LWE from Non-commutative Group Rings

Qi Cheng[1], Jun Zhang[2], and Jincheng Zhuang[3,4]

[1] School of Computer Science, University of Oklahoma
Norman, OK 73019, USA.
Email: qcheng@ou.edu
[2] School of Mathematical Sciences, Capital Normal University
Beijing 100048, China
Email: junz@cnu.edu.cn
[3] Key Laboratory of Cryptologic Technology and Information Security
Ministry of Education, Shandong University
[4] School of Cyber Science and Technology, Shandong University
Qingdao 266237, China
Email: jzhuang@sdu.edu.cn

Abstract. The Learning-With-Errors (LWE) problem (and its variants including Ring-LWE and Module-LWE), whose security are based on hard ideal lattice problems, has proven to be a promising primitive with diverse applications in cryptography. For the sake of expanding sources for constructing LWE, we study the LWE problem on group rings in this work. One can regard the Ring-LWE on cyclotomic integers as a special case when the underlying group is cyclic, while our proposal utilizes non-commutative groups. In particular, we show how to build public key encryption schemes from dihedral group rings, while maintaining the efficiency of the Ring-LWE. We prove that the PKC system is semantically secure, by providing a reduction from the SIVP problem of group ring ideal lattice to the decisional group ring LWE problem. It turns out that irreducible representations of groups play important roles here. We believe that the introduction of the representation view point enriches the tool set for studying the Ring-LWE problem.

Keywords: Ring-LWE, Non-commutative group rings, Dihedral group rings
MSC 2010 Codes: 94A60, 16S34

1 Introduction

1.1 Lattice-based cryptography and the LWE problem

Lattice-based cryptography has attracted much attention recently. It has a few advantages over classical number theoretic cryptosystems such as RSA or Diffie-Hellman. First, it is widely believed to resist quantum attacks, in contrast to the traditional hard problems such as integer factorization, or discrete logarithms [40]. Second, it enjoys the worst case to the average case reduction, shown in the pioneering work of Ajtai [3]. Third, computation can be done on small numbers.

No large number exponentiations are needed, which tend to slow down the other public key cryptosystems. It does have a major drawback in key sizes. The NTRU cryptosystem [22] is the first successful cryptosystem based on lattices.

Regev [37] introduced the learning with errors (LWE) problem as a generalization of the classic learning parity with noise (LPN) problem. To be precise, let q be a prime, $\mathbf{s} \in \mathbb{F}_q^n$ be a fixed private vector, $\mathbf{a_i} \in \mathbb{F}_q^n, 1 \leq i \leq m$ be randomly chosen, $e_i \in \mathbb{F}_q, 1 \leq i \leq m$ be chosen independently according to an error distribution $\mathbb{F}_q \to \mathbb{R}^+$, which is a discrete Gaussian distribution that centers around 0 with width $qn^{-0.5-\epsilon}$, and $b_i = \langle \mathbf{a_i}, \mathbf{s} \rangle + e_i$. Given a list of pairs $(\mathbf{a}_i, b_i), 1 \leq i \leq m$, the LWE problem asks to solve for $\mathbf{s}$, and the LPN problem is the special case when $q = 2$.

Informally speaking, it is believed that LWE is hard in the sense that even though e_i tends to be small, when $\mathbf{s}$ is hidden, $(\mathbf{a_i}, b_i)$ can not be distinguished from a random vector in $\mathbb{F}_q^{n+1}$. In fact, Regev [37] proved the hardness for certain parameters q and error distributions by showing quantum reductions from approx-SVP and approx-SIVP problems for lattices. Later, Peikert [32] showed a classical reduction from approx-SVP to the LWE problem under more restrictive constraints.

For the sake of improving efficiency, Stehlé et al. [42] and Lyubashevsky et al. [25] proposed instantiating LWE instances from ideal lattices. Furthermore, they established the hardness of Ring-LWE by showing the reduction from a certain ideal lattice problem to the Ring-LWE problem via different approaches. The cryptography systems based on Ring-LWE are much more efficient in terms of key sizes and encryption and decryption complexity. However, the security of these systems is based on conjecturally hard problems on ideal lattices rather than on general lattices. Peikert et al. [34] managed to give to a quantum reduction from worst-case lattice problems directly to the decision version of Ring-LWE. Brakerski et al. [7]introduced Module-LWE , which interpolates between the standard LWE and Ring-LWE. Langlois and Stehlé [23] established that its hardness is at least as that of certain lattice problems restricted to module lattices. Albrecht and Deo [4] showed a reduction from Module-LWE to Ring-LWE with large modulus, Wang and Wang [44] established a reduction from decision Module-LWE to Ring-LWE. Peikert and Pepin [33] proposed a general framework that includes all known LWE variants over commutative base rings and gave a universe analysis of the reductions from Ring-LWE to other algebraic LWE variants.

The LWE problem, including its many variants, have proven to be versatile primitives for cryptographic purposes. Besides many other schemes, these applications include public key encryption schemes proposed by Regev [37], Peikert and Waters [35], Peikert [32], Lindner and Peikert [24], Stehlé and Steinfeld [41], Micciancio and Peikert [26]; digital signature schemes proposed by Gentry, Peikert, and Vaikuntanathan [20]; identity-based encryption (IBE) schemes proposed by Gentry, Peikert, and Vaikuntanathan [20], Cash et al. [10], Agrawal, Boneh, and Boyen [2, 1]; fully homomorphic encryption (FHE) schemes proposed by

Brakerski and Vaikuntanathan [8, 9], Brakerski, Gentry, and Vaikuntanathan [7], Fan and Vercauteren [18].

1.2 Our results

LWE from group rings The main contribution of the paper is to propose a general framework of generating LWE instances from group rings. In particular, we demonstrate our approach by generating LWE instances from dihedral group rings (GR-LWE for short). Recall that given a finite group $G = \{g_1, \ldots, g_n\}$ and a commutative ring R, the elements in the group ring $R[G]$ are formal sums

$$\sum_{i=1}^{n} r_i g_i, r_i \in R.$$

If $R = \mathbb{Z}$, and we provide a $\mathbb{Z}$-module homomorphism from $\mathbb{Z}[G]$ to $\mathbb{R}^n$ (otherwise known as an embedding), then (one-side) ideals in group rings naturally correspond to integral lattices. We can generalize LWE to the group ring setting. In particular, let n be a power of 2, D_{2n} be the dihedral group of order $2n$, and $\mathfrak{r} \in D_{2n}$ be an element that generates the cyclic subgroup of order n, then we should use the ring

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

which is also a free $\mathbb{Z}$-module of rank n. Note that $(\mathfrak{r}^{n/2}+1)\mathbb{Z}[D_{2n}]$ is a two-sided ideal, thus the quotient ring is well defined.

In Ring-LWE, there are two types of embeddings of rings of algebraic integers into Euclidean spaces: the canonical embedding used in [25] and the coefficient embedding used in [42]. When using the canonical embedding, multiplication is component-wise. This is the main reason that the work [25] preferred the canonical embedding. Note that the canonical embedding of cyclotomic integers is basically the combined map:

$$\mathbb{Z}[x]/(x^n + 1) \hookrightarrow \mathbb{C}[x]/(x^n + 1) \to \bigoplus_{0 \le k \le n, 2 \nmid k} \mathbb{C}[x]/(x - e^{2\pi\sqrt{-1}k/(2n)}),$$

where the first map is an inclusion, and the second one is an isomorphism. A component of the canonical embedding of $\mathbb{Z}[x]/(x^n + 1)$ corresponds to a group representation of the cyclic group $\langle x \rangle$ of order $2n$:

$$\rho_k(x^j) = e^{2\pi\sqrt{-1}kj/(2n)}, 2 \nmid k.$$

If a group is not commutative, we can use irreducible group representations to build an embedding of the group ring. However, some irreducible representations will have dimensions larger than one, thus multiplication in the group ring is still not component-wise. In this paper, we use coefficient embedding to make implementation simpler.

There are recent discoveries of faster SVP algorithms for principal ideal lattices, which generalize to non-principal ideal lattices. See [14, 15] and references

therein. To understand the attack, first observe that the ratio between two generators of a principal ideal is an integral unit. The main idea of the attacks comes from the Dirichlet unit theorem: the group of integral units in a number field is a direct product of a finite group with a free abelian group, whose generators are known as fundamental units. When taking logarithms of complex norms of their conjugates, the units are sent to the so-called log-unit lattice, whose SVP is not hard in many cases. In [28], the decomposition group is used to solve ideal SVP over random rational primes. Nevertheless, the Ring-LWE cryptosystems are not under direct threat, since lattice problems in ideal lattices form lower bounds for their security, and the approximation factors in the attack are too large.

The principal ideals from non-commutative integral group rings do not appear to suffer from the weakness directly, since multiplications of units may not commute [38].

Comparison with known instantiations

- Constructing LWE instances from group rings is more general framework than original Ring-LWE which restricts to algebraic number rings that are commutative. Indeed, the ring $R = \mathbb{Z}[x]/(x^n + 1)$, used in many Ring-LWE cryptosystems, is a direct summand of a group ring from C_{2n} (the cyclic group of order $2n$):

  $$\mathbb{Z}[C_{2n}] = \mathbb{Z}[x]/(x^{2n} - 1) \cong \mathbb{Z}[x]/(x^n + 1) \oplus \mathbb{Z}[x]/(x^n - 1)$$

  One should avoid using the ring $\mathbb{Z}[x]/(x^{2n} - 1)$, as the map

  $$\mathbb{Z}[x]/(x^{2n} - 1) \to \mathbb{Z}[x]/(x - 1)$$

  may leak secret information.
- The relations of GR-LWE with other generalizations of Ring-LWE including Module-LWE and multivariate Ring-LWE are discussed in Section 5.
- Using groups with only constant dimensional irreducible representations is important for our approach. If a group has high dimensional irreducible representations, then there is no efficient method to multiply two elements in the group ring. Furthermore, the coordinate separation technique [25, 34] will not work any more, and we do not know how to complete the proof of security.
- Even though rings of algebraic integers in number fields may not be principal ideal domains (PID), their reductions modulo primes are always principal ideal rings. The group ring $\mathbb{F}_p[G]$, however, is not necessarily a principal ideal ring if G is non-commutative (see, e.g., the main theorem in [19]). We believe that this property provides an extra protection against attacks.

