Learning with Errors over Group Rings Constructed by Semi-direct Product[†]

Jiaqi Liu, Fang-Wei Fu

Abstract

The Learning with Errors (LWE) problem has been widely utilized as a foundation for numerous cryptographic tools over the years. In this study, we focus on an algebraic variant of the LWE problem called *Group ring* LWE (GR-LWE). We select group rings (or their direct summands) that underlie specific families of finite groups constructed by taking the semi-direct product of two cyclic groups. Unlike the Ring-LWE problem described in [1], the multiplication operation in the group rings considered here is non-commutative. As an extension of Ring-LWE, it maintains computational hardness and can be potentially applied in many cryptographic scenarios. In this paper, we present two polynomial-time quantum reductions. Firstly, we provide a quantum reduction from the worst-case shortest independent vectors problem (SIVP) in ideal lattices with polynomial approximate factor to the search version of GR-LWE. This reduction requires that the underlying group ring possesses certain mild properties; Secondly, we present another quantum reduction for two types of group rings, where the worst-case SIVP problem is directly reduced to the (average-case) decision GR-LWE problem. The pseudorandomness of GR-LWE samples guaranteed by this reduction can be consequently leveraged to construct semantically secure public-key cryptosystems.

Index Terms

Learning with errors; Group rings; Semi-direct product; Group representations; Lattice-based cryptography; Computational hardness

I. Introduction

A. Lattice-based cryptography

Lattice-based cryptography has been playing a significant role in post-quantum cryptography. It is well-known that traditional cryptographic systems such as RSA and Diffie-Hellman protocol rely on the computational hardness of certain number-theoretic problems. However, Shor [2] introduced a quantum algorithm that can solve integer factorization and discrete logarithm problems in polynomial time, rendering these classical cryptosystems vulnerable to quantum attacks. In contrast, lattice-based cryptosystems have several advantages over such traditional cryptosystems. First, no efficient quantum algorithms have been discovered for lattice problems that are used to construct cryptographic tools for the moment. Consequently, efforts are currently underway to establish post-quantum cryptographic standards, with lattice-based schemes as leading candidates. Second, there is an inherent disparity between the average-case hardness required by cryptography and the worst-case hardness concerned in computational complexity theory. Unlike other types of cryptosystems, lattice-based cryptosystems own security guaranteed by the worst-case hardness of certain lattice problems when their parameters are suitably chosen. Ajtai [3] proposed the first public-key cryptosystem from the *short integer solution* (SIS) problem whose security is based on the worst-case hardness of well-studied lattice problems. Third, lattice-based cryptography is computationally efficient in comparison with RSA and the Diffie-Hellman protocol, as it only requires linear operations on vectors or matrices modulo relatively small integers, without the need for large number exponentiations.

Regev [4] was the first to demonstrate the hardness of the *learning with errors* (LWE) problem, which is an extension of *learning parity with noise* (LPN) problem. The LWE problem has gained considerable attention in recent years, due to its strong hardness and practical applications in various fields, including cryptography, machine learning, and quantum computing. The LWE problem can be formulated as follows:

Jiaqi Liu and Fang-Wei Fu are with Chern Institute of Mathematics and LPMC, Nankai University, Tianjin 300071, China, Emails: ljqi@mail.nankai.edu.cn, fwfu@nankai.edu.cn

[†]This research is supported by the National Key Research and Development Program of China (Grant No. 2022YFA1005000), the National Natural Science Foundation of China (Grant Nos. 12141108 and 62371259), the Fundamental Research Funds for the Central Universities of China (Nankai University), and the Nankai Zhide Foundation.

Let $q > \mathrm{poly}(n)$ be a positive integer, fix a secret vector $\mathbf{s} \in \mathbb{Z}_q^n$, sample arbitrarily many $\mathbf{a}_i \in \mathbb{Z}_q^n$ independently from the uniform distribution, where $1 \leq i \leq m$, and let $e_i \in \mathbb{Z}_q$ be independent "short" elements which are typically sampled from a discrete Gaussian distribution. Then, compute the LWE samples as

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

where $\langle \cdot, \cdot \rangle$ denotes the Euclidean inner product in $\mathbb{R}^n$. The LWE problem asks to recover the secret vector $\mathbf{s}$ given LWE samples (search version) or distinguish LWE samples from uniformly random samples in $\mathbb{Z}_q^n \times \mathbb{Z}_q$ with a non-negligible advantage within polynomial time (decision version).

In [4], Regev initially proved the hardness of the LWE problem for certain parameters, assuming the hardness of finding short vectors in lattices. Specifically, Regev established a (quantum) reduction from worst-case (decisional) approximate SVP (*shortest vector problem*) and SIVP (*shortest independent vectors problem*) for n-dimensional lattices to the average-case LWE problem with the same dimension n as the corresponding lattices. Informally speaking, the reduction suggests that if someone could solve LWE in polynomial time with non-negligible probability, it would imply the existence of a quantum algorithm capable of solving approximate SVP or SIVP in arbitrary lattices with the same dimension as in LWE problem. Later, Peikert [5] presented a classical reduction from worst-case approximate SVP, but with worse parameters than those in [4].

While Regev's LWE enjoys worst-case hardness, it suffers from drawbacks regarding efficiency. It scales poorly with increasing dimension n, which makes it impractical for high-dimensional settings. Inspired by the NTRU [6] cryptosystem proposed by Hoffstein et al., which is constructed from algebraic lattices, Stehlé et al. [7] proposed a more efficient variant of the LWE problem over a cyclotomic ring. Lyubashevsky et al. [1] then presented a (quantum) worst-case-to-average-case reduction from ideal lattice problems in the ring of integers of certain number fields (notably cyclotomic/Galois ones) to the Ring-LWE problem. The improved efficiency of this problem stems from the additional algebraic structures of the rings. The utilization of number-theoretic transformation (NTT), a variant of fast Fourier transformation (FFT) also accelerates the multiplication of ring elements in certain cyclotomic rings, contributing to its computational efficiency. Precisely, Ring-LWE also considers equations of the form $b_i = a_i \cdot s + e_i$ for a secret element $s \in R^\vee/qR^\vee$ and public uniformly random $a_i \in R/qR$, where q is the modulus, R is a commutative ring typically chosen as the ring of algebraic integers of a number field and $R^\vee$ is the dual ideal of R. Although some algorithms are more efficient on ideal lattices than on general lattices due to their additional algebraic structures, none are currently known to threaten well-designed cryptographic constructions. In particular, no algorithms are known that significantly outperform the best general lattice algorithms in attacking such schemes. Later, Peikert et al. [8] gave a direct quantum reduction from worst-case (ideal) lattice problems to the decision version of (Ring)-LWE. Brakerski et al. [9] introduced Module-LWE, balancing the efficiency and compactness of Ring-LWE and the hardness of Regev's plain LWE. Module-LWE has more flexible parameters than Ring-LWE and Regev's standard LWE, making it a reasonable choice for standardization. Many schemes submitted to NIST for post-quantum standardization such as CRYSTALS-Kyber, CRYSTALS-Dilithium, and Saber, rely on the assumed hardness of LWE variants. Additionally, there are several other algebraically structured LWE variants, e.g., Polynomial-LWE [10], Order-LWE [11], and Middle-Product LWE [12]. Peikert et al. [13] have developed a unified framework for all proposed LWE variants (over commutative base rings), which encompasses all prior "algebraic" LWE variants defined over number fields. This work has led to more simplified and tighter reductions to Ring-LWE.

SIS and LWE are two off-the-shelf problems possessing reductions from worst-case lattice problems. They are both widely used to construct powerful cryptographic primitives. LWE and its variants have numerous applications in cryptography including secure public-key encryption [1], [4], [5], [14], [15], key-homomorphism PRF [16], [17], oblivious transfer [14], identity-based encryption (IBE) [18]–[20], attribute-based encryption (ABE) [21]–[24], fully homomorphic encryption (FHE) [25]–[27], and multi-linear maps [28], [29].

B. Our results

Similar to the work in [30], we consider the LWE problems over group rings. Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group, and let R be a commutative ring, elements in the group ring $R[G]$ are formal sums

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

In this paper, two types of non-commutative finite groups are constructed, each of which is a semi-direct product of two cyclic groups (e.g. $\mathbb{Z}_m \ltimes \mathbb{Z}_n, \mathbb{Z}_n^* \ltimes \mathbb{Z}_n$). We use them as the underlying groups of the group rings.

To study the relationship between an algebraic structure and a lattice in $\mathbb{R}^n$, we need to embed the structure into the Euclidean space $\mathbb{R}^n$. For LWE variants based on rings, there are two types of embeddings into $\mathbb{R}^n$: *canonical embedding* and *coefficient embedding*. Canonical embedding provides nice geometric and algebraic properties. One can refer to the work of Lyubashevsky et al. in [1]. They embed the base ring R (such as the cyclotomic ring $\mathbb{Z}[x]/\langle x^n + 1\rangle$) into a linear space $H \subset \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2}$ defined as

$$H = \{(x_1, x_2, \ldots, x_n) \in \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} : x_{s_1+s_2+i} = \overline{x_{s_1+s_2}} \text{ for } 1 \le i \le s_2\}$$

where $s_1 + 2s_2 = n$. Every element $a \in R$ is mapped into H by taking n distinct embeddings of a (s_1 real embeddings and $2s_2$ complex embeddings). It can be easily verified that H, with the Hermite inner product, is isomorphic to the Euclidean inner product space $\mathbb{R}^n$. Canonical embedding often leads to tighter error rates and enables to obtain more compact systems due to its component-wise multiplication. On the other hand, the coefficient embedding used in [7] directly maps the ring elements to real vectors according to its coefficients under a specific basis. In this paper, we primarily use coefficient embedding for the sake of simplicity, following the approach described in [30]. However, we also need to use an extended version of canonical embedding to analyze the generalized LWE problem due to its connection to irreducible group representations.

Taking an example for the canonical embedding in [1], the ring $\mathbb{C}[x]/\langle x^n+1\rangle$ can be viewed as a direct summand of $\mathbb{C}[C_{2n}]$ where C_{2n} denotes the cyclic group of order $2n$. Precisely,

$$\mathbb{C}[C_{2n}] \cong \mathbb{C}[x]/\langle x^{2n} - 1\rangle \cong \mathbb{C}[x]/\langle x^n + 1\rangle \oplus \mathbb{C}[x]/\langle x^n - 1\rangle \cong \bigoplus_{i=0}^{2n-1} \mathbb{C}[x]/\left\langle x - \mathrm{e}^{2\pi i\sqrt{-1}/2n}\right\rangle. \quad (1)$$

One can observe that each direct summand above corresponds to a (one-dimensional) irreducible representation of C_{2n}. The canonical embedding of $\mathbb{Z}[x]/\langle x^n+1\rangle$ consists of a natural inclusion into $\mathbb{C}[x]/\langle x^n+1\rangle$ and an isomorphism obtained from (1):

$$\mathbb{C}[x]/\langle x^n + 1\rangle \cong \bigoplus_{0\le i\le 2n-1, 2\nmid i} \mathbb{C}[x]/\left\langle x - \mathrm{e}^{2\pi i\sqrt{-1}/2n}\right\rangle.$$

To generalize the canonical embedding to the group ring constructed from a non-commutative group, we have to deal with irreducible representations of which the dimensions are greater than 1. By applying the Artin-Wedderburn theorem [31], we can decompose the group algebra $\mathbb{C}[G]$ into the direct sum of matrix algebra over $\mathbb{C}$ uniquely. Each direct summand, denoted by $\mathbb{C}^{d\times d}$ matches exactly an irreducible representation of dimension d for the group G. The complicated form of this decomposition is one of the reasons to use coefficient embedding in this paper rather than canonical embedding.

In the case of a group ring $\mathbb{Z}[G]$, we can regard it as a free $\mathbb{Z}$-module. All the group elements form a $\mathbb{Z}$-basis of $\mathbb{Z}[G]$ inherently. An element $\sum_{i=1}^{n} r_i g_i \in \mathbb{R}[G]$ can be represented by an n-dimensional vector $(r_1, r_2, \ldots, r_n) \in \mathbb{R}^n$. Under this embedding, each ideal of $\mathbb{Z}[G]$ corresponds to a lattice in $\mathbb{R}^n$, which is called an *ideal lattice*. In our paper, we mainly study the relationship between the hard problems in ideal lattices and the LWE problem over group rings.

1) Avoiding the potential attack: For "hard" problems such as SVP and SIVP in certain ideal lattices, several potential attacks have been discovered. Various quantum polynomial-time algorithms have been developed to solve these problems in specific principal ideal lattices as mentioned in [32]–[34]. Some studies generalized the SVP algorithms to non-principal ideal lattices such as mentioned in [35]. However, it is important to note that the Ring-LWE problem present in [1] is not under direct threat from the attacks above, as the corresponding lattice problem serves as a lower bound of the security. Regarding the LWE problem over group rings studied in this paper, it may not be affected by these algorithms for some reasons. On the one hand, the ideals of the group rings may not be principal. On the other hand, these attacks are basically designed for rings with commutative operation. Therefore, the attack can not be directly applied to the scenarios discussed in this paper, where the multiplication operation is not commutative.

2) Why selecting such group rings: In this paper, we have chosen the quotient ring $\mathbb{Z}[\mathbb{Z}_m \ltimes \mathbb{Z}_n]/\langle t^{n/2}+1\rangle$ instead of $\mathbb{Z}[\mathbb{Z}_m \ltimes \mathbb{Z}_n]$ as a candidate, where t is the generator of $\mathbb{Z}_n$, though two reductions for $\mathbb{Z}[\mathbb{Z}_m \ltimes \mathbb{Z}_n]$ are both correct. For Ring-LWE, there are some attacks by mapping the ring elements into small order elements to extract useful information. For instance, in [36], [37], they tell us that it is not secure to use $\mathbb{Z}[C_{2n}] \cong \mathbb{Z}[x]/\langle x^{2n}-1\rangle$ as the underlying ring due to its vulnerability arising from the mapping $\mathbb{Z}[x]/\langle x^{2n}-1\rangle \to \mathbb{Z}[x]/\langle x-1\rangle$, which may leak some information that allows for secret recovery. Nevertheless, we often select polynomial rings of the form $\mathbb{Z}[x]/\langle x^n+1\rangle$, a direct summand of $\mathbb{Z}[C_{2n}]$, to avoid the information leakage resulting from such attacks.

Additionally, when performing the multiplication of two elements in the group ring, it is necessary to exploit all irreducible representations of the finite group due to the coefficient embedding. This implies that the highest dimension of irreducible representation cannot be excessively large. It can be verified that the dimension of irreducible representations of $\mathbb{Z}_m \ltimes \mathbb{Z}_n$ (Type I) is no more than 2, and that the dimension of irreducible representations of $\mathbb{Z}_n^* \ltimes \mathbb{Z}_n$ (Type II) is no more than $n - n/p_1p_2\cdots p_s$, where $p_1, p_2, \ldots, p_s$ are all the distinct prime factors of n.

3) Relationship with other LWE *variants:* LWE over group rings involves a non-commutative multiplication operation, unlike the LWE variants studied in [13], where commutative algebraic systems are mainly concerned. Consider a group ring $R[G]$, where $G = \{g_1, g_2, \ldots, g_n\}$ is a finite group of order n. In this settings, $g_1, g_2, \ldots, g_n$ naturally form a R-basis of $R[G]$. Let $a, s \in R[G]$, then the product $a \cdot s$ can also be expressed as product of a matrix and a vector with entries from R. Precisely, the left multiplication determined by a is an R-linear transformation over $\mathbb{R}^n$, then a uniquely specifies a unique matrix from $\mathbb{R}^{n\times n}$ under the natural basis, denoted by $\mathcal{M}(a)$. Then the product $a \cdot s$ can be equivalently represented as the product of $\mathcal{M}(a)$ with the coefficient vector of s.

LWE over group rings can also be viewed as a "structured-module" LWE. As stated in [30], the group ring is selected as $\mathbb{Z}[D_{2n}]$, i.e., $\mathbb{Z}[\mathbb{Z}_2 \ltimes \mathbb{Z}_n]$. Let r, t be generators of $\mathbb{Z}_2$ and $\mathbb{Z}_n$, respectively. Let $s = s_1(t)+s_2(t)\cdot r, a = a_1(t)+a_2(t)\cdot r, b = b_1(t)+b_2(t)\cdot r \in \mathbb{Z}[D_{2n}]$, where $s_1(t), s_2(t), a_1(t), a_2(t), b_1(t), b_2(t) \in \mathbb{Z}[t]/\langle t^n-1\rangle$, then the equation $b \approx s \cdot a$ can be expressed in the matrix form as follows:

$$\begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \approx \mathbf{M} \cdot \begin{pmatrix} s_1 \\ s_2 \end{pmatrix}.$$

Here, $\mathbf{M}$ is a structured 2×2 matrix with elements in $\mathbb{Z}[t]/\langle t^n-1\rangle$ all of which can be computed from $a_1(t), a_2(t)$ efficiently. It is worth noting that the matrix $\mathbf{M}$ is structured, since only two elements ($a_1(t)$ and $a_2(t)$) of the four need to be sampled randomly, while in the situation of unstructured-module LWE, all entries in $\mathbf{M}$ are sampled randomly as in [38]. That's the reason why the LWE over group rings can be viewed as a "structured-module" LWE. Compared with the classical module LWE, to produce the same number of pseudorandom LWE samples, the additional structure can reduce the cost of uniform randomness for sampling $\mathbf{M}$ by a factor of $1/2$.

In [39], Pedrouzo et al. introduced an extension of the Ring-LWE framework proposed in [1] by adding other indeterminates to the polynomial ring. Specifically, they generalized the univariate polynomials in ring $\mathbb{Z}[x]/\langle x^n+1\rangle$ to multivariate polynomials in ring $\mathbb{Z}[x_1, x_2, \ldots, x_m]/\langle x_1^n+1, \ldots, x_m^n+1\rangle$. In particular, multivariate Ring-LWE with two indeterminates can also be interpreted as an instance of LWE over the

group ring discussed here. In this setting, the underlying group is represented by the direct product of two cyclic groups. However, in this paper, we primarily focus on the semi-direct product of two cyclic groups. It should be emphasized that, in some sense, the LWE considered in this paper can be regarded as two-variate Ring-LWE, but the two variables are not algebraically independent.

