \theta\left(a_{d-2}\right) & \theta^2\left(a_{d-3}\right) & \cdots & \theta^{d-1}\left(a_0\right) \end{pmatrix}.$$

We define the *dual* (or *codifferent* ideal) of Λ to be

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

where $Tr(a) := T_{K/\mathbb{Q}}(tr(\Phi(a)))$, $T_{K/\mathbb{Q}}(\cdot)$ is the field trace, and $tr(\cdot)$ is the matrix trace. The trace $Tr(\cdot)$ is symmetric.

2.7 CLWE

In [10], the Learning with Errors (LWE) problem was instantiated using the natural order inside a CDA. To do this, the following distribution was defined, where $L_\mathbb{R} = L \otimes_\mathbb{Q} \mathbb{R}$:

Definition 9 (The CLWE Distribution). *Let L/K be a Galois extension of number fields of dimension $[L : K] = d$, $[K : \mathbb{Q}] = n$, with cyclic Galois group generated by θ. Let $\mathcal{A} := (L/K, \theta, \gamma)$ be 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 $\Lambda_q = \Lambda/q\Lambda$. 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 $(a, b) = (a, (a \cdot s)/q + e \bmod \Lambda^\vee) \in \Lambda_q \times \left(\oplus_{i=0}^{d-1} u^i L_\mathbb{R}\right)/\Lambda^\vee$.*

If we take a CLWE sample as above and consider $(a \cdot s)/q + e$ in matrix form, we obtain $\frac{1}{q}\Phi(a)\mathbf{s} + \mathbf{e}$. Then each column of $\Phi(a)$ corresponds to an MLWE instance over L^d with secret $\mathbf{s}$. Interpreting MLWE instances as structured LWE instances, we see that CLWE also gives a structured form of LWE.

As with GRLWE, we can consider instances with discretized error by taking instances $(a, a \cdot s + e) \in \Lambda_q \times \Lambda_q$. From the above distribution, a search problem and a decision problem can be defined:

Definition 10. *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 11. *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.*

Security reductions from SIVP to the search CLWE problem, and from the search CLWE problem to the decision CLWE problem, were given in [10]. Here the particular SIVP variant is as follows (where ideals are embedded into $\mathbb{R}^{nd^2}$ under the canonical embedding):

Definition 12. *Let $\mathcal{A}$ be a CDA, $\mathcal{I} \subset \Lambda$ be an ideal, and $\xi \geq 1$. The approximate Shortest Independent Vectors Problem, $\mathcal{A}$-$SIVP_\xi$ is to find n linearly independent non-zero vectors $x_1, \ldots, x_n$ such that $\max_i(\|x_i\|) \leq \xi \cdot \lambda_n(\mathcal{I})$.*

We write $|x| = 1$ for $x \in K$ if the complex absolute value of every field embedding of K applied to x equals 1. It was then shown that

Theorem 2. *[10, 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 reduction from search CLWE to DCLWE for a (exponentially large) subset of possible secrets was also given.

3 Attacking Non-division Cyclic Algebras

In this section we explain how cyclic algebras which are not division algebras are open to an attack which converts a larger-dimensional CLWE sample into multiple lower-dimensional CLWE samples, which are easier to solve. Whether a cyclic algebra is division or not depends on the choice of γ: recall from Proposition 1 that a cyclic algebra is division if and only if γ^i is not in the image of the norm, for $i = 1, ..., d-1$. This condition, that γ is a non-norm element of L/K, is required in order to stop parallelizing attacks applying to the CLWE problem. We will later see that the group rings used in GRLWE are isomorphic to cyclic algebras with $\gamma = 1$; a choice of γ which is insecure.

3.1 An Isomorphism from Non-division Algebras to Easy Algebras

As stated above, to create a division algebra γ is chosen so that γ^i is not in the norm group of L into K for $i = 1, 2, \ldots, d-1$. Here, we demonstrate that picking γ that violates this condition leads to vulnerable instances of the CLWE problem. We need the following lemma, a rephrasing of [23, Theorem 30.4].

Lemma 1. *Let $\mathcal{A} = (L/K, \theta, \gamma)$ be a cyclic algebra with $[L : K] = d$. Let $\gamma, \delta \in K \setminus \{0\}$. Then*

1. *$\mathcal{A} \cong \mathcal{A}_i := \left(L/K, \theta^i, \gamma^i\right)$ for each i such that $\gcd(i, d) = 1$.*
2. *If $\gamma = 1$ then $\mathcal{A} \cong M_d(K)$.*
3. *If $\delta = N_{L/K}(\beta)\gamma$ for some non-zero $\beta \in L$ then $\mathcal{A} \cong \mathcal{A}' := (L/K, \theta, \delta)$.*

Armed with this lemma, we demonstrate potential weaknesses of choosing γ poorly. Let $\mathcal{A} = (L/K, \theta, \gamma)$ be a cyclic algebra where $\gamma \in \mathcal{O}_K$ violates the non-norm condition, and suppose γ lies in the norm group $N_{L/K}\left(L^\times\right)$. Consider the CLWE instance $(a, a \cdot s + e) \in \Lambda_q \times \Lambda_q$, where a, s are uniform and $e \leftarrow \chi$ is drawn from an error distribution which is of Gaussian shape. Applying the above lemma transforms our sample into one over $M_d\left(\mathcal{O}_{Kq}\right) \times M_d\left(\mathcal{O}_{Kq}\right)$. That is, we construct a sample in the form

$$(\mathbf{A}, \mathbf{A} \cdot \mathbf{S} + \mathbf{E})$$

where $\mathbf{A}, \mathbf{S}, \mathbf{E} \in M_d(\mathcal{O}_{Kq})$. Assume for the time being that the homomorphisms are smallness preserving, so that if e is a small element of Λ_q then the corresponding matrix $\mathbf{E}$ will have entries that are small elements of $\mathcal{O}_K$.

Let $\mathbf{s}_i, \mathbf{e}_i$ denote the ith columns of $\mathbf{S}$ and $\mathbf{E}$ respectively. Then, for each i the pair $(\mathbf{A}, \mathbf{A}\mathbf{s}_i + \mathbf{e}_i)$ constitutes d samples from the MLWE distribution in dimension n and rank d. That is, the single CLWE sample provides a collection of d samples from d instances of the MLWE distribution with different secrets $\mathbf{s}_1, \ldots, \mathbf{s}_d$, where each set of samples shares the same uniformly random matrix $\mathbf{A}$. Since the difficulty of LWE problems is assumed to be superlinear in dimension N, solving d instances of the MLWE problem in dimension n and module rank d is easier than solving a single instance in dimension nd and rank d, the targeted dimension of our CLWE problem, which is essentially the parallelizing argument of the attack of [4] on multivariate RLWE [18] discussed below. Furthermore, the matrix $\mathbf{A}$ being common to each set of samples potentially weakens the resulting MLWE instances. Thus, assuming that $\mathbf{e}_i$ is suitably distributed, it is clear that choosing a γ that is the norm of an element of L compromises security.

3.2 Analysis of the Error

We are left to consider the distribution of the error matrix $\mathbf{E}$. In order to understand this, we discuss the proof of the lemma further. Let $\gamma = N_{L/K}(\beta)$, so that the isomorphism mapping $\mathcal{A}$ to $\mathcal{A}' = (L/K, \theta, 1)$ fixes L and sends u to $u\beta$. It is sufficient for our purposes to restrict to the case when γ is a root of unity, and the γ which are both roots of unity and norm elements are precisely norms of another root of unity, so β is a root of unity and the isomorphism maps a Gaussian distribution on $\mathcal{A}$ to a Gaussian distribution on $\mathcal{A}'$.

The isomorphism mapping $\mathcal{A}'$ to $M_d(K)$ consists of the composition of two maps. The first is a mapping from $\mathcal{A}'$ to $\mathrm{Hom}_K(L, L)$, the space of K-linear endomorphisms of L, and is defined by sending $x \in L$ to the multiplication function $m_x(y) = x \cdot y$ for $y \in L$ and sending u to θ. Then, it applies the well-known isomorphism sending $\mathrm{Hom}_K(L, L)$ to $M_d(K)$, which can be defined constructively as follows:

1. Fix a K-basis $\{\ell_1, \ldots, \ell_d\}$ of L over K.
2. Define $f_j : K \to L$ as $f_j(x) = \ell_j x$, a mapping onto the j coordinate of the basis.
3. Let $\pi_j : L \to K$ denote the projection onto ℓ_j sending $\pi_j\left(\sum_{i=1}^{d} x_i \ell_i\right) = x_j$.
4. Define $\Delta : \mathrm{Hom}_K(L, L) \to M_d(K)$ coordinatewise as

$$\Delta(\psi)_{i,j} = (\pi_i \circ \psi \circ f_j)(1).$$

Since it permits an arbitrary choice of K-basis, this isomorphism is non-unique. Furthermore, an attacker trying to apply this isomorphism would be able to use their choice of basis and still compute the isomorphism efficiently. We are interested in the image of a Gaussian sample $e \in \Lambda_q$ under this isomorphism, with

$e = \sum_{i=0}^{d-1} u^i e_i$, having each e_i sampled independently from a discrete Gaussian over $\mathcal{O}_L$, being sent to $\psi_e = \sum_{i=0}^{d-1} e_i \theta^i$. Correspondingly, the i, j coordinate of the matrix $\mathbf{E} = \Delta(e)$ is

$$\pi_i \left(\sum_{k=0}^{d-1} e_k \theta^k \left(\ell_j \right) \right)$$

For the jth column of $\mathbf{E}$ (the error vector in the set of d MLWE samples with secret $\mathbf{s}_i$), the error is precisely the ℓ_i coordinate of $\sum_{k=0}^{d-1} e_k \theta^k \left(\ell_j \right)$.