Comparison of the security proof The proof of security adapts the steps in the case of Ring-LWE [34], which follows the framework of [37, 25]. In other words, we show a direct reduction from certain worst case lattice problems to average

case decision GR-LWE problem. Then the security of encryption scheme based on GR-LWE can be obtained. There are, however, a few important differences:

- Unlike the ring of algebraic integers in a number field, group rings have ideals that are not invertible. The security of GR-LWE should be based on lattice problems of invertible ideals.
- One of the main components is to study the distribution of the sum of a Gaussian e, with a product of a fixed short ring element s with another ring element a sampled from a discrete Gaussian. It is much harder to analyze than the commutative case, since when putting in matrix forms, a and s can not be simultaneously diagonalized. We have to rely on more general framework to overcome the difficulty. See Lemma 5 for details.
- It is known that in number fields, inverse ideals and dual lattices are closely related. In non-commutative group rings, it is not obvious. See Lemma 3 for details.
- In order to show the pseudorandomness of GR-LWE, we follow the general framework developed by [34]. However, the role of coordinates of canonical embedding [34] is taken place by eigenvalues of certain linear transformations. See Lemma 9 for details.

Other cryptosystems using non-commutative structures We note that there have been attempts to use non-commutative algebraic structures, especially the group structures, in designing cryptographical systems [27]. The approaches that relate closely to ours include using group rings to replace $(\mathbb{Z}/q\mathbb{Z})[x]/(x^n-1)$ in NTRU [45, 13, 43] and using the learning problem of non-commutative groups. The former approach has no security proof from lattice problems. The latter approach is not based on lattice problems. Grover et al. [21] proposed to generate LWE instances from cyclic algebras.

1.3 Paper organization

The paper is organized as follows. In Section 2, we review the mathematical background. In Section 3, we propose generating LWE instances from non-commutative group rings and establish a public key encryption scheme from dihedral group rings. We will not try to optimize the parameters in this paper, leaving it to future work. In Section 4, we establish the hardness of decisional group ring LWE problem, and show the security of the proposed PKE scheme. In Section 5, we discuss the relation of GR-LWE with other generalizations of Ring-LWE. In Section 6, we conclude the paper.

2 Mathematical preliminary

In this section, we review the mathematical background on lattices and group rings.

2.1 Lattices and related problem

Given a list of linearly independent column vectors $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{n \times n}$, the (full rank) *lattice* $\mathcal{L}(\mathbf{B})$ is the set

$$\mathcal{L}(\mathbf{B}) = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i \,|\, x_i \in \mathbb{Z} \right\}.$$

The *determinant* of the lattice is

$$\det(\mathcal{L}) := |\det(\mathbf{B})|.$$

The *minimum distance* of the lattice is

$$\lambda_1(\mathcal{L}) := \min_{0 \neq v \in \mathcal{L}} ||v||$$

where $||\cdot||$ is the Euclidean norm. The *dual lattice* is

$$\mathcal{L}^* := \{u \in \mathbb{R}^n \,|\, \forall v \in \mathcal{L}, \langle u, v \rangle \in \mathbb{Z}\}.$$

Definition 1. *Let $\mathcal{L} \in \mathbb{R}^n$ be a full rank lattice. The Shortest Vector Problem (SVP) is to find a vector $v \in \mathcal{L}$ such that*

$$||v|| = \lambda_1.$$

Given a target vector $t \in \mathbb{R}^n$, the Closest Vector Problem (CVP) is to find a vector $v \in \mathcal{L}$ such that

$$||v - t|| \leq ||v' - t||, \forall v' \in \mathcal{L}.$$

Definition 2. *Let $0 < \beta < 1/2$ be a constant, and $\mathcal{L}$ be a lattice. Let $y = x + e$ where $x \in \mathcal{L}$, and $||e|| < \beta\lambda_1(\mathcal{L})$. Given y, the β-BDD problem is to find x.*

Definition 3. *Let $0 < \beta < 1/2$ be a constant, and $\mathcal{L}$ be a lattice. Let $y = x + e$ where $x \in \mathcal{L}$, and $||e|| < \beta\lambda_1(\mathcal{L})$. Given y, the (q, β)-BDD problem is to find any x' such that $x \equiv x' \pmod{q\mathcal{L}}$.*

The β-BDD problem can be reduced to (q, β)-BDD problem. In fact, if $x - x' \in q\mathcal{L}$, then $(x - x')/q \in \mathcal{L}$. The distance between $(y - x')/q$ and $(x - x')/q$ is $||e/q||$. So we have a new BDD problem on the same lattice but with smaller error. Repeating the procedure will give us a BDD problem that can be solved by approx-CVP algorithms such as Babai's algorithm.

Definition 4 (Gaussian Distribution). *For any vector $c \in \mathbb{R}^n$ and positive definite matrix $\Sigma \in \mathbb{R}^{n \times n}$, the Gaussian distribution $\chi_{c,\Sigma}$ with mean vector c and covariance matrix $\frac{1}{2\pi}\Sigma$ is defined as*

$$\chi_{c,\Sigma}(x) = \frac{1}{\sqrt{\det \Sigma}} \exp(-\pi(x - c)^T \Sigma^{-1}(x - c)), \qquad \forall x \in \mathbb{R}^n.$$

In particular, if $c = 0$ is the origin and Σ is the diagonal matrix with diagonal entries $\alpha_1^2, \alpha_2^2, \cdots, \alpha_n^2$ (wlog, we always assume $\alpha_i > 0$ for any $i = 1, \cdots, n$), we denote $\chi_{c,\Sigma}$ by $\chi_{\alpha_1,\alpha_2,\cdots,\alpha_n}$. Moreover, if $\alpha_1 = \alpha_2 = \cdots = \alpha_n = \alpha$, denote $\chi_{\alpha_1,\alpha_2,\cdots,\alpha_n}$ by χ_α. Let $\Psi_{\leq\alpha}$ be the set of all the Gaussian distributions $\chi_{\alpha_1,\alpha_2,\cdots,\alpha_n}$ such that $\alpha_i \leq \alpha$ for all $1 \leq i \leq n$.

Definition 5 (Discrete Gaussian Distribution). *Let $S \subset \mathbb{R}^n$ be a discrete set. The discrete Gaussian distribution over S is defined by*

$$D_{S,r}(x) = \chi_r(x) / \sum_{x \in S} \chi_r(x).$$

The Discrete Gaussian Sampling problem $DGS_{\mathcal{L},r}$ problem is to sample lattice points of a lattice $\mathcal{L}$ according to $D_{\mathcal{L},r}$.

Definition 6 (General Discrete Gaussian Sampling). *For any non-degenerate matrix $A \in \mathbb{R}^{n\times n}$ and lattice $L \subset \mathbb{R}^n$, the general discrete Gaussian sampling problem is to give a sample from the lattice L according to the Gaussian distribution χ_{0,AA^T}. Denote the distribution by $D_{L,A}$ and the problem by $DGS_{L,A}$.*

Note that if we take $A = rI_n$ then

$$D_{L,A} = D_{L,r}.$$

Definition 7 (Smoothness condition). *Let $L \subset \mathbb{R}^n$ be a lattice and L^* be its dual. For any $\epsilon > 0$, the smoothing parameter $\eta_\epsilon(L)$ is defined to be the smallest s such that*

$$\sum_{y \in L^* \setminus \{0\}} \exp(-\pi s^2 y^T y) \leq \epsilon.$$

For any $A \in \mathbb{R}^{n\times n}$ we denote

$$A \geq \eta_\epsilon(L)$$

if

$$\sum_{y \in L^* \setminus \{0\}} \exp(-\pi y^T A A^T y) \leq \epsilon.$$

Note that for matrices $A = rI_n$, $A \geq \eta_\epsilon(L)$ is equivalent to $r \geq \eta_\epsilon(L)$.

2.2 Group representation

Representation theory is used to study abstract algebraic structures by connecting the objects and operations to linear transformations and their operations over vector spaces, which is well understood. Specifically, given a group G, a *representation* of G is a pair (V, φ) (V for short) such that V is a vector space and φ is a group homomorphism

$$\varphi : G \longrightarrow GL(V),$$

where $GL(V)$ is the group of linear transformations on V. If a linear subspace U of V is preserved by the action of G, ie. $\varphi(g)u \in U$ for any $g \in G, u \in U$, then U is called a *subrepresentation*. Every representation has two trivial subrepresentations: $\{0\}$ and V. If there is other non-trivial subrepresentations, then V is *reducible*. Otherwise, V is *irreducible*. For more information on group representation, we refer the reader to [39].

2.3 Dihedral groups and group rings

Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group of order n. The elements in group ring $R[G]$ are formal sums

$$\sum_{i=1}^{n} r_i g_i, r_i \in R.$$

Addition is defined by

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

Multiplication is defined by

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

If $R = \mathbb{Z}$, a (one-side) ideal of $\mathbb{Z}[G]$ is mapped to a lattice, under an embedding of $\mathbb{Z}[G]$ to $\mathbb{R}^n$. Here we use coefficient embedding, i.e. a group element is sent to a unit vector in $\mathbb{Z}^n$. The whole group ring $\mathbb{Z}[G]$ corresponds to $\mathbb{Z}^n$. Denote the length of a group ring element X in the Euclidean norm under the embedding by $||X||$. The following lemma shows that lengths of group ring elements behave nicely under multiplication.

Lemma 1. *Let $X, Y \in \mathbb{R}[G]$ be two elements. Then*

$$||XY|| \leq \sqrt{n}||X|| \cdot ||Y||$$

Proof. From Equation (1), the l_∞ norm of XY is less than $||X||||Y||$ by the Cauchy-Schwarz inequality.

Next, we introduce matrix norm of elements in the group ring $\mathbb{R}[G]$. For any element $\mathfrak{h} = \sum_{i=1}^{n} a_i g_i \in \mathbb{R}[G]$, by the multiplication law (1), it defines a linear transformation from $\mathbb{R}^n = \mathbb{R}[G]$ to itself, with transformation matrix denoted by $\mathcal{M}(\mathfrak{h})$. Indeed, it corresponds to the regular representation of the finite group G. Then we define the matrix-norm $|\mathfrak{h}|_{\text{Mat}}$ of $\mathfrak{h}$ to be the square root of the (spectral) norm of the matrix $\mathcal{M}(\mathfrak{h})\mathcal{M}(\mathfrak{h})^T$, i.e.,

$$|\mathfrak{h}|_{\text{Mat}} = \sqrt{\text{Norm}(\mathcal{M}(\mathfrak{h})\mathcal{M}(\mathfrak{h})^T)} = \sqrt{\text{Largest Eigenvalue of } \mathcal{M}(\mathfrak{h})\mathcal{M}(\mathfrak{h})^T}.$$

Remark 1. This definition should be the right definition for Ring-LWE under any given embedding. In particular, if the transformation matrix $\mathcal{M}$ is diagonal, then it reduces to the case ℓ_∞-norm used in the literature for the canonical embedding of number fields.

