LWE from Non-commutative Group Rings

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

[1] School of Computer Science, University of Oklahoma
Norman, OK 73019, USA.
Email: qcheng@ou.edu
[2] School of Mathematical Sciences, Capital Normal University
Beijing 100048, China.
Email: junz@cnu.edu.cn
[3] State Key Laboratory of Information Security, Institute of Information Engineering
Chinese Academy of Sciences, Beijing 100093, China
Email: zhuangjincheng@iie.ac.cn

Abstract. The Ring Learning-With-Errors (LWE) problem, whose security is based on hard ideal lattice problems, has proven to be a promising primitive with diverse applications in cryptography. There are however recent discoveries of faster algorithms for the principal ideal SVP problem, and attempts to generalize the attack to non-principal ideals. In this work, we study the LWE problem on group rings, and build cryptographic schemes based on this new primitive. One can regard the LWE on cyclotomic integers as a special case when the underlying group is cyclic, while our proposal utilizes non-commutative groups, which eliminates the weakness associated with the principal ideal lattices. In particular, we show how to build public key encryption schemes from dihedral group rings, which maintains the efficiency of the ring-LWE and improves its security.

Keywords: ring-LWE, Non-commutative group ring, Dihedral group ring

1 Introduction

1.1 The LWE problem

Regev [32] introduced the learning with errors (LWE) problem as a generalization of the classic learning parity with noise (LPN) problem. To be precise, let q be a prime, $\mathbf{s} \in \mathbb{F}_q^n$ be a fixed private vector, $\mathbf{a_i} \in \mathbb{F}_q^n, 1 \leq i \leq m$ be randomly chosen, $e_i \in \mathbb{F}_q, 1 \leq i \leq m$ be chosen independently accordingly to an error distribution $\mathbb{F}_q \mapsto \mathbb{R}^+$, which is a discrete Gaussian distribution that centers around 0 with width $qn^{-0.5-\epsilon}$, and $b_i = \langle \mathbf{a_i}, \mathbf{s} \rangle + e_i$. Given a list of pairs $(\mathbf{a}_i, b_i), 1 \leq i \leq m$, the LWE problem asks to solve for $\mathbf{s}$, and the LPN problem is the special case when $q = 2$.

Informally speaking, it is believed that LWE is hard in the sense that even though e_i tends to be small, when $\mathbf{s}$ is hidden, $(\mathbf{a_i}, b_i)$ can not be distinguished

from a random vector in $\mathbb{F}_q^{n+1}$. In fact, Regev [32] proved the hardness for certain parameters q and error distributions by showing quantum reductions from approx-SVP and approx-SIVP problems for lattices. Later, Peikert [27] showed a classical reduction from approx-SVP to the LWE problem under more restrictive constraints.

Lyubashevsky, Peikert, and Regev [24] introduced an analogous version of standard LWE over rings, and coined it ring-LWE. Furthermore, they established the hardness of ring-LWE by showing the reduction from a certain ideal lattice problem to the ring-LWE problem. The cryptography systems based on ring-LWE are much more efficient in terms of key sizes and encryption and decryption complexity. However, the security of systems is based on conjecturally hard problems on ideal lattices rather than on general lattices.

The LWE problem and ring-LWE problem have proven to be versatile primitives for cryptographic purposes. Besides many other schemes, these applications include public key encryption schemes proposed by Regev [32], Peikert and Waters [31], Peikert [27], Lindner and Peikert [22], Stehlé and Steinfeld [35], Micciancio and Peikert [25]; identity-based encryption (IBE) schemes proposed by Gentry, Peikert, and Vaikuntanathan [19], Cash, Hofheinz, Kiltz, and Peikert [8], Agrawal, Boneh, and Boyen [2, 1]; fully homomorphic encryption (FHE) schemes proposed by Brakerski and Vaikuntanathan [6, 7], Brakerski, Gentry, and Vaikuntanathan [5], Fan and Vercauteren [17].

1.2   Our results

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

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

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

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

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

In ring-LWE, there are two types of embeddings of rings of algebraic integers into Euclidean spaces: canonical embedding and coefficient embedding. If using canonical embedding, multiplication is component-wise. This is the main reason

2

that the original ring-LWE paper preferred canonical embedding. Nevertheless, the whole ring is embedded as a lattice that is not self-dual, which complicates the implementation [28]. Note that the canonical embedding of cyclotomic integers is basically the combined map:

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

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

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

If a group is not commutative, we can use irreducible group representations to find a canonical embedding of the group ring. However, some irreducible representations will have dimensions larger than one, thus multiplication in the group ring is not component-wise under these representations. We should use coefficient embedding to make implementation simpler.

There are recent discoveries of faster SVP algorithms for principal ideal lattices, and attempts to generalize the idea to non-principal ideal lattices. See [12, 13] and references therein. First observe that the ratio between two generators of a principal ideal is an integral unit. The main idea of the attacks comes from the Dirichlet unit theorem: the group of integral units in a number field is a direct product of a finite group with a free abelian group, whose generators are known as fundamental units. If taking logarithms of complex norms of their conjugates, the units are sent to the so-called log-unit lattice, whose SVP is not hard in many cases. Nevertheless, the ring-LWE cryptosystems are not under direct threat, since lattice problems in ideal lattices form lower bounds for their security, and the approximation factors in the attack are too large.

The principal ideals from non-commutative integral group rings do not appear to suffer from the weakness, since multiplications of units may not commute [33]. A few remarks are in order:

1. The group ring LWE includes LWE on cyclotomic integers as a special case, thus has security no less than the ring-LWE. Indeed, the ring $R = \mathbb{Z}[x]/(x^n + 1)$, used in many ring-LWE cryptosystems, is a direct summand of a group ring from C_{2n} (the cyclic group of order $2n$):

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

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

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

   may leak secret information.