Now the distribution of the error in each collection of MLWE samples depends on the properties of the chosen basis. Since the e_k are independent Gaussian samples from L, j is fixed and θ represents a permutation of the canonical embedding coordinates of L elements. Hence, $\sum_{k=0}^{d-1} e_k \theta^k \left(\ell_j \right)$ is an elliptical Gaussian with n blocks of d different parameters. In addition, the coordinates of the image of the projections are not independent and are potentially highly correlated.

We will denote the isomorphism $\mathcal{A} \to M_d(K)$ by φ in future sections. We give some examples of the image of this isomorphsim.

Example 1. For any $x = x_0 + ux_1 = a_0 + ia_1 + u(b_0 + ib_1) \in \Lambda \subset \mathcal{A} = (\mathbb{Q}(i)/\mathbb{Q}, \theta, 1)$, where $\theta \in \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ is the element sending $i \mapsto -i$ and fixing $\mathbb{Q}$, the image of x under the isomorphism of Lemma 1 with respect to the basis $\{1, i\}$ is

$$\varphi(x) = \begin{pmatrix} a_0 + b_0 & b_1 - a_1 \\ a_1 + b_1 & a_0 - b_0 \end{pmatrix}.$$

Proof. The isomorphism comprises the composition of a map from $\mathcal{A}$ to $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(i), \mathbb{Q}(i))$, sending $x \in \mathbb{Q}(i)$ to the multiplication function $f_x(y) = x \cdot y$ for $y \in \mathbb{Q}(i)$ and sending u to θ, and the isomorphism sending $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(i), \mathbb{Q}(i))$ to $M_d(\mathbb{Q})$. We have the basis $\{1, i\}$. We then find

$$\begin{aligned} \Delta(x)_{j,1} &= \left(\pi_j \circ x \circ f_1\right)(1) = (\pi_j \circ x)(1) = \pi_j(x_0\theta^0(1) + x_1\theta(1)) = \pi_j(x_0 + x_1) \\ &= \begin{cases} a_0 + b_0, & j = 1 \\ a_1 + b_1, & j = 2 \end{cases} \end{aligned}$$

$$\begin{aligned} \Delta(x)_{j,2} &= \left(\pi_j \circ x \circ f_2\right)(1) = (\pi_j \circ x)(i) = \pi_j(x_0\theta^0(i) + x_1\theta(i)) = \pi_j(i(x_0 - x_1)) \\ &= \pi_j(b_1 - a_1 + i(a_0 - b_0)) = \begin{cases} b_1 - a_1, & j = 1 \\ a_0 - b_0, & j = 2 \end{cases}. \end{aligned}$$

Example 2. More generally, for any $x = x_0 + ux_1 = a_0 + \zeta_n a_1 + u(b_0 + \zeta_n b_1) \in \Lambda \subset \mathcal{A} = (\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+, \theta, 1)$, where $\mathbb{Q}(\zeta_n)^+ := \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, $\theta \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n + \zeta_n^{-1}))$ sends $\zeta_n \mapsto \zeta_n^{-1}$, fixing $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, and $n = 2^r$ for some $r \geq 2$, the image of x under the isomorphism of Lemma 1 with respect to the basis $\{1, \zeta_n\}$ is

$$\varphi(x) = \begin{pmatrix} a_0 + b_0 & b_1 - a_1 + b_0(\zeta_n + \zeta_n^{-1}) \\ a_1 + b_1 & a_0 - b_0 + a_1(\zeta_n + \zeta_n^{-1}) \end{pmatrix}.$$

Proof. We again compute

$$\begin{aligned}\Delta(x)_{j,1} &= (\pi_j \circ x \circ f_1)(1) = (\pi_j \circ x)(1) = \pi_j(x_0\theta^0(1) + x_1\theta(1)) = \pi_j(x_0 + x_1)\\ &= \begin{cases} a_0 + b_0, & j = 1 \\ a_1 + b_1, & j = 2 \end{cases}\end{aligned}$$

$$\begin{aligned}\Delta(x)_{j,2} &= (\pi_j \circ x \circ f_2)(1) = (\pi_j \circ x)(\zeta_n) = \pi_j(x_0\theta^0(\zeta_n) + x_1\theta(\zeta_n))\\ &= \pi_j((a_0 + \zeta_n a_1)\zeta_n + (b_0 + \zeta_n b_1)\zeta_n^{-1})\\ &= \pi_j(a_0\zeta_n + \zeta_n^2 a_1 + b_0\zeta_n^{-1} + b_1)\\ &= \pi_j(a_0\zeta_n + a_1(\zeta_n + \zeta_n^{-1})\zeta_n - a_1 + b_0(\zeta_n + \zeta_n^{-1}) - \zeta_n b_0 + b_1)\\ &= \pi_j(-a_1 + b_0(\zeta_n + \zeta_n^{-1}) + b_1 + \zeta_n(a_0 - b_0 + a_1(\zeta_n + \zeta_n^{-1})))\\ &= \begin{cases} b_1 - a_1 + b_0(\zeta_n + \zeta_n^{-1}), & j = 1 \\ a_0 - b_0 + a_1(\zeta_n + \zeta_n^{-1}), & j = 2 \end{cases}.\end{aligned}$$

Example 3. Likewise, for any $x = x_0 + ux_1 = a_0 + \zeta_n a_1 + u(b_0 + \zeta_n b_1) \in \Lambda \subset \mathcal{A} = (\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+, \theta, 1)$, where $\mathbb{Q}(\zeta_n)^+ := \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, $\theta \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n + \zeta_n^{-1}))$ sends $\zeta_n \mapsto \zeta_n^{-1}$, fixing $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, and $n = 2^r$ for some $r \geq 2$, the image of $\zeta_n^{-1}x = \zeta_n^{-1}x_0 + \zeta_n^{-1}ux_1 = \zeta_n^{-1}x_0 + u\zeta_n x_1$ under the isomorphism of Lemma 1 with respect to the basis $\{1, \zeta_n\}$ is

$$\varphi(x) = \begin{pmatrix} a_1 - b_1 + a_0(\zeta_n + \zeta_n^{-1}) & a_0 + b_0 \\ b_0 - a_0 + b_1(\zeta_n + \zeta_n^{-1}) & a_1 + b_1 \end{pmatrix}.$$

Proof. We compute

$$\begin{aligned}\Delta(x)_{j,1} &= \left(\pi_j \circ \zeta_n^{-1}x \circ f_1\right)(1) = (\pi_j \circ \zeta_n^{-1}x)(1) = \pi_j(\zeta_n^{-1}x_0\theta^0(1) + \zeta_n x_1\theta(1))\\ &= \pi_j(\zeta_n^{-1}(a_0 + \zeta_n a_1) + \zeta_n(b_0 + \zeta_n b_1))\\ &= \pi_j(a_0\zeta_n^{-1} + a_1 + b_0\zeta_n + b_1\zeta_n^2)\\ &= \pi_j(a_0(\zeta_n + \zeta_n^{-1}) - a_0\zeta_n + a_1 + b_0\zeta_n + b_1(\zeta_n + \zeta_n^{-1})\zeta_n - b_1)\\ &= \pi_j(a_1 - b_1 + a_0(\zeta_n + \zeta_n^{-1}) + \zeta_n(b_0 - a_0 + b_1(\zeta_n + \zeta_n^{-1})))\\ &= \begin{cases} a_1 - b_1 + a_0(\zeta_n + \zeta_n^{-1}), & j = 1 \\ b_0 - a_0 + b_1(\zeta_n + \zeta_n^{-1}), & j = 2, \end{cases}\end{aligned}$$

$$\begin{aligned}\Delta(x)_{j,2} &= \left(\pi_j \circ \zeta_n^{-1}x \circ f_2\right)(1) = (\pi_j \circ \zeta_n^{-1}x)(\zeta_n) = \pi_j(\zeta_n^{-1}x_0\theta^0(\zeta_n) + \zeta_n x_1\theta(\zeta_n))\\ &= \pi_j(a_0 + \zeta_n a_1 + b_0 + \zeta_n b_1)\\ &= \begin{cases} a_0 + b_0, & j = 1 \\ a_1 + b_1, & j = 2 \end{cases}.\end{aligned}$$

We observe, fixing the basis $\{1, \zeta_n\}$, that the first column of $\varphi(x)$ is identical to the second column of $\varphi(\zeta_n^{-1} \cdot x)$. We will use this fact in subsequent sections of this work.

3.3 Summary

The end result of this exposition is that, depending on the properties of the basis of $\mathcal{O}_L/\mathcal{O}_K$, and given the choice of γ as a norm element, from a single CLWE instance we can construct d parallel copies of d MLWE instances in dimension n and rank d with correlated error. These lower-dimensional correlated instances of the MLWE problem are substantially more tractable than the claimed security of the CLWE instance, which is that it is roughly as hard as an MLWE instance in the same dimension nd and rank d, if the resulting errors are small. Of course, the error distributions in the underlying MLWE instances are non-standard. In summary, solving the CLWE problem with norm element γ can be simplified by some parallelization into MLWE instances, and thus for security, one should stick to γ that is non-norm. When γ is not a norm, the algebra is division, and no such parallelization attack is possible.