Let I be a right ideal, the left inverse of I is defined as

$$I^{-1} = \{x \in \mathbb{Q}[G] \mid \forall y \in I, xy \in \mathbb{Z}[G]\}$$

It can be verified that the left inverse is a left $\mathbb{Z}[G]$ module, and

$$I \subseteq \mathbb{Z}[G] \subseteq I^{-1}.$$

We call an ideal invertible if $I^{-1}I = \mathbb{Z}[G]$. If I is invertible, then I^{-1} is a left fractional ideal, namely, there is an integer t such that $tI^{-1} \subseteq \mathbb{Z}[G]$.

A dihedral group of order $2n$, denoted by D_{2n}, is the set

$$\{\mathfrak{r}^i\mathfrak{s}^j \mid 0 \le i \le n-1, 0 \le j \le 1\}$$

satisfying the relations

$$\mathfrak{r}^n = \mathfrak{s}^2 = 1, \mathfrak{s}\mathfrak{r}\mathfrak{s} = \mathfrak{r}^{-1}.$$

In some sense, the dihedral group is the non-commutative group that is the closest to the commutative one, since the dimension of any irreducible representation is bounded by 2, while commutative groups only have one-dimensional irreducible representations.

If n is even, there are $(n+6)/2$ irreducible representations for D_{2n}. Four of them are one-dimensional:

$$\rho_0(\mathfrak{r}^i) = 1, \rho_0(\mathfrak{s}\mathfrak{r}^j) = 1,$$
$$\rho_1(\mathfrak{r}^i) = 1, \rho_1(\mathfrak{s}\mathfrak{r}^j) = -1,$$
$$\rho_2(\mathfrak{r}^i) = (-1)^i, \rho_2(\mathfrak{s}\mathfrak{r}^j) = (-1)^j,$$
$$\rho_3(\mathfrak{r}^i) = (-1)^i, \rho_3(\mathfrak{s}\mathfrak{r}^j) = (-1)^{j+1}.$$

The rest are two-dimensional: for $4 \le k \le (n+4)/2$,

$$\rho_k(\mathfrak{r}^i) = \begin{pmatrix} e^{2\pi\sqrt{-1}i(k-3)/n} & 0 \\ 0 & e^{-2\pi\sqrt{-1}i(k-3)/n} \end{pmatrix},$$
$$\rho_k(\mathfrak{s}\mathfrak{r}^i) = \begin{pmatrix} 0 & e^{2\pi\sqrt{-1}i(k-3)/n} \\ e^{-2\pi\sqrt{-1}i(k-3)/n} & 0 \end{pmatrix}.$$

By the Artin-Wedderburn theorem, the group ring $\mathbb{C}[D_{2n}]$ can be decomposed into

$$\mathbb{C}[D_{2n}] \cong \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \bigoplus_{i=4}^{(n+4)/2} \mathbb{C}^{2\times 2},$$

where the first four copies of $\mathbb{C}$ correspond to $\rho_0, \rho_1, \rho_2, \rho_3$, the last $(n-2)/2$ copies of 2×2 matrix algebras corresponds to the two-dimensional representations ρ_i $(4 \le k \le (n+4)/2$).

2.4 Group ring LWE (GR-LWE)

To guarantee the hardness results of LWE based on the group ring of dihedral group, we need to study the matrix-norm of any element in $\mathbb{R}(D_{2n})$.

Lemma 2. *For any element* $\mathfrak{h} = f(\mathfrak{r}) + \mathfrak{s}g(\mathfrak{r}) \in \mathbb{R}[D_{2n}]$ *where*

$$f(x) = \sum_{i=0}^{n-1} a_i x^i \text{ and } g(x) = \sum_{i=0}^{n-1} b_i x^i$$

are two polynomials over $\mathbb{R}$*, the eigenvalues of the matrix* $\mathcal{M}(\mathfrak{h}) \cdot \mathcal{M}(\mathfrak{h})^T$ *are* $(|f(\xi^i)| \pm |g(\xi^i)|)^2$ *for* $i = 0, 1, \cdots, n-1$*, where* $\xi = e^{2\pi\sqrt{-1}/n}$ *is the* n*-th root of unity and* $|*|$ *is the complex norm. So the matrix-norm of* $\mathfrak{h}$ *is bounded from above by* $\max\{|f(\xi^i)| + |g(\xi^i)| \,|\, i = 0, 1, \cdots, n-1\}$.

Proof. Denote by Λ the following Fourier transformation matrix

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \xi & \xi^2 & \dots & \xi^{n-1} \\ 1 & \xi^2 & \xi^4 & \dots & \xi^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \xi^{n-1} & \xi^{2(n-1)} & \dots & \xi^{(n-1)^2} \end{pmatrix}.$$

Let $\mathbf{e}_i = \mathfrak{r}^{i-1}$ and $\mathbf{e}_{n+i} = \mathfrak{s}\mathfrak{r}^{i-1}$ for $i = 1, 2, \cdots, n$ be a normal basis for the vector space $\mathbb{C}[D_{2n}]$. Consider the base transformation matrix

$$\psi = \frac{1}{\sqrt{2n}} \begin{pmatrix} \Lambda & \sqrt{-1}\Lambda \\ \sqrt{-1}\Lambda & \Lambda \end{pmatrix}$$

and the new basis

$$(\mathbf{e}'_1, \mathbf{e}'_2, \cdots, \mathbf{e}'_{2n})^T = \psi^{-1}(\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_{2n})^T.$$

It is easy to check that ψ is unitary, i.e., $\psi \cdot \bar{\psi}^T = I_{2n}$. Under the basis $\mathbf{e}'_1, \mathbf{e}'_2, \cdots, \mathbf{e}'_{2n}$, the linear transformation of left-multiplication by $\mathfrak{h}$ has the following matrix form

$$\mathcal{M}(\mathfrak{h})' = \left(\begin{array}{cccc:cccc} f(1) & & & & \overline{g(1)} & & & \\ & f(\xi) & & & & \overline{g(\xi)} & & \\ & & \ddots & & & & \ddots & \\ & & & f(\xi^{n-1}) & & & & \overline{g(\xi^{n-1})} \\ \hdashline g(1) & & & & \overline{f(1)} & & & \\ & g(\xi) & & & & \overline{f(\xi)} & & \\ & & \ddots & & & & \ddots & \\ & & & g(\xi^{n-1}) & & & & \overline{f(\xi^{n-1})} \end{array}\right).$$

Since the transformation ψ is unitary, $\mathcal{M}(\mathfrak{h}) \cdot \mathcal{M}(\mathfrak{h})^T$ have the same eigenvalues as $\mathcal{M}(\mathfrak{h})' \cdot \overline{\mathcal{M}(\mathfrak{h})'}^T$. Indeed, as $\mathcal{M}(\mathfrak{h})$ is a real matrix, we have

$$\begin{aligned}\mathcal{M}(\mathfrak{h}) \cdot \mathcal{M}(\mathfrak{h})^T &= \mathcal{M}(\mathfrak{h}) \cdot \overline{\mathcal{M}(\mathfrak{h})}^T = (\psi \cdot \mathcal{M}(\mathfrak{h})' \cdot \psi^{-1}) \cdot \overline{(\psi \cdot \mathcal{M}(\mathfrak{h})' \cdot \psi^{-1})}^T \\ &= \psi \cdot \mathcal{M}(\mathfrak{h})' \cdot \psi^{-1} \cdot (\bar{\psi}^{-1})^T \cdot \overline{\mathcal{M}(\mathfrak{h})'}^T \cdot \bar{\psi}^T = \psi \cdot \mathcal{M}(\mathfrak{h})' \cdot \overline{\mathcal{M}(\mathfrak{h})'}^T \cdot \psi^{-1}.\end{aligned}$$

So eigenvalues of $\mathcal{M}(\mathfrak{h}) \cdot \mathcal{M}(\mathfrak{h})^T$ are the eigenvalues of the 2 by 2 submatrices

$$\begin{pmatrix} |f(\xi^i)|^2 + |g(\xi^i)|^2 & 2f(\xi^i)\overline{g(\xi^i)} \\ 2\overline{f(\xi^i)}g(\xi^i) & |f(\xi^i)|^2 + |g(\xi^i)|^2 \end{pmatrix},$$

for $i = 0, 1, \cdots, n-1$. Hence, eigenvalues of the matrix $\mathcal{M}(\mathfrak{h}) \cdot \mathcal{M}(\mathfrak{h})^T$ are $(|f(\xi^i)| \pm |g(\xi^i)|)^2$ for $i = 0, 1, \cdots, n-1$.

Given an invertible ideal of $\mathbb{Z}[D_{2n}]$, the following lemma establishes the close connection between *inverse ideal lattices* and *dual ideal lattices*.

Lemma 3. *For any invertible (right) ideal I of $\mathbb{Z}[D_{2n}]$, let I^{-1} be the left inverse of I. Let Λ and Λ^{-1} be the lattices defined by coefficients embedding of I and I^{-1} respectively. Then Λ^* and Λ^{-1} are the same under a permutation of coordinates.*

Proof. For any $(x_0, x_1, \cdots, x_{n-1}) \in \mathbb{Q}^n$, let

$$(z_0, z_1, \cdots, z_{n-1}) = (x_0, x_{n-1}, x_{n-2} \cdots, x_1).$$

We claim that

$$(x_0, x_1, \cdots, x_{n-1}, y_0, y_1, \cdots, y_{n-1}) \in \Lambda^{-1}$$

if and only if

$$(z_0, z_1, \cdots, z_{n-1}, y_0, y_1, \cdots, y_{n-1}) \in \Lambda^*.$$

And hence, we finish the proof.