2. We regard one-dimensional representations over finite fields as security risks that should be eliminated. Many attacks on the ring-LWE (implicitly) explores a one-dimensional representation that sends x to a small order element $[9, 10, 15, 16]$, for example,

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

   if $(x-1)|f(x)$ over $\mathbb{F}_q$.
3. Even though rings of algebraic integers in number fields may not be principal ideal domains (PID), their reductions modulo primes are always principal ideal rings. The group ring $\mathbb{F}_p[G]$, however, is not necessarily a principal ideal rings if G is non-commutative. We believe that this property provides an extra protection against attacks.

The proof of security is largely similar to the case of ring-LWE. There is, however, an important difference: unlike the ring of algebraic integers in a number field, group rings have ideals that are not invertible. The security of group-ring-LWE should be based on lattice problems of invertible ideals.

We note that there have been attempts to use non-commutative algebraic structures, especially the group structures, in designing cryptographical systems $[26]$. The approaches that relate closely to ours include using group rings to replace $(\mathbb{Z}/q\mathbb{Z})[x]/(x^n - 1)$ in NTRU $[37, 11, 36]$ and using the learning problem of non-commutative groups. The former approach has no security proof from lattice problems. The latter approach is not based on lattice problems.

1.3 Paper organization

The paper is organized as follows. In Section 2, we review the mathematical background. In Section 3 we briefly discuss previous works. In Section 4, we propose generating LWE instances from non-commutative group rings and establish public key cryptosystem from dihedral group rings. In Section 5 we analyse the security of the new approach. Section 6 concludes the paper. We will not try to optimize the parameters in this paper, leaving it to future work.

2 Mathematical preliminary

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

2.1 Efficiency of cryptographic schemes

To use a cryptography algorithm, one should first establish a security level n. It is expected that the cryptosystem cannot be broken in 2^n bit operations. In terms of efficiency, the most important parameters for an encryption algorithm are block size, public/secret key sizes, cipher-text expansion factor and time

complexity per bit in encryption and decryption. Ideally these parameters should have sizes that grow slowly with the security level.

Let us first calculate the parameters for the popular public key cryptosystem RSA, whose security is based on the integer factorization problem. To factor a number of l bits, the best algorithm – Number Field Sieve – takes heuristic time at most $2^{l^{1/3+\epsilon}}$. Thus for security level n, the RSA-OAEP system, a practical implementation of RSA, should have key size $l = n^{3-\epsilon}$. To encrypt a block of $O(l)$ bits, it adds some padding into the message and computes an exponentiation modulo a number of l bits. Thus it has cipher-text expansion $O(1)$. The public exponent is small (e.g. $e = 65537$), but the private exponent has l bits. Therefore, encryption takes time $\tilde{O}(l)$ and decryption takes time $\tilde{O}(l^2)$, assuming that we use the fast multiplication algorithm for each modular multiplication. This results in bit complexity $n^{3-\epsilon}$ per ciphertext bit for decryption, and $(\log n)^{O(1)}$ per message bit for encryption if using small encryption exponent. Asymptotically the key size for RSA is not so good. However, the ϵ part has played an important role in its favor when n is small. To achieve a security level $n = 80$, one can use a public modulus of size 1000 bits rather than $80^3 = 512000$ bits, although a public modulus of 2000-bits is recommended now.

2.2 Lattices and ring-LWE

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

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

The determinant of the lattice is

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

The minimum distance of the lattice is

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

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

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

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

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

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

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

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

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

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

2.3 Dihedral groups and group rings

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

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

Addition is defined by

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

Multiplication is defined by

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

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

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

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

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

Next, we introduce a new norm of elements in the group ring $\mathbb{R}(G)$. For any element $\mathfrak{h} = \sum_{i=1}^{n} a_i g_i \in \mathbb{R}[G]$, by the multiplication law (1), it defines a linear transformation from $\mathbb{R}^n = \mathbb{R}[G]$ to itself, denoted by $A(\mathfrak{h})$. Indeed, it corresponds

the regular representation of the finite group G. Then we define the matrix-norm $|\mathfrak{h}|_{\mathrm{Mat}}$ of $\mathfrak{h}$ to be the square root of the norm of the matrix $A(\mathfrak{h})A(\mathfrak{h})^T$, i.e.,

$$|\mathfrak{h}|_{\mathrm{Mat}} = \sqrt{\mathrm{Norm}(A(\mathfrak{h})A(\mathfrak{h})^T)} = \sqrt{\mathrm{Largest\,Eigenvalue\,of\,} A(\mathfrak{h})A(\mathfrak{h})^T}.$$

Remark 1. This definition should be the right definition for ring-LWE under any given embedding. In particular, if the transformation matrix A is diagonal, then it reduces to the case ℓ_∞-norm used in [24] for caninocal embedding.

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

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

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

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

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

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

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

satisfying the relations

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

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

If n is odd, there are $(n+1)/2$ irreducible representations for D_{2n}. Two of them are one-dimensional:

$$\rho_0(\mathfrak{r}^i) = 1, \rho_0(\mathfrak{s}\mathfrak{r}^j) = 1$$

and

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

The rest are two-dimensional: for $2 \le k \le (n+1)/2$,

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

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

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

$$\mathbb{C}[D_{2n}] \equiv \mathbb{C} \oplus \mathbb{C} \oplus \bigoplus_{i=2}^{(n+1)/2} \mathbb{C}^{2\times 2},$$

7

where the first two copies of $\mathbb{C}$ correspond to ρ_0 and ρ_1, the last $(n-1)/2$ copies of 2×2 matrix algebras corresponds to the two-dimensional representations ρ_i $(2 \leq k \leq (n+1)/2$).