4 An Isomorphism Between Dihedral Group Rings and Cyclic Algebras

We now connect the preceeding with group rings. Any element a of $R = \mathbb{Z}[D_{2n}]/(\mathfrak{r}^{n/2}+1)\mathbb{Z}[D_{2n}]$ can be written $a = a_0(\mathfrak{r}) + \mathfrak{s}a_1(\mathfrak{r})$. This motivates the following map: set $\Lambda = \mathcal{O}_L \oplus u\mathcal{O}_L$ to be the natural order in the degree 2 cyclic algebra $\mathcal{A} = (L/K, \theta, \gamma)$, where $L = \mathbb{Q}(\zeta_n)$ is the nth cyclotomic field, θ is the map on $L = \mathbb{Q}(\zeta_n)$ sending $\zeta_n \mapsto \zeta_n^{-1}$ and extended linearly, K is the subfield of L fixed by this map, $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, and $\gamma = 1$. Then define

$$\phi : R \to \Lambda, \text{ mapping } \mathfrak{r} \mapsto \zeta_n \text{ and } \mathfrak{s} \mapsto u,$$

for ζ_n a primitive nth root of unity, extended linearly.

In this section, we show that the map ϕ is a ring isomorphism. We first show that it is a homomorphism, for completeness, before proving bijectivity.

Lemma 2. *The map ϕ defined above is an isomorphism of rings from R to Λ.*

Proof. Firstly, we show that ϕ does indeed map into Λ. Clearly $\phi(R)$ lies in $\mathbb{Z}[\zeta_n] \oplus u\mathbb{Z}[\zeta_n]$, so $\phi(R)$ lies in $\mathcal{O}_L \oplus u\mathcal{O}_L$. To see that the structures of R and Λ are compatible, first note that $\phi(\mathfrak{s}^2) = 1 = u^2$. Next, $\mathfrak{s}\overline{a}(\mathfrak{r}) = \mathfrak{s}\mathfrak{s}a(\mathfrak{r})\mathfrak{s} = a(\mathfrak{r})\mathfrak{s}$, so $\phi(\mathfrak{s}\overline{a}(\mathfrak{r})) = \phi(\mathfrak{s})\phi(\overline{a}(\mathfrak{r})) = u\phi(\overline{a}(\mathfrak{r}))$, and $\phi(\mathfrak{s}\overline{a}(\mathfrak{r})) = \phi(a(\mathfrak{r})\mathfrak{s}) = a(\zeta_n)u$, so $u\theta(a(\zeta_n)) = a(\zeta_n)u = u\phi(\overline{a}(\mathfrak{r}))$, and since Λ is an integral domain we find $\theta(a(\zeta_n)) = \phi(\overline{a}(\mathfrak{r}))$. Thus u has the desired properties. Finally, since θ corresponds to $\bar{\cdot}$, and the center of R is the elements $a = a_0(\mathfrak{r}) + \mathfrak{s}a_1(\mathfrak{r})$ such that $a_1(\mathfrak{r}) = 0$ and $a_0(\mathfrak{r}) = \overline{a_0}(\mathfrak{r})$, $\phi(Z(R)) = K$, and ϕ maps elements of R to elements of Λ.

We now show that ϕ is a ring homomorphism. Clearly $\phi(0) = 0$ and $\phi(1) = 1$. Moreover, to show additivity, let $a, b \in R$. Then $\phi(a+b) = \phi(a_0(\mathfrak{r}) + \mathfrak{s}a_1(\mathfrak{r}) + b_0(\mathfrak{r}) + \mathfrak{s}b_1(\mathfrak{r})) = \phi(a_0(\mathfrak{r}) + b_0(\mathfrak{r}) + \mathfrak{s}(a_1(\mathfrak{r}) + b_1(\mathfrak{r}))) = \phi(c_0(\mathfrak{r}) + \mathfrak{s}c_1(\mathfrak{r})) =$

$c_0(\zeta_n) + uc_1(\zeta_n) = a_0(\zeta_n) + b_0(\zeta_n) + s(a_1(\zeta_n) + b_1(\zeta_n)) = \phi(a) + \phi(b)$.

To show multiplicativity:

$$\begin{aligned}
\phi(ab) &= \phi((a_0(\mathfrak{r}) + \mathfrak{s}a_1(\mathfrak{r}))(b_0(\mathfrak{r}) + \mathfrak{s}b_1(\mathfrak{r}))) \\
&= \phi(a_0(\mathfrak{r})b_0(\mathfrak{r}) + a_0(\mathfrak{r})\mathfrak{s}b_1(\mathfrak{r}) + \mathfrak{s}a_1(\mathfrak{r})b_0(\mathfrak{r}) + \mathfrak{s}a_1(\mathfrak{r})\mathfrak{s}b_1(\mathfrak{r})) \\
&= \phi(a_0(\mathfrak{r})b_0(\mathfrak{r}) + \overline{a_1}(\mathfrak{r})b_1(\mathfrak{r}) + \mathfrak{s}(\overline{a_0}(\mathfrak{r})b_1(\mathfrak{r}) + a_1(\mathfrak{r})b_0(\mathfrak{r}))) \\
&= \phi(a_0(\mathfrak{r})b_0(\mathfrak{r})) + \phi(\overline{a_1}(\mathfrak{r})b_1(\mathfrak{r})) + \phi(\mathfrak{s}\overline{a_0}(\mathfrak{r})b_1(\mathfrak{r})) + \phi(\mathfrak{s}a_1(\mathfrak{r})b_0(\mathfrak{r})) \\
&= a_0(\zeta_n)b_0(\zeta_n) + \overline{a_1}(\zeta_n)b_1(\zeta_n) + u\overline{a_0}(\zeta_n)b_1(\zeta_n) + ua_1(\zeta_n)b_0(\zeta_n).
\end{aligned}$$

By definition, $\overline{a_0}(\zeta_n)$ and $\overline{a_1}(\zeta_n)$ are equal to $\theta(a_0(\zeta_n))$ and $\theta(a_1(\zeta_n))$ in L: for example, $\overline{a_0}(\zeta_n) = \phi(\overline{a_0}(\mathfrak{r})) = \phi(a_0(\mathfrak{r}^{-1})) = a_0(\zeta_n^{-1}) = \theta(a_0(\zeta_n))$. Since $\gamma = 1$, we can write

$$\begin{aligned}
\phi(ab) &= a_0(\zeta_n)b_0(\zeta_n) + \overline{a_1}(\zeta_n)b_1(\zeta_n) + u\overline{a_0}(\zeta_n)b_1(\zeta_n) + ua_1(\zeta_n)b_0(\zeta_n) \\
&= a_0(\zeta_n)b_0(\zeta_n) + \gamma\theta(a_1(\zeta_n))b_1(\zeta_n) + u\theta(a_0(\zeta_n))b_1(\zeta_n) + ua_1(\zeta_n)b_0(\zeta_n) \\
&= (a_0(\zeta_n) + ua_1(\zeta_n)(b_0(\zeta_n) + ub_1(\zeta_n)) \\
&= \phi(a)\phi(b),
\end{aligned}$$

as required, so ϕ is a ring homomorphism.

Finally, we need to show bijectivity. Surjectivity is clear. To prove injectivity, suppose $x \in \ker(\phi)$ is non-zero. Then $\phi(x_0(\mathfrak{r})) = x_0(\zeta_n) = 0$ and $\phi(x_1(\mathfrak{r})) = x_1(\zeta_n) = 0$. The x_i, $i = 1, 2$, are polynomials in $\mathbb{Z}[X]/(X^{n/2} + 1)$ and since ζ_n is a complex root of $X^{n/2} + 1$ when n is a power of two, $\mathbb{Z}[X]/(X^{n/2} + 1) \cong \mathbb{Z}[\zeta_n]$. So if an integer polynomial evaluated at ζ_n is 0, the polynomial in indeterminate X is 0 mod $X^{n/2} + 1$. Thus $x_0(\mathfrak{r})$ and $x_1(\mathfrak{r})$ are equal to 0 in $\mathbb{Z}[\mathfrak{r}]/(\mathfrak{r}^{n/2} + 1)$, which is a contradiction. So ϕ is a ring isomorphism.

In summary, there is an isomorphism between $R = \mathbb{Z}[D_{2n}]/(\mathfrak{r}^{n/2}+1)\mathbb{Z}[D_{2n}]$ and $\Lambda = \mathcal{O}_L \oplus u\mathcal{O}_L$ when n is a power of two and L is the nth cyclotomic field, θ is complex conjugation, and $\gamma = 1$. Thus $\mathbb{Z}[D_{2n}]/(\mathfrak{r}^{n/2} + 1)\mathbb{Z}[D_{2n}]$ injects into a cyclic algebra with γ which is a norm, and hence GRLWE samples are invertibly mapped to CLWE samples which are vulnerable to the attack stated in the previous section. In the following sections, we explain the attack concretely, and analyse and discuss the consequences.