On one hand, if $\sum_{i=0}^{n-1} x_i \mathfrak{r}^i + \sum_{j=0}^{n-1} y_j \mathfrak{s}\mathfrak{r}^j \in I^{-1}$, then

$$(\sum_{i=0}^{n-1} x_i \mathfrak{r}^i + \sum_{j=0}^{n-1} y_j \mathfrak{s}\mathfrak{r}^j)(\sum_{k=0}^{n-1} w_k \mathfrak{r}^k + \sum_{l=0}^{n-1} v_l \mathfrak{s}\mathfrak{r}^l) \in \mathbb{Z}[D_{2n}]$$

for any $\sum_{k=0}^{n-1} w_k \mathfrak{r}^k + \sum_{l=0}^{n-1} v_l \mathfrak{s}\mathfrak{r}^l \in I$. Expanding the product, this is equivalent to that for any $a, b = 0, 1, \cdots, n-1$,

$$\sum_{i=0}^{n-1} x_i w_{a-i \mod n} + \sum_{j=0}^{n-1} y_j v_{a+j \mod n} \in \mathbb{Z},$$

and

$$\sum_{i=0}^{n-1} x_i v_{b+i \mod n} + \sum_{j=0}^{n-1} y_j w_{b-j \mod n} \in \mathbb{Z}.$$

So $\sum_{i=0}^{n-1} x_i\mathfrak{r}^i+\sum_{j=0}^{n-1} y_j\mathfrak{s}\mathfrak{r}^j \in I^{-1}$ if and only if for any $\sum_{k=0}^{n-1} w_k\mathfrak{r}^k+\sum_{l=0}^{n-1} v_l\mathfrak{s}\mathfrak{r}^l \in I$ and for any $a, b = 0, 1, \cdots, n-1$,

$$\sum_{i=0}^{n-1} z_i w_{a+i \mod n} + \sum_{j=0}^{n-1} y_j v_{a+j \mod n} \in \mathbb{Z},$$

and

$$\sum_{i=0}^{n-1} z_i v_{b-i \mod n} + \sum_{j=0}^{n-1} y_j w_{b-j \mod n} \in \mathbb{Z}.$$

On the other hand, we have

$$(z_0, z_1, \cdots, z_{n-1}, y_0, y_1, \cdots, y_{n-1}) \in \Lambda^*$$

if and only if for any $\sum_{k=0}^{n-1} w_k\mathfrak{r}^k + \sum_{l=0}^{n-1} v_l\mathfrak{s}\mathfrak{r}^l \in I$,

$$\sum_{i=0}^{n-1} z_i w_i + \sum_{j=0}^{n-1} y_j v_j \in \mathbb{Z}.$$

Note that I is a right ideal of $\mathbb{Z}[D_{2n}]$, so for any $a, b = 0, 1, \cdots, n-1$,

$$(\sum_{k=0}^{n-1} w_k\mathfrak{r}^k + \sum_{l=0}^{n-1} v_l\mathfrak{s}\mathfrak{r}^l)\mathfrak{r}^{-a} = \sum_{k=0}^{n-1} w_{k+a \mod n}\mathfrak{r}^k + \sum_{l=0}^{n-1} v_{l+a \mod n}\mathfrak{s}\mathfrak{r}^l \in I$$

and

$$(\sum_{k=0}^{n-1} w_k\mathfrak{r}^k + \sum_{l=0}^{n-1} v_l\mathfrak{s}\mathfrak{r}^l)\mathfrak{s}\mathfrak{r}^b = \sum_{k=0}^{n-1} v_{b-k}\mathfrak{r}^k + \sum_{l=0}^{n-1} w_{b-l}\mathfrak{s}\mathfrak{r}^l \in I.$$

So we have

$$(z_0, z_1, \cdots, z_{n-1}, y_0, y_1, \cdots, y_{n-1}) \in \Lambda^*$$

if and only if for any $\sum_{k=0}^{n-1} w_k\mathfrak{r}^k + \sum_{l=0}^{n-1} v_l\mathfrak{s}\mathfrak{r}^l \in I$ for any $a, b = 0, 1, \cdots, n-1$,

$$\sum_{i=0}^{n-1} z_i w_{a+i \mod n} + \sum_{j=0}^{n-1} y_j v_{a+j \mod n} \in \mathbb{Z},$$

and

$$\sum_{i=0}^{n-1} z_i v_{b-i \mod n} + \sum_{j=0}^{n-1} y_j w_{b-j \mod n} \in \mathbb{Z}.$$

So the claim is proved.

In this paper we assume that n is a power of two, and let

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

which is also without one-dimensional component. Denote

$$\mathbf{R}_{\mathbb{R}} = \mathbf{R} \otimes_{\mathbb{Z}} \mathbb{R}$$

which is $\mathbb{R}^n$ under coefficients embedding, and let $\mathbb{T} = \mathbf{R}_{\mathbb{R}}/\mathbf{R}$.

Let q be an odd prime. Define

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

Definition 8 (Search $\mathbf{R}_q$-LWE). *The $\mathbf{R}_q$-LWE problem is to find the secret $s \in \mathbf{R}_q$, given a sequence of samples $(a_i, b_i) \in \mathbf{R}_q \times \mathbb{T}$, where a_i is selected uniformly and independently from $\mathbf{R}_q$, $b_i = (a_i s)/q + e_i \mod \mathbf{R}$, e_i is selected independently according to some fixed distribution $\chi \in \Psi_{\leq \alpha}$.*

Definition 9 (Decision $\mathbf{R}_q$-LWE). *The decision $\mathbf{R}_q$-LWE problem is to distinguish with non-negligible advantage between many independent samples from a $\mathbf{R}_q$-LWE instance, and the same number of uniformly random samples from $\mathbf{R}_q \times \mathbb{T}$.*

Remark 2. Not every ideal is invertible. For example, $1 + \mathfrak{s} \in \mathbf{R}$ generates an ideal that is not invertible. It is very important to have an ideal that is invertible in order to have hard lattice problems. In the later proof such as Lemma 9, we need dual lattices, which are essentially lattices corresponding to inverses of ideals by Lemma 3.

The following lemma characterises when an element in $\mathbf{R}$ is invertible in $\mathbf{R} \otimes \mathbb{Q}$, which will be used in the proof of Lemma 6 where we need the matrix A be invertible.

Lemma 4. *The element $\sum_{0 \leq i \leq (n/2)-1} a_i \mathfrak{r}^i + \sum_{0 \leq i \leq (n/2)-1} b_i \mathfrak{s}\mathfrak{r}^i \in \mathbf{R}$ is invertible in $\mathbf{R} \otimes \mathbb{Q}$ iff for all odd $1 \leq k \leq n/2$,*

$$\left| \sum_{0 \leq i \leq (n/2)-1} a_i e^{2\pi\sqrt{-1}ki/n} \right| - \left| \sum_{0 \leq i \leq (n/2)-1} b_i e^{2\pi\sqrt{-1}ki/n} \right| \neq 0,$$

where $|*|$ is the complex norm.

Proof. The criterion follows from Lemma 2.

Remark 3. Many attacks on the Ring-LWE (implicitly) exploits a one-dimensional representation that sends x to a small order element [11, 12, 16, 17], for example,

$$\mathbb{F}_q[x]/(f(x)) \to \mathbb{F}_q[x]/(x-1),$$

if $(x-1)|f(x)$ over $\mathbb{F}_q$.

For LWE samples instantiated from $\mathbb{F}_q[D_{2n}]$, one may also try to extract secret information by mapping variables to small order matrices, such as the following

$$\mathbb{Z}[D_{2n}] \to \mathbb{Z}^{2\times 2} : \mathfrak{r} \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \mathfrak{s} \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

However, this map is not well-defined on $\mathbb{Z}[D_{2n}]/(\mathfrak{r}^{n/2}+1)$.

Remark 4. To eliminate the influence of one-dimensional representations, one can also let n be a prime, and use the direct summand of the ring $\mathbb{Z}[D_{2n}]$:

$$\mathbb{Z}[D_{2n}]/((\mathfrak{r}^{n-1}+\mathfrak{r}^{n-2}+\cdots+1)\mathbb{Z}[D_{2n}]).$$

Note that $(\mathfrak{r}^{n-1}+\mathfrak{r}^{n-2}+\cdots+1)\mathbb{Z}[D_{2n}]$ is a two-sided ideal, so the above ring is well defined, and it can be regarded as a projection of $\mathbb{Z}[D_{2n}]$ to $\bigoplus_{i=2}^{(n+1)/2}\mathbb{C}^{2\times 2}$.

2.5 Oracle hidden center problem

In order to show the pseudorandom of GR-LWE detailed in Section 4, we follow the general framework developed in [34]. First recall the definition of the oracle hidden center problem.

Definition 10 ([34]). *Fix parameters $\varepsilon,\delta\in[0,1)$ and $\beta\geq 1$. An instance of $(\varepsilon,\delta,\beta)$-OHCP consists of a scale parameter $d>0$ and a randomized oracle $\mathcal{O}:\mathbb{R}^k\times\mathbb{R}_{\geq 0}\to\{0,1\}$ such that*

$$Pr(\mathcal{O}(\boldsymbol{z},t)=1)=p(t+\log||\boldsymbol{z}-\boldsymbol{z}^*||),$$

where $\boldsymbol{z}^*\in\mathbb{R}^k$ is an unknown center with $\delta d\leq||\boldsymbol{z}^*||\leq d$, $\boldsymbol{z}\in\mathbb{R}^k$ satisfies $||\boldsymbol{z}-\boldsymbol{z}^*||\leq\beta d$, $t\in\mathbb{R}_{\geq 0}$, and $p(\cdot)$ is an unknown function. The goal of the OHCP problem is to output $\hat{\boldsymbol{z}}\in\mathbb{R}^k$ which approximates $\boldsymbol{z}^*$ such that $||\hat{\boldsymbol{z}}-\boldsymbol{z}^*||\leq\epsilon d$.

Peikert *et al.* [34] give an efficient algorithm solving the OHCP problem assuming certain properties are satisfied as follows.

Proposition 1 ([34]). *There exists a poly(κ,k) algorithm that takes a confidence parameter $\kappa\geq 20\log(k+1)$, the scale parameter $d>0$, and solves $(\exp(-\kappa),\exp(-\kappa),1+1/\kappa)$-OHCP in dimension k with probability greater than $1-\exp(-\kappa)$, assuming the oracle $\mathcal{O}$ corresponding to the OHCP instance satisfies the following conditions. For some $p_\infty\in[0,1]$ and $s^*\geq 0$,*

1. *$p(s^*)-p_\infty\geq 1/\kappa$;*
2. *$|p(s)-p_\infty|\leq 2\exp(-s/\kappa)$ for any $s\geq 0$;*
3. *$\forall\ s_1,s_2\geq 0$, p satisfies $|p(s_1)-p(s_2)|\leq\kappa|s_1-s_2|$.*

Informally, the algorithm takes a "guarded random walk" towards the hidden center $\mathbf{z}^*$ with the aid of the oracle.

3 PKC from dihedral group rings

In this section, we describe a cryptosystem based on the dihedral group ring. The protocol is identical to one based on the ideal lattice, except that since multiplication is not commutative, one needs to pay attention to the order of multiplication. The discretization $\bar{\chi}:\mathbb{Z}/q\mathbb{Z}\to\mathbb{R}$ of a Gaussian χ on $\mathbb{R}$ can be done as follows. First, reduce χ by modulo $\mathbb{Z}$ to obtain a distribution $\chi \mod \mathbb{Z}$

on $[0,1)$. Then divide $[0,1)$ into q parts $[1-1/2q,1)\cup[0,1/2q)$, $[1/2q,3/2q)$, $\cdots$, $[1-3/2q,1-1/2q)$, and integrate the distribution ($\chi \mod \mathbb{Z}$) on each part to define $\bar{\chi}(0),\bar{\chi}(1),\cdots,\bar{\chi}(q-1)$.