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

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

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

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

Proof (Sketch of Proof). By representation theory, we have decomposition of the regular representation ρ_{reg}:

$$
\begin{array}{ccc}
\mathbb{C}[D_{2n}] & \xrightarrow{\rho_{\text{reg}}} & \mathbb{C}[D_{2n}] \\
\cong \downarrow \psi & & \cong \downarrow \psi \\
\oplus_i \dim(V_i) V_i & \xrightarrow{\rho_{\text{bd}}} & \oplus_i \dim(V_i) V_i,
\end{array}
$$

where V_i runs over all irreducible representations of D_{2n} such that $\rho_{\text{bd}}(g)$ $(\forall g \in D_{2n})$ is block-diagonal. One can show the isomorphism ψ is unitary, i.e., $\psi \cdot \bar{\psi}^T = I_{2n}$. Then

$$A(\mathfrak{h}) \cdot A(\mathfrak{h})^T = \rho_{\text{reg}}(\mathfrak{h}) \cdot \overline{\rho_{\text{reg}}(\mathfrak{h})}^T = (\psi^{-1} \cdot \rho_{\text{bd}}(\mathfrak{h}) \cdot \psi) \cdot \overline{(\psi^{-1} \cdot \rho_{\text{bd}}(\mathfrak{h}) \cdot \psi)}^T$$

$$= \psi^{-1} \cdot \rho_{\text{bd}}(\mathfrak{h}) \cdot \psi \cdot \bar{\psi}^T \cdot \overline{\rho_{\text{bd}}(\mathfrak{h})}^T \cdot \bar{\psi}^{-T} = \psi^{-1} \cdot \rho_{\text{bd}}(\mathfrak{h}) \cdot \overline{\rho_{\text{bd}}(\mathfrak{h})}^T \cdot \bar{\psi}^{-T}.$$

So $A(\mathfrak{h}) \cdot A(\mathfrak{h})^T$ have the same eigenvalues as $\rho_{\text{bd}}(\mathfrak{h}) \cdot \overline{\rho_{\text{bd}}(\mathfrak{h})}^T$. Moreover, $\rho_{\text{bd}}(\mathfrak{h}) \cdot \overline{\rho_{\text{bd}}(\mathfrak{h})}^T$ is block-diagonal with blocks of size at most 2×2. By direct computation of eigenvalues of each block, it is easy to obtain the eigenvalues of $\rho_{\text{bd}}(\mathfrak{h}) \cdot \overline{\rho_{\text{bd}}(\mathfrak{h})}^T$ are $(|f(\xi^i)| \pm |g(\xi^i)|)^2$ for $i = 0, 1, \cdots, n-1$. And hence eigenvalues of the matrix $A(\mathfrak{h}) \cdot A(\mathfrak{h})^T$ are $(|f(\xi^i)| \pm |g(\xi^i)|)^2$ for $i = 0, 1, \cdots, n-1$.

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

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

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

We claim that

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

8

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

And hence, we finish the proof.

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

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

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

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

and

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

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

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

and

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

On the other hand, we have

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

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

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

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

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

and

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

9

So we have
$$(z_0, z_1, \cdots, z_{n-1}, y_0, y_1, \cdots, y_{n-1}) \in \Lambda^*$$
if and only if for any $\sum_{k=0}^{n-1} w_k \mathfrak{r}^k + \sum_{l=0}^{n-1} v_l \mathfrak{s}\mathfrak{r}^l \in I$ for any $a, b = 0, 1, \cdots, n-1$,

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

and

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

So the claim is proved.

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

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

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

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

which is also without one-dimensional component. Denote

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

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

Let q be a prime such that $\gcd(q, 2n) = 1$. Define

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

Definition 4. *Let* $\chi_{\alpha_1, \alpha_2, \cdots, \alpha_n}$ *be a Gauss distribution in* $\mathbb{R}^n$ *such that*

$$\chi_{\alpha_1, \alpha_2, \cdots, \alpha_n}(x_1, x_2, \cdots, x_n) = e^{-\pi((x_1/\alpha_1)^2 + (x_2/\alpha_2)^2 + \cdots + (x_n/\alpha_n)^2)}$$

Let $\Psi_{\leq \alpha}$ *be the set of all the Gaussian distributions* $\chi_{\alpha_1, \alpha_2, \cdots, \alpha_n}$ *such that* $\alpha_i \leq \alpha$ *for all* $1 \leq i \leq n$. *The* $\mathbf{R}_q$-*LWE problem is to find the secret* $s \in \mathbf{R}_q$, *given a sequence of* $(a_i, b_i) \in \mathbf{R}_q \times \mathbb{T}$, *where* a_i *is selected uniformly and independently from* $\mathbf{R}_q$, $b_i = (a_i s)/q + e_i \mod \mathbf{R}$, e_i *is selected independently according to some fixed distribution* $\chi \in \Psi_{\leq \alpha}$.

Remark 2. Not every ideal is invertible. For example, $1 + \mathfrak{s} \in \mathbf{R}$ generates an ideal that is not invertible. It is very important to have an ideal that is invertible in order to have hard lattice problems. In the later proof, we need an onto $\mathbf{R}$-module morphism $I \to \mathbf{R}_q$, which requires I to be invertible.

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

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

where $|*|$ is the complex norm.

Proof. It is easy from Lemma 2.

3 Previous works

Lattice-based cryptography has attracted much attention recently. It has a few advantages over classical number theoretic cryptosystems such as RSA or Diffie-Hellman. First, it resists quantum attacks, in contrast to the traditional hard problems such as integer factorization, or discrete logarithms [34]. Second, it enjoys the worst case to the average case reduction, shown in the pioneering work of Ajtai [3]. Third, computation can be done on small numbers. No large number exponentiations are needed, which tend to slow down the other public key cryptosystems. It does have a major drawback in key sizes. The NTRU cryptosystem [20] is the first successful cryptosystem based on lattices.

3.1 Regev's scheme

Regev [32] introduced the Learning With Errors (LWE) problem as a generalization of the classic learning parity with noise (LPN) problem to higher moduli and proposed a public key encryption system based on the LWE problem. In the following description of Regev's scheme, n is the security parameter, $q \in [n^2, 2n^2]$ is a prime number and $m = O(n \log q), \alpha = o(\frac{1}{\sqrt{n} \log n})$.