5 Attacking Group Ring LWE

Recall the above notation: let n be a power of two,

$$R = \mathbb{Z}\left[D_{2n}\right] / \left(\mathfrak{r}^{n/2} + 1\right) \mathbb{Z}\left[D_{2n}\right],$$

For q be an odd prime, set

$$R_q = R/qR = \mathbb{F}_q\left[D_{2n}\right] / \left(\left(\mathfrak{r}^{n/2} + 1\right) \mathbb{F}_q\left[D_{2n}\right]\right).$$

We outline the structure of our attack on GRLWE. Let $(a, b) = (a, as + e \bmod q) \in R_q \times R_q$ be a primal GRLWE sample. Write

$$b = (a_0(\mathfrak{r}) + \mathfrak{s}a_1(\mathfrak{r})) \cdot (s_0(\mathfrak{r}) + \mathfrak{s}s_1(\mathfrak{r})) + e_0(\mathfrak{r}) + \mathfrak{s}e_1(\mathfrak{r})$$

By extending ϕ to R_q by setting $\phi(x + qR) = \phi(x) + q\Lambda$, we have $\phi(R_q) = \Lambda_q$, and denoting the image of element $x \in R$ in Λ by x', we have that a is mapped to $a' \in \Lambda_q$. Moreover, $\phi(b) = b' = a's' + e' \in \Lambda_q$, with $s', e' \in \Lambda_q$, as above. In addition, it is clear that ϕ preserves the size of the error term e, and the image of the GRLWE sample is distributed correctly, according to a CLWE sample with $L/K = \mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, some power-of-two n, integer modulus q, and some error distribution. Then, using the isomorphism of Lemma 1 for algebras with $\gamma = 1$, transform $(\phi(a), \phi(b)) = (a', b')$ into a sample over $M_2(\mathcal{O}_{K_q}) \times M_2(\mathcal{O}_{K_q})$, denoted $(A, B = AS + E)$, with A, S, and $E \in M_2(\mathcal{O}_{K_q})$.

Solving the instances of MLWE given by (A, B) is easier than solving the one instance of CLWE given by (a', b'), if the error E is small: observe that (A, B) represents two CLWE samples from each of two instances of CLWE (that is, CLWE instances with two different secrets, S_1 and S_2, which comprise the columns of S), and writing $(A, AS_i + E_i)$, $i = 1, 2$, for the two samples from each instance of CLWE, one can see that $(A, AS_i + E_i)$ corresponds to two MLWE samples of dimension $[K : \mathbb{Q}] = n/2$ and module rank 2, whereas (a', b') represents two MLWE samples from one CLWE instance (that is, with only one secret, s), each in dimension $2 \cdot [K : \mathbb{Q}] = n$ and module rank 2.

However, there are two technical issues with the strategy outlined above: the first is that, as can be seen from Examples 2 and 3, the size of the second column of E is not necessarily small. Moreover, the restriction of φ to Λ, $\varphi|_\Lambda$, gives a map $\Lambda \hookrightarrow M_2(\mathcal{O}_K)$ which is injective but not surjective. This means that there is no isomorphism between Λ and $M_2(\mathcal{O}_K)$, so it is not obvious that once one has solved the resulting MLWE samples above that one can invert $\varphi|_\Lambda$ to solve the GRLWE problem. To address this latter issue, we now prove that the 'mod q' map induced by taking φ modulo q from $\Lambda_q \to M_2(\mathcal{O}_{K_q})$ is surjective for certain primes, and thus we have a bijection which can be inverted. We require a technical lemma.

Lemma 3. *[5, Proposition 2] Let Φ_n^+ be the minimal polynomial of $\zeta_n + \zeta_n^{-1}$. For $r \geq 2$ and $k \geq 3$ odd, we have*

$$\Phi_{2^r}^+(1) = \pm 1; \quad \Phi_{2^r}^+(2) = 2; \quad \Phi_{2^r k}^+(1) = \Phi_{2^r k}^+(2) = 1$$

Theorem 3. *Let $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, $L = \mathbb{Q}(\zeta_n)$, $\theta = \bar{\cdot}$ denote complex conjugation, and $n = 2^r$, $r \geq 2$. Let $q > 2$ be a prime unramified in $\mathcal{O}_L$. Then $\varphi : \Lambda_q \to M_2(\mathcal{O}_{K_q})$ is bijective.*

Proof. Write the factorisations of q as $q\mathcal{O}_K = \prod_{i=1}^{g_K^q} \mathfrak{p}_i$ and $q\mathcal{O}_L = \prod_{i=1}^{g_L^q} \mathcal{P}_i$. Observe that $|\Lambda_q| = |\mathcal{O}_L/q\mathcal{O}_L|^2 = |\mathcal{O}_L/\mathcal{P}_j|^{2g_L^q} = q^{2f_L^q g_L^q} = q^{2[L:\mathbb{Q}]}$, where the second equality holds for any index j, since L is Galois over $\mathbb{Q}$. We also have $|M_2(\mathcal{O}_K/q\mathcal{O}_K)| = |M_2(\mathcal{O}_K/\prod_{i=1}^{g_K^q} \mathfrak{q}_i)| = |M_2(\mathcal{O}_K/\mathfrak{q}_j)|^{g_K^q} = (q^{4f_K^q})^{g_K^q} =$

$q^{4f_K^q g_K^q} = q^{4[K:\mathbb{Q}]}$. Since $[L:\mathbb{Q}] = 2[K:\mathbb{Q}]$, the sets have equal cardinality, that is Λ_q and $M_2(\mathcal{O}_{K_q})$ have the same size.

Next, fix the basis $\{1, \zeta_n\}$ of L/K. Write $x = x_0 + ux_1 \in \Lambda_q$ with $x_0 = a_0 + \zeta_n a_1$, $x_1 = b_0 + \zeta_n b_1 \bmod q\mathcal{O}_L$, where the a_i, b_i lie in $\mathcal{O}_K$. Then by Example 2,

$$\varphi(x) = \begin{pmatrix} a_0 + b_0 & b_1 - a_1 + b_0(\zeta_n + \zeta_n^{-1}) \\ a_1 + b_1 & a_0 - b_0 + a_1(\zeta_n + \zeta_n^{-1}) \end{pmatrix} \bmod q\mathcal{O}_K.$$

Suppose $x \in \ker \varphi$, so the entries of $\varphi(x)$ are 0 mod $q\mathcal{O}_K$. Then we have

$$a_0 + b_0 = qv_1,\ b_1 - a_1 + b_0(\zeta_n + \zeta_n^{-1}) = qv_2,\ a_1 + b_1 = qv_3,\ a_0 - b_0 + a_1(\zeta_n + \zeta_n^{-1}) = qv_4,$$

with the $v_i \in \mathcal{O}_K$. This then yields

$$2a_0 + a_1(\zeta_n + \zeta_n^{-1}) = q(v_1 + v_4) \text{ and } -2a_1 - a_0(\zeta_n + \zeta_n^{-1}) = q(v_2 + v_3),$$

so $2(a_0 - a_1) - (a_0 - a_1)(\zeta_n + \zeta_n^{-1}) = q(v_1 + v_2 + v_3 + v_4)$, from which we obtain

$$(a_1 - a_0)\left(\zeta_n + \zeta_n^{-1} - 2\right) \equiv 0 \bmod q \tag{1}$$

Now, if $\zeta_n + \zeta_n^{-1} - 2 \equiv 0 \bmod q$ then $\zeta_n + \zeta_n^{-1} \equiv 2 \bmod q$. Applying $\Phi_{2^r}^+(\cdot)$ to both sides, we obtain $\phi_{2^r}^+(2) \equiv 0 \bmod q$. However, by Lemma 3 we have $\phi_{2^r}^+(2) = 2$, so we do not have $\phi_{2^r}^+(2) \equiv 0 \bmod q$. Thus $\zeta_n + \zeta_n^{-1} - 2 \not\equiv 0 \bmod q$.

Since the statement (1) is true if and only if it holds modulo $\mathfrak{p}_i$ for all i by the Chinese Remainder Theorem, and since $\zeta_n + \zeta_n^{-1} - 2 \not\equiv 0 \bmod q$, there exists a j such that $a_0 = a_1 \bmod \mathfrak{p}_j$. But since a_0 and a_1 were chosen arbitrarily this is a contradiction.

We then have an injection between finite sets of equal cardinality, so φ is a bijection.

This resolves the second objection. What about the size of the error term E? Observe that if $e = a_0 + \zeta_n a_1 + u(b_0 + \zeta_n b_1)$ then $\varphi(e) = E$ has the form

$$\begin{pmatrix} a_0 + b_0 & b_1 - a_1 + b_0(\zeta_n + \zeta_n^{-1}) \\ a_1 + b_1 & a_0 - b_0 + a_1(\zeta_n + \zeta_n^{-1}) \end{pmatrix}$$

Thus the two LWE instances obtained from the image of the GRLWE sample have error terms of different size: the first instance has error $E_1 = \begin{pmatrix} a_0 + b_0 \\ a_1 + b_1 \end{pmatrix}$ while the second has error $E_2 = \begin{pmatrix} b_1 - a_1 + b_0(\zeta_n + \zeta_n^{-1}) \\ a_0 - b_0 + a_1(\zeta_n + \zeta_n^{-1}) \end{pmatrix}$ which may have large coefficients. We resolve this by using the observation of Example 3: if $(a, b) = (a, a \cdot s + e)$ is a CLWE sample, then we note that $(a \cdot \zeta_n, b) = (a \cdot \zeta_n, a\zeta_n \cdot \zeta_n^{-1} s + e)$ is a well-defined CLWE sample with secret $\zeta_n^{-1} \cdot s$ and error e. We thus apply the map φ to both (a, b) and $(a \cdot \zeta_n, b)$. This yields samples

$$(A, B = AS + E) \text{ and } (A', B = A'S' + E)$$

From these samples we take the instances

$$(A, AS_1 + E_1) \text{ and } (A', A'S_1' + E_1),$$

since the error E_1 is bounded, and shared by both samples. Then, since solving both instances recovers both columns of S', we may invert φ on S' to obtain $\zeta_n^{-1}s$, and hence recover s.