There are several schemes that exploit non-commutative algebraic structures. The idea of LWE problem over group rings originates from non-commutative NTRU schemes [40] where the authors employ group rings $\mathbb{Z}[G]$ instead of $\mathbb{Z}[x]/\langle x^n - 1\rangle$ considered in the original NTRU scheme [6]. Grover et al. [41] showed another non-commutative LWE variant over cyclic algebras and provided hardness proof by giving a reduction from hard lattice problems.

4) Proof of reductions: In this paper, we present two reductions for the GR-LWE problem. Both reductions make full use of *iterative steps* (Lemma 12 and Lemma 18) mentioned in [4] and [1]. One can refer to Section III and Section IV for detailed information.

The first reduction is from a worst-case lattice problem to the search GR-LWE problem. The reduction is based on the work of [1] and [13]. It can be applied to any group ring that satisfies certain mild properties. Precisely, the reduction applies to those group rings satisfying if the ideal of the group ring has an inverse ideal, then the inverse ideal and the dual ideal are essentially equivalent, up to a certain permutation of the coefficients. Since not every ideal of the group rings is invertible, this reduction only considers those invertible ones. With the help of the search GR-LWE oracle, we are capable of sampling from discrete Gaussian distributions with narrower and narrower widths in (invertible) ideal lattices through iterative steps. This process continues until the Gaussian parameter reaches our expectations. Consequently, we can obtain "short" vectors in the lattice except with negligible probability.

The second one is a direct reduction from a (worst-case) lattice problem to the (average-case) decision GR-LWE problem. The procedure closely follows the approaches outlined in [8] and [30]. The coefficient embedding and generalized canonical embedding both play crucial roles in this reduction. We establish the hardness by providing the reduction from solving *bounded distance decoding* (BDD), the problem of finding the closest lattice vector to a target $\mathbf{t} \in \mathbb{R}^n$ that is sufficiently close to a lattice $\mathcal{L}$, to the decision GR-LWE problem. During the reduction process, the decision LWE oracle behaves like an oracle with a "hidden center" defined by [8]. To see how the oracle works for reduction, [4] states that one can transform an BDD instance into an LWE sample whose secret corresponds to the closest lattice vector $\mathbf{v} \in \mathcal{L}$ to $\mathbf{t}$. With a suitable oracle for decision LWE and by incrementally moving $\mathbf{t}$ towards the closest lattice vector $\mathbf{v}$ by carefully measuring the behavior of the oracle, we can detect the distance between the moving point $\mathbf{t}$ and $\mathcal{L}$ by monitoring the acceptance probability of the oracle, which is a monotonically decreasing function of $\mathrm{dist}(\mathbf{t}, \mathcal{L})$. This makes it possible to solve BDD by repeatedly perturbing $\mathbf{t}$ to a new point $\mathbf{t}'$, and testing whether the new point is significantly closer to the lattice. For further details, we refer to Section IV.

C. Applications

Due to the pseudorandomness of LWE samples over group rings, it is possible to construct a public-key cryptosystem that provides semantic security. The security is based upon the hardness of the worst-case SIVP problem with a polynomial approximate factor. We can combine the result of this paper with the cryptosystem present in [1], which is also similar to both Diffie-Hellman protocol [42] and ElGamal protocol [43].

Informally, let R be some group ring or a quotient ring of some group ring. For instance, we can select a ring $R = \mathbb{Z}[G]/\langle t^{n/2} + 1\rangle$, where G is a semi-direct product of cyclic groups $\mathbb{Z}_m = \langle s\rangle$ and $\mathbb{Z}_n = \langle t\rangle$. Let q be a positive integer. The public-key cryptosystem based on GR-LWE is as follows: The key-generation algorithm first generates a uniformly random element $a \in R_q := R/qR$ (under coefficient embedding) and two "short" elements $s, e \in R_q$ from error distribution (typically selected from a discrete Gaussian distribution with "narrow" error). It outputs a GR-LWE sample $(a, b = s \cdot a + e) \in R_q \times R_q$ as the public key and s as the secret key. To encrypt a $|G|/2$-bit message $m \in \{0,1\}^{|G|/2}$ that can be viewed

as a polynomial of degree $n/2-1$ with 0 or 1 coefficients, the encryption algorithm first generates three "short" random elements r, e_1 and $e_2 \in R_q$ from error distribution and outputs $(u, v) \in R_q \times R_q$ with $u = a \cdot r + e_1 \bmod q$ and $v = b \cdot r + e_2 + \lfloor q/2 \rceil \cdot m \bmod q$. To decrypt $(u, v) \in R_q \times R_q$, the decrypt algorithm computes

$$\hat{m} = v - s \cdot u = (e \cdot r - s \cdot e_1 + e_2) + \lfloor q/2 \rceil \cdot m \bmod q.$$

By choosing appropriate parameters, the element $e \cdot r - s \cdot e_1 + e_2$ can be restricted to be very "short". By rounding the coefficient of $\hat{m}$ to either 0 or $\lfloor q/2 \rceil$, we can efficiently recover the bit string except with negligible probability.

To understand why this cryptosystem is semantically secure, we first observe that the public key is generated as a GR-LWE sample, though with "short" secret s, which can also be proved to be pseudo-random, as the "normal form LWE" discussed in [44]. Such a sample becomes indistinguishable from a truly random sample except with negligible probability. By replacing the public key with a randomly uniform sample (it makes negligible difference to this system), the encrypted message $(a, u) \in R_q \times R_q$ and $(b, v) \in R_q \times R_q$ both become exact GR-LWE samples with "random" secret vector r. Therefore, these two encrypted messages are pseudorandom, which implies the semantic security of the system.

D. Paper organization

In Section 2, we give some basic knowledge of lattice and related computationally hard problems. In Section 3, we provide a reduction from worst-case lattice problems to the search version of GR-LWE over some group rings with special properties. In Section 4, we present a direct reduction from worst-case lattice problems to the decision version of GR-LWE, considering two types of group rings. This generalizes the results of [30] and enables to construct some cryptographic primitives. In Section 5, we summarize our findings and offer some thoughts for further study.

II. Preliminaries

First, we present some notations used throughout this paper.

For $x \in \mathbb{R}$, we denote $\lfloor x \rfloor$ as the largest integer not greater than x and $\lfloor x \rceil := \lfloor x + \frac{1}{2} \rfloor$ as the nearest integer to x (if there exist two nearest integers, select the larger one). For integer $n \geq 2$, we denote $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ as the cyclic group of order n with addition modulo n. Denote $\varphi(m)$ as the Euler's totient function of m for any positive integer m, i.e., the number of positive integers that are coprime with m and also not greater than m.

Throughout this paper, we use bold lower-case letters to denote column vectors, e.g., $\mathbf{x}, \mathbf{y}, \mathbf{z}$. We use bold upper-case letters to denote matrices, e.g., $\mathbf{A}, \mathbf{B}, \mathbf{C}$. The transpose of vector $\mathbf{x}$ and matrix $\mathbf{A}$ is denoted as $\mathbf{x}^t$ and $\mathbf{A}^t$, respectively. The rounding function mentioned above can be applied element-wise to vectors, e.g. $\lfloor \mathbf{u} \rceil$ round each entry of $\mathbf{u}$ to its nearest integer. The inner product of two vectors $\mathbf{u}, \mathbf{v}$ is denoted by $\langle \mathbf{u}, \mathbf{v} \rangle$.

If S is a nonempty finite set, then $x \leftarrow S$ denotes that x is a random variable uniformly distributed over S. If φ is a probability density function, then $x \leftarrow \varphi$ denotes that x is a random variable distributed as φ. Given two probability distribution functions ρ_1, ρ_2 over $\mathbb{R}^n$, the *statistical distance* between ρ_1 and ρ_2 is defined as

$$\Delta(\rho_1, \rho_2) := \frac{1}{2} \int_{\mathbb{R}^n} |\rho_1(\mathbf{x}) - \rho_2(\mathbf{x})| d\mathbf{x}.$$

A. Lattice Background

In this section, we introduce some definitions and discuss some related "hard" problems regarding lattices.

A *lattice* is defined as a discrete additive subgroup of $\mathbb{R}^n$. Equivalently, an n-dimensional lattice $\mathcal{L}$ is a set of all integer combinations of n linearly independent basis column vectors $\mathbf{B} := (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n) \in \mathbb{R}^{n\times n}$, i.e.,

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

Then lattice $\mathcal{L}$ can be viewed as a full-rank free $\mathbb{Z}$-module with basis $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$.

Since a lattice $\mathcal{L}$ is an additive subgroup of $\mathbb{R}^n$, we can obtain quotient group $\mathbb{R}^n/\mathcal{L}$ (with operation induced by addition from $\mathbb{R}^n$), which has cosets

$$\mathbf{x} + \mathcal{L} = \{\mathbf{x} + \mathbf{y} : \mathbf{y} \in \mathcal{L}\}, \quad \text{for all } \mathbf{x} \in \mathbb{R}^n$$

as its elements.

The *fundamental parallelepiped* of a lattice $\mathcal{L}$ is defined as

$$\mathcal{P}(\mathbf{B}) := \mathbf{B} \cdot [0,1)^n = \left\{ \sum_{i=1}^{n} c_i \mathbf{b}_i : 0 \le c_i < 1, 1 \le i \le n \right\}.$$

It is clear that the definition of the fundamental parallelepiped depends on the choice of basis. Fixing a basis $\mathbf{B}$, every coset $\mathbf{x} + \mathcal{L} \in \mathbb{R}^n/\mathcal{L}$ has a unique representative in $\mathcal{P}(\mathbf{B})$. In fact, coset $\mathbf{x} + \mathcal{L}$ has representative $\mathbf{x} - \mathbf{B} \cdot \lfloor \mathbf{B}^{-1} \cdot \mathbf{x} \rfloor \in \mathcal{P}(\mathbf{B})$, which we denote by $\mathbf{x} \bmod \mathcal{L}$.

The *determinant* of a lattice $\mathcal{L}$ is the absolute value of the determinant of a basis $\mathbf{B}$[1], i.e.,

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

The *minimum distance* of a lattice $\mathcal{L}$ in a given norm $\|\cdot\|$ is the length of a shortest nonzero lattice vector, i.e.,

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

The *i-th successive minimum* $\lambda_i(\mathcal{L})$ is defined as the smallest $r \in \mathbb{R}$ such that $\mathcal{L}$ has i linearly independent vectors with norm no greater than r. In this paper, we use ℓ_2-norm unless otherwise specified.

The *dual lattice* of $\mathcal{L}$ is defined as

$$\mathcal{L}^\vee := \{\mathbf{x} \in \mathbb{R}^n : \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}, \text{ for all } \mathbf{y} \in \mathcal{L}\},$$

where $\langle \cdot, \cdot \rangle$ represents inner product (Euclidean inner product by default). And it is easy to prove that $\mathcal{L}^\vee$ is also a lattice in $\mathbb{R}^n$ and if $\mathbf{B}$ is a basis of $\mathcal{L}$, then $\mathbf{B}^{-t} := (\mathbf{B}^{-1})^t = (\mathbf{B}^t)^{-1}$ is a basis of $\mathcal{L}^\vee$, hence $(\mathcal{L}^\vee)^\vee = \mathcal{L}$.

B. Gaussian measures

For any (column) vector $\mathbf{u} \in \mathbb{R}^n$ and definite positive matrix $\mathbf{\Sigma} \in \mathbb{R}^{n\times n}$, we define the *Gaussian distribution* with mean vector $\mathbf{u}$ and covariance matrix $\frac{1}{2\pi}\mathbf{\Sigma} \in \mathbb{R}^{n\times n}$ as distribution with the probability density function

$$D_{\mathbf{u},\mathbf{\Sigma}}(\mathbf{x}) = \frac{1}{\sqrt{\det \mathbf{\Sigma}}} \exp(-\pi(\mathbf{x}-\mathbf{u})^t \mathbf{\Sigma}^{-1}(\mathbf{x}-\mathbf{u}))$$

for any $\mathbf{x} \in \mathbb{R}^n$. If $\mathbf{u}$ is a zero vector, we denote $D_{\mathbf{u},\mathbf{\Sigma}}$ by $D_{\mathbf{\Sigma}}$ for short.

In particular, if $\mathbf{u}$ is a zero vector and $\mathbf{\Sigma}$ is a diagonal matrix with diagonal entries $r_1^2, r_2^2, \ldots, r_n^2 \in \mathbb{R}^+$, then $D_{\mathbf{u},\mathbf{\Sigma}}$ degrades to an elliptical (non-spherical) Gaussian distribution, which we denote $D_{\mathbf{r}}$ for convenience, where $\mathbf{r} = (r_1, r_2, \ldots, r_n) \in \mathbb{R}^n$. Furthermore, if $r_1 = r_2 = \ldots = r_n = r$, then this distribution degrades to a spherical Gaussian distribution with probability density function $\frac{1}{\sqrt{\det \mathbf{\Sigma}}} \exp(-\pi\|\mathbf{x}\|^2/r^2)$,

[1]It can be proved that the value of determinant is independent from the selection of the basis $\mathbf{B}$.

which we denote D_r for short. These functions can be extended to sets in the usual way, e.g., $D_{\mathbf{u},\mathbf{\Sigma}}(S) = \sum_{\mathbf{x}\in S} D_{\mathbf{u},\mathbf{\Sigma}}(\mathbf{x})$, where $S \subseteq \mathbb{R}^n$ is a countable set.

For an n-dimensional lattice $\mathcal{L}$, a vector $\mathbf{u} \in \mathbb{R}^n$, and a real $r > 0$, we define *discrete Gaussian probability distribution over* the coset $\mathcal{L} + \mathbf{u}$ with parameter $\mathbf{\Sigma} \in \mathbb{R}^{n\times n}$ as

$$D_{\mathcal{L}+\mathbf{u},\mathbf{\Sigma}}(\mathbf{x}) := \frac{D_{\mathbf{\Sigma}}(\mathbf{x})}{D_{\mathbf{\Sigma}}(\mathcal{L}+\mathbf{u})}, \quad \text{for all } \mathbf{x} \in \mathcal{L} + \mathbf{u}.$$

Note that the support set of $D_{\mathcal{L}+\mathbf{u},\mathbf{\Sigma}}$ is $\mathcal{L} + \mathbf{u}$, a discrete set in $\mathbb{R}^n$.

The (continuous or discrete) Gaussian distribution owns numerous helpful properties. We list some of them as follows:

Lemma 1 ([4], Claim 2.2)**.** *For $0 < \alpha < \beta \leq 2\alpha$, the statistical distance between D_α and D_β is no greater than $10(\beta/\alpha - 1)$.*

As in the continuous version, almost all samples from n-dimensional discrete Gaussian distribution can be bounded in a sphere with a radius factor of $\sqrt{n}$.

Lemma 2 ([45], Lemma 1.5 (i))**.** *For any n-dimensional lattice $\mathcal{L}$ and real $r > 0$, a point sampled from $D_{\mathcal{L},r}$ has ℓ_2 norm at most $r\sqrt{n}$, except with probability at most 2^{-2n}.*

Micciancio et al. [46] first introduced *smoothing parameter* of lattices, which can be used to characterize the similarity between discrete Gaussian distribution over the lattice and continuous Gaussian distribution with the same parameter. However, for this paper, we require a more generalized definition mentioned in [30] as below.

Definition 1 (Smoothing parameter, [30], [46])**.** *Let $\mathcal{L}$ be a lattice in $\mathbb{R}^n$ and $\mathcal{L}^\vee$ be its dual lattice. For a real $\varepsilon > 0$, the* smoothing parameter $\eta_\varepsilon(\mathcal{L})$ *is defined to be the smallest s such that*

$$\sum_{\mathbf{y}\in\mathcal{L}^\vee\setminus\{0\}} D_{1/s}(\mathbf{y}) = \sum_{\mathbf{y}\in\mathcal{L}^\vee\setminus\{0\}} \exp(-\pi s^2 \cdot \|\mathbf{y}\|^2) \leq \varepsilon.$$

For any $\mathbf{A} \in \mathbb{R}^{n\times n}$, $\mathbf{A}$ is defined to satisfy smoothing condition *if*

$$\sum_{\mathbf{y}\in\mathcal{L}^\vee\setminus\{0\}} \exp(-\pi \cdot \mathbf{y}^t\mathbf{A}\mathbf{A}^t\mathbf{y}) \leq \varepsilon,$$

which we denote as $\mathbf{A} \geq \eta_\varepsilon(\mathcal{L})$.

The following lemma states an important property of the smoothing parameter and also explains the term "smoothing" to some extent. Suppose we have a vector $\mathbf{v} \in \mathbb{R}^n$ sampling from Gaussian distribution D_r where r exceeds the smoothing parameter of a certain lattice $\mathcal{L}$, then $\mathbf{v} \bmod \mathcal{L}$ is approximately uniform distributed over any fundamental parallelepiped $\mathcal{P}$ except with small statistical distance. Since the volume of any fundamental parallelepiped $\mathcal{P}$ of $\mathcal{L}$ is equal to $\det(\mathcal{L})$, then the uniform distribution over $\mathcal{P}$ has probability density function $1/\det(\mathcal{L})$. To summarize, the results can be stated as follows.

Lemma 3 ([46], Lemma 4.1)**.** *For any n-dimensional lattice $\mathcal{L}$, $\varepsilon > 0$ and $r \geq \eta_\varepsilon(\mathcal{L})$, the statistical distance between $D_r \bmod \mathcal{L}$ and the uniform distribution over $\mathbb{R}^n/\mathcal{L}$ is at most $\varepsilon/2$, then we have*

$$D_r(\mathcal{L} + \mathbf{u}) \in (1 \pm \varepsilon)\frac{1}{\det(\mathcal{L})},$$

where $\mathbf{u}$ is an arbitrary vector in $\mathbb{R}^n$.