Let n be a power of two, let q be an odd prime, and $q\in[n^2,2n^2]$. Recall

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

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

$$\mathbf{R}_q=\mathbb{F}_q[D_{2n}]/((\mathfrak{r}^{n/2}+1)\mathbb{F}_q[D_{2n}]),$$

and the error distribution $\bar{\chi}$ on $\mathbf{R}_q$ is to select coefficients independently according to the discretization of a Gaussian of width $\tilde{O}(1/\sqrt{n})$.

- **Private key:** The private key is $s,e\in\mathbf{R}_q$ from the error distribution.
- **Public key:** Select a random $a\in\mathbf{R}_q$ uniformly. Output $(a,b)\in\mathbf{R}_q^2$, where $b=sa+e$.
- **Encryption:** To encrypt a bit string z of length n, we view it as an element in $\mathbf{R}_q$ so that bits in z become coefficients of a polynomial. The cipher-text is (u,v) obtained by

  $$u=ar+e_1, v=br+e_2+\lfloor q/2\rfloor z,$$

  where r,e_1,e_2 are chosen from an error distribution.
- **Decryption:** For cipher-text (u,v), one computes $v-su$, which equals

  $$(er-se_1+e_2)+\lfloor q/2\rfloor z.$$

  One can read z from $v-su$, since r,s,e,e_1 and e_2 have small coefficients.

One can verify that the public and private key sizes are linear in the security level, and the ciphertext expansion is almost a constant. The following theorem shows that the encryption/decryption complexity is logarithmic per bit.

Theorem 1. *The multiplication in $(\mathbb{Z}/q\mathbb{Z})[D_{2n}]$ can be done in $\tilde{O}(n\log q)$ time.*

In this theorem, we use the whole group ring for generality. One can check that it applies to $\mathbf{R}$ as well.

Proof. The main idea is to separate the terms in $(\mathbb{Z}/q\mathbb{Z})[D_{2n}]$ into two parts. Let $f_1+\mathfrak{s}f_2$ and $f_3+\mathfrak{s}f_4$ be two elements where f_1,f_2,f_3 and f_4 are polynomials in $\mathfrak{r}$. We have

$$\begin{aligned}&(f_1+\mathfrak{s}f_2)(f_3+\mathfrak{s}f_4)\\ =&f_1f_3+\mathfrak{s}f_2f_3+f_1\mathfrak{s}f_4+\mathfrak{s}f_2\mathfrak{s}f_4\\ =&f_1f_3+\mathfrak{s}f_2f_3+\mathfrak{s}(\mathfrak{s}f_1\mathfrak{s})f_4+(\mathfrak{s}f_2\mathfrak{s})f_4\\ =&(f_1f_3+(\mathfrak{s}f_2\mathfrak{s})f_4)+\mathfrak{s}(f_2f_3+(\mathfrak{s}f_1\mathfrak{s})f_4)\end{aligned}$$

where $\mathfrak{s}f_1\mathfrak{s}$ and $\mathfrak{s}f_2\mathfrak{s}$ are polynomials in $\mathfrak{r}$ that can be calculated in linear time. To find the product, we need to compute four polynomial multiplications in $(\mathbb{Z}/q\mathbb{Z})[\mathfrak{r}]$, that can be done in time $\tilde{O}(n\log q)$.

In the *normal version* of GR-LWE, s and e are both selected according to error distribution, while in the regular version, only e is selected according to error distribution. The following theorem shows that these two versions are equivalent.

Theorem 2. *The regular version of dihedral GR-LWE can be reduced to the normal version of dihedral GR-LWE.*

Proof. Suppose that the input of the LWE problem is (a_1, b_1) and (a_2, b_2). With high probability, a_1 is invertible, we construct the input for normal version of LWE as

$$(a_2 a_1^{-1}, a_2 a_1^{-1} b_1 - b_2).$$

Note that

$$a_2 a_1^{-1} b_1 - b_2 = a_2 a_1^{-1}(a_1 s + e_1) - (a_2 s + e_2) = a_2 a_1^{-1} e_1 - e_2.$$

Theorem 3. *The encryption scheme is semantic secure assuming the pseudo-randomness of the underlying LWE.*

The proof is essentially the same as that of [25]. Next, we show the pseudo-randomness of the underlying LWE.

4 Pseudo-randomness of GR-LWE

4.1 Main theorem

In this section, we prove the main theorem as follows.

Theorem 4. *Let $\alpha = \alpha(n) \in (0, 1)$, and let $q = q(n)$ be a prime such that $\alpha q \geq \sqrt{n}\omega(\sqrt{\log n})$. Given an average case of decision version of dihedral GR-LWE$_{q,\Psi_{\leq\alpha}}$ oracle with error distributions $\Psi_{\leq\alpha}$, there is a quantum polynomial time algorithm that solves the search version of the SIVP problem for any invertible ideal I of $\mathbf{R}, q \nmid \det(I)$ with approximate factor $\tilde{O}(n/\alpha)$.*

Proof. The proof is adapted from [34], which follows the framework of [36, 25]. The reduction is a repeat of a core reduction step, which is a combination of two parts. Roughly speaking, the first part of iteration is classic algorithm that solves BDD given decision GR-LWE oracle and samples from discrete Gaussian samples with wider width; the second part of iteration is a quantum algorithm that generates Gaussian samples with smaller width based on the first part.

It is from Lemmas 9 and 11 that with dihedral GR-LWE$_{q,\Psi_{\leq\alpha}}$ oracle one can sample a discrete Gaussian on the ideal I of width $\lambda_n\sqrt{n}\omega(\log n)/\alpha$, starting with a sufficiently large value of width $r \geq 2^{2n}\lambda_n(I)$ where any polynomial number of samples can be generated classically [37]. A sample from the discrete Gaussian has the Euclidean length at most $\sqrt{n} \cdot \lambda_n(I)\sqrt{n}\omega(\log n)/\alpha$ with an overwhelming probability. So the sample solves the search version of the SVP problem for the ideal I with approximate factor $\tilde{O}(n/\alpha)$.

4.2 The error distribution and smoothness condition

The precise error distribution in the definition of Ring-LWE to ensure the hardness result is one important issue. In [25], the authors generalized one dimensional Gaussian error distribution in plain-LWE [37] to n-dimensional (elliptical) Gaussian which is described by an $n \times n$-covariance matrix. However, in [25] they chose the canonical embedding which makes the Gaussian error distributions during the reduction always diagonal. In our case, the error distributions in the reduction do not appear as diagonal any more. Thus, we need to consider a more general setting as follows.

Lemma 5. *Let L be a lattice, let $u \in \mathbb{R}^n$ be a vector, let $r, s > 0$ be two reals, let $A, B \in \mathbb{R}^{n\times n}$ be two non-singular matrices. Assume that smoothness property $\sum_{y\in L^*\setminus\{0\}} \exp(-\pi y^T(A^{-T}A^{-1} + \frac{1}{s^2}B^TB)^{-1}y) \leq \epsilon$ holds for some ϵ. The distribution of $Bv + e$ where v is distributed according to $D_{L+u,A}$ and e is the n dimensional Gaussian multivariable with mean vector 0 and diagonal covariance matrix $\frac{s^2}{2\pi}I_n$ is within statistical distance 4ϵ of a Gaussian multivariable with mean vector 0 and covariance matrix $\frac{1}{2\pi}BAA^TB^T + \frac{s^2}{2\pi}I_n$.*

Proof. Let $Y = v + B^{-1}e$. Using linear algebra and Poisson summation formula, one can compute the distribution of Y is

$$Y(x) = \frac{\exp(-\pi x^T\Sigma^{-1}x)}{\det(\Sigma)^{1/2}} \frac{\sum_{y\in L^*} e^{-2\pi\sqrt{-1}\langle c_0,y\rangle} \exp(-\pi y^T(A^{-T}A^{-1} + \frac{1}{s^2}B^TB)^{-1}y)}{\sum_{y\in L^*} e^{2\pi\sqrt{-1}\langle u,y\rangle} \exp(-\pi y^TAA^Ty)}$$

where $\Sigma = AA^T + s^2B^{-1}B^{-T}$ and c_0 is a certain vector computed from u and x, explicitly,

$$c_0 = u - (A^TA + \frac{1}{s^2}B^TB)^{-T}\frac{1}{s^2}B^TBx.$$

Since we have

$$\begin{aligned}
&|1 - \sum_{y\in L^*} e^{-2\pi\sqrt{-1}\langle c_0,y\rangle} \exp(-\pi y^T(A^{-T}A^{-1} + \frac{1}{s^2}B^TB)^{-1}y)| \\
\leq &\sum_{y\in L^*\setminus\{0\}} \exp(-\pi y^T(A^{-T}A^{-1} + \frac{1}{s^2}B^TB)^{-1}y) \\
\leq &\epsilon,
\end{aligned}$$

and

$$\begin{aligned}
&|1 - \sum_{y\in L^*} e^{2\pi\sqrt{-1}\langle u,y\rangle} \exp(-\pi y^TAA^Ty)| \\
\leq &|\sum_{y\in L^*\setminus\{0\}} \exp(-\pi y^TAA^Ty)| \\
\leq &\sum_{y\in L^*\setminus\{0\}} \exp(-\pi y^T(A^{-T}A^{-1} + \frac{1}{s^2}B^TB)^{-1}y) \\
\leq &\epsilon,
\end{aligned}$$

we deduce

$$|Y(x) - \frac{1}{\det(\Sigma)^{1/2}} \exp(-\pi x^T \Sigma^{-1} x)| \leq 4\epsilon \frac{\exp(-\pi x^T \Sigma^{-1} x)}{\det(\Sigma)^{1/2}}.$$

So by integrating over $\mathbb{R}^n$, the statistical distance between $Y = v + B^{-1}e$ and the Gaussian distribution $\frac{1}{\det(\Sigma)^{n/2}} \exp(-\pi x^T \Sigma^{-1} x)$ is at most 4ϵ. Finally, since non-singular linear transformation of multivariable Gaussian is still Gaussian, $Bv + e = BY$ has statistical distance at most 4ϵ with the Gaussian distribution with mean vector 0 and covariance matrix

$$\frac{1}{2\pi} B\Sigma B^T = \frac{1}{2\pi}(BAA^T B^T + s^2 I_n).$$

Applying the above lemma to the group ring considered in this paper, together with Lemma 2, the following corollary is immediate.