The distribution $\Psi_\alpha = \chi_\alpha \pmod{\mathbb{Z}}$ is defined to be a normal distribution on $R/\mathbb{Z}$ with mean 0 and standard deviation $\frac{\alpha}{\sqrt{2\pi}}$. And $\bar{\Psi}_\alpha$ is the discrete distribution of the random variable $\lfloor q \cdot \mathbf{X} \rceil \mod q$ over $\mathbb{F}_q$, where $a \mod b = a - \lfloor a/b \rfloor b$ and $\mathbf{X}$ is from the distribution Ψ_α.

- **Private key:** Choose a random $\mathbf{s} \in (\mathbb{Z}/q\mathbb{Z})^n$ uniformly.
- **Public key:** Choose a random matrix $\mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{n \times m}$ uniformly. Choose an error vector $\mathbf{x}$ from $(\mathbb{Z}/q\mathbb{Z})^m$, where each component of $\mathbf{x}$ is chosen according to the distribution $\bar{\Psi}_\alpha$. Announce the public key $(\mathbf{A}, \mathbf{P})$ where $\mathbf{P} \in (\mathbb{Z}/q\mathbb{Z})^m$ should be calculated as $\mathbf{s}\mathbf{A} + \mathbf{x}$.
- **Encryption:** First select a random vector $\mathbf{e}^T \in \{0, 1\}^m$. For a message bit $v \in \{0, 1\}$, the encryption is $(\mathbf{A}\mathbf{e}, v\lfloor \frac{q}{2} \rfloor + \mathbf{P}\mathbf{e})$.
- **Decryption:** For the cipher-text $(\mathbf{a}, b)$, output 0 if $b - \langle \mathbf{a}, \mathbf{s} \rangle$ is closer to 0 than to $q/2$; Otherwise de-crypt to 1.

For security level n, the private key has $\tilde{O}(n)$ bits. The public key has $\tilde{O}(n^2)$ bits, and can be reduced to $\tilde{O}(n)$. The cipher-text expansion is $\tilde{O}(n)$. The encoding and decoding complexity is $\tilde{O}(n^2)$ per bit. Hence this system is not efficient, especially in terms of cipher-text expansion and encryption/decryption complexity.

To find the private key from the public key, one can solve a CVP problem in the lattice $\mathcal{L} = \{v\mathbf{A} \mid v \in (\mathbb{Z}/q\mathbb{Z})^n\}$, which is a sub-lattice of $q\mathbb{Z}^m$. Note that $q^{m-n} \mid \det(\mathcal{L})$. The shortest vector of $\mathcal{L}$ has length $\tilde{O}(q\sqrt{m})$. This means that the secret key is likely unique.

3.2 PVW improvement

Peikert, Vaikuntanathan, and Waters [30] proposed a more efficient system based on LWE. They made two important changes: first the secret and the error in the public key are matrices, and the message space consists of vectors; secondly the alphabet of the message is $\mathbb{Z}/p\mathbb{Z}$ for some p that may be greater than 2. The latter idea has also been utilized by Kawachi, Tanaka, and Xagawa [21] to improve the efficiency of several single-bit cryptosystems based on lattice problems.

Suppose that $p = poly(n)$, $l = poly(n)$, $m = O(n \log n)$, $\alpha = 1/(p\sqrt{m} \log n)$ and $q > p$ is a prime. Let t be a function from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}/q\mathbb{Z}$ defined by $t(x) = [x \times \frac{q}{p}]$ and extended to act component-wise on vector spaces over $\mathbb{Z}/p\mathbb{Z}$.

- **Private key:** Choose a random matrix $\mathbf{S} \in (\mathbb{Z}/q\mathbb{Z})^{n \times l}$ uniformly.
- **Public key:** Choose a random matrix $\mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{n \times m}$ uniformly. Find an error matrix $\mathbf{X} \in (\mathbb{Z}/q\mathbb{Z})^{l \times m}$ where each entry is chosen independently according to the error distribution $\chi = \bar{\Psi}_\alpha$. The public key is $(\mathbf{A}, \mathbf{P})$ where $\mathbf{P} = \mathbf{S}^T \mathbf{A} + \mathbf{X} \in (\mathbb{Z}/q\mathbb{Z})^{l \times m}$.
- **Encryption:** The message is assumed to be a vector $\mathbf{v} \in (\mathbb{Z}/p\mathbb{Z})^l$. First convert it to a vector $t(\mathbf{v})$ in $(\mathbb{Z}/q\mathbb{Z})^l$. Then select $\mathbf{e}^T \in \{0,1\}^m$ uniformly at random. The encryption is $(\mathbf{Ae}, \mathbf{Pe} + t(\mathbf{v})) \in (\mathbb{Z}/q\mathbb{Z})^n \times (\mathbb{Z}/q\mathbb{Z})^l$.
- **Decryption:** For the cipher-text $(\mathbf{u}, \mathbf{c})$, compute $\mathbf{d} = \mathbf{c} - \mathbf{S}^T\mathbf{u}$, and output $\mathbf{v} \in (\mathbb{Z}/p\mathbb{Z})^l$, where v_i is the element in $\mathbb{Z}/p\mathbb{Z}$ that makes $d_i - t(v_i)$ closest to 0 $(\mathrm{mod}\ q)$.

Note that one may set $l = n$ in the cryptosystem. In this case, the public key size and secure key size are $\tilde{O}(n^2)$. The algorithm has cipher-text expansion $O(1)$. The encryption and decryption complexity is $\tilde{O}(n)$ per bit.

The security of the cryptosystem comes from the fact that if $\mathbf{S}$ is hidden, the public key $(\mathbf{A}, \mathbf{P})$ is computationally indistinguishable from uniform distribution over $(\mathbb{Z}/q\mathbb{Z})^{n \times m} \times (\mathbb{Z}/q\mathbb{Z})^{l \times m}$, for suitable parameters, under the hypothesis that LWE is hard.