The following lemma states two useful bounds about smoothing parameters.

Lemma 4 ([46], Lemma 3.2, 3.3)**.** *For any n-dimensional lattice $\mathcal{L}$, we have $\eta_{2^{-2n}}(\mathcal{L}) \leq \sqrt{n}/\lambda_1(\mathcal{L}^\vee)$, and $\eta_\varepsilon(\mathcal{L}) \leq \sqrt{\ln(n/\varepsilon)}\lambda_n(\mathcal{L})$ for all $0 < \varepsilon < 1$.*

C. Representations of finite groups

Let G be a finite group, a pair (V, ρ) (V for short) is called a *representation* of G if V is a linear space and ρ is a group homomorphism that maps G to $\mathrm{GL}(V)$, where $\mathrm{GL}(V)$ is the group of all invertible linear transformations over V. If a linear subspace U of V is preserved by the action of any element in G, i.e., $\rho(g)u \in U$ for all $g \in G, u \in U$, then (U, ρ) (U for short) is called a *subrepresentation* of V. It follows immediately that every representation (V, ρ) has two *trivial subrepresentations*: $\{0\}$ and V itself. V is called *irreducible* if V has no subrepresentations other than the trivial subrepresentations. Otherwise, V is called *reducible*. The dimension of V is called the *dimension* of the representation.

D. Group ring

We follow the formulation of this definition as presented in [30]. Let $G = \{g_1, g_2, \cdots, g_n\}$ be a finite group of order n, and let R be a commutative ring with identity. The group ring $R[G]$ is the set of all finite formal sums

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

Addition is defined coefficient-wise

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

Multiplication is defined by extending the group operations R-bilinearly:

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

In particular, $R[G]$ is a free R-module of rank $|G| = n$ in a natural way, with $\{g_1, g_2, \ldots, g_n\}$ as an R-basis.

Next, we need to define the matrix form of the elements in a group ring. For any element $\mathfrak{h} = \sum_{i=1}^{n} a_i g_i \in R[G]$, it defines a linear transformation on $R[G]$, by its left multiplication law. We denote the $n \times n$ transformation matrix corresponding to $\mathfrak{h}$ with respect to the basis $\{g_1, g_2, \ldots, g_n\}$[2] by $\mathcal{M}(\mathfrak{h})$. Define the matrix-norm $\|\mathfrak{h}\|_{\mathrm{Mat}}$ of $\mathfrak{h}$ as the spectral norm of the matrix $\mathcal{M}(\mathfrak{h})$, i.e., the square root of the largest eigenvalue of $\mathcal{M}(\mathfrak{h})\mathcal{M}(\mathfrak{h})^T$.

E. Semi-direct product

In this paper, we construct some finite groups mainly by taking semi-direct products on two cyclic groups.

Definition 2. *Let G and H be two groups, and $\varphi : G \to \mathrm{Aut}(H)$ be a group homomorphism, where $\mathrm{Aut}(H)$ represents the automorphism group of H. The* semi-direct product *group of G and H induced by φ is defined as a set $K = \{(g, h) \mid g \in G, h \in H\}$ with multiplication law "$\cdot$":*

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, \varphi(g_2^{-1})(h_1) \cdot h_2).$$

We denote K with multiplication "$\cdot$" by $G \ltimes_{\varphi} H$, or simply $G \ltimes H$.

It should be emphasized that semi-direct product as a binary operation of groups is not commutative. From the definition provided above, we can verify that H is a normal subgroup of K, but G may not be. Additionally, the semi-direct product $G \ltimes H$ may not be unique, as its structure varies depending on φ.

[2]The choice of the basis doesn't significantly affect the analysis in the following essentially, we provide this definition here to avoid ambiguity.

In particular, if we consider the identity mapping for φ, i.e., for every element $g \in G$, $\varphi(g) = \mathrm{id}_H$, then the semi-direct product degrades to direct product, namely $G \times H$. In this case, the elements of G and H act "independently" of each other.

Example 1. *The dihedral group D_{2n} can be generated by two elements s and t with the relation $sts = t^{-1}$, where the order of s and t are 2 and n, respectively. Precisely,*

$$D_{2n} := \langle s, t : s^2 = t^n = 1, sts = t^{-1} \rangle.$$

Then D_{2n} can also be represent as $\mathbb{Z}_2 \ltimes_\varphi \mathbb{Z}_n$, where $\varphi(s) = \mathrm{inv}$, where inv *maps each element of $\mathbb{Z}_n$ to its inverse (under addition modulo n).*

Inspired by Example 1, we first give two types of groups which are utilized in this paper.

Type I: $\mathbb{Z}_m \ltimes_\varphi \mathbb{Z}_n$: Let m be an even positive integer, and n be an arbitrary positive integer. Denote $\mathbb{Z}_m$ and $\mathbb{Z}_n$ as two cyclic groups with generators s and t, respectively, i.e., $\mathbb{Z}_m = \langle s \rangle$ and $\mathbb{Z}_n = \langle t \rangle$. Let σ be an element in the automorphism group $\mathrm{Aut}(H)$, which maps each element of H to its inverse. Define a homomorphism $\varphi : G \to \mathrm{Aut}\, H$ with $\varphi(s) = \sigma$. Induced by φ, we can define $\mathbb{Z}_m \ltimes_\varphi \mathbb{Z}_n$, denoted as $\mathbb{Z}_m \ltimes \mathbb{Z}_n$ below:

$$\mathbb{Z}_m \ltimes \mathbb{Z}_n := \langle s, t : s^m = 1, t^n = 1, sts^{-1} = t^{-1} \rangle. \tag{2}$$

Type II: $\mathbb{Z}_n^* \ltimes_\psi \mathbb{Z}_n$: Let n be an arbitrary positive integer and let $\mathbb{Z}_n$ denote a multiplicative cyclic group with generator g. Denote $\mathbb{Z}_n^*$ as the set of all positive integers no more than n that are coprime with n. For instance, $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$. It is easy to verify that $\mathbb{Z}_n^*$ forms a group under the operation of multiplication modulo n.

It is also known that the automorphism group of $\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_n^*$. Thus we have a natural isomomorphism ψ mapping $\mathbb{Z}_n^*$ to $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$, where $\psi(a) = \psi_a \in \mathrm{Aut}(\mathbb{Z}_n)$ and

$$\psi_a(g) = g^a.$$

Similar to Type I, the semi-direct product of $\mathbb{Z}_n^*$ and $\mathbb{Z}_n$ can be induced by ψ. Here we use the symbol $a \odot g^k$ to represent the element (a, g^k) in the group $\mathbb{Z}_n^* \ltimes \mathbb{Z}_n$. Then the semi-direct product can be expressed as follows:

$$\mathbb{Z}_n^* \ltimes \mathbb{Z}_n := \{a \odot g^k : a \in \mathbb{Z}_n^*, 0 \le k < n\}, \tag{3}$$

the multiplication of which is induced by ψ and satisfies

$$(a \odot g^{k_1})(b \odot g^{k_2}) = ab \odot g^{k_1 b^{-1} + k_2}$$

as in Definition 2.

Remark 1. *In particular, when $m = 2$ is additionally satisfied in Type I, the group $\mathbb{Z}_m \ltimes \mathbb{Z}_n$ defined by* (2) *is exactly the dihedral group $D_{2n} = \mathbb{Z}_2 \ltimes \mathbb{Z}_n$.*

We select these two types of groups mainly because their irreducible representations can be computed by the representation theory of finite groups. We provide two lemmas in this paper to present the irreducible representations of these two types of groups. The proofs require some basic knowledge and techniques in representation theory. They are attached in the appendix section in details.

Lemma 5 (Irreducible representations of Type I)**.** *Let $G_1 = \mathbb{Z}_m \ltimes_\varphi \mathbb{Z}_n = \langle s \rangle \ltimes_\varphi \langle t \rangle$ be a finite group defined by* (2)*, where $m = 2r$ is even and let ω and ξ be the m-th and n-th primitive roots of unity, respectively.*

(i) *If $n = 2u+1$ is odd, then G_1 has $m = 2r$ (non-equivalent) 1-dimensional irreducible representations χ_i $(i = 1, 2, \ldots, 2r)$, satisfying*

$$\chi_i(t) = 1, \quad \chi_i(s) = \omega^i;$$

and ru (non-equivalent) 2-dimensional irreducible representations $\rho_{i,j}$ $(i = 1, 2, \ldots, r,\ j = 1, 2, \ldots, u)$, satisfying

$$\rho_{i,j}(t) = \begin{pmatrix} \xi^j & \\ & \xi^{n-j} \end{pmatrix},$$
$$\rho_{i,j}(s) = \begin{pmatrix} 0 & \omega^{2i} \\ 1 & 0 \end{pmatrix}.$$

(ii) *If $n = 2u$ is even, then G_1 has $2m = 4r$ (non-equivalent) 1-dimensional irreducible representations χ_i $(i = 1, 2, \ldots, 4r)$, satisfying*

$$\chi_i(t) = 1, \quad \chi_i(s) = \omega^i,\ i = 1, \ldots, 2r,$$
$$\chi_i(t) = -1, \quad \chi_i(s) = \omega^i,\ i = 2r+1, 2r+2, \ldots, 4r,$$

and $r(u-1)$ (non-equivalent) 2-dimensional irreducible representations $(i = 1, 2, \ldots, r,\ j = 1, 2, \ldots, u-1)$ satisfying

$$\rho_{i,j}(t) = \begin{pmatrix} \xi^j & \\ & \xi^{n-j} \end{pmatrix},$$
$$\rho_{i,j}(s) = \begin{pmatrix} 0 & \omega^{2i} \\ 1 & 0 \end{pmatrix},$$

As for finite groups of Type II, we only provide an upper bound of the dimensions of all irreducible representations for simplicity, which is sufficient for the analysis in this paper. It can be verified that if r is coprime with s, then $\mathbb{Z}_{rs} \cong \mathbb{Z}_r \times \mathbb{Z}_s$ and $\mathbb{Z}_{rs}^* \cong \mathbb{Z}_r^* \times \mathbb{Z}_s^*$. Furthermore, $\mathbb{Z}_{rs}^* \ltimes \mathbb{Z}_{rs} \cong (\mathbb{Z}_r^* \times \mathbb{Z}_s^*) \ltimes (\mathbb{Z}_r \times \mathbb{Z}_s) \cong (\mathbb{Z}_r^* \ltimes \mathbb{Z}_r) \times (\mathbb{Z}_s^* \ltimes \mathbb{Z}_s)$, hence it suffices to list all the irreducible representations of $\mathbb{Z}_{p^k}^* \ltimes \mathbb{Z}_{p^k}$ where p is a prime and k is a positive integer. By tensoring the irreducible representations of $\mathbb{Z}_{p_i^{k_i}}^* \ltimes \mathbb{Z}_{p_i^{k_i}}$ for each prime factor p_i in the decomposition $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$, where $i = 1, 2, \cdots, m$, we can obtain all irreducible representations of $\mathbb{Z}_n^* \ltimes \mathbb{Z}_n$. For groups constructed by the semi-direct product of two Abelian groups, we can determine all their irreducible representations. Refer to [31] for detailed information.

Lemma 6 (Irreducible representations of Type II)**.** *Let $G_2 = \mathbb{Z}_{p^k}^* \ltimes \mathbb{Z}_{p^k}$ is defined as* (3)*, where p is prime and k is a positive integer. Then G_2 only has irreducible representations with dimension no greater than p^{k-1}.*

Proof. Let $n_1, n_2, \ldots, n_s$ be the dimensions of all (non-equivalent) irreducible representations of G_2. According to the representation theory, we have

$$n_1^2 + n_2^2 + \cdots + n_s^2 = |G_2| = p^{2k-1}(p-1),$$
$$n_i \mid |G_2| \quad \text{for } 1 \le i \le s.$$

Thus it follows immediately that $n_i \le p^{k-1}$ for all i. □

It is also crucial to analyze all the eigenvalues of the group ring elements when regarded as a linear transformation induced by the left multiplication law. In fact, we can compute all eigenvalues of the linear transformations determined by the elements in $\mathbb{C}[G]$, where G belongs to Type I or Type II. To perform these computations, we need to use some fundamental representation theory and techniques.

Lemma 7. 1) *Let m be an even positive integer and n be an arbitrary positive integer. Consider the group $G_1 := \mathbb{Z}_m \ltimes_\varphi \mathbb{Z}_n = \langle s \rangle \ltimes_\varphi \langle t \rangle$ defined by* (2)*. Let $\mathfrak{h} = \sum_{i=0}^{m-1} s^i f_i(t) \in \mathbb{C}[G]$, where $f_i(t)$ is a polynomial of degree no more than n. All the eigenvalues of the matrix $\mathcal{M}(\mathfrak{h})$ are given by*

$$f_0(\xi^j) + \omega^i f_1(\xi^j) + \cdots + \omega^{i(m-1)} f_{m-1}(\xi^j), \quad i = 0, 1, \ldots, m-1, j = 0, 1, \ldots, n-1,$$

where ω, ξ are m-th,n-th primitive roots of unity, respectively.

2) *Let p be a prime and k be a positive integers. Denote $m := p^k - p^{k-1}$ and consider the group $\mathbb{Z}_{p^k}^* \ltimes_\psi \mathbb{Z}_{p^k}$ defined by* (3)*. Let a be a multiplicative primitive element of $\mathbb{Z}_{p^k}^*$. Let $\mathfrak{h} = \sum_{r=0}^{m-1} \sum_{s=0}^{p^k-1} f_{rs}(a^r \odot g^s)$, where f_{rs} are complex numbers, then all the eigenvalues of the matrix $\mathcal{M}(\mathfrak{h})$ are given by*

$$\sum_{r=0}^{m-1} \sum_{s=0}^{p^k-1} f_{rs}(\omega^{ir} \cdot \xi^{js}), \quad i = 0, 1, \ldots, m-1, j = 0, 1, \ldots, p^k - 1,$$

where ω, ξ are m-th, p^k-th primitive roots of unity, respectively.

Proof. It is natural that each element in $\mathbb{C}[G]$ determines a left multiplication action on $\mathbb{C}[G]$ itself. Here we consider the groups of Type I for instance, and the analysis for Type II follows essentially the same approach. Each irreducible subrepresentation of group G_1 can be found as a summand of left regular representation. Referring to Lemma 5 and representation theory, the matrix determined by the regular representation over a specific basis is similar to a block diagonal matrix with block size no greater than 2, where each block corresponds to an irreducible subrepresentation of G. By Lemma 5, we know all irreducible subrepresentations of G. Therefore, all the eigenvalues can be calculated by considering the eigenvalues of each subrepresentation. □

F. Ideal lattice and coefficient embedding

A *left (integral) ideal* $\mathcal{I}$ of the group ring $\mathbb{Z}[G]$ is an additive subgroup of G that is closed under left multiplication by any element in $\mathbb{Z}[G]$, i.e., $\mathfrak{h}x \in \mathcal{I}$ holds for any $\mathfrak{h} \in \mathbb{Z}[G]$ and $x \in \mathcal{I}$. A left ideal has a $\mathbb{Z}$-basis as a free left $\mathbb{Z}$-submodule of rank n. The *left inverse* of the ideal $\mathcal{I}$ is defined as

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

An ideal $\mathcal{I}$ is referred to as *left invertible* if its left inverse $\mathcal{I}^{-1}$ is such that $\mathcal{I}^{-1}\mathcal{I} = \mathbb{Z}[G]$. And it can be verified that $\mathcal{I}^{-1}$ is a *left fractional ideal* of $\mathbb{Z}[G]$ which means there exists $t \in \mathbb{Z}$, such that $t\mathcal{I}^{-1} \subseteq \mathbb{Z}[G]$.

In algebraically structured LWE, an algebraic number field is typically embedded into the real Euclidean space $\mathbb{R}^n$ using canonical embedding as described in [1]. However, when dealing with group ring LWE, we choose the coefficient embedding for simplicity due to the relatively complicated non-commutative multiplicative operation.

Since the group ring $\mathbb{Z}[G]$ is a free $\mathbb{Z}$-module, and the elements of G naturally form a $\mathbb{Z}$-basis of $\mathbb{Z}[G]$, we have an embedding

$$\varphi : \mathbb{Z}[G] \to \mathbb{R}^n, \quad \sum_{i=1}^{n} a_i g_i \mapsto (a_1, a_2, \ldots, a_n)$$

referred to as the *coefficient embedding* of $\mathbb{Z}[G]$, which means the mapping embeds the elements in $\mathbb{Z}[G]$ into $\mathbb{R}^n$ according to their coefficients. Moreover, we can also extend the domain of φ to the module tensor product $\mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{R}[G]$, which we denoted by $\bar{\varphi}$. The extension $\bar{\varphi} : \mathbb{R}[G] \to \mathbb{R}^n$ is bijective. For simplicity, in this paper, we also use the notation φ instead of $\bar{\varphi}$.

Under the coefficient embedding φ, any element $\sum_{i=1}^{n} a_i g_i \in \mathbb{R}[G]$ can be represented uniquely by a vector in $\mathbb{R}^n$, where n is the rank of $\mathbb{R}[G]$ as an $\mathbb{R}$-module. This allows us to define *norm* on elements of $\mathbb{R}[G]$ by taking the corresponding norm of the vector representation. For an element $\mathfrak{h} \in \mathbb{R}[G]$, its norm is defined as

$$\|\mathfrak{h}\| = \left\| \sum_{i=1}^{n} a_i g_i \right\| := \|(a_1, a_2, \ldots, a_n)\|,$$

where $\|\cdot\|$ on the right-hand side is any norm defined on vectors in $\mathbb{R}^n$.