Corollary 1. *Let Λ be the ideal lattice obtained by coefficients embedding of $I \subset \mathbf{R}$ to $\mathbb{R}^n$. Let $\mathfrak{h} = f(\mathfrak{r}) + \mathfrak{s}g(\mathfrak{r}) \in \mathbf{R}_{\mathbb{R}}$ for some polynomials of degree at most $\frac{n}{2} - 1$ over $\mathbb{R}$, and let $\lambda = |\mathfrak{h}|_{\mathrm{Mat}}$. Let $r, s > 0$ be two reals, denote $t = 1/\sqrt{\frac{1}{r^2} + \frac{\lambda^2}{s^2}}$. Assume that smoothness property $\sum_{y \in L^* \setminus \{0\}} \exp(-\pi t^2 ||y||^2) \leq \epsilon$ holds for some ϵ. The distribution of $\mathfrak{h}v + e$ where v is distributed according to $D_{\Lambda + u, r}$ and e is the n dimensional Gaussian multivariable with mean vector 0 and diagonal covariance matrix $\frac{s^2}{2\pi} I_n$ is within statistical distance 4ϵ of a Gaussian multivariable that is equivalent to the diagonal Gaussian*

$$\prod_i \chi_{\sqrt{r^2(|f(\xi^i)| + |g(\xi^i)|)^2 + s^2}} \times \prod_i \chi_{\sqrt{r^2(|f(\xi^i)| - |g(\xi^i)|)^2 + s^2}}$$

up to certain unitary base change.

Remark 5. If we take matrices A, B to be matrix-representatives of two elements in the group ring via the left multiplication, saying

$$A = \mathcal{M}(r_1(\mathfrak{r}) + \mathfrak{s}r_2(\mathfrak{r})),\ B = \mathcal{M}(f_1(\mathfrak{r}) + \mathfrak{s}f_2(\mathfrak{r})),$$

then

$$BA = \mathcal{M}((f_1(\mathfrak{r})r_1(\mathfrak{r}) + f_2(\mathfrak{r}^{-1})r_2(\mathfrak{r})) + \mathfrak{s}(f_2(\mathfrak{r})r_1(\mathfrak{r}) + f_1(\mathfrak{r}^{-1})r_2(\mathfrak{r}))).$$

By Lemma 2, the matrix $BAA^T B^T$ has eigenvalues

$$(|(f_1(\xi^i)r_1(\xi^i) + f_2(\bar{\xi^i})r_2(\xi^i))| \pm |(f_2(\xi^i)r_1(\xi^i) + f_1(\bar{\xi^i})r_2(\xi^i))|)^2.$$

In particular, let $r_2 = 0$, then the matrix $BAA^T B^T$ has eigenvalues

$$|r_1(\xi^i)|^2(|f_1(\xi^i) \pm f_2(\xi^i)|)^2,\ i = 1, 3, 5, \cdots, n-1.$$

As with Lemma 6.9 in [34], which is the critical ingredient in the proof of pseudorandomness of Ring-LWE for number fields, we have the following result.

Lemma 6 (Large $\prod_i |r_1(\xi^i)|$ implies smoothness.). *Let $r(x) \in \mathbb{R}[x]$ be any polynomial of degree $\leq n/2-1$, and let*

$$c = \left(\prod_{i=1}^{n/2} (r/\sqrt{n})(\xi^{2i-1})\right)^{2/n} \geq 1.$$

Then the matrix $A = \mathcal{M}(r(\mathfrak{r}))$ satisfies the smoothness condition

$$A \geq \eta_\epsilon(\mathbf{R}),$$

where $\epsilon = \exp(-c^2 n)$.

Proof. By the criterion described in Lemma 4, $r(\mathfrak{r})$ is invertible, which implies A^{-1} exists. By [5, Lemma 1.5],

$$\eta_\epsilon(A^{-1}\mathbf{R}) \leq c\sqrt{n}/\lambda_1((A^{-1}\mathbf{R})^*),$$

where $\lambda_1((A^{-T}\mathbf{R})^*)$ is the length of the shortest vector in the dual lattice

$$(A^{-1}\mathbf{R})^* = A^T\mathbb{Z}^n.$$

Note that the lattice $A^T\mathbb{Z}^n$ is the concatenation of the lattices corresponding to $r(x)\mathbb{Z}[x]/(x^{n/2}+1)$ and $r(x^{n-1})\mathbb{Z}[x]/(x^{n/2}+1)$ respectively (under coefficient embedding). For any $f(x) = \sum_{i=0}^{n/2-1} f_i x^i \in \mathbb{R}[x]$, it is easy to see that

$$||f||_2^2 = \sum_{i=0}^{n/2-1} f_i^2 = \sum_{i=1}^{n/2} |(f/\sqrt{n/2})(\xi^{2i-1})|^2.$$

So for any $g(x) \in \mathbb{Z}[x]$ has degree $\leq n/2-1$, let $f(x) = r(x)g(x)$, we have

$$||f||_2^2 = \sum_{i=1}^{n/2} |(r/\sqrt{n/2})(\xi^{2i-1})g(\xi^{2i-1})|^2 \geq c^2 n \prod_{i=1}^{n/2} |g(\xi^{2i-1})|^2 \geq c^2 n.$$

By the same reason, for any $g(x) \in \mathbb{Z}[x]$ has degree $\leq n/2-1$, we have

$$||r(x^{n-1})g(x)||_2^2 \geq c^2 n.$$

Putting them together, we get

$$\lambda_1((A^{-1}\mathbf{R})^*) \geq c\sqrt{n}.$$

So

$$\eta_\epsilon(A^{-1}\mathbf{R}) \leq c\sqrt{n}/\lambda_1((A^{-1}\mathbf{R})^*) \leq 1.$$

And hence,

$$A \geq \eta_\epsilon(\mathbf{R}).$$

4.3 First part of iteration

We first define an explicit set of polynomials which will be used later to define certain discrete Gaussian distribution.

Definition 11. *For $r > 0, \iota > 0$, and $T \geq 1$, define $W_{r,\iota,T}$ to be the set of polynomials $r^{i,j}(x) = \sum_{k=0}^{n/2-1} r_k^{i,j} x^k$ with $i = 1, \cdots, n/4$, $j = 0, 1, \cdots, T$, and coefficients*

$$r_0^{i,j} = \sqrt{n} r \left(n/2 + 2(1+\iota)^j - 2\right)$$

and

$$r_k^{i,j} = \sqrt{n} r \left(2(1+\iota)^j - 2\right) \cos \frac{(2i-1)j}{n} \pi \qquad k = 1, 2, \cdots, n/2 - 1.$$

A simple lemma, connecting polynomials in $W_{r,\iota,T}$ and eigenvalues of the corresponding action on the ideal lattice, is the following.

Lemma 7. *Let $\xi = e^{\frac{2\pi\sqrt{-1}}{n}}$. For any polynomial $r^{i,j}(x) = \sum_{k=0}^{n/2-1} r_k^{i,j} x^k \in W_{r,\iota,T}$, the evaluations of $r^{i,j}(x)$ at ξ^k, $k = 1, 3, 5, \cdots, n-1$ are*

$$r^{i,j}(\xi^k) = \sqrt{n} r, \qquad \forall k \neq 2i-1,\ n-2i+1,$$

and

$$r^{i,j}(\xi^{2i-1}) = r^{i,j}(\xi^{n-2i+1}) = \sqrt{n} r (1+\iota)^j.$$

Let I be an invertible ideal of $\mathbb{Z}[D_{2n}]$ with left inverse I^{-1}. Under coefficient embedding, denote by Λ and Λ^{-1} the corresponding lattices of I and I^{-1}. By Lemma 3, the dual lattice Λ^* and Λ^{-1} are essentially the same. Next we show how to generate near GR-LWE distribution combining $BDD_{I^{-1},d}$ instances and $D_{I,r}$ instances.

Lemma 8. *There is an efficient algorithm that takes an input an invertible ideal I of $\mathbf{R}$, an integer $q \geq 2, q \nmid \det(I)$, a coset $e + I^{-1}$, where e has matrix norm $\leq \alpha q/\sqrt{2} r$, and samples from $D_{I,r}$, $r > 0$ such that*

$$\sum_{y \in I^{-1} \setminus \{0\}} \exp\left(-\pi \frac{r^2}{2q^2} ||y||^2\right) \leq \epsilon.$$

It outputs samples that are within negligible statistical distance of $GR{-}LWE_{q,\leq\Psi_\alpha}$.

Proof. Suppose $y = x + e$, where $e = f(\mathfrak{r}) + \mathfrak{s} g(\mathfrak{r})$. We sample a $v \in I$ according to the Gaussian distribution $D_{I,r}$, and let $a = \phi_1(v) \pmod{q\mathbf{R}} \in \mathbf{R}/(q\mathbf{R})$, where ϕ_1 is the inclusion $I \to \mathbf{R}$, which is also a left $\mathbf{R}$-module homomorphism. Note that $q\mathbf{R}$ is a two-sided ideal, $\mathbf{R}/q\mathbf{R}$ is a direct summand of the ring $\mathbb{F}_q[D_{2n}]$. Since $\det(I)$ is not divisible by q, ϕ_1 induces a natural left $\mathbf{R}$-module surjective homomorphism $I \to \mathbf{R}/(q\mathbf{R})$. We then calculate $b = yv + e'$ (in $\mathbf{R}_\mathbb{R}$), where e' is a Gaussian $\chi_{\alpha/\sqrt{2}}$ on $\mathbf{R}_\mathbb{R}$. We have $b = xv + ev + e' \pmod{q\mathbf{R}}$, where $xv \in \mathbf{R}$ and the distribution of $ev + e'$ has statistic distance within 4ϵ to the Gaussian $\prod_i \chi_{\sqrt{(r/q)^2(|f(\xi^i)|+|g(\xi^i)|)^2+(\alpha/\sqrt{2})^2}} \times \prod_i \chi_{\sqrt{(r/q)^2(|f(\xi^i)|-|g(\xi^i)|)^2+(\alpha/\sqrt{2})^2}}$ by Corollary 1.

Lemma 9 (Reduction from BDD to Decisional GR-LWE). *There is a probabilistic polynomial time algorithm that given an oracle that solves decisional GR-LWE and input a number $\alpha = \alpha(n) \in (0,1)$, a right ideal $I \subset \mathbf{R}$, and a prime $q = q(n)$, $q \nmid \det(I)$, an integer $r > 0$ such that*

$$\sum_{y \in I^{-1} \setminus \{0\}} \exp\left(-\pi \frac{r^2}{2q^2} ||y||^2\right) \leq \epsilon$$

for some negligible $\epsilon = \epsilon(n)$, and polynomially many samples from the discrete Gaussian distribution $D_{L,A}$ where A are the matrix representations of elements in $W_{r,\iota,T}$ (for some $\iota = 1/\mathrm{poly}(n)$ and $T = \mathrm{poly}(n)$, see Definition 11), solves $BDD_{I^{-1},\alpha q/\sqrt{2}r}$ in the matrix norm.