3.3 PKC based on ideal lattices

To improve the efficiency of the LWE-based system, Lyubashevsky, Peikert, and Regev [24] proposed the primitive of ring-LWE. Let $R = \mathbb{Z}[x]/(x^n + 1)$, where n is a power of two. Let $R_q = (\mathbb{Z}/q\mathbb{Z})[x]/(x^n + 1)$.

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

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

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

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

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

The algorithm is very efficient. Public and private key size is $\tilde{O}(n)$. Cipher-text expansion is $O(1)$, and encryption/decryption complexity per bit is $(\log n)^{O(1)}$, assuming that we use the fast multiplication algorithm. The parameters are optimal asymptotically, however, the security is based on approx-SVP of ideal lattices, rather than general lattices.

4   PKC from dihedral group rings

In this section, we describe a cryptosystem based on the dihedral group ring. The protocol is identical to one based on the ideal lattice, except that since multiplication is not commutative, one needs to pay attention to the order of multiplication. The discretization $\bar{\chi} : \mathbb{Z}/q\mathbb{Z} \to \mathbb{R}$ of a Gaussian χ on $\mathbb{R}$. First, reduce χ by modulo $\mathbb{Z}$ to obtain a distribution $\chi \mod \mathbb{Z}$ on $[0, 1)$. Then divide $[0, 1)$ into q parts $[1 - 1/2q, 1) \cup [0, 1/2q), [1/2q, 3/2q), \cdots$, and $[1 - 3/2q, 1 - 1/2q)$, and integrate the distribution $(\chi \mod \mathbb{Z})$ on each part to define $\bar{\chi}(0), \bar{\chi}(1), \cdots, \bar{\chi}(q-1)$.

Let n be a power of two, let q be a prime such that $\gcd(q, 2n) = 1$, and $q \in [n^2, 2n^2]$. Recall

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

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

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

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

- **Private key:** The private key is $s, e \in \mathbf{R}_q$ from the error distribution.
- **Public key:** Select a random $a \in \mathbf{R}_q$ uniformly. Output $(a, b) \in \mathbf{R}_q^2$, where $b = sa + e$.

– **Encryption:** To encrypt a bit string z of length n, we view it as an element in $\mathbf{R}_q$ so that bits in z become coefficients of a polynomial. The cipher-text is (u, v) obtained by

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

where r, e_1, e_2 are chosen from an error distribution.

– **Decryption:** For cipher-text (u, v), one computes $v - su$, which equals

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

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

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

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

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

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

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

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

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

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

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

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

Note that

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

14

5 Security analysis of the group ring LWE

In this section, we prove the main theorem

Theorem 3. *Let $\alpha = \alpha(n) \in (0,1)$, and let $q = q(n)$ be a prime such that $\alpha q \geq \sqrt{n}\omega(\sqrt{\log n})$. Given an average case of search version of dihedral GR-$LWE_{q,\Psi_{\leq\alpha}}$ oracle with error distributions $\Psi_{\leq\alpha}$, there is a quantum polynomial time algorithm that solves the search version of the SVP problem for any invertible ideal I of $\mathbf{R}$ with approximate factor $\tilde{O}(n/\alpha)$.*

Proof. It is from Lemmas 6 and 8 that with dihedral GR-LWE$_{q,\Psi_{\leq\alpha}}$ oracle one can sample a discrete Gaussian on the ideal I of width $\lambda_n \sqrt{n}\omega(\log n)/\alpha$, starting with a sufficiently large value of width $r \geq 2^{2n}\lambda_n(I)$ where any polynomial number of samples can be generated classically [32]. As a sample from the discrete Gaussian has Euclidean length at most $\sqrt{n}\cdot\lambda_n(I)\sqrt{n}\omega(\log n)/\alpha$ with overwhelming probability. So the sample solves the search version of the SVP problem for the ideal I with approximate factor $\tilde{O}(n/\alpha)$.

Let us first review the main ideas in Regev's reduction from approx-SVP to LWE, which inspires our proof. The reduction can be divided into iterative steps. We will solve the *Discrete Gaussian Sampling* problem (DGS) for a lattice, that has a comparable hardness as approx-SVP. The DGS$_{\mathcal{L},r}$ problem is to sample lattice points of a lattice $\mathcal{L}$ according to a Gaussian centering at O with width r. For precise definition, see [32]. The DGS will be reduced, by a quantum algorithm, to a β-BDD problem on its dual lattice $\mathcal{L}^*$, which will then be reduced to a (q,β)-BDD problem. The (q,β)-BDD will be reduced to a DGS problem of larger width. This step needs help from the search LWE oracle. After a few iterations, we arrive at DGS with a width that allows a polynomial time algorithm.

The only step that needs an LWE oracle is the reduction from (q,β)-BDD to DGS. Suppose we have a (q,β)-BDD instance $y(= x + e)$, where $x \in \mathcal{L}^*$ and $||e|| \leq \lambda_1(\mathcal{L}^*)\beta$. We wish to find $x \pmod{q\mathcal{L}^*}$. We are able to sample a random element $z \in \mathcal{L}$ by the DGS algorithm, such that $||z|| \leq m/\lambda_1(\mathcal{L}^*)$, where $m \geq q\sqrt{n}$. So we have

$$m/\lambda_1(\mathcal{L}^*) \geq q\sqrt{n}/\lambda_1(\mathcal{L}^*) \approx q\eta(\mathcal{L}) = \eta(q\mathcal{L}),$$

where $\eta(*)$ is the smoothing parameter of a lattice. Let a be $z \mod q\mathcal{L}$. Then a is a random element in $\mathbb{F}_q^n$ by the definition of a smoothing parameter. We compute a by writing down the coefficients of z in the base B and modulo them by q. There is a map from $\mathbb{F}_q^n$ to $\mathcal{L} \pmod{q\mathcal{L}}$ given by the base matrix $\mathbf{B}$, such that $\psi\mathbf{B} = 1$, where ψ is a map in the $\mathbb{Z}$-module exact sequence:

$$0 \to q\mathcal{L} \to \mathcal{L} \xrightarrow{\psi} \mathbb{F}_q^n \to 0$$

Note that the map given by $\mathbf{B}$ is not a $\mathbb{Z}$-module homomorphism, since the exact sequence is not splitting. Let $b = z(x + e)^T = zx^T + ze^T \pmod{q\mathbb{Z}}$, and