Furthermore, it can be easily verified that the coefficient embedding φ maps any (fractional) ideal of the ring to a full-rank discrete additive subgroup in $\mathbb{R}^n$, which is consequently a lattice. Here, n is both the rank of the group ring and the lattice. Such lattices induced by a fractional ideal are commonly referred

to as *ideal lattices*. Every (left, right, two-sided/fractional) ideal $\mathcal{I}$ of $\mathbb{Z}[G]$ can be viewed as a lattice in $\mathbb{R}^n$ under coefficient embedding. Moreover, if $\{u_1, u_2, \ldots, u_n\}$ forms a $\mathbb{Z}$-basis of the ideal $\mathcal{I}$, then $\{\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_n)\} \subset \mathbb{R}^n$ forms a basis for the lattice induced by $\mathcal{I}$. Therefore, we can always identify $\mathcal{I}$ as a lattice in $\mathbb{R}^n$.

Through the study of ideal lattice $\mathcal{I}$ of a group ring, it is crucial to consider the relationship between dual ideal lattice $\mathcal{I}^\vee$ and inverse ideal $\mathcal{I}^{-1}$. In the following lemma, we primarily consider the two types of groups defined by (2) and (3). We show that the dual ideal lattice and the inverse ideal lattice of the same invertible ideal lattice are equivalent, up to a specific permutation of the coordinates. The following lemma generalizes the result of Lemma 3 of [30] to Type I and Type II. The proof is attached in the appendix.

Lemma 8. *For any invertible (right) ideal $\mathcal{I}$ of $\mathbb{Z}[G]$ where G is any group of Type I and Type II, let $\mathcal{I}^{-1}$ be the left inverse of $\mathcal{I}$. Then the dual lattice $\mathcal{I}^\vee$ of $\mathcal{I}$ (under coefficient embedding) and $\mathcal{I}^{-1}$ are the same by rearranging the order of the coordinates.*

In the following lemma, we establish the connection between ℓ_2 norm of the elements in $\mathbb{Z}[G]$ as defined above, and the matrix norm $\|\cdot\|_{\mathrm{Mat}}$.

Lemma 9. *Let $\mathbb{R}[G]$ be a group ring where G is a finite group of order n. If $\mathfrak{h} \in \mathbb{R}[G]$ is sampled from D_r (which means every coefficient of $\mathfrak{h}$ is sampled independently from one-dimensional Gaussian D_r), then the matrix norm of $\mathfrak{h}$ is at most nr except with negligible probability.*

Proof. We bound the matrix norm of $\mathfrak{h}$ by analyzing its relationship with ℓ_2 norm. Since all group elements of G inherently form an $\mathbb{R}$-basis of $\mathbb{R}[G]$, we obtain a transformation matrix $\mathcal{M}(\mathfrak{h})$ which represents the left multiplication action determined by $\mathfrak{h}$ over such a basis. For any element $\tau \in \mathbb{R}[G]$ with an ℓ_2-norm equal to 1, we denote its coefficient vector as $\mathbf{t}$, i.e., $\|\mathbf{t}\|_{\ell_2} = 1$. By considering the ℓ_2-norm of $\mathcal{M}(\mathfrak{h}) \cdot \mathbf{t} \in \mathbb{R}^n$, we have

$$\|\mathcal{M}(\mathfrak{h}) \cdot \mathbf{t}\|_{\ell_2} \leq \sqrt{n} \cdot \|\mathfrak{h}\|_{\ell_2} \|\mathbf{t}\|_{\ell_2}$$

after applying the Cauchy-Schwarz inequality. From Lemma 2, the ℓ_2 norm of $\mathfrak{h}$ is less than $r\sqrt{n}$ except with probability exponentially closed to 0. Therefore, we obtain

$$\|\mathcal{M}(\mathfrak{h}) \cdot \mathbf{t}\|_{\ell_2} \leq nr,$$

which means $\|\mathfrak{h}\|_{\mathrm{Mat}} \leq nr$ except with negligible probability. □

Remark 2. *When applying the same process as described in Lemma 10 of [30], we can obtain a tighter bound compared to the one given by Lemma 9 in this paper when restricting G to a specific group. It should be pointed out that for group $G = \mathbb{Z}_m \ltimes \mathbb{Z}_n$ of Type I, the matrix norm of the elements in $\mathbb{R}[G]$ which are sampled from D_r can be bounded by $\omega(\sqrt{\log |G|}) \cdot \sqrt{|G|} \cdot r$, which is asymptotically smaller than $|G| \cdot r$ obtained from Lemma 9. However, in this paper, we also use the more general bound as mentioned in Lemma 9 for generality.*

G. Lattice problems

We introduce some important and useful problems which are believed to be computionally hard. They are commonly used to characterize the hardness of LWE variants. These problems include *Shortest Vector Problem* (SVP), *Shortest Independent Vectors Problem* (SIVP), *Closest Vector Problem* (CVP), and *Bounded Distance Decoding* (BDD). The following definitions follow the standard formulations used in [8].

Definition 3 (SVP and SIVP)**.** *Let $\mathcal{L}$ be an n-dimensional lattice and let $\gamma = \gamma(n) \geq 1$. The SVP_γ problem in the given norm is: find some nonzero vector $\mathbf{v} \in \mathcal{L}$ such that $\|\mathbf{v}\| \leq \gamma \cdot \lambda_1(\mathcal{L})$. The SIVP_γ problem is to find n linearly independent vectors in $\mathcal{L}$ whose norms are all no more than $\gamma \cdot \lambda_n(\mathcal{L})$.*

Definition 4 (CVP)**.** *Let $\mathcal{L}$ be an n-dimensional lattice and let $\gamma \geq 1$. The CVP_γ problem in the given norm is: given a target vector $\mathbf{t} \in \mathbb{R}^n$ (which may not be a lattice vector), find some vector $\mathbf{v} \in \mathcal{L}$ such that $\|\mathbf{v} - \mathbf{t}\| \leq \gamma \cdot \|\mathbf{v}' - \mathbf{t}\|$ for any lattice vector $\mathbf{v}'$.*

The following problem is a variant version of CVP where the distance between the target vector and the lattice is bounded.

Definition 5 (BDD)**.** *Let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice, and let $d < \lambda_1(\mathcal{L})/2$. The $\mathsf{BDD}_{\mathcal{L},d}$ problem in the given norm is: given $\mathcal{L}$ and $\mathbf{y}$ of the form $\mathbf{y} = \mathbf{x} + \mathbf{e}$ for some $\mathbf{x} \in \mathcal{L}$ and $\mathbf{e} \in \mathbb{R}^n$ with $\|\mathbf{e}\| \leq d$, find $\mathbf{x}$.*

Another problem called *Gaussian Decoding Problem* (GDP), is essentially BDD when the offset is sampled from a Gaussian distribution.

Definition 6 (GDP)**.** *For a lattice $\mathcal{L} \subset \mathbb{R}^n$ and a Gaussian parameter $g > 0$. The $\mathsf{GDP}_{\mathcal{L},g}$ problem is: given a coset $\mathbf{e} + \mathcal{L}$ where $\mathbf{e}$ is sampled from D_g, find $\mathbf{e}$.*

The following lemma states that if the bound d in BDD is significantly smaller compared to the length of the shortest nonzero vector in a lattice $\mathcal{L}$, then there exists an efficient (within time $\mathrm{poly}(n)$, where n is the dimension of the lattice) algorithm, that can solve $\mathsf{BDD}_{\mathcal{L},d}$.

Lemma 10 ([47], [48], Babai's Algorithm)**.** *There is an polynomial-time algorithm that solves $\mathsf{BDD}_{\mathcal{L},d}$ for $d = 2^{-n/2}\lambda_1(\mathcal{L})$.*

The following problem, which is called *Discrete Gaussian Sampling* (DGS) problem, is needed in the process of reduction mentioned in Section III and Section IV.

Definition 7 (DGS)**.** *Let R be a ring. R-DGS_γ asks that given an (invertible) ideal $\mathcal{I}$ of R and a real number $s \geq \gamma = \gamma(\mathcal{I})$, produce samples from the distribution $D_{\mathcal{I},s}$.*

In the following text, we only consider above problems in the context of (invertible) ideal lattices in a certain group ring.

H. Natural inclusion mapping

When establishing reductions from hard problems in ideal lattices, it is common to consider the relationship between different (ideal) lattices.

Let q be a positive integer and $\mathcal{L}$ be a lattice. Denote $\mathcal{L}_q$ as the quotient $\mathcal{L}/q\mathcal{L}$. For any lattices $\mathcal{L}' \subseteq \mathcal{L}$, the *natural inclusion map* is defined as $\varphi : \mathcal{L}'_q \to \mathcal{L}_q$ which maps $x + q\mathcal{L}'$ to $x + q\mathcal{L}$.[3] The natural inclusion map can be viewed as a composition of a natural homomorphism $\mathcal{L}/q\mathcal{L}' \to (\mathcal{L}/q\mathcal{L}')/(q\mathcal{L}/q\mathcal{L}') = \mathcal{L}/q\mathcal{L}$ and an inclusion map $\mathcal{L}'/q\mathcal{L}' \to \mathcal{L}/q\mathcal{L}'$.The following lemma is an important result from [13]. It describes under what condition the natural inclusion map φ is a bijection.

Lemma 11 ([13], Lemma 2.13)**.** *Let $\mathcal{L}' \subseteq \mathcal{L}$ be n-dimensional lattices and q be a positive integer. Then the natural inclusion map $\varphi : \mathcal{L}'_q \to \mathcal{L}_q$ is a bijection if and only if q is coprime with the index $|\mathcal{L}/\mathcal{L}'|$; In this case, φ is efficiently computable and invertible given an arbitrary basis of $\mathcal{L}'$ relative to a basis of $\mathcal{L}$.*

Remark 3. *We can also apply Lemma 11 to dual lattice $\mathcal{L}^\vee$. As $|\mathcal{L}/\mathcal{L}'| = |(\mathcal{L}')^\vee/\mathcal{L}^\vee|$, we can obtain that*

$$\psi : (\mathcal{L}'_q)^\vee \to \mathcal{L}_q^\vee, \quad \psi(x + q(\mathcal{L}')^\vee) = x + q\mathcal{L}^\vee$$

is also a bijection with the same condition as specified Lemma 11.

[3]It can be verified that the definition of natural inclusion map is well-defined under the condition that $\mathcal{L}' \subseteq \mathcal{L}$.

I. Group ring LWE

To prevent the potential attacks that exploit one-dimensional (irreducible) representations of the group G, one can use the quotient ring of $\mathbb{Z}[G]$ modulo the sum of ideals associated with its corresponding information-leaking representations. According to the Artin-Wedderburn theorem, we can uniquely decompose the group algebra $\mathbb{C}[G]$ into the direct sum of simple ideals (also simple left $\mathbb{C}[G]$-modules). Moreover, these ideals are isomorphic to matrix rings over $\mathbb{C}$. Precisely,

$$\mathbb{C}[G] \cong M_{n_1}(\mathbb{C}) \oplus M_{n_2}(\mathbb{C}) \oplus \cdots \oplus M_{n_r}(\mathbb{C}),$$

where $M_{n_i}(\mathbb{C}) \cong \mathbb{C}^{n_i \times n_i}$ denotes the ring of all $n_i \times n_i$ matrices over $\mathbb{C}$. For each i, $M_{n_i}(\mathbb{C})$ is a simple ideal corresponding to an n_i-dimensional irreducible representation of G and r equals the number of non-equivalent irreducible representations of G.

For instance, we consider group $G_1 = \mathbb{Z}_m \ltimes \mathbb{Z}_n$ defined by (2). According to Lemma 5, the group algebra $\mathbb{C}[G_1]$ can be decomposed as follows:

$$\mathbb{C}[G_1] \cong \begin{cases} \bigoplus_{i=1}^{m} \mathbb{C} \oplus \bigoplus_{j=1}^{rt} \mathbb{C}^{2\times 2}, & \text{if } n \text{ is even;} \\ \bigoplus_{i=1}^{2m} \mathbb{C} \oplus \bigoplus_{j=1}^{r(t-1)} \mathbb{C}^{2\times 2}, & \text{if } n \text{ is odd.} \end{cases}$$

From representation theory, each direct summand $\mathcal{B}$ in the Artin-Wedderburn decomposition of $\mathbb{C}[G]$ above is a minimal principal ideal of $\mathbb{C}[G]$ with a generator referred to as *central primitive idemptotent*. [49] provides a method to determine all central primitive idempotents of the group algebra $\mathbb{C}[G]$ where G is the semi-direct product of two finite Abelian groups. Consequently, we can easily compute the simple ideal of $\mathbb{C}[G]$ corresponding to one-dimensional representations of G when G is either of Type I or Type II.

Example 2. *According to the Artin-Wedderburn theorem, we can decompose $\mathbb{C}[D_{2n}]$ into the direct sum of simple ideals. When n is even, we have*

$$\mathbb{C}[D_{2n}] \cong \bigoplus_{i=0}^{3} \mathbb{C} \oplus \bigoplus_{i=4}^{(n+4)/2} \mathbb{C}^{2\times 2}.$$

By [49], we can obtain all the central primitive idempotents corresponding to one-dimensional representation of D_{2n} as follows:

$$(1 + t + t^2 + \cdots + t^{n-1})(1 \pm s),$$
$$(1 - t + t^2 + \cdots - t^{n-1})(1 \pm s).$$

Each of these four idempotents generates a simple ideal and each of these ideal divides $\langle t^{n/2} + 1\rangle$ when $4 \mid n$. Thus we can assert that $\mathbb{C}[D_{2n}]/\langle t^{n/2} + 1\rangle$ eliminate the potential attack making use of the 1-dimensional representations of D_{2n}.

When n is odd, there are two one-dimensional irreducible representations for D_{2n}, and the corresponding central primitive idempotents are given by

$$(1 + t + t^2 + \cdots + t^{n-1})(1 \pm s).$$

In this case, we can select $\mathbb{C}[D_{2n}]/\langle 1 + t + t^2 + \cdots + t^{n-1}\rangle$ for our purpose.

Here we describe the LWE problem over group rings. We use the following conventional notations from [1], [30]. Let G be a finite group and let R be the group ring $\mathbb{Z}[G]$ itself or one of its quotient rings. For an integer modulus $q \geq 2$, let R_q denote the quotient ring R/qR. Likewise, for any (fractional) ideal $\mathcal{I}$ of a ring R, let $\mathcal{I}_q$ denote $\mathcal{I}/q\mathcal{I}$. We also denote $R_{\mathbb{R}}$ as the tensor product $R \otimes_{\mathbb{Z}} \mathbb{R}$ and let $\mathbb{T} := R_{\mathbb{R}}/R$.

Definition 8 (Group ring-LWE distribution)**.** *For a secret element $s \in R_q$ and an error distribution ψ over $R_{\mathbb{R}}$, a sample chosen from the R-*LWE *distribution $A_{s,\psi}$ over $R_q \times \mathbb{T}$ is generated by sampling $a \in R_q$ uniformly and $e \leftarrow \psi$, and then outputting $(a, (s \cdot a)/q + e \bmod R)$.*

Definition 9 ([30], Search Group ring-LWE)**.** *Let Ψ be a family of distributions over $R_{\mathbb{R}} \times \mathbb{T}$. The* search *version Group ring-*LWE *problem asks to find the secret element $s \in R_q$, given arbitrarily many independent samples $(a_i, b_i) \in R_q \times \mathbb{T}$ chosen from the R-*LWE *distribution $A_{s,\psi}$ for some arbitrary $s \in R_q$, where ψ is a distribution of Ψ. We denote such search problem by R-$\mathsf{LWE}_{q,\Psi}$.*

Definition 10 ([30], Average-case decision Group ring-LWE)**.** *Let Υ be a distribution over a family of distributions, each over $R_{\mathbb{R}}$. The* (average-case) decision *version Group ring-*LWE *problem asks to distinguish between polynomially many samples from R-*LWE *distribution $A_{s,\psi}$ for a uniformly random $(s, \psi) \leftarrow R_q \times \Upsilon$, and the same number of uniformly random and independent samples from $R_q \times \mathbb{T}$ with non-negligible advantage. We denote such decision problem by R-$\mathsf{DLWE}_{q,\Upsilon}$.*

J. Oracle hidden center problem

In the process of reduction to R-DLWE, it is necessary to analyze the properties of the given R-DLWE oracle. In [8], Peikert et al. provided a direct reduction from worst-case lattice problem to decision Ring-LWE. This reduction possesses tighter parameters and more compact error rates compared to those in [1], where the authors established hardness by additionally reducing search Ring-LWE to decision Ring-LWE. The technique introduced in [8] exploits the properties of a suitable decision LWE oracle, which is abstracted as an "oracle with a hidden center". Such an oracle enables dealing with BDD problem in ideal lattices as needed in the proof of the reduction, thus facilitating the hardness proof.

Definition 11 ([8], Oracle Hidden Center Problem (OHCP))**.** *For any $\varepsilon, \delta \in [0, 1)$ and $\beta \geq 1$, the $(\varepsilon, \delta, \beta)$-OHCP is an approximate search problem defined as below. An instance consists of a scale parameter $d > 0$ and randomized oracle $\mathcal{O} : \mathbb{R}^k \times \mathbb{R}^{\geq 0} \to \{0, 1\}$ which satisfies for an input $(\mathbf{z}, t)$ for $\|\mathbf{z} - \mathbf{z}^*\| \leq \beta d$,*

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

for some (unknown) "hidden center" $\mathbf{z}^* \in \mathbb{R}^k$ with $\delta d \leq \|\mathbf{z}^*\| \leq d$ and some (unknown) function p. The goal is to output some $\tilde{\mathbf{z}} \in \mathbb{R}^k$ such that $\|\tilde{\mathbf{z}} - \mathbf{z}^*\| \leq \varepsilon d$.

In [8], Peikert et al. showed that there is an efficient algorithm to solve OHCP if the oracle of the instance satisfies certain conditions. Specifically, it states as follows.