Proof. We adapt the OHCP framework [34] to proceed the reduction. Suppose $y = x + e \in e + I^{-1}$, where $e = e_1(\mathfrak{r}) + \mathfrak{s}e_2(\mathfrak{r})$ is the error. The goal is to recover e.

We will show how to use decisional GR-LWE to decode the $e^+ = e_1 + e_2$ and $e^- = e_1 - e_2$ respectively, from which we can recover e_1 and e_2. To this end, we will use the OHCP framework and obtain values of $e^+(\xi_i)$, $e^-(\xi_i)$ and recover e^+, e^-. Recall that in the algebraic ring case [34], such values are exactly the coordinates under canonical embedding.

However, our situation is essentially different. In our setting, these values are related to certain eigenvalues. Recall from Remark 5, if we take matrices A, B to be matrix-representatives of perturbation element and e in the group ring via the left multiplication, saying

$$A = \mathcal{M}(s_1(\mathfrak{r}) + \mathfrak{s}s_2(\mathfrak{r})),\ B = \mathcal{M}(e_1(\mathfrak{r}) + \mathfrak{s}e_2(\mathfrak{r})),$$

then the matrix BAA^TB^T has eigenvalues

$$(|(e_1(\xi^i)s_1(\xi^i) + e_2(\bar{\xi}^i)s_2(\xi^i))| \pm |(e_2(\xi^i)s_1(\xi^i) + e_1(\bar{\xi}^i)s_2(\xi^i))|)^2.$$

In particular, let $s_2 = 0$, then the matrix BAA^TB^T has eigenvalues

$$|s_1(\xi^i)|^2(|e_1(\xi^i) \pm e_2(\xi^i)|)^2,\ i = 1, 3, 5, \cdots, n-1.$$

From the above conclusion, when solving the OHCP problem using the GR-LWE oracle, we can choose the perturbation $s_1(\mathfrak{r}) + \mathfrak{s}s_2(\mathfrak{r})$ such that $s_2 = 0$, which allows us to decode e^+ and e^-.

The following explains how to compute e^+, which proceeds closely with the proof of Lemma 6.6 in [34]. The computation of e^- is similar. For the sake of completeness, we include the proof here.

If $\alpha < \exp(-n)$, then the error length is small enough such that the problem can be solved efficiently using Babai's algorithm. So we assume $\alpha > \exp(-n)$. Let $\kappa = poly(n)$ with $\kappa \geq 100n^2\ell$ be parameters such that the advantage of GR-LWE oracle is at least $2/\kappa$, where ℓ is the number of samples required by the oracle.

The reduction will use the decisional GR-LWE oracle to simulate oracles

$$\mathcal{O}_i : \mathbb{C} \times \mathbb{R}_{\geq 0} \to \{0,1\},\ 1 \leq i \leq n/2$$

such that the probability that $\mathcal{O}_i(z,t)$ outputs 1 only depends on $\exp(t)|z - \sigma_i(e^+)|$ (for $z \in \mathbb{C}$, where $\sigma_i(e^+) = e^+(\xi^i)$, $\xi = e^{2\pi\sqrt{-1}/n}$ with $|z - \sigma_i(e^+)|$ small enough). Equivalently, $\mathcal{O}_i$ is an oracle with a hidden center $\sigma_i(e^+)$ as in the definition of OHCP, with $k = 2$ for $1 \leq i \leq n/2$. Then we will use Proposition 1 to find good approximations to $e^+(\xi^i)$ and recover e^+ by the Lagrange interpolation.

For this purpose, define $k_i : \mathbb{C} \to \mathbf{R}_{\mathbb{R}}, 1 \leq i \leq n/2$ as $k_i(z) = \sigma^{-1}(z \cdot \mathbf{e}_i + \bar{z} \cdot \mathbf{e}_{i+n/2})$ where $\mathbf{e}_i$ has 1 in the ith coordinate and 0 otherwise and $\sigma(a) = (\sigma_1(a), \ldots, \sigma_n(a))$. On input (z,t), the oracle $\mathcal{O}_i$ uses fresh samples from $D_{I,\sigma(r^{i,j})}$, where $(1+\iota)^j = \exp(t)$. Then it performs the transformation from Lemma 8 on these samples, the coset $e^+ - k_i(z) + I^{-1}$, parameter r, and distance bound $\omega(\sqrt{\log n})\alpha q/(\sqrt{2}r)$. Let $A_{i,z,t}$ be the output samples. Then $\mathcal{O}_i$ calls the GR-LWE oracle on $A_{i,z,t}$ and outputs 1 if and only if it accepts.

Then the reduction runs the algorithm from Proposition 1 for each $i = 1, 2, \cdots, n/2$, with oracle $\mathcal{O}_i$, confidence parameter κ, and distance bound $d' = d/(1 + 1/\kappa)$, and outputs some approximation z_i to the oracle's center. Finally, the reduction runs Babai's algorithm on the coset $e^+ - \sum k_i(z_i) + \Lambda(I)^*$, receiving as output $\hat{e}^+$, and returns $\hat{e}^+ + \sum k_i(z_i)$ as output.

The running time of the reduction essentially depends on Proposition 1, which is polynomial. Assuming the z_i are valid solutions to $(\exp(-\kappa), \exp(-\kappa), 1+1/\kappa)$-OHCP with hidden center $\sigma_i(e^+)$, we check that the output is correct. Since z_i are valid solutions, we have

$$|z_i - \sigma_i(e^+)| \leq \exp(-\kappa)d' \leq 2^{-n}\lambda_1(I^{-1})/\sqrt{n}.$$

Thus $||e^+ - \sum k_i(z_i)|| \leq 2^{-n}\lambda_1(I^{-1})$, and Babai's algorithm will return exactly $\hat{e}^+ = e^+ - \sum k_i(z_i)$. Therefore, the reduction returns the correct answer.

Finally, we need to check that, with non-negligible probability over the choice of e^+, for all i:

1. $\mathcal{O}_i$ represents valid instances of $(\exp(-\kappa), \exp(-\kappa), 1 + 1/\kappa)$-OHCP with hidden center $\sigma_i(e^+)$.
2. $\mathcal{O}_i$ satisfies the conditions as shown in Proposition 1.

The check procedure is essentially the same as shown in the proof of Lemma 6.6 in [34], where the first property follows from Lemma 8 and the second property follows from Lemma 6.

This finishes the proof.

Lemma 10. *If $\mathfrak{h} = f(\mathfrak{r}) + \mathfrak{s}g(\mathfrak{r}) \in \mathbf{R}_{\mathbb{R}}$ is taken from the Gaussian distribution χ_σ, then $\mathfrak{h}$ has matrix-norm at most $\sigma\sqrt{n}\omega(\sqrt{\log n})$ except with negligible probability.*

Proof. Let $\theta = 2\pi/n$ and $\xi = e^{\theta\sqrt{-1}}$. By Lemma 2, the eigenvalues of $\mathcal{M}(\mathfrak{h})\mathcal{M}(\mathfrak{h})^T$ is contained in $\{(|f(\xi^i)| \pm |g(\xi^i)|)^2 \,|\, i \neq 0, n/2\}$ as $\xi^0 = 1, \xi^{n/2} = -1$ appear in the one dimensional irreducible representations. So

$$|\mathfrak{h}|_{\mathrm{Mat}} \leq \max_{i=1}^{n/2-1} \{|f(\xi^i)| + |g(\xi^i)|\}.$$

Next, we give an upper bound for $|f(\xi^i)|$ and $|g(\xi^i)|$ for any $i = 1, 2, \cdots, n/2-1$. We can rewrite

$$|f(\xi^i)| = \sqrt{\left(\sum_{j=0}^{n/2-1} a_j \cos(ji\theta)\right)^2 + \left(\sum_{j=0}^{n/2-1} a_j \sin(ji\theta)\right)^2}.$$

Since $a_0, a_1, \cdots, a_{n/2-1}$ are independently distributed from Gaussian χ_σ, the sum $\sum_{j=0}^{n/2-1} \cos(ji\theta)a_j$ is Gaussian $\chi_{\sqrt{\sum_{j=0}^{n/2-1} \cos^2(ji\theta)}\cdot\sigma}$. Because $i = 1, 2, \cdots, n/2-1$, we have

$$\sum_{j=0}^{n/2-1} \cos^2(ji\theta) = \frac{n}{2} + \frac{1}{2}\sum_{j=0}^{n/2-1} \cos(j2i\theta) = \frac{n}{2} + \frac{1}{2}\mathrm{Re}(\sum_{j=0}^{n/2-1} e^{j2i\theta\sqrt{-1}}) = \frac{n}{2}.$$

So the sum $\sum_{j=0}^{n/2-1} \cos(ji\theta)a_j$ is one dimensional Gaussian $\chi_{\sqrt{n/2}\cdot\sigma}$. It is well-known that a sample from $\chi_{\sqrt{n/2}\cdot\sigma}$ has length at most $\omega(\sqrt{\log n})\sqrt{n}\cdot\sigma$ except with negligible probability. Similarly, the sum $\sum_{j=0}^{n/2-1} a_j \sin(ji\theta)$ is bounded by $\omega(\sqrt{\log n})\sqrt{n}\cdot\sigma$ except with negligible probability. And hence, $|f(\xi^i)|$ is bounded by $\omega(\sqrt{\log n})\sqrt{n}\cdot\sigma$ except with negligible probability. By the same reason, $|g(\xi^i)|$ is bounded by $\omega(\sqrt{\log n})\sqrt{n}\cdot\sigma$ except with negligible probability. Then the lemma is proved.

4.4 Second part of iteration

The second (quantum) part of the iteration algorithm in [37] was improved by [25] using BDD for error distributed from a Gaussian. By the above lemma, samples from a Gaussian $\chi_{d/\sqrt{2n}}$ are distributed in the ball $B_{d\omega(\sqrt{\log n})}$ under the matrix norm except with a negligible probability. So it is enough to have a BDD oracle which can solve errors of matrix-norm $\leq d\omega(\sqrt{\log n})$.

Lemma 11. *[Second part of iteration [25]] There is an efficient quantum algorithm that, given any n-dimensional lattice Λ, a number $d < \lambda_1(\Lambda^*)/2$ (here, λ_1 is under Euclidean norm), and an oracle that solves $BDD_{\Lambda^*, d\omega(\sqrt{\log n})}$ in matrix-norm, outputs a sample from $D_{\Lambda,\sqrt{n}/d}$.*

5 Relation with other variants

In this section, we discuss the relation of GR-LWE with other variants of Ring-LWE.