15

$s = x\mathbf{B}^T$. Note that $|ze^T|_\infty \leq m\beta$, and $zx^T = a\mathbf{B}x^T = a\mathbf{B}(s(\mathbf{B}^{-1})^T)^T = as$. Call the search LWE oracle, we will get s, which gives us $x \pmod{q\mathcal{L}^*}$, and completes the reduction. We can see that working with the dual lattice is very important.

Remark 3. Here the transformation by $\mathbf{B}$ is important. We can not just mod z by $q\mathbb{Z}^n$, since it may be the case that $\mathcal{L} \subseteq q\mathbb{Z}^n$, or $\mathcal{L}$ is not even an integral lattice.

For LWE on the ring $R = \mathbb{Z}[x]/(x^n + 1)$, the idea is similar. Any ideal in the number field $\mathbb{Q}[x]/(x^n + 1)$ is a $\mathbb{Z}$-module thus corresponds to a lattice if we provide an embedding. There are two ways of embedding: canonical and coefficient. If we use canonical embedding, then the dual is $I^\vee$ [24], instead of I^{-1}. To keep the multiplicative structure of the ring, we need a R-module isomorphism from $I/(qI)$ to $R/(qR) = \mathbb{F}_q[x]/(f(x))$, and from $I^\vee/(qI^\vee)$ to $R^\vee/(qR^\vee) = \mathbb{F}_q[x]/(f(x))$, so we can recover $I^\vee/(qI^\vee)$ from a polynomial in $R/(qR)$. As pointed out in [24], it is important to clear ideals while preserving the R-module structure.

Example 1. Let $R = \mathbb{Z}$, $q = 5$ and $I = (3)$. Suppose that $z = 24 \in I$, $z \pmod{qI}$ should be 9 in the parallelepiped $[0, 15)$. Dividing by $t = 3$, we send z to 3 in $\mathbb{Z}/q\mathbb{Z}$. Hence multiplying by 3 is a $\mathbb{Z}$-module isomorphism from $\mathbb{Z}/5\mathbb{Z}$ to $I/5I$.

On the other hand, $\mathbb{Z}$-module isomorphism is not unique. If we can just use the inclusion $I \hookrightarrow R$, we have $z = 4 \pmod 5$. This is another $\mathbb{Z}$-module isomorphism. If $\psi : I \to R$ is a R-module isomorphism, so is $t\psi$ for any $t \in R$.

To complete the reduction, one needs to send an element in $\mathbb{Z}/5\mathbb{Z}$ back to $I^{-1}/5I^{-1}$. Here $I^{-1} = (1/3)\mathbb{Z}$. One can see that the inclusion $\mathbb{Z} \subseteq I^{-1}$ induces an isomorphism $\mathbb{Z}/5\mathbb{Z} \to I^{-1}/5I^{-1}$.

Now we will extend the idea to non-commutative group ring LWE. We should use coefficient embedding to map ideals to lattices. In the following discussion, we will use the same symbol for an ideal and its corresponding lattice under coefficient embedding.

The precise error distribution in the definition of ring-LWE to ensure the hardness result is one important issue. In [24], the authors generalized one dimensional Gaussian error distribution in plain-LWE [32] to n-dimensional (ellipitcal) Gaussian which is described by an $n \times n$-covariance matrix. However, in [24] they chose the canonical embedding which makes the Gaussian error distributions during the reduction always diagonal. In our case, the error distributions in the reduction do not appear as diagonal any more.

Lemma 5. *Let L be a lattice, let $u \in \mathbb{R}^n$ be a vector, let $r, s > 0$ be two reals, let $A \in \mathbb{R}^{n \times n}$ be a non-singular matrix. Assume that smooth property $\sum_{y \in L^* \setminus \{0\}} \exp(-\pi y^T (\frac{1}{r^2} I_n + \frac{1}{s^2} A^T \cdot A)^{-1} y) \leq \epsilon$ holds for some ϵ, where I_n denotes the $n \times n$ identity matrix. The distribution of $Av + e$ where v is distributed according to $DGS_{L+u,r}$ and e is the n dimensional Gaussian multivariable with*

mean vector 0 *and diagonal covariance matrix* $\frac{s^2}{2\pi}I_n$ *is within statistical distance* 4ϵ *of a Gaussian multivariable with mean vector* 0 *and covariance matrix* $\frac{r^2}{2\pi}A \cdot A^T + \frac{s^2}{2\pi}I_n$.

Proof (Skecth of Proof). Note that non-singular linear transformation of Gaussian multivariable is still Gaussian, and $Av + e = A(v + A^{-1}e)$. Let $Y = v + A^{-1}e$. One can directly compute the distribution of Y

$$Y(x) = \frac{\exp(-\pi x^T \Sigma^{-1} x)}{\det(\Sigma)^{1/2}} \frac{\sum_{y \in L^*} e^{-2\pi\sqrt{-1}<c_0,y>} \exp(-\pi y^T (\frac{1}{r^2}I_n + \frac{1}{s^2}A^T \cdot A)^{-1}y)}{\sum_{y \in L^*} e^{2\pi\sqrt{-1}<u,y>} \exp(-\pi r^2||y||^2)}$$

where $\Sigma = r^2 I_n + s^2 A^{-1} \cdot A^{-T}$ and c_0 is a certain vector computed from u and x. Since we have