Proposition 1 ([8], Proposition 4.4)**.** *There is a $\mathrm{poly}(\kappa, k)$-time algorithm that takes as input a confidence parameter $\kappa \geq 20 \log(k + 1)$ with the scale parameter $d > 0$ and solves $(\exp(-\kappa), \exp(-\kappa), 1 + 1/\kappa)$-OHCP in dimension k with accept probablity greater than $1 - \exp(-\kappa)$, provided that 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;*
3) *$p(s)$ is κ-Lipschitz in s, i.e., $|p(s_1) - p(s_2)| \leq \kappa |s_1 - s_2|$ for all s_1, s_2,*

where $p(s)$ is the acceptance probability of $\mathcal{O}$ on input $(\mathbf{0}, s)$.

III. The hardness of search GR-LWE

For $G_1 = \mathbb{Z}_m \ltimes \mathbb{Z}_n = \langle s \rangle \ltimes \langle t \rangle$ of Type I with m an even integer and $4 \mid n$, we choose the group ring $R^{(1)} = \mathbb{Z}[G_1]/\langle t^{n/2} + 1 \rangle$. The reason for selecting this group is the same as mentioned in [30]. This ring does not have direct summands corresponding to one-dimensional representations, thereby ensuring its resistance against the aforementioned potential attacks. Similarly, for $G_2 = \mathbb{Z}_{p^k}^* \ltimes \mathbb{Z}_{p^k}$ of Type II where we denote the generator of $\mathbb{Z}_{p^k}$ as g, we select the group ring $R^{(2)} = \mathbb{Z}[G_2]/\langle 1 + g + g^2 + \cdots + g^{p^k - 1} \rangle$.

A. Main result

We claim that for rings $R^{(1)}$ and $R^{(2)}$ (or more generally, the group ring with equivalent dual ideal and inverse ideal up to a certain permutation under coefficient embedding), the hardness of search LWE problems over them is based on the hardness of finding short vectors in related ideal lattices, similar to the reduction in [1]. To be specific, we state the results as follows. From this section, we denote $\omega(f(n))$ as some fixed function that grows asymptotically faster than $f(n)$. Additionally, we define the family $\Psi_{\leq\alpha}$ for a positive real α as the set of all elliptical Gaussian distributions $D_{\mathbf{r}}$ with each coordinate $r_i \leq \alpha$.

Theorem 1 (Main Result)**.** *Let $R = \mathbb{Z}[G]$ be a group ring where G is of Type I or Type II with n elements. Let $\alpha = \alpha(n) > 0$, and let $q = q(n) \geq 2$ be such that $\alpha q \geq 2n$. For some negligible $\varepsilon = \varepsilon(n)$, there is a probabilistic polynomial-time quantum reduction from R-DGS_γ (and hence SIVP with approximate factor $\tilde{O}(n^{3/2}/\alpha)$) to (search) R-$\mathsf{LWE}_{q,\Psi_{\leq\alpha}}$, where*

$$\gamma = \max\{\eta_\varepsilon(\mathcal{I}) \cdot (\sqrt{2}n/\alpha), 2\sqrt{n}/\lambda_1(\mathcal{I}^\vee)\}. \tag{4}$$

Recall that the R-DGS problem asks to sample from discrete Gaussian distribution over the (invertible) ideal $\mathcal{I}$ efficiently. In [4], the author presented a direct reduction from standard lattice problems to the DGS problem. Combining this result, Theorem 1 accomplishes the reduction from lattice problems to search GR-LWE. To be precise, based on Lemma 4 and Claim 2.13 in [4], we know that $1/\lambda_1(\mathcal{I}^\vee) \leq \eta_\varepsilon(\mathcal{I}) \leq \lambda_n(\mathcal{I}) \cdot \omega(\sqrt{\log n})$ for any ideal lattice $\mathcal{I}$ in $\mathbb{R}^n$. By Lemma 2, we obtain the ℓ_2-norm of samples from $D_{\mathcal{I},\gamma}$ is at most $\gamma\sqrt{n}$ except with negligible probability. Consequently, we can use the outputs of DGS_γ as a solution of SIVP with approximate factor $\tilde{O}(n^{3/2}/\alpha)$ when α is restricted to be no greater than $\sqrt{n}$. This problem is believed to be a computationally hard problem, and the restriction is always satisfied to make the problem information-theoretically solvable.

Remark 4. *For the sake of completeness, we prove the results for the group ring $\mathbb{Z}[G_1]$ and $\mathbb{Z}[G_2]$ rather than the quotient groups $R^{(1)}$ and $R^{(2)}$. In fact, using the same procedure and fundamental homomorphism theorem, we can also prove the same result for $R^{(1)}$ and $R^{(2)}$. It is also worth noting that by applying the results mentioned in Remark 2, the approximate factor can be further optimized to $\tilde{O}(n/\alpha)$ on these two particular groups.*

Proof of Theorem 1. According to Lemma 3.2 in [4], one can sample efficiently from $D_{\mathcal{I},r}$ for sufficiently large r, say $r > 2^{2n}\lambda_n(\mathcal{I})$. In this case, polynomially many samples from $D_{\mathcal{I},r}$ can be generated typically by the following steps. First, generate sample y from (continuous) Gaussian distribution D_r using the standard method, then output $y - (y \bmod \mathcal{I}) \in \mathcal{I}$. Next, we can repeatedly apply the reduction specified by Lemma 12 (but still polynomial times) mentioned later. This allows us to sample from discrete Gaussian distribution with narrower and narrower parameters. Since $\alpha q \geq 2n$, the iterative steps enable us to sample from $D_{\mathcal{I},r/2}$ given polynomially many samples from $D_{\mathcal{I},r}$. The repeating iteration continues until the Gaussian parameter reaches the desired value $s \geq \gamma$. Finally, the procedure ends up with one (or more) sample from $D_{\mathcal{I},s}$. □

B. The iterative step

The proof of the iterative step basically follows the procedure outlined in [4] and [1]. The reduction uses repeated *iterative steps* to achieve the goal. The iterative step states that when the initial Gaussian parameter r is sufficiently larger than the smoothing parameter, we can sample efficiently from another discrete Gaussian distribution with narrower parameters, say $r/2$.

Lemma 12 (The iterative step)**.** *Let $R = \mathbb{Z}[G]$ be a group ring where G is of Type I or Type II with n elements. Let $\alpha > 0$ and let $q > 2$ be an integer. There exists an efficient quantum algorithm that, given an invertible ideal $\mathcal{I}$ in R satisfying that $\det(\mathcal{I})$ is coprime with q, a real number $r \geq \sqrt{2}q \cdot \eta_\varepsilon(\mathcal{I})$ for some negligible $\varepsilon = \varepsilon(n) > 0$ such that $r' := rn/\alpha q > 2\sqrt{n}/\lambda_1(\mathcal{I}^\vee)$, an oracle to R-$\mathsf{LWE}_{q,\Psi_{\leq\alpha}}$, and a*

list of samples from the discrete Gaussian distribution $D_{\mathcal{I},r}$ (as many as required by the R-LWE oracle), outputs an independent sample from $D_{\mathcal{I},r'}$.

The iterative step stated above can be partitioned into two parts as in [4]. The first part of the iteration is classical, which shows that given a search R-LWE oracle, we can solve GDP on $\mathcal{I}^\vee$ making use of the given discrete Gaussian samples. The proof of this part (Lemma 13) is presented in Section 3.3.

Lemma 13 (Reduction from GDP to LWE)**.** *Let $\varepsilon = \varepsilon(n)$ be some negligible function, let $q > 2$ be an integer, and let $\alpha \in (0, 1)$ be a real number. Let $R = \mathbb{Z}[G]$ be a group ring where G is of Type I or Type II with n elements, and let $\mathcal{I}$ be an invertible ideal in R satisfying that $\det(\mathcal{I})$ is coprime with q. Given an oracle for discrete Gaussian distribution $D_{\mathcal{I},r}$, where $r \geq \sqrt{2}q \cdot \eta_\varepsilon(\mathcal{I})$, there is a probabilistic polynomial-time (classical) reduction from $\mathsf{GDP}_{\mathcal{I}^\vee,d/n}$ to $R\text{-}\mathsf{LWE}_{q,\Psi_{\leq\alpha}}$, where $d = \alpha q/(\sqrt{2}r)$.*

The second part of the iteration was initially proposed by [4] and later improved by [1]. It is worth noting that this part is the only quantum component of the whole reduction. The lemma in the following states that we can use a GDP oracle to sample polynomially many lattice vectors with a narrower width. By employing Lemma 9, we can essentially derive a similar lemma as in [30].

Lemma 14 ([4], Lemma 3.14)**.** *There is an efficient quantum algoithm that, given any n-dimensional lattice $\mathcal{L}$, a number $d' < \lambda_1(\mathcal{L}^\vee)/2$ (where λ_1 is in ℓ_2-norm), and an oracle that solves $\mathsf{GDP}_{\mathcal{L}^\vee,d'/\sqrt{2n}}$, outputs a sample from $D_{\mathcal{L}^\vee,\sqrt{n}/\sqrt{2}d'}$.*

Combining the results of Lemma 13 and Lemma 14. We can prove Lemma 12 as follows.

Proof of Lemma 12. By Lemma 13, given samples from $D_{\mathcal{I},r}$ and oracle for search $R\text{-}\mathsf{LWE}_{q,\Psi_{\leq\alpha}}$, we can solve $\mathsf{GDP}_{\mathcal{I}^\vee,d/n}$ problem with parameter $d = \alpha q/\sqrt{2}r$. By Lemma 14 and setting $d/n = d'/\sqrt{2n}$, we have

$$d' = \sqrt{2}d/\sqrt{n} = \sqrt{n}/r' < \lambda_1(\mathcal{I}^\vee)/2,$$

where the last equality comes from the condition mentioned in Lemma 13. Thus we obtain samples from $D_{\mathcal{I},r'}$. □

C. The GDP *to Search* GR-LWE *reduction*

In this section, our goal is to prove Lemma 13, which means providing a reduction from GDP problem in ideal lattices to GR-LWE. In [4], it has been proven that to solve BDD in some lattice $\mathcal{L}$, it is sufficient to find a close vector modulo $q\mathcal{L}$. We present a special case of Lemma 3.5 in [4] as follows and the proof follows essentially the same approach.

Lemma 15 ([4], Lemma 3.5)**.** *For any $q \geq 2$, there is a deterministic polynomial-time reduction from $\mathsf{BDD}_{\mathcal{I},d}$ (in matrix norm) to $q\text{-}\mathsf{BDD}_{\mathcal{I},d}$ (in the same norm).*

When dealing with coefficient embedding, it is common to consider sampling vectors from an (ideal) lattice according to a discrete Gaussian distribution. In the work of [4], the spherical Gaussian distribution was considered, and later in [1], this distribution was generalized to non-spherical Gaussians. However, in the case of GR-LWE, especially with coefficient embedding, a more generalized Gaussian is required. This distribution should have an arbitrary definite positive matrix as its covariance matrix, rather than a diagonal matrix. According to Lemma 15, it suffices to give a reduction from q-GDP to GR-LWE. Before showing this reduction, it is necessary to introduce some lemmas concerning smoothing parameters. The smoothing parameter characterizes how a discrete Gaussian over a certain lattice behaves similarly to a continuous Gaussian. As a generalization of Claim 3.9 of [4], we provide the following lemma and corollary, illustrating that when a discrete Gaussian with the smoothness condition is added to a continuous Gaussian, it "acts like" a continuous Gaussian with the same covariance matrix, up to a negligible statistical distance under certain "smoothness condition".

Lemma 16 ([30], Lemma 5)**.** *Let $\mathcal{L}$ be a lattice of $\mathbb{R}^n$. Let $\mathbf{A}, \mathbf{B}$ be two fixed non-singular matrices. Assume that smoothness condition*

$$\sum_{\mathbf{y}\in\mathcal{L}^\vee\setminus\{0\}} \exp(-\pi\mathbf{y}^t(\mathbf{A}^{-t}\mathbf{A}^{-1}+\frac{1}{s^2}\mathbf{B}^t\mathbf{B})^{-1}\mathbf{y}) \le \varepsilon$$

holds for some negligible ε. Let $\mathbf{v}$ be distributed as discrete Gaussian $D_{\mathcal{L}+\mathbf{u},\mathbf{A}}$ for arbitrary $\mathbf{u}\in\mathbb{R}^n$ and let $\mathbf{e}'\in\mathbb{R}^n$ be distributed as n-dimensional spherical (continuous) Gaussian D_σ. Then the distribution of $\mathbf{B}\cdot\mathbf{v}+\mathbf{e}'$ is within statistical distance 4ε of Gaussian distribution $D_{\mathbf{C}}$, where $\mathbf{C}=\frac{1}{2\pi}\mathbf{B}\mathbf{A}\mathbf{A}^t\mathbf{B}^t+\frac{\sigma^2}{2\pi}\mathbf{I}_n$.

By applying this lemma to a fractional ideal in $\mathbb{R}[G]$ (where the elements are under coefficient embedding), we obtain the following corollary, which generalizes Corollary 1 of [30].

Corollary 1. *Let G be a finite group of order n, and let $\mathcal{I}$ be an arbitrary fractional ideal in the group ring $\mathbb{R}[G]$. Let $\mathfrak{h}$ be some element from $\mathbb{R}[G]$ and $\alpha=\|\mathfrak{h}\|_{\mathrm{Mat}}$. Let $r,s>0$ be two reals and $t=1/\sqrt{1/r^2+\alpha^2/s^2}$. Assume that the smoothness condition*

$$\sum_{y\in\mathcal{I}^\vee\setminus\{0\}} \exp(-\pi t^2\cdot\|y\|^2) \le \varepsilon$$

holds for some negligible $\varepsilon=\varepsilon(n)>0$. Let v be ditributed as $D_{\mathcal{I}+u,r}$ for arbitrary $u\in\mathbb{R}[G]$, and let e be sampled from n-dimensional Gaussian D_s. Then the distribution of $\mathfrak{h}\cdot v+e$ belongs to n-dimensional family $\Psi_{\le\sqrt{r^2\alpha^2+s^2}}$ (under some unitary base transformation).

Proof. Under coefficient embedding φ, each element in the group ring $\mathbb{R}[G]$ is mapped to a vector in $\mathbb{R}^n$. Let $\mathcal{M}(\mathfrak{h})$ be the matrix representation of $\mathfrak{h}$. Then the element $\mathfrak{h}v+e$ is mapped to $\mathcal{M}(\mathfrak{h})\varphi(v)+\varphi(e)\in\mathbb{R}^n$. By setting $\mathbf{A}=r\cdot I_n$ and $\mathbf{B}=\mathcal{M}(\mathfrak{h})$, we can easily obtain that the largest absolute eigenvalues of $\mathbf{A}^{-1},\mathbf{B}$ are $1/r$ and s, respectively. Thus, the smallest absolute eigenvalue of $(\mathbf{A}^{-t}\mathbf{A}^{-1}+1/s^2\cdot\mathbf{B}^t\mathbf{B})^{-1}$ is bounded by $\sqrt{1/(1/r^2+\alpha^2/s^2)}=t$. Consequently,

$$\mathbf{y}^t(\mathbf{A}^{-t}\mathbf{A}^{-1}+\frac{1}{s^2}\mathbf{B}^t\mathbf{B})^{-1}\mathbf{y}\ge t^2\|\mathbf{y}\|^2$$

holds for any $\mathbf{y}\in\mathbb{R}^n$, which means smoothness condition described in Lemma 16 is satisfied. □

Remark 5. *Through a certain unitary basis transformation, we can obtain an alternative $\mathbb{Z}$-basis of $\mathbb{Z}[G]$. By adjusting the $\mathbb{Z}$-basis properly, the n coefficients of $\mathbf{B}\cdot\varphi(v)+\varphi(e)$ are distributed according to a Gaussian distribution with a diagonal covariance matrix. In this matrix, the absolute value of each diagonal element is not greater than $\sqrt{r^2\alpha^2+s^2}$. Based on the aforementioned proof, it can be observed that if all the eigenvalues of $\mathcal{M}(\mathfrak{h})$ are $\lambda_1,\lambda_2,\ldots,\lambda_n$, then we can perform a (known) unitary basis transformation to convert $\mathfrak{h}v+e$ to a sample from the diagonal Gaussian distribution $\prod_{i=1}^n D_{\sqrt{r^2\lambda_i^2+s^2}}$. Thus, for group rings where the underlying finite group is of Type I and Type II, we could compute the resulting diagonal Gaussian distribution by combining the results of Lemma 7.*

To achieve this goal, we introduce the following lemma, which demonstrates how to convert a q-BDD instance to a GR-LWE instance. As mentioned in [4], it suffices to use an $\mathsf{LWE}_{q,\Psi_{\le\alpha}}$ oracle to give a solution efficiently to an instance of $\mathsf{LWE}_{q,\Psi_{\le\beta}}$ for any $\beta\le\alpha$, even without knowing the exact value of β. Therefore, it is unnecessary to compute all the entries of the covariance matrix of $\mathfrak{h}\cdot v+e$. We only need to give an upper bound of the eigenvalues of the covariance matrix. The following lemma plays a crucial role in reductions for both the search version and the decision version of GR-LWE. It states that under certain mild conditions, given an BDD instance, there exists an efficient algorithm that generates an GR-LWE sample.

Lemma 17. *Let $R=\mathbb{Z}[G]$ be a group ring, where G is a group of Type I or Type II with n elements. Let $\alpha>0$ be a real, let $q>2$ be an integer, and let $r>\sqrt{2}q\cdot\eta_\varepsilon(\mathcal{I})$ be a real. Then given an invertible right ideal $\mathcal{I}$ of R with index $|R/\mathcal{I}|=\det(\mathcal{I})$ coprime with q, there exists an efficient algorithm that*

given an instance from $\mathsf{BDD}_{\mathcal{I}^{-1},d}$ *(in matrix norm), where* $\mathcal{I}^{-1}$ *is the left inverse of* $\mathcal{I}$ *and samples from* $D_{\mathcal{I},r}$*, outputs samples that have* R-LWE *distribution* $A_{q,\psi}$ *(up to negligible statistical distance) for some* $\psi \in \Psi_{\leq\alpha}$*, where* $d = \alpha q/(\sqrt{2}r)$.