5.1 Relation with Ring-LWE

Although the LWE instance from non-commutative group ring is not directly threatened by the work of Cramer et al. [14, 15], one can show that the LWE from dihedral group ring can be reduced to the LWE from cyclotomic ring with a larger modulus. Given an GR-LWE instance $(a, b = as + e)$, where $a = a_1 + \mathfrak{s}a_2$, $s = s_1 + \mathfrak{s}s_2$ and $e = e_1 + \mathfrak{s}e_2$ and $a_i, s_i, e_i (i = 1, 2)$ are polynomials module $\mathfrak{r}^{n/2} + 1$. Thus

$$\begin{aligned} b &= as + e \\ &= (a_1 + \mathfrak{s}a_2)(s_1 + \mathfrak{s}s_2) + e_1 + \mathfrak{s}e_2 \\ &= (a_1 s_1 + \bar{a}_2 s_2 + e_1) + \mathfrak{s}(\bar{a}_1 s_2 + a_2 s_1 + e_2) \\ &= b_1 + b_2, \end{aligned}$$

where $\bar{a}_1, \bar{a}_2$ can be computed from a_1 and a_2, and

$$\begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 & \bar{a}_2 \\ a_2 & \bar{a}_1 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} + \begin{pmatrix} t_1 \\ t_2 \end{pmatrix}.$$

Thus b can equivalently be seen as a structured Module-LWE instance over $R' = \mathbb{Z}[x]/(x^{n/2} + 1)$. Combing the result of [4], it can be reduced to LWE over cyclotomic ring with modulus q^2. However if we use other groups, the relation to Ring-LWE needs further investigation. See below for more discussions.

5.2 Relation with multivariate Ring-LWE

Pedrouzo-Ulloa et al. [29–31] proposed Multivariate Ring-LWE problem (M-RLWE), which can also be regarded as one kind of "structured Module-LWE". Instead of working with residue polynomial rings with one variable, they extended to consider residue polynomial rings with multivariate.

However, Bootland et al. [6] proposed an algorithm solving M-RLWE for some instantiations more efficient than originally believed.

In some sense, M-RLWE can be viewed as GR-LWE from direct products of cyclic groups, whereas dihedral groups $D_{2n} = \mathbb{Z}/n\mathbb{Z} \rtimes \{\pm 1\}$ are *semi*-direct products of cyclic groups. Thus the algorithms by [6] can not be used to the latter setting directly.

From this point of view, one may derive other good candidates to build GR-LWE. For instance, we can use semi-direct products $\mathbb{Z}/n\mathbb{Z} \rtimes G$ where G is a group acting on $\mathbb{Z}/n\mathbb{Z}$ other than $\{\pm 1\}$, e.g., G could be $(\mathbb{Z}/n\mathbb{Z})^*$ acting by exponentiation. More generally, we can extend the idea to simple non-commutative groups. Even though there is no rigorous proof, we believe that these systems provide alternative ways to prevent known attacks on Ring-LWE.

6 Conclusion

We propose generating LWE instances from non-commutative group rings and illustrate the approach by presenting a public key scheme based on dihedral

group rings. We regard the introduction of representation theory in studying ring LWE as an important contribution of the paper. As with the original LWE and Ring-LWE, we hope that the new approach is a versatile primitive, so we can build various cryptographic schemes based on this primitive besides public-key encryption. In our approach, the dimension of irreducible representations has to be small for the current proof of security to work, and for the encryption/decryption to be efficient. This leaves one open problem which we find very interesting: Can we generalize the approach to other non-commutative groups and keep the efficiency of Ring-LWE?

Acknowledgements

This work was partially supported by US NSF (Grant Nos. CCF-1409294, CCF-1900820) for Q. Cheng, by the National Natural Science Foundation of China (Grant Nos. 11971321, 11826102) and by National Key Research and Development Program of China (Grant No. 2018YFA0704703) for J. Zhang, and by the National Key Research and Development Project (No. 2018YFA0704702) for J. Zhuang. The authors thank the editor and anonymous reviewers for helpful suggestions, especially for pointing out the relation outlined in Section 5.

References

1. Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (H)IBE in the standard model. In *Advances in Cryptology - EUROCRYPT 2010*, pages 553–572, 2010.
2. Shweta Agrawal, Dan Boneh, and Xavier Boyen. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE. In *Advances in Cryptology - CRYPTO 2010*, pages 98–115, 2010.
3. Miklós Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing - STOC*, pages 99–108, 1996.
4. Martin R. Albrecht and Amit Deo. Large modulus Ring-LWE $\geq$ Module-LWE. In *Advances in Cryptology - ASIACRYPT*, volume 10624 of *Lecture Notes in Computer Science*, pages 267–296. Springer, 2017.
5. W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(4):625–636, 1993.
6. Bootland, Carl and Castryck, Wouter and Vercauteren, Frederik. On the security of the multivariate ring learning with errors problem. In *ANTS-XIV, Fourteenth Algorithmic Number Theory Symposium, Proceedings*. MSP, 2020.
7. Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (Leveled) Fully homomorphic encryption without bootstrapping. In *Innovations in Theoretical Computer Science - ICTS*, pages 309–325, 2012.
8. Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS*, pages 97–106, 2011.

9. Zvika Brakerski and Vinod Vaikuntanathan. Fully homomorphic encryption from Ring-LWE and security for key dependent messages. In *Advances in Cryptology - CRYPTO 2011*, pages 505–524, 2011.
10. David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. In *Advances in Cryptology - EUROCRYPT 2010*, pages 523–552, 2010.
11. Hao Chen, Kristin E. Lauter, and Katherine E. Stange. Attacks on search RLWE. Cryptology ePrint Archive, Report 2015/971, 2015.
12. Hao Chen, Kristin E. Lauter, and Katherine E. Stange. Vulnerable Galois RLWE families and improved attacks. Cryptology ePrint Archive, Report 2016/193, 2016.
13. Don Coppersmith. Attacking non-commutative NTRU. IBM Research Report, 1997.
14. Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. Recovering short generators of principal ideals in cyclotomic rings. In *Advances in Cryptology - EUROCRYPT 2016*, pages 559–585, 2016.
15. Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. Short stickelberger class relations and application to Ideal-SVP. Cryptology ePrint Archive, Report 2016/885, 2016.
16. Kirsten Eisenträger, Sean Hallgren, and Kristin E. Lauter. Weak instances of PLWE. In *Selected Areas in Cryptography - SAC 2014*, pages 183–194, 2014.
17. Yara Elias, Kristin E. Lauter, Ekin Ozman, and Katherine E. Stange. Provably weak instances of Ring-LWE. In *Advances in Cryptology - CRYPTO 2015*, pages 63–92, 2015.
18. Junfeng Fan and Frederik Vercauteren. Somewhat practical fully homomorphic encryption. Cryptology ePrint Archive, Report 2012/144, 2012.
19. James L. Fisher and Sudarshan K. Sehgal. Principal ideal group rings. *Communications in algebra*, 4(4):319–325, 1976.
20. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, pages 197–206, 2008.
21. Charles Grover, Cong Ling, and Roope Vehkalahti. Non-commutative ring learning with errors from cyclic algebras. Cryptology ePrint Archive, Report 2019/680, 2019.
22. Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In *Algorithmic Number Theory, Third International Symposium, ANTS-III*, pages 267–288, 1998.
23. Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for module lattices. *Des. Codes Cryptography*, 75(3):565–599, June 2015.
24. Richard Lindner and Chris Peikert. Better key sizes (and attacks) for LWE-based encryption. In *Topics in Cryptology - CT-RSA 2011*, pages 319–339, 2011.
25. Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In *Advances in Cryptology - EUROCRYPT*, volume 6110 of *Lecture Notes in Computer Science*, pages 1–23. Springer, 2010.
26. Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *Advances in Cryptology - EUROCRYPT 2012*, pages 700–718, 2012.
27. Alexei G. Myasnikov, Vladimir Shpilrain, and Alexander Ushakov. *Non-commutative Cryptography and Complexity of Group-theoretic Problems*. American Mathematical Society, 2011.

28. Yanbin Pan, Jun Xu, Nick Wadleigh, and Qi Cheng. On the ideal shortest vector problem over random rational primes. In *Advances in Cryptology - EUROCRYPT*, volume 12696 of *Lecture Notes in Computer Science*, pages 559–583. Springer, 2021.
29. Alberto Pedrouzo-Ulloa, Juan Ramón Troncoso-Pastoriza, and Fernando Pérez-González. Multivariate lattices for encrypted image processing. In *IEEE International Conference on Acoustics, Speech and Signal Processing*, pages 1707–1711. IEEE, 2015.
30. Alberto Pedrouzo-Ulloa, Juan Ramón Troncoso-Pastoriza, and Fernando Pérez-González. On ring learning with errors over the tensor product of number fields. https://arxiv.org/abs/1607.05244, 2016.
31. Alberto Pedrouzo-Ulloa, Juan Ramón Troncoso-Pastoriza, and Fernando Pérez-González. Multivariate cryptosystems for secure processing of multidimensional signals. CoRR,abs/1712.00848, 2017.
32. Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009*, pages 333–342. ACM, 2009.
33. Chris Peikert and Zachary Pepin. Algebraically structured LWE, revisited. In *Theory of Cryptography - TCC 2019,Proceedings, Part I*, volume 11891 of *Lecture Notes in Computer Science*, pages 1–23. Springer, 2019.
34. Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. Pseudorandomness of ring-LWE for any ring and modulus. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017, pages 461–473, 2017.
35. Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, pages 187–196, 2008.
36. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing*, STOC '05, pages 84–93, New York, NY, USA, 2005. ACM.
37. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 56(6):34, 2009. Preliminary version in STOC'05.
38. Sudarshan K Sehgal. *Units in integral group rings*. Longman, 1993.
39. Jean-Pierre Serre. *Linear Representations of Finite Groups*. Springer-Verlag, 1977.
40. Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science - FOCS*, pages 124–134, 1994.
41. Damien Stehlé and Ron Steinfeld. Making NTRU as secure as worst-case problems over ideal lattices. In *Advances in Cryptology - EUROCRYPT 2011*, pages 27–47, 2011.
42. Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. Efficient public key encryption based on ideal lattices. In Mitsuru Matsui, editor, *Advances in Cryptology - ASIACRYPT*, volume 5912 of *Lecture Notes in Computer Science*, pages 617–635. Springer, 2009.
43. K. R. Truman. *Analysis and extension of non-commutative NTRU*. PhD thesis, University of Maryland, 2007.
44. Yang Wang and Mingqiang Wang. Module-LWE versus Ring-LWE, revisited. Cryptology ePrint Archive, Report 2019/930, 2019.
45. Takanori Yasuda, Xavier Dahan, and Kouichi Sakurai. Characterizing NTRU-variants using group ring and evaluating their lattice security. Cryptology ePrint Archive, Report 2015/1170, 2015.