$$|1 - \sum_{y \in L^*} e^{-2\pi\sqrt{-1}<c_0,y>} \exp(-\pi y^T (\frac{1}{r^2}I_n + \frac{1}{s^2}A^T \cdot A)^{-1}y)|$$

$$\leq \sum_{y \in L^* \backslash \{0\}} \exp(-\pi y^T (\frac{1}{r^2}I_n + \frac{1}{s^2}A^T \cdot A)^{-1}y)$$

$$\leq \epsilon$$

and

$$|1 - \sum_{y \in L^*} e^{2\pi\sqrt{-1}<u,y>} \exp(-\pi r^2||y||^2)|$$

$$\leq | \sum_{y \in L^* \backslash \{0\}} \exp(-\pi r^2||y||^2)|$$

$$\leq \sum_{y \in L^* \backslash \{0\}} \exp(-\pi y^T (\frac{1}{r^2}I_n + \frac{1}{s^2}A^T \cdot A)^{-1}y)$$

$$\leq \epsilon,$$

we immediately have

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

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

$$\frac{1}{2\pi}A\Sigma A^T = \frac{1}{2\pi}(r^2 A \cdot A^T + s^2 I_n).$$

Remark 4. $-$ If the transformation matrix A is diagonal, then it reduces to the case in [24].

– The proof relies on the invertibility of the matrix A. In the application to BDD problem, the errors in BDD are invertible with very high probability except a zero-measure set.

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

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

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

up to certain unitary base change.

Now we can prove the first part of the iteration algorithm in our scenario.

Lemma 6. *[First part of iteration] Let $\alpha = \alpha(n) \in (0,1)$, prime $q = q(n) > 2$, let I be a right ideal of $\mathbf{R}$ and integer $r > 0$ such that*

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

for some negligible $\epsilon = \epsilon(n)$. There is a probabilistic polynomial time classical reduction from $BDD_{I^{-1}, \alpha q/\sqrt{2}r}$ in the matrix norm to $GR\text{-}LWE_{q, \Psi_{\leq \alpha}}$.

Proof (Sketch of Proof). Suppose $y = x + \mathfrak{h} \in \mathfrak{h} + I^{-1}$, where the error $\mathfrak{h}$ has matrix-norm $\leq q/\sqrt{2}r$. We want to recover x. We sample a $v \in I$ according to the Gaussian distribution $DGS_{I,r}$, and let $a = \phi_1(v) \pmod{q\mathbf{R}} \in \mathbf{R}/(q\mathbf{R})$, where ϕ_1 is the inclusion $I \to \mathbf{R}$, which is also a left $\mathbf{R}$-module homomorphism. Note that $q\mathbf{R}$ is a two-sided ideal, $\mathbf{R}/q\mathbf{R}$ is a direct summand of the ring $\mathbb{F}_q[D_{2n}]$. Since $det(I)$ is not divisible by q, ϕ_1 induces a natural left $\mathbf{R}$-module surjective homomorphism $I \to \mathbf{R}/(q\mathbf{R})$. We then calculate $b = yv + e$ (in $\mathbb{R}_{\mathbf{R}}$), where e is a Gaussian $\chi_{\alpha/\sqrt{2}}$ on $\mathbb{R}_{\mathbf{R}}$. We have $b \equiv yv = xv + \mathfrak{h}v + e \pmod{q\mathbf{R}}$, where $xv \in \mathbf{R}$ and the distribution of $\mathfrak{h}v + e$ has statistic distance within 4ϵ to the Gaussian $\prod_i \chi_{\sqrt{(r/q)^2(|f(\xi^i)|+|g(\xi^i)|)^2+(\alpha/\sqrt{2})^2}} \times \prod_i \chi_{\sqrt{(r/q)^2(|f(\xi^i)|-|g(\xi^i)|)^2+(\alpha/\sqrt{2})^2}}$ by Corollary 1. We generate several instances of (a, b), and send them to the GR-$LWE_{q, \Phi_{\leq \alpha}}$ oracle. Then the oracle answers s in $\mathbf{R}/q\mathbf{R}$, as long as

$$\sqrt{(r/q)^2|\mathfrak{h}|_{\text{Mat}}^2 + (\alpha/\sqrt{2})^2} \leq \alpha, \text{ or } |\mathfrak{h}|_{\text{Mat}} \leq \alpha q/\sqrt{2}r.$$

18

Let ϕ_2 be the inclusion $\mathbf{R} \to I^{-1}$, which is also a right $\mathbf{R}$-module homomorphism. It induces a natural right module homomorphism $I^{-1} \to \mathbf{R}/(q\mathbf{R})$, since $q \nmid det(I)$. So pulling s back along the homomorphism gives us the residue class of $x \pmod{qI^{-1}}$.

Lemma 7. *If $\mathfrak{h} = f(\mathfrak{r}) + \mathfrak{s}g(\mathfrak{r}) \in \mathbf{R}_{\mathbb{R}}$ is taken from the Gaussian distribution χ_σ, then $\mathfrak{h}$ has matrix-norm at most $\sigma\sqrt{n}\omega(\sqrt{\log n})$ except with negligible probability.*

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

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

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

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

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

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

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

The second (quantum) part of the iteration algorithm in [32] was improved by [24] using BDD for error distributed from a Gaussian. By the above lemma, samples from a Gaussian $\chi_{d/\sqrt{2n}}$ are distributed in the ball $B_{d\omega(\sqrt{\log n})}$ under the matrix norm except with a negligible probability. So it is enough to have a BDD oracle which can solve errors of matrix-norm $\leq d\omega(\sqrt{\log n})$.