Thus when q is unramified in $\mathcal{O}_L$, applying lattice reduction techniques such as the BKZ algorithm to the resulting MLWE samples and applying the inverse transformations allows an attacker to recover the secret s in less time than on the original CLWE samples. We demonstrate the approximate loss in security of this procedure to GRLWE in the next section. We conclude the present section with the theorem statement and proof of our main result, considering the GRLWE errors to be sampled from discrete Gaussians, for convenience. Recall $\mathrm{MLWE}_{n,q,s,\alpha,d,m}$ denotes the search MLWE problem on samples with ring dimension n, modulus q, secret s, error distribution $\mathcal{D}_{\Lambda,\alpha}$, module rank d, and number of samples m. Similarly, we let $\mathrm{GRLWE}_{n,q,s,\alpha,m}$ denote a search GRLWE problem on samples with ring dimension n, modulus q, secret s, error distribution $\mathcal{D}_{\Lambda,\alpha}$, and number of samples m.

Theorem 4. *Let $q \geq 3$ be an odd prime, $n \geq 2$ a power of 2, $m \geq 1$, $\epsilon = \mathrm{neg}(n) > 0$, and $\sqrt{2}\eta_\epsilon(\mathcal{O}_K) < \alpha \ll \frac{1}{\sqrt{2}}\eta_\epsilon(q\mathcal{O}_K)$. Let $L := \mathbb{Q}(\zeta_n)$ be the nth cyclotomic field, $K := L \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, $R := \mathbb{Z}[D_{2n}]/\left(\mathfrak{r}^n + 1\right)\mathbb{Z}[D_{2n}]$ and $R_q := \mathbb{Z}[D_{2n}]/\left(\mathfrak{r}^n + 1, q\right)\mathbb{Z}[D_{2n}]$. Let $s \in R_q$. Then $\mathrm{GRLWE}_{n,q,s,\alpha,m}$ reduces to solving $\mathrm{MLWE}_{\frac{n}{2},q,S_1,\sqrt{2}\alpha,2,2m}$ and $\mathrm{MLWE}_{\frac{n}{2},q,S_1',\sqrt{2}\alpha,2,2m}$, where S_i (S_i' resp.) $\in \mathcal{O}_{K_q}^2$ is the ith column of $\varphi(s)$ ($\varphi(\zeta_n^{-1}s)$ resp.), $i = 1, 2$.*

Proof. We apply φ to m samples from $\Pi^G_{n,q,s,\mathcal{D}_{\Lambda,\alpha}}$, denoted $(a^{(i)}, b^{(i)} \bmod q) = (a^{(i)}, a^{(i)}s + e^{(i)} \bmod q)$, $i = 1, ..., m$, and to $(a^{(i)}\zeta_n, b^{(i)} \bmod q) = (a^{(i)}\zeta_n, a^{(i)}\zeta_n \cdot \zeta_n^{-1}s + e^{(i)} \bmod q)$, $i = 1, ..., m$. Each application yields a sample of the form

$$\left(\varphi(a^{(i)}), \varphi\left(a^{(i)}s + e^{(i)}\right) \bmod q\right) = \left(A^{(i)}, A^{(i)}S + E^{(i)} \bmod q\right),$$

which lies in $M_2\left(\mathcal{O}_{K_q}\right) \times M_2\left(\mathcal{O}_{K_q}\right)$, and likewise for $(a^{(i)}\zeta_n, a^{(i)}\zeta_n \cdot \zeta_n^{-1}s + e^{(i)} \bmod q)$. Denote the columns of $\varphi(s) = S$ by S_k, $k = 1, 2$, and of $\varphi(\zeta_n^{-1}s)$ by S_k', $k = 1, 2$. Since the $A^{(i)}$ and $E^{(i)}$ are 2×2 matrices, $\left(A^{(i)}, A^{(i)}S + E^{(i)}\right)$ can be rewritten

$$\left(A^{(i)}, A^{(i)}S_k + E_k^{(i)}\right) \in \mathcal{O}_{K_q}^2 \times \mathcal{O}_{K_q}^2,$$

where $E_k^{(i)}$ denotes the kth column of $E^{(i)}$. This constitutes two samples of $\Pi^M_{\frac{n}{2},q,S_k,\mathcal{D}_{\Lambda,\alpha_k}}$, $k = 1, 2$, for some α_k, so overall we obtain $2m$ such samples. We also obtain $2m$ samples from the samples with secret S'. Since we now have both columns of S', since $S_2' = S_1 \bmod q$, solving the m samples from $\Pi^M_{\frac{n}{2},q,S_1,\mathcal{D}_{\Lambda,\alpha_k}}$ with error $E_1^{(i)}$ and the m samples from $\Pi^M_{\frac{n}{2},q,S_1',\mathcal{D}_{\Lambda,\alpha_k}}$ with error $E_1^{(i)}$ allows us to reconstruct $\zeta_n^{-1}s$ by computing $\varphi^{-1}(S')$, and hence find s. It only remains to compute α_k.

The image of an error e under φ is $\begin{pmatrix} a_0 + b_0 & b_1 - a_1 + b_0(\zeta_n + \zeta_n^{-1}) \\ a_1 + b_1 & a_0 - b_0 + a_1(\zeta_n + \zeta_n^{-1}) \end{pmatrix} \bmod q$, where we write $e = e_0 + ue_1 = a_0 + \zeta_n a_1 + u(b_0 + \zeta_n b_1)$, considering e as an

element of $\Lambda_{\mathbb{R}}$. Since we sample a discrete Gaussian over Λ by sampling $\mathcal{D}_{\mathbb{Z},\alpha}$ nd^2 times, the a_i, b_i are all sampled independently from $\mathcal{D}_{\mathcal{O}_K,\alpha}$. Then $a_i + b_i$ is distributed statistically close to $\mathcal{D}_{\mathcal{O}_K,\sqrt{2}\alpha}$ for $i = 1, 2$, by assumption on α using Theorem 1. Thus $E_1^{(i)} \sim \mathcal{D}_{\mathcal{O}_K^2,\sqrt{2}\alpha}$, as required.

Algorithm 1: Dimension-reducing transformation on GRLWE samples
Input: GRLWE sample $(a, b) = (a, as + e) \in R_q \times R_q$, a K-basis of L.
Output: Secret s.
1. $(a', b') := (\phi(a), \phi(b))$.
2. $(A, B) := (\varphi(a'), \varphi(b'))$ and $(A', B) := (\varphi(a' \cdot \zeta_n), \varphi(b'))$.
3. Solve (A, B_1) for $S_1 = \varphi(\phi(s))_1$ and (A', B_1) for $S_1' = -\varphi(\phi(s))_2$.
4. $s = \phi^{-1} \circ \varphi^{-1}(S_1 \vert - S_1')$.

5.1 Examples

Here we use the estimator [1] to estimate the runtime of solving an instance of GRLWE before and after applying the above dimension-reducing transformation. We ran the estimator on GRLWE samples with parameters equivalent to those of the Crystals-Kyber [2], namely with the Kyber512 parameters: ring dimension $n = 512$, module rank $d = 2$, modulus $q = 3329$, and parameter $\sigma = 1.22$. The transformed sample yields plain LWE instances in half the dimension of those yielded by the original samples. The estimator ignores the extra algebraic structure of samples, interpreting the parameters as plain LWE instances. Below is a table summarising the results: β is the block size for the BKZ reduction, δ is the root Hermite factor, d_L is the lattice dimension, and m is the number of samples used.

GRLWE Sample					
$n = 512$	m	β	δ	d_L	Hardness estimate
Primal	-	406	1.003941	985	143.8
Dual	531	423	-	1043	149.6
Transformed Sample					
$n = 256$	m	β	δ	d_L	Hardness estimate
Primal	-	165	1.007055	511	76.4
Dual	293	170	-	549	78.9

Table 1: Estimating GRLWE

As can be seen from the table, ignoring the algebraic structure of the samples, the lattices obtained from the transformed samples are significantly less secure than those obtained from the original GRLWE samples. Moreover, since the transform doubles the number of available samples while halving the dimension of each sample, this greater number of samples may be of use to an attacker, compounding the results of the hardness estimation; for instance, a number of attacks on binary error LWE need only polynomially many samples in the dimension, e.g. [26].

In order to achieve the initially expected security level in some fixed dimension for GRLWE as constructed in [6], one could double the initial dimension of the samples; however, this is likely to negatively affect the efficiency of schemes based on such parameters.

5.2 Extending the Attack to other Groups

The authors of [6] observe that D_{2n} is isomorphic to the semi-direct product $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, and comment that their construction can be extended to semi-direct products $\mathbb{Z}/n\mathbb{Z} \rtimes H$, where H is a group acting on $\mathbb{Z}/n\mathbb{Z}$. Here $\mathbb{Z}/n\mathbb{Z} \rtimes H$ is a group with underlying set $\mathbb{Z}/n\mathbb{Z} \times H$ equipped with the multiplication rule $(a,b)(c,d) = (a^d c, bd)$ for $a, c \in \mathbb{Z}/n\mathbb{Z}$, $b, d \in H$. When n is a power of two and H is a cyclic group acting on $\mathbb{Z}/n\mathbb{Z}$ by exponentiation, one obtains a group ring again isomorphic to a cyclic algebra: if $|H| = m$, then $m \mid n/2$ so m is a power of two, and $G = \langle \mathfrak{r}, \mathfrak{s} : \mathfrak{r}^n = \mathfrak{e}, \mathfrak{s}^m = \mathfrak{e}, \mathfrak{s}\mathfrak{r}\mathfrak{s}^{-1} = \mathfrak{r}^k \rangle$ with $\gcd(k,n) = 1$ and $k^m \equiv 1 \bmod n$. Then if $G = \mathbb{Z}/n\mathbb{Z} \rtimes H$, $R = \mathbb{Z}[G]/(\mathfrak{r}^{n/2}+1)\mathbb{Z}[G]$ is isomorphic to the natural order of $\mathcal{A} = (L/K, \theta, \gamma)$ where $L = \mathbb{Q}(\zeta_n)$, θ is an automorphism of L sending $\zeta_n \mapsto \zeta_n^k$, K is the subfield fixed by θ, and $\gamma = 1$. Note $[L:K] = m$.