Proof. For an $\mathsf{BDD}_{\mathcal{I}^{-1},d}$ instance $y = x + e$ where x is an element of $\mathcal{I}^{-1}$ and the matrix norm of e is bounded by d, we can construct an R-LWE sample as follows.

First, sample $z \leftarrow D_{\mathcal{I},r}$ from the oracle of discrete Gaussian distribution. Since r exceeds the smoothing parameter of $\mathcal{I}$, $z \bmod q\mathcal{I}$ is almost uniformly distributed in $\mathcal{I}_q$ (up to negligible statistical distance). According to Lemma 11, we know the natural inclusion map

$$\varphi : \mathcal{I}/q\mathcal{I} \to R/qR$$

is a bijection. Thus $a := \varphi(z \bmod q\mathcal{I}) = z \bmod qR$, which is also uniform in R_q. Moreover, we have another natural inclusion map

$$\rho : R/qR \to \mathcal{I}^{-1}/q\mathcal{I}^{-1},$$

where $\mathcal{I}^{-1}$ is the left inverse of $\mathcal{I}$. We construct an element

$$b = (y \cdot z)/q + e' \bmod R = (x \cdot z)/q + (e \cdot z)/q + e' \bmod R,$$

where e' is an error sampled from continuous Gaussian $D_{\alpha/\sqrt{2}}$. We claim that the pair (a, b) is an R-LWE sample.

We first consider the element $x \cdot z \bmod qR$. From the property of natural inclusion mapping, there exists a unique $\bar{s} = s + qR \in R/qR$, such that

$$\rho(\bar{s}) = s \bmod q\mathcal{I}^{-1} = x + q\mathcal{I}^{-1},$$

Note that

$$x \cdot z + qR = (x + qR)(z + qR) = \rho^{-1}(x + q\mathcal{I}^{-1})\varphi(z + q\mathcal{I}) = (s + qR)(z + qR) = \bar{s} \cdot \bar{a}.$$

We obtain that $x \cdot z = s \cdot a \bmod qR$.

It remains to analyze the covariance matrix of $(e \cdot z)/q + e'$. Since $\|e\|_{\mathrm{Mat}} \leq \alpha \cdot q/(\sqrt{2}r)$, and z is distributed as $D_{\mathcal{I},r}$, then it can be verified the smoothness condition holds:

$$\sum_{y \in \mathcal{I}^{-1} \setminus \{0\}} \exp(-\pi t^2 \|y\|^2) = \sum_{y \in \mathcal{I}^{-1} \setminus \{0\}} \exp(-\pi \frac{r^2}{2q^2} \|y\|^2) \leq \varepsilon$$

where $t = 1/\sqrt{(q/r)^2 + q^2/r^2}$ as in Lemma 1, we know $(e \cdot z)/q + e'$ is distributed as some $\psi \in \Psi_{\leq\alpha}$. □

From the reduction above, we can obtain an R-LWE sample given some samples from $D_{\mathcal{I},r}$ with r exceeding the smoothing parameter of $\mathcal{I}$. By employing the search R-LWE oracle, we can recover $s \bmod qR$ except with negligible probability, allowing us to use the bijective mapping from R/qR to $\mathcal{I}/q\mathcal{I}$ to address the BDD problem. Thus, we can prove Lemma 13.

Proof of Lemma 13. We can observe that an instance of $\mathsf{GDP}_{\mathcal{I}^{-1},d/n}$ can be inherently regarded as an instance of $\mathsf{BDD}_{\mathcal{I}^{-1},d}$ (in the matrix norm). According to Lemma 13, we can convert the instance into an R-LWE sample (a, b). After inputting (a, b) into the given search R-LWE oracle, we can get a solution $\bar{s} \in R/qR$. Next, we calculate $\rho(\bar{s}) \in \mathcal{I}^{-1}/q\mathcal{I}^{-1}$ which equals $x \bmod q\mathcal{I}^{-1}$. Consequently, we obtain a solution of the q-$\mathsf{GDP}_{\mathcal{I}^{-1},d/n}$ with the instance y. Additionally, we have exploited the mild properties of groups of Type I and Type II. Specifically, the dual ideal $\mathcal{I}^{\vee}$ and inverse ideal $\mathcal{I}^{-1}$ (if it exists) of $\mathbb{Z}[G]$ are equivalent up to a (known) permutation, which means $\mathsf{GDP}_{\mathcal{I}^{\vee},d/n}$ and $\mathsf{GDP}_{\mathcal{I}^{-1},d/n}$ are essentially equivalent. Hence we have proven the lemma. □

IV. HARDNESS OF DECISION GR-LWE

Having given the reduction from worst-case lattice problem to search LWE, Regev [4] also established a reduction from search LWE to (average-case) decision LWE, which provides the basis for hardness in the decisional setting. Similarly, Lyubashevsky et al. [1] also presented such reductions in the cyclotomic ring version. However, these reductions from search Ring-LWE to decision Ring-LWE have more restrictions on the underlying rings and result in worse parameters. Later in [8], Peikert et al. showed a direct and tighter reduction from worst-case (ideal) lattice problem to decision Ring-LWE with more compact error rates. In this section, we study the hardness of the decisional version of GR-LWE, with a proof similar to [8].

Theorem 2 (Main Result)**.** *Let $R = \mathbb{Z}[G]$ be a group ring where G is of Type I or Type II with n elements. Let $\alpha = \alpha(n) > 0$, and let $q = q(n) > 2$ be an integer such that $\alpha q \geq 2n$. For some negligible $\varepsilon = \varepsilon(n)$, there is a probabilistic polynomial-time quantum reduction from R-DGS_γ (and hence SIVP with approximate factor $\tilde{O}(n^{3/2}/\alpha)$) to R-$\mathsf{DLWE}_{q,\Psi_{\leq\alpha}}$, where*

$$\gamma = \max\{\eta_\varepsilon(\mathcal{I}) \cdot (\sqrt{2}n/\alpha), 2\sqrt{n}/\lambda_1(\mathcal{I}^\vee)\}. \tag{5}$$

Remark 6. *When employing the tighter bound mentioned in Remark 2, it is possible to improve the parameter γ to*

$$\max\{\eta_\epsilon(\mathcal{I}) \cdot (\sqrt{2n}/\alpha) \cdot \omega(\sqrt{\log n}), \sqrt{2n}/\lambda_1(\mathcal{I}^\vee)\},$$

provided that $\alpha q \geq \sqrt{n} \cdot \omega(\sqrt{\log n})$, which shows a reduction from SIVP problem with approximate factor $\tilde{O}(n/\alpha)$.

For simplicity, we only provide the reduction for group ring with underlying group of Type I. The one for Type II is essentially the same. The reduction process remains the same through repeated iterative steps, as stated in Section III. The only difference is that we have access to a decision GR-LWE oracle instead of a search version one. To begin with, we introduce some notations of a special family of polynomials in $\mathbb{R}[x]$.

Definition 12. *Let reals $r > 0, \iota > 0$, an integer $T \geq 1$ and let ξ be a v-th primitive root of unity. Let $W_{r,\iota,T}$ be any set*[4] *of polynomials containing for each $i = 0, 1, \ldots, v-1, k = 0, 1, \ldots, T$, $r_k^{(i)}(x) \in \mathbb{R}[x]$ which denotes a polynomial such that*

$$r_k^{(i)}(\xi^\ell) = r, \quad \forall \ell \neq i, v-i, \tag{6}$$

$$r_k^{(i)}(\xi^i) = r_k^{(i)}(\xi^{v-i}) = r(1+\iota)^k. \tag{7}$$

Example 3. *Let's consider the group ring with an underlying group of Type I: $G = \mathbb{Z}_u \ltimes \mathbb{Z}_v = \langle s \rangle \ltimes \langle t \rangle$, where t has order v. Any element $\mathfrak{h} \in \mathbb{R}[G]$ of the form*

$$\mathfrak{h} = \sum_{i=0}^{v-1} f_i t^i, \quad f_i \in \mathbb{R},$$

can also be regarded as a polynomial in $\mathbb{R}[x]$ with degree no greater than $v-1$ by replacing t with the indeterminate x. It can be easily verified that there is at least one element in $\mathbb{R}[G]$ satisfying the evaluation (6) *and* (7) *in Definition 12, which means $W_{r,\iota,T}$ is well-defined. In fact, we can choose the elements by the same method as Definition 11 in [30]. through Lagrange interpolation.*

The lemma in the following, referred to as iterative steps, combines the results of Lemma 20 and Lemma 14.

[4]The specific selection of $W_{r,\iota,T}$ does not affect the analysis in the following.

Lemma 18 (The iterative step)**.** *Let $R = \mathbb{Z}[G]$ be a group ring where G is of Type I or Type II with n elements. There exists an efficient quantum algorithm that given an oracle that can solve R-$\mathsf{DLWE}_{q,\Psi_{\leq\alpha}}$ on input a number $\alpha \in (0,1)$ and an integer $q \geq 2$, an (invertible) ideal $\mathcal{I} \in \mathbb{Z}[G]$ with $\det(\mathcal{I})$ coprime with q, a real number $r \geq \sqrt{2}q \cdot \eta(\mathcal{I})$ such that $r' := r \cdot n/(\alpha q) > 2\sqrt{n}/\lambda_1(\mathcal{I}^\vee)$, polynomially many samples from discrete Gaussian distribution $D_{\mathcal{I},\mathbf{A}}$ where $\mathbf{A}$ is the matrix representation for each $r_k^{(i)} \in W_{r,\iota,T}$, and a vector $\mathbf{r}' \in \mathbb{R}^n$ with each coordinates $r'_i > r$, outputs an independent sample from $D_{\mathcal{I},\mathbf{r}'}$.*

The following lemma originates from Lemma 6.6 of [8] and is a slightly stronger version of Lemma 6 of [30].

Lemma 19. *Let $R = \mathbb{Z}[G]$ be a group ring of order n with $G = \mathbb{Z}_u \ltimes \mathbb{Z}_v = \langle s \rangle \ltimes \langle t \rangle$ of Type I, where t is an element of order v. Let ξ be a v-th primitive root of unity. Let $r(x) \in \mathbb{R}[x]$ be a polynomial with degree no greater than $v-1$, and let*

$$c = \left(\prod_{i=0}^{v-1} (1/\sqrt{v}) r(\xi^i) \right)^{1/v} \geq 1.$$

Then the matrix determined by $r(t)$, which is denoted by $\mathbf{A}$, satisfies the smoothness condition:

$$\sum_{y \in R^\vee \setminus \{0\}} \exp(-\pi \cdot \mathbf{y}^t \mathbf{A}\mathbf{A}^t \mathbf{y}) \leq \varepsilon,$$

where $\varepsilon = \exp(-c^2 v)$.

Proof. Since $r(t)$ is invertible, the matrix $\mathbf{A}$ is also invertible. According to Lemma 4, we have

$$\eta_\varepsilon(\mathbf{A}^{-1}R) \leq c\sqrt{v}/\lambda_1((\mathbf{A}^{-1}R)^\vee), \tag{8}$$

where the dual lattice satisfies $(\mathbf{A}^{-1}R)^\vee = \mathbf{A}^T\mathbb{Z}^n$ under coefficient embedding. Note that the lattice $\mathbf{A}^T\mathbb{Z}^n$ can be viewed as the concatenation of a series of $r(t)\mathbb{Z}[t]/\langle t^v - 1\rangle$ and $r(t^{-1})\mathbb{Z}[t]/\langle t^v - 1\rangle$ (each number of which is dependent on the order of s). For any polynomial $f = \sum_{i=0}^{v-1} f_i x^i \in \mathbb{R}[x]$, the norm of f (under coefficient embedding) is given by

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

For any polynomial $g(x) \in \mathbb{Z}[x]$ of degree less than v, if $g(x) = r(x)g_1(x)$, then

$$\|g\|_2^2 = \sum_{i=0}^{v-1} |r(\xi^i)g_1(\xi^i)/\sqrt{v}|^2 \geq c^2 v \prod_{i=0}^{v-1} |g_1(\xi^i)|^{2/v} \geq c^2 v,$$

where the first inequality follows from the arithmetic-geometric mean inequality. Similarly, when $g(x) = r(x^{v-1})g_2(x)$, then $\|g\|_2^2 \geq c^2 v$ holds for the same reason. Therefore, from (8), we have $\mathbf{A} \geq \eta_\varepsilon(R)$. □

Lemma 20. *Let $R = \mathbb{Z}[G]$ be a group ring with $G = \mathbb{Z}_u \ltimes \mathbb{Z}_v = \langle s \rangle \ltimes \langle t \rangle$ defined by (2) and let $n := uv$. There exists a probabilistic polynomial-time (classical) algorithm that given an oracle that solves R-$\mathsf{DLWE}_{q,\Psi_{\leq\alpha}}$ and input a number $\alpha \in (0,1)$ and an integer $q \geq 2$, an invertible right ideal $\mathcal{I}$ in $R[G]$ with $\det(\mathcal{I})$ coprime with q, a parameter $r \geq \sqrt{2}q \cdot \eta_\varepsilon(\mathcal{I})$, and polynomially many samples from the discrete Gaussian distribution $D_{\mathcal{I},\mathbf{A}}$, where $\mathbf{A}$ is the matrix representation of any $r(x) \in W_{r,\iota,T}$ (where $\iota = 1/\operatorname{poly}(n), T = \operatorname{poly}(n)$) viewed as an element in $\mathbb{R}[G]$, solves $\mathsf{GDP}_{\mathcal{I}^\vee,g}$ for $g = 1/n \cdot \alpha q/(\sqrt{2}r)$.*

Proof. Let φ denote the coefficient embedding of the group ring $\mathbb{R}[G]$ into $\mathbb{R}^n$.

If $\alpha < \exp(-n)$, then except with negligible probability the coset representative e from the instance will satisfy

$$\|\varphi(e)\| \leq \sqrt{n}g \leq \alpha/(2\sqrt{n} \cdot \eta_\varepsilon(\mathcal{I})) \leq 2^n \lambda_1(\mathcal{I}^\vee),$$

where the last equality is derived from Lemma 4, which means $\|\varphi(e)\|$ is short enough for us to use Babai's algorithm [48] to obtain the solution of the GDP instance. Hence we can assume $\alpha > \exp(-n)$ without loss of generality. We let $\kappa = \mathrm{poly}(n)$ with $\kappa \geq 100n^2\ell$ such that the advantage of R-DLWE oracle is at least $2/\kappa$, where ℓ is the number of samples required by the oracle.

We first view e as a bivariate polynomial with indeterminates s and t:

$$e(s,t) := f_0(t) + sf_1(t) + \cdots + s^{u-1}f_{u-1}(t)$$

and denote the univariate polynomial $e_j(t) := e(\omega^j, t) = f_0(t) + \omega^j f_1(t) + \cdots + \omega^{j(u-1)}f_{u-1}(t)$. Denote $\rho_j(e) = (e_j(0), e_j(\xi), e_j(\xi^2), \ldots, e_j(\xi^{v-1})) := (\rho_j^{(0)}(e), \rho_j^{(1)}(e), \ldots, \rho_j^{(v-1)}(e))$ for $j = 0, 1, \ldots, u-1$, where ω and ξ are the u-th and v-th primitive roots of unity, respectively. In the following, we determine ρ_j by determining each of its coordinates $\rho_j^{(i)}$ for $i = 0, 1, 2, \ldots, v-1$.

The reduction uses the decisional GR-LWE oracle to simulate oracles

$$\mathcal{O}_j^{(i)} : \mathbb{C} \times \mathbb{R}_{\geq 0} \to \{0, 1\}, \quad 0 \leq i \leq v-1,$$

such that the probability that $\mathcal{O}_j^{(i)}(z, m)$ outputs 1 only depends on $\exp(m)\left|z - \frac{\rho_j^{(i)}(e)+\rho_{u-j}^{(i)}(e)}{2}\right|$, where $z \in \mathbb{C}$ with $\left|z - \frac{\rho_j^{(i)}(e)+\rho_{u-j}^{(i)}(e)}{2}\right|$ sufficiently small. Hence, $\mathcal{O}_j^{(i)}$ serves as an oracle with "hidden center" $\frac{\rho_j^{(i)}(e)+\rho_{u-j}^{(i)}(e)}{2}$ as defined in Definition 11. Likewise, we can also use the decision GR-LWE oracle to simulate oracles with "hidden centers" $\frac{\rho_j^{(i)}(e)-\rho_{u-j}^{(i)}(e)}{2}$. Combining these results, we can retrieve $\rho_j^{(i)}(e)$ and $\rho_{u-j}^{(i)}(e)$.

Fix an index j and apply Proposition 1 to obtain a sufficiently accurate approximation of $\frac{\rho_j^{(i)}(e)\pm\rho_{u-j}^{(i)}(e)}{2}$ for each i, which in turn enables recovery of $e_j(t) \pm e_{u-j}(t)$ via a system of linear equations. Having all e_j for every j, we can efficiently reconstruct e except with negligible probability.