Lemma 8. *[Second part of iteration] There is an efficient quantum algorithm that, given any n-dimensional lattice Λ, a number $d < \lambda_1(\Lambda^*)/2$ (here, λ_1 is under Euclidean norm), and an oracle that solves $BDD_{\Lambda^*, d\omega(\sqrt{\log n})}$ in matrix-norm, outputs a sample from $DGS_{\Lambda, \sqrt{n}/d}$.*

6 Conclusion

We propose generating LWE instances from non-commutative group rings and illustrate the approach by presenting a public key scheme based on dihedral group rings. We believe that LWE on dihedral group rings achieves the right trade-off between security and efficiency. As with the original LWE and ring-LWE, we hope that the new approach is a versatile primitive, so we can build various cryptographic schemes based on this primitive besides public-key encryption. There is one open problem that we find very interesting: Can we generalize the approach to other non-commutative groups and keep the efficiency of ring-LWE?

References

1. Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (H)IBE in the standard model. In *Advances in Cryptology - EUROCRYPT 2010*, pages 553–572, 2010.
2. Shweta Agrawal, Dan Boneh, and Xavier Boyen. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE. In *Advances in Cryptology - CRYPTO 2010*, pages 98–115, 2010.
3. Miklós Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing - STOC*, pages 99–108, 1996.
4. Joppe W. Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila. Frodo: Take off the ring! practical, quantum-secure key exchange from LWE. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1006–1018, 2016.
5. Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. In *Innovations in Theoretical Computer Science - ICTS*, pages 309–325, 2012.
6. Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS*, pages 97–106, 2011.
7. Zvika Brakerski and Vinod Vaikuntanathan. Fully homomorphic encryption from ring-lwe and security for key dependent messages. In *Advances in Cryptology - CRYPTO 2011*, pages 505–524, 2011.
8. David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. In *Advances in Cryptology - EUROCRYPT 2010*, pages 523–552, 2010.
9. Hao Chen, Kristin E. Lauter, and Katherine E. Stange. Attacks on search RLWE. Cryptology ePrint Archive, Report 2015/971, 2015.
10. Hao Chen, Kristin E. Lauter, and Katherine E. Stange. Vulnerable galois RLWE families and improved attacks. Cryptology ePrint Archive, Report 2016/193, 2016.
11. D. Coppersmith. Attacking non-commutative ntru. IBM Research Report, 1997.
12. Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. Recovering short generators of principal ideals in cyclotomic rings. In *Advances in Cryptology - EUROCRYPT 2016*, pages 559–585, 2016.

13. Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. Short stickelberger class relations and application to ideal-svp. Cryptology ePrint Archive, Report 2016/885, 2016.
14. Jintai Ding. New cryptographic constructions using generalized learning with errors problem. Cryptology ePrint Archive, Report 2012/387, 2012.
15. Kirsten Eisenträger, Sean Hallgren, and Kristin E. Lauter. Weak instances of PLWE. In *Selected Areas in Cryptography - SAC 2014*, pages 183–194, 2014.
16. Yara Elias, Kristin E. Lauter, Ekin Ozman, and Katherine E. Stange. Provably weak instances of ring-lwe. In *Advances in Cryptology - CRYPTO 2015*, pages 63–92, 2015.
17. Junfeng Fan and Frederik Vercauteren. Somewhat practical fully homomorphic encryption. Cryptology ePrint Archive, Report 2012/144, 2012.
18. Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. A simple bgn-type cryptosystem from LWE. In *Advances in Cryptology - EUROCRYPT 2010*, pages 506–522, 2010.
19. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, pages 197–206, 2008.
20. Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In *Algorithmic Number Theory, Third International Symposium, ANTS-III*, pages 267–288, 1998.
21. Akinori Kawachi, Keisuke Tanaka, and Keita Xagawa. Multi-bit cryptosystems based on lattice problems. In *Public Key Cryptography - PKC*, volume 4450 of *Lecture Notes in Computer Science*, pages 315–329. Springer, 2007.
22. Richard Lindner and Chris Peikert. Better key sizes (and attacks) for lwe-based encryption. In *Topics in Cryptology - CT-RSA 2011*, pages 319–339, 2011.
23. Richard Lindner and Chris Peikert. Better key sizes (and attacks) for lwe-based encryption. In *Topics in Cryptology - CT-RSA 2011*, pages 319–339, 2011.
24. Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In *Advances in Cryptology - EUROCRYPT*, volume 6110 of *Lecture Notes in Computer Science*, pages 1–23. Springer, 2010.
25. Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *Advances in Cryptology - EUROCRYPT 2012*, pages 700–718, 2012.
26. Alexei G. Myasnikov, Vladimir Shpilrain, and Alexander Ushakov. *Non-commutative Cryptography and Complexity of Group-theoretic Problems*. American Mathematical Society, 2011.
27. Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009*, pages 333–342. ACM, 2009.
28. Chris Peikert. How (not) to instantiate ring-lwe. In *Security and Cryptography for Networks - 10th International Conference, SCN 2016*, pages 411–430, 2016.
29. Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. Pseudorandomness of ring-lwe for any ring and modulus. *IACR Cryptology ePrint Archive*, 2017:258, 2017.
30. Chris Peikert, Vinod Vaikuntanathan, and Brent Waters. A framework for efficient and composable oblivious transfer. In *Advances in Cryptology - CRYPTO 2008*, volume 5157 of *Lecture Notes in Computer Science*, pages 554–571. Springer, 2008.
31. Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, pages 187–196, 2008.

32. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 56(6):34, 2009. Preliminary version in STOC'05.

33. Sudarshan K Sehgal. *Units in integral group rings*. Longman, 1993.

34. Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science - FOCS*, pages 124–134, 1994.

35. Damien Stehlé and Ron Steinfeld. Making NTRU as secure as worst-case problems over ideal lattices. In *Advances in Cryptology - EUROCRYPT 2011*, pages 27–47, 2011.

36. K. R. Truman. *Analysis and extension of non-commutative NTRU*. PhD thesis, University of Maryland, 2007.

37. Takanori Yasuda, Xavier Dahan, and Kouichi Sakurai. Characterizing ntru-variants using group ring and evaluating their lattice security. Cryptology ePrint Archive, Report 2015/1170, 2015.