We can represent samples from such group rings in matrix-vector form as usual. Suppose our sample is of the form $(a, as+e) \in R_q \times R_q$ for an appropriate modulus q and secret s. Then we can rewrite this as $(\Phi(a), \Phi(a)\mathbf{s} + \mathbf{e}) \in M_m(\mathbb{Z}_q[\mathfrak{r}]/(\mathfrak{r}^{n/2}+1)) \times (\mathbb{Z}_q[\mathfrak{r}]/(\mathfrak{r}^{n/2}+1))^m$, where

$$\Phi(a) = \begin{pmatrix} a_0 & \mathfrak{s}^{-1}a_{m-1}\mathfrak{s} & \cdots & \mathfrak{s}^{-(m-1)}a_1\mathfrak{s}^{(m-1)} \\ a_1 & \mathfrak{s}^{-1}a_0\mathfrak{s} & \cdots & \mathfrak{s}^{-(m-1)}a_2\mathfrak{s}^{(m-1)} \\ a_2 & \mathfrak{s}^{-1}a_1\mathfrak{s} & \cdots & \mathfrak{s}^{-(m-1)}a_3\mathfrak{s}^{(m-1)} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m-1} & \mathfrak{s}^{-1}a_{m-2}\mathfrak{s} & \cdots & \mathfrak{s}^{-(m-1)}a_0\mathfrak{s}^{(m-1)} \end{pmatrix}.$$

This has the form of the matrix representation of a cyclic algebra, where θ corresponds to conjugation by s and $\gamma = 1$. Thus γ is a norm, and again we can apply the attack outlined above. We prove a version of Theorem 3 for any m:

Theorem 5. *Let $L = \mathbb{Q}(\zeta_n)$, $k > 0$: $(k,n) = 1$ and $k^m \equiv 1 \bmod n$, $\theta : \zeta_n \mapsto \zeta_n^k$ of order m, $K \subset L$ the subfield fixed by θ, and $n = 2^r$, $r \geq 2$. Let $q \in \mathbb{Z}$ be a prime unramified in L, and $\alpha_1, ..., \alpha_m$ a basis of L/K such that the matrix B with ijth entry $\theta^{j-1}(\alpha_i)$ is invertible modulo q. Then $\varphi : \Lambda_q \to M_m(\mathcal{O}_{K_q})$ is bijective.*

Proof. Write the factorisations of q as $q\mathcal{O}_K = \prod_{i=1}^{g_K^q} \mathfrak{p}_i$ and $q\mathcal{O}_L = \prod_{i=1}^{g_L^q} \mathcal{P}_i$. We have $|\Lambda_q| = |\mathcal{O}_L/q\mathcal{O}_L|^m = |\mathcal{O}_L/\mathcal{P}_j|^{m g_L^q} = q^{m f_L^q g_L^q} = q^{m[L:\mathbb{Q}]}$, where the second equality holds for any index j, since L is Galois over $\mathbb{Q}$. We also have $|M_m(\mathcal{O}_K/q\mathcal{O}_K)| = |M_m(\mathcal{O}_K/\prod_{i=1}^{g_K^q}\mathfrak{q}_i)| = |M_m(\mathcal{O}_K/\mathfrak{q}_j)|^{g_K^q} = (q^{m^2 f_K^q})^{g_K^q} = q^{m^2 f_K^q g_K^q} = q^{m^2[K:\mathbb{Q}]}$. Since $[L:\mathbb{Q}] = m[K:\mathbb{Q}]$, the sets have equal cardinality, that is Λ_q and $M_m(\mathcal{O}_{K_q})$ have the same size.

If $\varphi : \Lambda_q \to M_m(\mathcal{O}_{K_q})$ were not injective, there would exist some $x \in \Lambda \setminus q\Lambda$

with coefficients x_i: $x + q\Lambda \mapsto z \in M_m(q\mathcal{O}_K)$. So $x + q\Lambda \mapsto (qz_{ij})_{i,j}$ with $z_{ij} \in \mathcal{O}_K$. This is equivalent to saying $\pi_i \circ x \circ f_j(1) \in q\mathcal{O}_K$, and therefore $x \circ f_j(1) \in q\mathcal{O}_L$. As above, writing $f_j(1) = \alpha_j$, this is the same as $\sum_{k=0}^{m-1} x_k \theta^k(\alpha_j) \in q\mathcal{O}_L$. Applying this for $j = 1, ..., m$, we obtain a system of equations each of the form $\sum_{k=0}^{m-1} x_k \theta^k(\alpha_j) = z_{j-1} \in q\mathcal{O}_L$, which we can write in matrix-vector notation as

$$\begin{pmatrix} \alpha_1 & \theta(\alpha_1) & ... & \theta^{m-1}(\alpha_1) \\ \alpha_2 & \theta(\alpha_2) & ... & \theta^{m-1}(\alpha_2) \\ \vdots & \vdots & ... & \vdots \\ \alpha_m & \theta(\alpha_m) & ... & \theta^{m-1}(\alpha_m) \end{pmatrix} \begin{pmatrix} x_0 \\ x_2 \\ \vdots \\ x_{m-1} \end{pmatrix} = \begin{pmatrix} z_0 \\ z_2 \\ \vdots \\ z_{m-1} \end{pmatrix} \in q\mathcal{O}_L^m.$$

If the matrix B with entries $\theta^k(\alpha_j)$ is invertible, the vector of x_i lies in $q\mathcal{O}_L^m$ - and this holds by assumption on B. But then we have $x \in q\Lambda$ after all.

6 On the Security of Quaternion Group Rings

We have shown that integral group rings of the form used for GRLWE, that is, dihedral group rings, are subject to a dimension-reducing transformation. In this section we show that if one changes the group from D_{2m} to Q_{4n}, the generalized quaternion group, one obtains group rings immune to the above attack. We stress however that we do not have a full security proof for decision GRLWE over Q_{4n} from the hardness of worst-case lattice problems.

Recall the definition of the generalized quaternion group:

$$Q_{4n} = \langle \mathfrak{r}, \mathfrak{s} : \mathfrak{r}^n = \mathfrak{s}^2, \mathfrak{r}^{2n} = \mathfrak{e}, \mathfrak{s}^{-1}\mathfrak{r}\mathfrak{s} = \mathfrak{r}^{-1} \rangle.$$

In [11] is stated the isomorphism problem for integral group rings of finite groups (denoted here by ISO) G and H:

$$\text{Does } \mathbb{Z}[G] \cong \mathbb{Z}[H] \text{ as rings imply } G \cong H? \text{ (ISO)}$$

Generalized quaternion groups are special cases of dicyclic groups, specifically dicyclic groups of power-of-two order. Dicyclic groups are metacyclic, and therefore metabelian. It has been shown that (ISO) is true for metabelian groups [27]; therefore (ISO) is true for generalized quaternion groups. This means that since $Q_{4n} \ncong D_{2m}$ for any pair n, m, their integral group rings satisfy $\mathbb{Z}[Q_{4n}] \ncong \mathbb{Z}[D_{2m}]$ for any pair n, m. Thus, prima facie, the integral quaternionic group ring is a candidate group ring to use to avoid the security issue identified in this work, which arises from the use of dihedral group rings.

We proceed to consider $R = \mathbb{Z}[Q_{4n}]/(\mathfrak{r}^n + 1)\mathbb{Z}[Q_{4n}]$, analogously to the GRLWE construction. One can see that the quotient by $(\mathfrak{r}^n + 1)$ sets $\mathfrak{r}^n = -1$, and since $\mathfrak{r}^n = \mathfrak{s}^2$, we obtain $\mathfrak{s}^2 = \mathfrak{r}^n = -1$. This also means that, in R, $\mathfrak{s}^3 = -\mathfrak{s}$.