First, we note that we can efficiently compute

$$\frac{e_j(t) \pm e_{u-j}(t)}{2} + \mathcal{I}^{-1}$$

from a representative of $e + \mathcal{I}^{-1}$ for all indices j. Consider a representative of the coset $e + \mathcal{I}^{-1}$, written as $e + x$ where $x \in \mathcal{I}^{-1}$. Let x be written as a bivariate polynomial in the indeterminates s and t, just as e is: $x(s,t) := x_0(t) + sx_1(t) + \cdots + s^{u-1}x_{u-1}(t)$. As we defined $e_j(t)$ previously, we can define $x_j(t)$ in the same manner. For each j, we can compute $e_j(t) + x_j(t)$ by evaluating $e(s,t) + x(s,t)$ at $s = \omega^j$. We claim that $(e_j(t) + e_{u-j}(t) + x_j(t) + x_{u-j}(t))/2$ is a representative of the coset $\frac{e_j(t)+e_{u-j}(t)}{2} + \mathcal{I}^{-1}$, which directly achieves our goal. It remains to show that $(x_j(t) + x_{u-j}(t))/2 \in \mathcal{I}^{-1}$. Since $x(s,t) \in \mathcal{I}^{-1} \supseteq \mathbb{Z}[G]$ and $x_j(t), x_{u-j}(t)$ have conjugate coefficients in $\mathbb{Z}[\omega]$, it follows that all the coefficients of $(x_j(t) + x_{u-j}(t))/2$ lie in $\mathbb{R} \cap \mathbb{Z}[\omega] = \mathbb{Z}$, which implies that $(x_j(t) + x_{u-j}(t))/2 \in \mathbb{Z}[G] \subseteq \mathcal{I}^{-1}$. The same argument also applies to $\frac{e_j(t)-e_{u-j}(t)}{2} + \mathcal{I}^{-1}$.

To achieve our goal, when $j = 0, u/2$, we can use similar process of Lemma 9 in [30] to recover $\rho_j^{(i)}$ (In this case, $\rho_j^{(i)}$ is real). For the following discussion, we may assume $j \neq 0, u/2$. Define $k_j^{(i)} : \mathbb{C} \to \mathbb{R}[G_1]$ satisfying $\rho_j(k_j^{(i)}(z)) = z \cdot \mathbf{e}_i + \bar{z} \cdot \mathbf{e}_{v-i}$, where $\mathbf{e}_i$ has 1 in the i-th coordinate and 0 otherwise, and we may restrict the image of $k_j^{(i)}$ within elements of $\mathbb{R}[G_1]$ which are of the form

$$a_0 + a_1 t + a_2 t^2 + \cdots + a_{v-1}t^{v-1} \in \mathbb{R}[G_1],$$

which has zero coefficients on $s^i t^j$ for any $1 \leq i \leq u-1$ and $0 \leq j \leq v-1$. On input (z, m), the oracle $\mathcal{O}_j^{(i)}$ uses fresh Gaussian samples from $D_{\mathcal{I},\mathbf{A}_k^{(i)}}$, where $\mathbf{A}_k^{(i)}$ is the matrix representation of $r_k^{(i)} \in W_{r,\iota,T}$ and $(1+\iota)^k = \exp(m)$ as in Definition 12. Then it performs the transformation from Lemma 17 on these samples, the coset $\frac{e_j+e_{u-j}}{2} - \sum k_j^{(i)}(z_j^{(i)}) + \mathcal{I}^{-1}$, parameter r and matrix norm bound $d = \alpha q/(\sqrt{2}r) \cdot \omega(1)$,

and convert them into GR-LWE samples. Denote these samples by $A^{(i)}_{j,z,m}$. Then $\mathcal{O}^{(i)}_j$ calls the R-DLWE oracle on these samples and outputs 1 if and only if it accepts.

Next, the reductions runs the algorithm for each $i = 1, 2, \ldots, v-1$ with oracle $\mathcal{O}^{(i)}_j$, confidence parameter κ, and distance bound $d' = d/(1+1/\kappa)$, and outputs some approximation $z^{(i)}_j$ to the oracle's center. Finally, the reduction runs Babai's algorithm on the coset $\frac{e_j+e_{u-j}}{2} - \sum k^{(i)}_j(z^{(i)}_j) + \mathcal{I}^{-1}$, receiving as $\tilde{e}^+_j$, and returns $\tilde{e}^+_j + \sum k^{(i)}_j(z^{(i)}_j)$ as output.

The running time of the reduction is polynomial time in the size of the group ring. Assuming $z^{(i)}_j$ are valid solution to $(\exp(-\kappa), \exp(-\kappa), 1+1/\kappa)$-OHCP with hidden center $\frac{\rho^{(i)}_j(e)+\rho^{(i)}_{u-j}(e)}{2}$, we check that the correctness of the algorithm. Since $z^{(i)}_j$ are valid solutions, we have

$$\left| z^{(i)}_j - \frac{\rho^{(i)}_j(e) + \rho^{(i)}_{u-j}(e)}{2} \right| \leq \exp(-\kappa)d' \leq \exp(-\kappa)/\eta(\mathcal{I}) \leq 2^{-n-1}\lambda_1(\mathcal{I}^{-1})/\sqrt{n}$$

by the definition of OHCP. Thus, $\left\| \sum k^{(i)}_j(z^{(i)}_j) - \frac{e_j(t)+e_{u-j}(t)}{2} \right\| \leq 2^{-n}\lambda_1(\mathcal{I}^{-1})$. Note that $e_j(t)$ and $e_{u-j}(t)$ have conjugate coefficients at each position, it follows that $\frac{e_j(t)+e_{u-j}(t)}{2}$ can be regarded as an element in $\mathbb{R}[G]$. The Babai's algorithm will return the exact value of $\frac{e_j(t)+e_{u-j}(t)}{2} - \sum k^{(i)}_j(z^{(i)}_j)$, which we denote by $\tilde{e}^+$, then finally we output $\frac{e_j+e_{u-j}}{2} = \tilde{e}^+ + \sum k^{(i)}_j(z^{(i)}_j)$. The analysis also applies to $\frac{e_j-e_{u-j}}{2}$, which in turn gives the value of e_j and e_{u-j}. Hence we prove the correctness of the algorithm.

It remains to prove, except with negligible probability over the choice of e and for all i, j:

(1) $\mathcal{O}^{(i)}_j$ represents valid instances of $(\exp(-\kappa), \exp(-\kappa), 1+1/\kappa)$-OHCP with "hidden center" $\frac{\rho^{(i)}_j(e)+\rho^{(i)}_{u-j}(e)}{2}$;
(2) $\mathcal{O}^{(i)}_j$ satisfies the condition of what is stated in Proposition 1.

To prove validity, we first observe that the distribution $A^{(i)}_{j,z,m}$ depends only on $\exp(m)\left|z - \frac{\rho^{(i)}_j(e)+\rho^{(i)}_{u-j}(e)}{2}\right|$ if $\left|z - \frac{\rho^{(i)}_j(e)+\rho^{(i)}_{u-j}(e)}{2}\right| \leq (1+1/\kappa)d' = d$. We have

$$\exp(-\kappa)d' \leq \exp(-n)d \leq \left| \frac{\rho^{(i)}_j(e) + \rho^{(i)}_{u-j}(e)}{2} \right| \leq d'.$$

Therefore, $\mathcal{O}^{(i)}_j, \kappa, d'$ correspond to a valid instance of $(\exp(-\kappa), \exp(-\kappa), 1+1/\kappa)$-OHCP with "hidden center" $\frac{\rho^{(i)}_j(e)+\rho^{(i)}_{u-j}(e)}{2}$, except with negligible probability.

Finally, we prove that the oracle $\mathcal{O}^{(i)}_j$ indeed satisfies the three conditions specified in Proposition 1.

(1) For fixed j, denote $p^{(i)}_j(z, m)$ as the probability that $\mathcal{O}^{(i)}_j$ outputs 1 on input (z, m) and $p^{(i)}_\infty$ for the probability that R-DLWE oracle outputs 1 on uniformly random inputs. It follows that $p^{(i)}_j(0,0) = p^{(i')}_{j'}(0,0)$ for all $(i,j), (i',j')$, and $p^{(i)}_j(0,0) - p^{(i)}_\infty$ is exactly the advantage that R-DLWE oracle has against the error rate that we derive from the transformation described by Corollary 1. Recall that e is drawn from $D_{d/n}$, then $\|e\|_{\mathrm{Mat}}$ is no more than d. Similar to the procedure in Lemma 17, the resulting R-LWE samples are exactly distributed from $\Psi_{\leq\alpha}$. Since the decisional GR-LWE oracle has an advantage $2/\kappa$ against this distribution of error rate. By Markov's inequality, we may assume that $p^{(i)}_j(0,0) - p^{(i)}_\infty \geq 1/\kappa$ holds with non-negligible probability. It means Item 1 in Proposition 1 is satisfied.
(2) For Item 2, the distribution of $A^{(i)}_{j,0,m}$ is within negligible statistical distance of distribution $A_{s,A^{(i)}_k}$. Recall that $r^{(i)}_k(\xi^i) = r^{(i)}_k(\xi^{v-i}) = r(1+\iota)^k$ and $r^{(i)}_k(\xi^h) = r$ for $h \neq i, v-i$. With Lemma 19

and the definition of the smoothness parameter, we can prove the distribution of $A^{(i)}_{j,0,m}$ is within statistical distance

$$\begin{aligned}\ell \exp\left(-v\prod_h\left(1/\sqrt{v}\cdot r_k^{(i)}(\xi^h)\right)^{2/v}\right) &\le \ell\exp\left(-\exp(4m/v)\cdot(r/q)^2\cdot\prod_i \rho_j^{(i)}(e_j+e_{m-j})^{2/v}\right)\\ &\le \ell\exp(-\exp(4m/v-4n-1))\\ &\le 2\exp(-m/\kappa) \qquad (9)\end{aligned}$$

of the uniform distribution. Here we use

$$|\rho_j^{(i)}(e_j+e_{m+j})| \ge \exp(-n)d > \exp(-n)\cdot\alpha q/(\sqrt{2}r) > \exp(-2n-1/2)\cdot q/r.$$

The inequality of (9) follows from the fact that $\exp(4m/v-4n-1) \gg m/\kappa+\log(\ell/2)$. Therefore, we can conclude that $|p_j^{(i)}(0,m)-p_\infty^{(i)}| \le 2\exp(-m/\kappa)$, which means Item 2 in Proposition 1 is satisfied.

(3) By Lemma 1, the distribution of $A^{(i)}_{j,z,m_1}$ and $A^{(i)}_{j,z,m_2}$ are within statistical distance

$$\min\{1, 10\ell(\exp(|m_1-m_2|)-1)\} \le \kappa|m_1-m_2|,$$

where ℓ is the number of the samples we have used as mentioned before. Thus, we have proved $p_j^{(i)}(z,m)$ is κ-Lipschitz.

Here we complete the proof. □

V. Summary

A. *Relation to Module-*LWE

Similar to the discussion in [30], our construction is closely related to the Module-LWE problems. As an illustrative example, consider the construction arising from Type I groups. Let $R^{(1)}$ be the group ring associated with the Type I group $G_1 = \mathbb{Z}_m \ltimes \mathbb{Z}_n = \langle s\rangle \ltimes \langle t\rangle$ specified in Section 3, and let $R_q^{(1)} = R^{(1)}/qR^{(1)}$. Define $\mathfrak{s} = \sum_{i=0}^{m-1} f_i(t)s^i$ and $\mathfrak{a} = \sum_{i=0}^{m-1} g_i(t)s^i$, where each $f_i(t), g_i(t)$ $(0 \le i \le m-1)$ is a polynomial over $\mathbb{Z}[t]/\langle t^{n/2}+1\rangle$ with coefficients sampled uniformly at random. Let $\mathfrak{b} = \sum_{i=0}^{m-1} b_i(t)s^i$ and let $\mathfrak{e} = \sum_{i=0}^{m-1} e_i(t)s^i$ be an error element in $R_q^{(1)}$. By the definition of the multiplication operation in the group ring, the equation $\mathfrak{b} = \mathfrak{s}\cdot\mathfrak{a}+\mathfrak{e}$ can can be written in matrix form:

$$\begin{pmatrix} b_0 \\ \vdots \\ b_{m-1}\end{pmatrix} = \mathbf{M}\cdot\begin{pmatrix} g_0 \\ \vdots \\ g_{m-1}\end{pmatrix} + \begin{pmatrix} e_0 \\ \vdots \\ e_{m-1}\end{pmatrix},$$

where each of the entries in $\mathbf{M}$ is a polynomial in $\mathbb{Z}[t]/\langle t^{n/2}+1\rangle$ that can be efficiently computed from $f_0,\ldots,f_{m-1}$. Additionally, our construction can be viewed as a structured variant of the Module-LWE problem. This structure contrasts with the standard Module-LWE setting proposed in [9], in which the corresponding matrix $\mathbf{M}$ is typically assumed to be unstructured, with entries sampled independently and uniformly at random. In our case, the m^2 entries of $\mathbf{M}$ are fully determined by only m polynomials. Consequently, to generate $O(mn)$ pseudorandom samples, our construction requires only $O(mn)$ random elements, namely, all the coefficients of $f_0,\ldots,f_{m-1},g_0,\ldots,g_{m-1}$, achieving a reduction by a factor of m compared to the standard Module-LWE problem. The construction in [30] can be viewed as a special case of our framework when $m=2$, whereas our approach allows more flexible parameter choices. Moreover, according to the reduction result in [50], an instance of our rank-m Module-LWE problem can be reduced to an instance of the Ring-LWE problem over a cyclotomic ring with modulus q^m.

B. Conclusion

Both the search and decisional version of the LWE problem over group rings in this paper enjoy the hardness due to the reductions from some computationally hard problems in ideal lattices. Specifically, we focus on the finite non-commutative groups constructed via the semi-direct product of two cyclic groups (in some sense, a group family that owns the simplest structure). While there are indeed various methods for constructing non-commutative groups from two smaller groups, we believe the results of this paper can be generalized to groups with more complex structures. In fact, the two types of groups discussed in this paper are special cases of metacyclic groups, i.e., any semi-direct product of two cyclic groups (which may not necessarily be induced by φ and ψ mentioned in the definition of (2) and (3)).

Additionally, the process of reduction extensively exploits properties of the irreducible representations and their eigenvalues. On the one hand, they are closely related to the left regular representation of the ring elements, which encompasses all irreducible subrepresentations of them to some extent. On the other hand, as mentioned in [30], the dimension of irreducible representations affects the efficiency of computing the multiplication of two elements of the group rings. Therefore, it is essential for the dimension of the irreducible representations of the group elements to be not exceedingly large. In this paper, we have chosen two types of rings that have been utilized to implement the LWE problem. These rings are quotient rings obtained by group rings modulo an ideal. Nevertheless, these selections are made heuristically such that the resulting rings would not suffer from the potential attack exploiting the one-dimensional subrepresentations of the group ring. However, it remains an open problem whether there is any general approach to selecting quotient rings that are not vulnerable to such kind of attack.

REFERENCES

[1] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Advances in Cryptology–EUROCRYPT*, 2010, pp. 1–23.

[2] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, 1997.

[3] M. Ajtai, "Generating hard instances of lattice problems," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, 1996, pp. 99–108.

[4] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *J. ACM*, vol. 56, no. 6, pp. 1–40, 2009.

[5] C. Peikert, "Public-key cryptosystems from the worst-case shortest vector problem," in *Proc. 41st Annu. ACM Symp. Theory Comput.*, 2009, pp. 333–342.

[6] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in *Proc. 3rd Int. Symp. ANTS*, 1998, pp. 267–288.

[7] D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa, "Efficient public key encryption based on ideal lattices," in *Advances in Cryptology–ASIACRYPT*, 2009, pp. 617–635.

[8] C. Peikert, O. Regev, and N. Stephens-Davidowitz, "Pseudorandomness of Ring-LWE for any ring and modulus," in *Proc. 49th Annu. ACM SIGACT Symp. Theory Comput.*, 2017, pp. 461–473.

[9] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(Leveled) fully homomorphic encryption without bootstrapping," *ACM Trans. Comput.Theory (TOCT)*, vol. 6, no. 3, pp. 1–36, 2014.

[10] M. Rosca, D. Stehlé, and A. Wallet, "On the ring-LWE and polynomial-LWE problems," in *Advances in Cryptology–EUROCRYPT*, 2018, pp. 146–173.

[11] M. Bolboceanu, Z. Brakerski, R. Perlman, and D. Sharma, "Order-LWE and the hardness of ring-LWE with entropic secrets," in *Advances in Cryptology–ASIACRYPT*, 2019, pp. 91–120.

[12] M. Roşca, A. Sakzad, D. Stehlé, and R. Steinfeld, "Middle-product learning with errors," in *Advances in Cryptology–CRYPTO*, 2017, pp. 283–297.

[13] C. Peikert and Z. Pepin, "Algebraically structured LWE, revisited," in *Theory of Cryptography Conference (TCC)*, 2019, pp. 1–23.

[14] C. Peikert, V. Vaikuntanathan, and B. Waters, "A framework for efficient and composable oblivious transfer," in *Advances in Cryptology–CRYPTO*, 2008, pp. 554–571.

[15] D. Micciancio and C. Peikert, "Trapdoors for lattices: Simpler, tighter, faster, smaller," in *Advances in Cryptology–EUROCRYPT*, 2012, pp. 700–718.

[16] D. Boneh, K. Lewi, H. W. Montgomery, and A. Raghunathan, "Key homomorphic PRFs and their applications," in *Advances in Cryptology–CRYPTO*, 2013, pp. 410–428.

[17] A. Banerjee and C. Peikert, "New and improved key-homomorphic pseudorandom functions," in *Advances in Cryptology–CRYPTO*, 2014, pp. 353–370.

[18] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. 41st Annu. ACM Symp. Theory Comput.*, 2008, pp. 197–206.

[19] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," *J. Cryptology*, vol. 25, pp. 601–639, 2012.