Consider multiplication of two elements of R: if $a, b \in \mathbb{Z}[Q_{4n}]$, we can write them in the form $a = a_0(\mathfrak{r}) + \mathfrak{s}a_1(\mathfrak{r}) + \mathfrak{s}^2 a_2(\mathfrak{r}) + \mathfrak{s}^3 a_3(\mathfrak{r})$. If we quotient by $\mathfrak{r}^n + 1$,

we also set $\mathfrak{s}^2 = -1$, and so get $a = a_0(\mathfrak{r}) - a_2(\mathfrak{r}) + \mathfrak{s}(a_1(\mathfrak{r}) - a_3(\mathfrak{r})) \bmod (\mathfrak{r}^n + 1)$. Rewrite this as $a = a^0(\mathfrak{r}) + \mathfrak{s}a^1(\mathfrak{r}) \bmod (\mathfrak{r}^n + 1)$, so ab then becomes

$$\begin{aligned} ab &= \left(a^0(\mathfrak{r}) + \mathfrak{s}a^1(\mathfrak{r})\right)\left(b^0(\mathfrak{r}) + \mathfrak{s}b^1(\mathfrak{r})\right) \\ &= a^0(\mathfrak{r})b^0(\mathfrak{r}) - \overline{a^1}(\mathfrak{r})b^1(\mathfrak{r}) + \mathfrak{s}\left(a^1(\mathfrak{r})b^0(\mathfrak{r}) + \overline{a^0}(\mathfrak{r})b^1(\mathfrak{r})\right) \bmod (\mathfrak{r}^n + 1). \end{aligned}$$

This is the same multiplication law as holds for cyclic algebras in $d = 2$ where $\gamma = -1$ and $\bar{\cdot}$ corresponds to the action of θ (as can be seen from the discussion in §2.4). One can see, like we showed above for dihedral groups, the following:

Proposition 2. *Let $R = \mathbb{Z}[Q_{4n}]/(\mathfrak{r}^n + 1)\mathbb{Z}[Q_{4n}]$. Let $\Lambda = \mathcal{O}_L \oplus u\mathcal{O}_L$ be the natural order in the degree 2 cyclic algebra $\mathcal{A} = (L/K, \theta, \gamma)$, where $L = \mathbb{Q}(\zeta_n)$, n is a power of 2, θ is the map on $L = \mathbb{Q}(\zeta_n)$ sending $\zeta_n \mapsto \zeta_n^{-1}$ extended linearly, $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is the subfield fixed by this map, and $\gamma = -1$. Define*

$$\phi : R \to \Lambda, \text{ mapping } \mathfrak{r} \mapsto \zeta_n \text{ and } \mathfrak{s} \mapsto u,$$

for ζ_n a primitive nth root of unity. Then ϕ is an isomorphism.

If the above cyclic algebra is division, that is, if -1 is not a norm, there will exist an isomorphism from R to the natural order of a cyclic division algebra in the same fashion as before; but the lemma we used to send GRLWE samples to samples over matrix rings will not apply, since it does not apply to division algebras. We proceed to verify this.

Recall an algebraic number field of degree n has n embeddings into $\mathbb{C}$. If these map the field into $\mathbb{R}$, they are real embeddings, else complex. If there are r_1 real embeddings and r_2 pairs of complex embeddings, we have $r_1 + 2r_2 = n$. A field with only complex embeddings is called *totally complex*, and a field with only real embeddings is *totally real*. Finally, a non-zero field element can be mapped to an r_1-tuple $\{\pm 1\}^{r_1}$ under the real embeddings of the field, with each entry depending on whether the image of an embedding is positive or negative; if it maps to $\{1\}^{r_1}$, we call it *totally positive*. For more on these definitions, see [16]. We now show:

Proposition 3. *Let $\mathcal{A} = (\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+, \bar{\cdot}, -1)$ be a cyclic algebra. Then $\mathcal{A}$ is a cyclic division algebra.*

Proof. It suffices to prove that -1 is not the norm of any element from $\mathbb{Q}(\zeta_n)$ to $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$; suppose the contrary. First, note that $\mathbb{Q}(\zeta_n)$ is totally complex and $\mathbb{Q}(\zeta_n)^+$ is totally real. Thus every non-zero element of $\mathbb{Q}(\zeta_n)$ is totally positive, which means that the image of the field norm map in $\mathbb{Q}(\zeta_n)^+$ is also totally positive - but -1 is clearly not totally positive in $\mathbb{Q}(\zeta_n)^+$, yielding a contraction, and -1 is thus not in the image of the norm.

Thus, if one constructs GRLWE over Q_{4n} as above, the dimension-reducing transformation, and hence attack, do not apply. In terms of the numerical results of Section 5.1, this means that a plausible security estimate of GRLWE with fixed dimension n (such as for Kyber512) is given by the output of the Lattice

Estimator on lattices of dimension n, rather than $n/2$.

We observe that since a reduction from SIVP to search CLWE (as in Theorem 2) may be obtained for CLWE in algebras defined by any pair of Galois number fields with $|\gamma| = 1$, even when Λ is not a maximal order (by restricting to invertible ideals) [13], a similar reduction applies to the image of quaternion-group GRLWE under the map sending the group ring to the CDA, if it is then embedded into $\mathbb{R}^{2n}$ via the canonical embedding. This gives a security proof for search GRLWE when $G = Q_{4n}$ under the canonical embedding; however, we note that [6] uses a coefficient embedding. One can relate the canonical and the coefficient embeddings via a linear transformation, and compute the distortion induced by this transformation, as was done in [24] for RLWE. We note that computing the distortion induced by this linear transformation between the embeddings of $(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+, \bar{\cdot}, -1)$ is a straightforward generalisation of the results in [24]. This provides some concrete evidence of the hardness of search GRLWE with $G = Q_{4n}$. We discuss this more in the appendix.

We leave the adaptation of the search-to-decision security proof of GRLWE for generalized quaternion groups, as well as further cryptanalysis, as topics for future research, and remark that the CLWE search-to-decision reduction likely adapts straightforwardly to algebras $(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+, \bar{\cdot}, -1)$, since -1 is a unit.

7 On Structured MLWE Variants

In this section we briefly discuss the relation between the security of the three structured MLWE variants given in the introduction, namely, m-RLWE, GRLWE, and CLWE, summarising the current condition of structured MLWE variants.

The oldest of the three is m-RLWE, or multivariate LWE, which was given in [18]. It defines LWE over the tensor product of rings (which are maximal orders in algebraic number fields). The m-RLWE distribution is defined as follows:

Definition 13. *For $s \in R_q^\vee$ and an error distribution χ over $K_{(T),\mathbb{R}}$, a sample from the m-RLWE distribution $A_{s,\psi}$ over $R_q \times \mathbb{T}$ is generated by $a \leftarrow R_q$ uniformly at random, $e \leftarrow \psi$, and outputting $(a, b = (a \cdot s)/q + e \bmod R^\vee)$.*

Here $K_{(T)} = \bigotimes_{i \in I} K_i$ for K_i cyclotomic, $R = \bigotimes_{i \in I} \mathcal{O}_{K_i}$, I is some indexing set, and $R^\vee$ denotes the dual ideal of R. Finally, set $\mathbb{T} = K_{(T),\mathbb{R}}/R^\vee$. The search and decision problems are defined as usual.

One can understand m-RLWE as follows. For simplicity, suppose the m-RLWE instance consists of the tensor product of two number fields, K_1 and K_2. Write the tensor product of fields as $K = K_1 \otimes K_2$ where K_1 and K_2 are defined by polynomials $f(x)$ and $g(y)$ respectively. This yields a m-RLWE problem over $R_q = \frac{\mathbb{Z}_q[x,y]}{(f(x),g(y))}$, and corresponds to a structured MLWE instance over $\mathbb{Z}_q[x]/(f(x))$ with dimension $\deg(g)$.

The primary case of interest is that of cyclotomics of power of two degree over $\mathbb{Q}$, defined by the polynomials $x^{k_1} + 1$ and $y^{k_2} + 1$ respectively. This gives an m-RLWE problem over $R_q = \frac{\mathbb{Z}_q[x,y]}{(x^{k_1}+1, y^{k_2}+1)}$, and corresponds to a structured MLWE instance over $\mathbb{Z}_q[x]/(x^{k_1} + 1)$ with dimension k_2.

In [4], m-RLWE was subjected to an attack, which runs along the following lines. The authors showed that when k_1 and k_2 are not coprime, there is a field K' containing K_1 such that there is a homomorphism from K into K', and that the image of y under the homomorphism is well-defined. When this happens, $g(y)$, say, has at least one root in $\mathbb{Z}[x](f(x))$. One can then define a map taking polynomials $h(x, y)$ to the l-tuple of evaluations of $h(x, \cdot)$ at the l such roots of $g(y)$. In this way, the problem can be reduced from one problem in dimension $\deg(f) \cdot \deg(g)$ to multiple lower dimensional problems.

For example, let $f(x) = x^8 + 1$ and $g(y) = y^4 + 1$. Consider the map taking y to x^2 and fixing $K_1 = \mathbb{Z}_q[x]/f(x)$. This is a well defined homomorphism from K to K_1. Using this map, the authors transform the problem of solving one m-RLWE instance to solving four RLWE instances in dimension 8, rather than one instance in dimension $k_1 \cdot k_2 = 32$. In general, the attack transforms one instance in dimension $k_1 \cdot k_2$ to k_2 RLWE instances of dimension k_1.

We echo the statement made in [10], that CLWE, as a structured MLWE variant, is immune from this style of attack. Let $\mathcal{A} = (L/K, \theta, \gamma)$ be a cyclic division algebra. Suppose that there is an injective homomorphism $\chi : \mathcal{A} \to L$. L is Galois over K, so the restriction of χ to L is an injective homomorphism of fields, and is thus an isomorphism from L to L, that is, an automorphism. Observe: $\chi(u) \cdot \chi(\ell) = \chi(u \cdot \ell) = \chi(\theta(\ell) \cdot u) = \chi(u) \cdot \chi(\theta(\ell))$ for any $\ell \in L$. This implies that $\chi(\ell) = \chi(\theta(\ell))$ - but this contradicts χ being injective on L. This contradiction implies that there is no injective homomorphism as above, so one cannot launch the attack of [4] to reduce a CLWE instance to an instance defined over a subfield of $\mathcal{A}$.

Furthermore, addressing the attack on GRLWE, if γ is chosen to make $\mathcal{A}$ division, then the isomorphism given in [23, Theorem 30.4] does not apply to $\mathcal{A}$. So the transformation delineated in this work does not apply to a CLWE instance as defined in [10] either.

We conclude from this that the presence of 1. 'twisting' field automorphisms, such as θ, and 2. well-chosen γ, secure CLWE from direct adaptations of the family of attacks which map a sample into a subspace, solve in the subspace, and then lift the solution. The automorphisms prevent the existence of a convenient subfied to injectively map into, and 'good' values of γ similarly prevent the LWE instance being reduced to a lower-dimensional matrix instance. In the case of the first attack, m-RLWE lacks the noncommutativity given by application of θ. In the case of the second attack, GRLWE using the group D_{2n} lacks a value of γ that aids security, and it is not clear how such a value of γ could be introduced (excepting instances where $\gamma = -1$ is not a norm). To conduct such 'subspace' attacks on CLWE, it appears a novel approach is needed.

8 Conclusion

Thus there is a dimension-reducing transformation which takes GRLWE samples and outputs multiple MLWE samples in half the dimension of the original samples. This map can be seen as the composition of two maps, both of which

we proved above to be bijective. This transformation can be converted into an attack on GRLWE by combining the transformation with any method to solve LWE instances. The attack holds for all such group rings as defined in [6], where $G = \mathbb{Z}/n\mathbb{Z} \rtimes H$ as in the relevant section, and leads to a significant loss in security, as can be seen from the results of §5.1. To counter this attack, one would have to double the initial dimension of the samples to obtain the original believed-level of security for the GRLWE problem.

We also gave an example of a group, the generalized quaternion group, for which GRLWE-style group rings are immune from our attack. This is because the corresponding cyclic algebra is a division algebra.

It remains to be seen if other group rings can be constructed for the LWE problem that are proven not to be subject to such an attack. The only groups which have been considered so far are dihedral or quaternionic; perhaps there are other noncommutative groups (not dihedral or quaternionic) that are immune from this strategy. There is certainly no shortage of groups to try. Alternatively, perhaps relaxing assumptions on the group, considering algebraic structures such as monoid rings, could lead to interesting results. Also outstanding is fully adapting the security proof to hold for quaternion group rings, and thus to instantiate LWE in a provably secure manner over such group rings.

References

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

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

[3] D. Boneh and D. M. Freeman. "Linearly Homomorphic Signatures over Binary Fields and New Tools for Lattice-Based Signatures". In: *PKC 2011*. Ed. by D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi. Vol. 6571. LNCS. Citations refer to the full version https://eprint.iacr.org/2010/453. Springer Berlin Heidelberg, 2011, pp. 1–16. DOI: 10.1007/978-3-642-19379-8_1.

[4] C. Bootland, W. Castryck, and F. Vercauteren. "On the security of the multivariate ring learning with errors problem". In: *ANTS-XIV*. New Zealand: MSP, 2020. URL: https://msp.org/obs/2020/4-1/p05.xhtml.

[5] I. B. Chacón and L. López-Hernanz. "RLWE/PLWE Equivalence for the Maximal Totally Real Subextension of the 2^{rpq}-th Cyclotomic Field". In: *Adv. Math. Commun.* 18.5 (2024), pp. 1343–1363. DOI: 10.3934/amc.2022093.

[6] Q. Cheng, J. Zhang, and J. Zhuang. "LWE from Non-commutative Group Rings". In: *Des. Codes, Cryptogr.* (Nov. 2021). DOI: 10.1007/s10623-021-00973-6.

[7] R. Cramer, L. Ducas, and B. Wesolowski. "Short Stickelberger Class Relations and Application to Ideal-SVP". In: *EUROCRYPT 2017*. Ed. by J.-S. Coron and J. B. Nielsen. Vol. 10210. LNCS. Springer International Publishing, 2017, pp. 324–348. DOI: 10.1007/978-3-319-56620-7_12.

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

[9] L. Ducas, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehle. *CRYSTALS-Dilithium: Digital Signatures from Module Lattices*. CRYSTALS Cryptographic Suite for Algebraic Lattices. 2017. URL: https://pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf.

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

[11] E. Jespers. "Structure of group rings and the group of units of integral group rings: an invitation". In: *Indian Journal of Pure and Applied Mathematics* (Sept. 2021). DOI: 10.1007/s13226-021-00179-5.

[12] 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.

[13] C. Ling and A. Mendelsohn. "Algebraic Equipage for Learning with Errors in Cyclic Division Algebras". In: *NuTMiC 2024* (2024). URL: https://eprint.iacr.org/2024/1617.

[14] J. Liu and F.-W. Fu. *Learning with Errors over Group Rings Constructed by Semi-direct Product*. Cryptology ePrint Archive, Paper 2023/1824. 2023. URL: https://eprint.iacr.org/2023/1824.

[15] 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.

[16] W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers*. Springer Monographs in Mathematics. Springer Berlin Heidelberg, 2004. ISBN: 9783540219026.

[17] Y. Pan, J. Xu, N. Wadleigh, and Q. Cheng. "On the Ideal Shortest Vector Problem over Random Rational Primes". In: *EUROCRYPT 2021*. Ed. by A. Canteaut and F.-X. Standaert. Vol. 12696. LNCS. Springer International Publishing, 2021, pp. 559–583. DOI: 10.1007/978-3-030-77870-5_20.

[18] 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). URL: http://arxiv.org/abs/1607.05244.

[19] A. Pedrouzo-Ulloa, J.R. Troncoso-Pastoriza, N. Gama, M. Georgieva, and F. Pérez-González. "Revisiting Multivariate Ring Learning with Errors and Its Applications on Lattice-Based Cryptography". In: *Mathematics* 9.8 (2021). DOI: 10.3390/math9080858.

[20] R. S. Pierce. *Associative Algebras*. Graduate Texts in Mathematics. Springer, 1982. ISBN: 978-1-4757-0165-4.

[21] C. Porter, A. Mendelsohn, and C. Ling. "Subfield Algorithms for Ideal- and Module-SVP Based on the Decomposition Group". In: *NuTMiC 2021* (2021). URL: https://arxiv.org/abs/2105.03219.

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

[23] I. Reiner. *Maximal Orders*. London Mathematical Society Monographs. Oxford University Press, 2003. ISBN: 9780198526735.

[24] M. Roşca, D. Stehlé, and A. Wallet. "On the Ring-LWE and Polynomial-LWE Problems". In: *EUROCRYPT 2018*. Vol. 10820. LNCS. Springer International Publishing, 2018, pp. 146–173. DOI: 10.1007/978-3-319-78381-9_6.

[25] D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa. "Efficient Public Key Encryption Based on Ideal Lattices". In: *ASIACRYPT 2009*. Ed. by M. Matsui. Vol. 5912. LNCS. Springer Berlin Heidelberg, 2009, pp. 617–635. DOI: 10.1007/978-3-642-10366-7_36.

[26] C. Sun, M. Tibouchi, and M. Abe. "Revisiting the Hardness of Binary Error LWE". In: *ACISP 2020*. Ed. by J. K. Liu and H. Cui. Vol. 12248. LNCS. Springer International Publishing, 2020, pp. 425–444. DOI: 10.1007/978-3-030-55304-3_22.

[27] A. Whitcomb. "The Group Ring Problem". PhD thesis. University of Chicago, 1968. URL: www.proquest.com/dissertations-theses/group-ring-problem/docview/302361327/se-2.

A Equivalence of Embeddings for GRLWE with $G = Q_{4n}$

Here we show that the linear transformation mapping between the coefficient and the canonical embedding of $\mathcal{A} = (\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n + \zeta_n^{-1}), \bar{\cdot}, -1)$ is polynomially bounded in n when $n = 2^r$ for $r \geq 2$. We begin by considering the embeddings of $\mathbb{Q}(\zeta_n)$, noting that the map V_f which sends the canonical embedding $\sigma_L(x)$ of an element $x \in \mathbb{Q}(\zeta_n)$ to a coefficient representation of x, that is

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

where $\text{coeff}(\cdot)$ is the vector of coefficients of $x \in \mathbb{Q}[x]/f(x)$ with $f(x) = x^{n/2} + 1$, is a scaled isometry, with scaling factor $\sqrt{n}$. This can be seen by considering the powerful basis $\overrightarrow{p}$ of L. Write $n = 2^r$ and $m = 2^{r-1}$. Set

$$\overrightarrow{p} := (1, \zeta_n, ..., \zeta_n^{m-1})$$

One obtains a matrix by applying the canonical embedding to $\overrightarrow{p}$ for $\sigma_L(\overrightarrow{p})$, and taking the matrix norm yields the result.

We now consider the generalisation to $\mathcal{A}$. Considering an element $x = x_0 + ux_1 \in \mathcal{A}$ with $x_i \in L$, $i = 0, 1$, we let the canonical embedding extend coefficient-wise for $\sigma_{\mathcal{A}}(x) := (\sigma_L(x_0), \sigma_L(x_1))$ and find that

$$V_{\mathcal{A}} = \begin{pmatrix} V_f & \mathbf{0} \\ \mathbf{0} & V_f \end{pmatrix}$$

sends $\mathrm{coeff}(x) = (\mathrm{coeff}(x_0), \mathrm{coeff}(x_1))$ to $\sigma_{\mathcal{A}}(x)$. The matrix norm of $V_{\mathcal{A}}$ can then be computed, using the powerful basis, as $\sqrt{2}\|\sigma_L(\overrightarrow{p})\| = \sqrt{2n}$. This implies that the distortion when mapping between the two embeddings applied to CLWE samples is polynomially bounded in n, as required.