[20] S. Agrawal, D. Boneh, and X. Boyen, "Efficient lattice (H)IBE in the standard model," in *Advances in Cryptology–EUROCRYPT*, 2010, pp. 553–572.
[21] S. Agrawal, D. M. Freeman, and V. Vaikuntanathan, "Functional encryption for inner product predicates from learning with errors," in *Advances in Cryptology–ASIACRYPT*, 2011, pp. 21–40.
[22] S. Gorbunov, V. Vaikuntanathan, and H. Wee, "Attribute-based encryption for circuits," *J. ACM*, vol. 62, no. 6, pp. 1–33, 2015.
[23] D. Boneh, C. Gentry, S. Gorbunov, S. Halevi, V. Nikolaenko, G. Segev, V. Vaikuntanathan, and D. Vinayagamurthy, "Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits," in *Advances in Cryptology–EUROCRYPT*, 2014, pp. 533–556.
[24] S. Gorbunov, V. Vaikuntanathan, and H. Wee, "Predicate encryption for circuits from LWE," in *Advances in Cryptology–CRYPTO*, 2015, pp. 503–523.
[25] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. 41st Annu. ACM Symp. Theory Comput.*, 2009, pp. 169–178.
[26] C. Gentry, A. Sahai, and B. Waters, "Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based," in *Advances in Cryptology–CRYPTO*, 2013, pp. 75–92.
[27] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," *SIAM J. Comput.*, vol. 43, no. 2, pp. 831–871, 2014.
[28] S. Garg, C. Gentry, and S. Halevi, "Candidate multilinear maps from ideal lattices," in *Advances in Cryptology–EUROCRYPT*, 2013, pp. 1–17.
[29] C. Gentry, S. Gorbunov, and S. Halevi, "Graph-induced multilinear maps from lattices," in *Theory of Cryptography Conference (TCC)*, 2015, pp. 498–527.
[30] Q. Cheng, J. Zhang, and J. Zhuang, "LWE from non-commutative group rings," *Des. Codes Cryptogr.*, vol. 90, no. 1, pp. 239–263, 2022.
[31] J.-P. Serre, *Linear Representations of Finite Groups*. Springer, New York, 1977.
[32] J. Biasse and F. Song, "Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields," in *SODA'16*, 2016, pp. 893–902.
[33] R. Cramer, L. Ducas, C. Peikert, and O. Regev, "Recovering short generators of principal ideals in cyclotomic rings," in *Advances in Cryptology–EUROCRYPT*, 2016, pp. 559–585.
[34] Y. Pan, J. Xu, N. Wadleigh, and Q. Cheng, "On the ideal shortest vector problem over random rational primes," in *Advances in Cryptology–EUROCRYPT*, 2021, pp. 559–583.
[35] R. Cramer, L. Ducas, and B. Wesolowski, "Short stickelberger class relations and application to ideal-svp," in *Advances in Cryptology–EUROCRYPT*, 2017, pp. 324–348.
[36] Y. Elias, K. E. Lauter, E. Ozman, and K. E. Stange, "Provably weak instances of Ring-LWE," in *Advances in Cryptology–CRYPTO*, 2015, pp. 63–92.
[37] H. Chen, K. Lauter, and K. E. Stange, "Attacks on the search RLWE problem with small errors," *SIAM J. Appl. Algebra Geom.*, vol. 1, no. 1, pp. 665–682, 2017.
[38] A. Langlois and D. Stehlé, "Worst-case to average-case reductions for module lattices," *Des. Codes Cryptogr.*, vol. 75, no. 3, pp. 565–599, 2015.
[39] A. Pedrouzo-Ulloa, J. R. Troncoso-Pastoriza, and F. Pérez-González, "Multivariate lattices for encrypted image processing," in *IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, 2015, pp. 1707–1711.
[40] T. Yasuda, X. Dahan, and K. Sakurai, "Characterizing NTRU-variants using group ring and evaluating their lattice security," Cryptology ePrint Archive, Report 2015/1170, 2015. [Online]. Available: https://eprint.iacr.org/2015/1170.
[41] C. Grover, A. Mendelsohn, C. Ling, and R. Vehkalahti, "Non-commutative ring learning with errors from cyclic algebras," *J. Cryptology*, vol. 35, no. 22, pp. 1–67, 2022.
[42] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.
[43] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 469–472, 1985.
[44] B. Applebaum, D. Cash, C. Peikert, and A. Sahai, "Fast cryptographic primitives and circular-secure encryption based on hard learning problems," in *Advances in Cryptology-CRYPTO*, 2009, pp. 595–618.
[45] W. Banaszczyk, "New bounds in some transference theorems in the geometry of numbers," *Math. Annalen*, vol. 296, no. 4, pp. 625–635, 1993.
[46] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on Gaussian measures." *SIAM J. Comput.*, vol. 37, no. 1, pp. 267–302, 2007.
[47] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, "Factoring polynomials with rational coefficients," *Math. Annalen*, vol. 261, no. 4, pp. 515–534, December 1982.
[48] L. Babai, "On Lovász' lattice reduction and the nearest lattice point problem," *Combinatorica*, vol. 6, no. 1, pp. 1–13, 1986.
[49] R. Endelman and M. Mukherjee, "Primitive central idempotents of the group algebra," *arXiv preprint arXiv:0803.1336*, 2008.
[50] M. R. Albrecht and A. Deo, "Large modulus ring-lwe $\geq$ module-lwe," in *International Conference on the Theory and Application of Cryptology and Information Security*, 2017, pp. 267–296.

APPENDIX A
PROOF OF LEMMA 5

Proof. (i) When m is even, by calculating the number of conjugate classes of G_1, we know the number of irreducible representations of G_1 is $st + 2s$.

To determine all 1-dimensional irreducible representations of G_1, it suffices to consider the quotient group $G_1/[G_1, G_1]$, where $[G_1, G_1]$ deontes the commutator group of G_1, which is isomorphic to $\mathbb{Z}_n = \langle t \rangle$. Then $G_1/[G_1, G_1] \cong \mathbb{Z}_m$ is also a cyclic group. According to the representation theory, the number of 1-dimensional representations of G and $\mathbb{Z}_m$ are identical, i.e., $m = 2r$. Furthermore, $\chi_i(s)$ is completely determined by all the (1-dimensional) representations of $\mathbb{Z}_m$, as stated in the lemma. Since t and st belong to the same conjugate class, then $\chi_i(t) = \chi_i(st)/\chi_i(s) = 1$.

It remains to determine all 2-dimensional irreducible representations of G_1. Let (ρ, V) be a 2-dimensional irreducible representation of G_1. We next consider the restriction of ρ over the subgroup $\mathbb{Z}_n$. Since $\mathbb{Z}_n$ is an Abelian group, then V can be decomposed into two 1-dimensional subrepresentations $V = V_1 \oplus V_2$ when viewed as a representation of $\mathbb{Z}_n$. It is important to emphasize that V_1 and V_2 are distinct. Since

$$\rho(t)(\rho(s)V_1) = \rho(s)\rho(s^{-1}ts)V_1 \in \rho(s)V_1,$$

$\rho(s)V_1$ is also a subrepresentation of $\mathbb{Z}_n$. It has to be $\rho(s)V_1 = V_2$ and similarly $\rho(s)V_2 = V_1$. Fixing a nonzero vector $v_1 \in V_1$, then there exists $\lambda \in \mathbb{C}$, such that $\rho(t)v_1 = \lambda v_1$. Let $v_2 = \rho(s)v_1 \in V_2$, and then there also exists $\zeta \in \mathbb{C}$, such that

$$\rho^2(s)v_1 = \rho(s)v_2 = \zeta v_1.$$

As s has order $m = 2r$, it follows that ζ is an r-th root of unity. Thus, the transformation matrix of $\rho(s)$ with respect to the basis v_1, v_2 is given by

$$\begin{pmatrix} 0 & \zeta \\ 1 & 0 \end{pmatrix}.$$

On the other hand, we notice that

$$\rho(t)v_2 = \rho(t)\rho(s)v_1 = \rho(s)\rho(t^{-1})v_1 = \bar{\lambda}\rho(s)v_1,$$

where $\bar{\lambda}$ is the complex conjugate of λ. If λ is real, then $\rho^2(t) = \mathrm{id}$. In this case, $G_1/\ker(\rho) \cong \mathbb{Z}_m \ltimes \mathbb{Z}_2 = \mathbb{Z}_m \times \mathbb{Z}_2$ is abelian, which implies it has no 2-dimensional irreducible representations, hence it makes a contradiction. Then λ has to be the nonreal root of $x^n - 1$. Hence the transformation matrix of $\rho(t)$ with respect to the basis v_1, v_2 is

$$\begin{pmatrix} \xi^j & 0 \\ 0 & \xi^{n-j} \end{pmatrix}, \quad j = 1, 2, \ldots, u.$$

(ii) It is essentially the same as the discussion in (i). □

APPENDIX B
PROOF OF LEMMA 8

Proof. **Type I**: Let m be an even positive integer and n an arbitrary positive integer, and let G_1 be a group defined as

$$\mathbb{Z}_m \ltimes_\varphi \mathbb{Z}_n = \langle s, t \mid s^m = 1, t^n = 1, sts^{-1} = t^{-1} \rangle,$$

where s and t are the generators of cyclic groups $\mathbb{Z}_m$ and $\mathbb{Z}_n$, respectively.

The group ring $\mathbb{Z}[G_1]$ naturally has a basis over $\mathbb{Z}$, which are exactly all the elements of G_1, i.e.,

$$\{s^i t^j \mid 0 \le i \le m-1, 0 \le j \le n-1\}. \tag{10}$$

Let I be a right ideal in $\mathbb{Z}[G]$, and denote the ideal lattice corresponding to I under coefficient embedding by $\mathcal{I}$. Suppose that

$$\mathfrak{h}_1 = \sum_{j=0}^{n-1} x_{0,j} t^j + \sum_{j=0}^{n-1} x_{1,j} s t^j + \cdots + \sum_{j=0}^{n-1} x_{m-1,j} s^{m-1} t^j \in I^{-1} \subseteq \mathbb{R}[G_1],$$

where $x_{i,j} \in \mathbb{R}$, then $\mathfrak{h}_1$ can be regareded as a mn-tuple with real components under coefficient embedding, i.e.,

$$\mathbf{x} := (\mathbf{x}_0, \mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{m-1}) \in \mathcal{I}^\vee \subset \mathbb{R}^{mn},$$

where $\mathbf{x}_i := (x_{i,0}, x_{i,1}, \ldots, x_{i,n-1})$. Denote $\tilde{\mathbf{x}}_i := (x_{i,0}, x_{i,n-1}, x_{i,n-2}, \ldots, x_{i,2}, x_{i,1})$, let

$$\begin{aligned}\mathbf{z} &:= (z_{0,0}, z_{0,1}, \ldots, z_{0,n-1}, z_{1,0}, z_{1,1}, \ldots, z_{1,n-1}, \ldots, z_{m-1,0}, \ldots, z_{m-1,n-1}) \\ &= (\tilde{\mathbf{x}}_0, \mathbf{x}_{m-1}, \tilde{\mathbf{x}}_{m-2}, \mathbf{x}_{m-3}, \ldots, \tilde{\mathbf{x}}_2, \mathbf{x}_1),\end{aligned}$$

then $\mathbf{z}$ is also an mn-tuple obtained by permutating the coordinates of $\mathbf{x}$.

It suffices to show that $\mathbf{x} \in \mathcal{I}^{-1}$ if and only if $\mathbf{z} \in \mathcal{I}^\vee$. For simplicity, the addition and multiplication operations with respect to the first (or second) subscript of x, y, z are all modulo m (or n) (also the same in the proof for Type II).

Note that $\mathbf{x} \in \mathcal{I}^{-1}$ if and only if, for any element $\mathfrak{h} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} y_{i,j} s^i t^j \in I$, we have $\mathfrak{h}_1 \mathfrak{h} \in \mathbb{Z}[G_1]$. By computing $\mathfrak{h}_1 \mathfrak{h}$ represented by the basis (10), we obtain that $\mathbf{x} \in \mathcal{I}$ is equivalent to the condition that for any $a = 0, 1, \ldots, m-1, b = 0, 1, \ldots, n-1$, we have

$$\sum_{j=0}^{n-1} x_{0,j} y_{a,b-(-1)^a j} + \sum_{j=0}^{n-1} x_{1,j} y_{a-1,b+(-1)^a j} + \cdots + \sum_{j=0}^{n-1} x_{m-1,j} y_{a+1-m,b+(-1)^a j} \in \mathbb{Z}$$

holds. Applying this result to $\mathbf{z}$, we get

$$\sum_{j=0}^{n-1} z_{0,j} y_{a,b+(-1)^a j} + \sum_{j=0}^{n-1} z_{m-1,j} y_{a-1,b+(-1)^a j} + \cdots + \sum_{j=0}^{n-1} z_{1,j} y_{a+1-m,b+(-1)^a j} \in \mathbb{Z}. \tag{11}$$

On the other hand, if $\mathbf{z} \in \mathcal{I}^\vee$, then for any element $\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} y_{i,j} s^i t^j \in I$, we have

$$\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} z_{i,j} y_{i,j} \in \mathbb{Z}.$$

Since I is a right ideal of $\mathbb{Z}[G]$,

$$\left(\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} y_{i,j} s^i t^j \right) s^{m-a} t^{(-1)^a b} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} y_{i,j} s^{m-a+i} t^{-(-1)^a (j-b)} \in I$$

holds. Then we have $\mathbf{z} \in \mathcal{I}^\vee$ if and only if for any $a \in [m], b \in [n]$,

$$\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} z_{m-a+i,(-1)^a (j-b)} y_{i,j} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} z_{m-a+i,j} y_{i,b+(-1)^a j} \in \mathbb{Z},$$

which is exactly the same as (11). Hence we have proved the claim with respect to groups of Type I.

Type II: Let $n > 2$ be an integer. We define G_2 as $\mathbb{Z}_n^* \ltimes_\psi \mathbb{Z}_n$, i.e.,

$$G_2 := \{a \odot g^k \mid a \in \mathbb{Z}_n^*, 0 \le k < n-1\},$$

where g is a generator of $\mathbb{Z}_n$ (with order n). The multiplication of G_2 is induced by ψ, i.e., for any $a, b \in \mathbb{Z}_n^*$, and $k_1, k_2 \in \mathbb{Z}$,

$$(a \odot g^{k_1})(b \odot g^{k_2}) = ab \odot g^{k_1 b^{-1} + k_2}.$$

Then the group ring $\mathbb{Z}[G_2]$ has a natural $\mathbb{Z}$-basis:

$$\{a \odot g^k \mid a \in \mathbb{Z}_n^*, k = 0, 1, 2, \ldots, n-1\}.$$

Since $m := \varphi(n)$ is even when $n > 2$, we can write

$$\mathbb{Z}_n^* = \left\{a_0 = 1, a_1, a_2, \ldots, a_{m/2-1}, a_{m/2} = m-1, a_{m/2+1}, \ldots, a_{m-1}\right\},$$

where $a_{m-i} = a_i^{-1}$ holds for any integer i (by arranging the order of the elements in $\mathbb{Z}_n^*$ appropriately). Let $\sigma : \mathbb{Z}_n^* \to [m]$ be an index mapping, which maps each element of $\mathbb{Z}_n^*$ to its index, i.e., $\sigma(a_i) = i$ for any $i \in [m]$.

Suppose that $\mathfrak{a}_1 = \sum_{j=0}^{n-1} x_{0,j}(a_0 \odot g^j) + \sum_{j=0}^{n-1} x_{1,j}(a_1 \odot g^j) + \cdots + \sum_{j=0}^{n-1} x_{m,j}(a_{m-1} \odot g^j) \in \mathbb{R}[G_2]$. Similar to the proof for Type I, $\mathfrak{a}_1$ can also be regarded as an mn-tuple $\mathbf{x}$ under coefficient embedding. Let $\mathbf{z}$ be another mn-tuple satisfying

$$z_{i,j} = x_{m-i,-ja_i}.$$

Since $\gcd(a_i, n) = 1$, it can be easily verified that $\mathbf{z}$ can be obtained by permutating the coordinates of $\mathbf{x}$.

We claim that $\mathbf{x} \in \mathcal{I}^{-1}$ if and only if $\mathbf{z} \in \mathcal{I}^{\vee}$ as in the case of Type I.

We have $\mathfrak{a}_1 \in I^{-1}$ if and only if for any $\mathfrak{a} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} y_{i,j}(a_i \odot g^j) \in I$, $\mathfrak{a}_1\mathfrak{a} \in \mathbb{Z}[G]$. It is equivalent to that for any integer r, s, the coefficient of $\mathfrak{a}_2\mathfrak{a}$ over $a_r \odot g^s$ is also an integer, i.e.,

$$\begin{aligned}
&\sum_{j=0}^{n-1} x_{r,s-j} y_{0,j} + \sum_{j=0}^{n-1} x_{\sigma(a_r a_1^{-1}),(s-j)a_1} y_{1,j} + \cdots + \sum_{j=0}^{n-1} x_{\sigma(a_r a_{m-1}^{-1}),(s-j)a_{m-1}} y_{m-1,j} \\
=&\sum_{j=0}^{n-1} z_{\sigma(a_0 a_r^{-1}),(j-s)a_r} y_{0,j} + \sum_{j=0}^{n-1} z_{\sigma(a_1 a_r^{-1}),(j-s)a_r} y_{1,j} + \cdots + \sum_{j=0}^{n-1} z_{\sigma(a_{m-1} a_r^{-1}),(j-s)a_r} y_{m-1,j} \in \mathbb{Z}. \qquad (12)
\end{aligned}$$

On the other hand, if $\mathbf{z} \in \mathcal{I}^{\vee}$, then

$$\langle \mathbf{z}, \mathbf{y} \rangle = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} z_{i,j} y_{i,j} \in \mathbb{Z}.$$

Since $\mathcal{I}$ is a right ideal, for any $r = 0, 1, 2, \ldots, m-1, s = 0, 1, 2, \cdots, n-1$, we have

$$\left(\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} y_{i,j} \left(a_i \odot g^j\right)\right) \left(a_r^{-1} \odot g^{-sa_r}\right) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} y_{i,j} \left(a_i a_r^{-1} \odot g^{(j-s)a_r}\right) \in I.$$

Thus, we could claim $\mathbf{z} \in \mathcal{I}^{\vee}$ if and only if for any $r \in [m], s \in [n]$,

$$\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} z_{\sigma(a_i a_r^{-1}),(j-s)a_r} y_{i,j} \in \mathbb{Z},$$

which is exactly the same as (12). □