Characterizing NTRU-Variants Using Group Ring and Evaluating their Lattice Security

Takanori Yasuda[1], Xavier Dahan[2], and Kouichi Sakurai[1,3]

[1] Institute of Systems, Information Technologies and Nanotechnologies
{yasuda,sakurai}@isit.or.jp
[2] Ochanomizu University
[3] Department of Informatics, Kyushu University

Abstract. The encryption scheme NTRU is designed over a quotient ring of a polynomial ring. Basically, if the ring is changed to any other ring, NTRU-like cryptosystem is constructible.

In this paper, we propose a variant of NTRU using group ring, which is called GR-NTRU. GR-NTRU includes NTRU as a special case. Moreover, we analyze and compare the security of GR-NTRU for several concrete groups. It is easy to investigate the algebraic structure of group ring by using group representation theory. We apply this fact to the security analysis of GR-NTRU. We show that the original NTRU and multivariate NTRU are most secure among several GR-NTRUs which we investigated.

Keywords: NTRU, lattice-based cryptography, group ring, group representation theory

1 Introduction

1.1 Background

The NTRU cryptosystem proposed by Hoffstein, Pipher, Silverman [14] is one of the most practical lattice-based schemes. NTRU is suitable for compact and high-speed implementation, and was standardized by IEEE as Standard IEEE 1363.1-200 [29]. Recently, NTRU attracts attention as a candidate for post-quantum cryptography [3]. One weakness of NTRU is that decryption may fail, but parameters may be chosen to minimize or eliminate this drawback.

1.2 Previous Works and Challenging Issue

NTRU makes use of analytic and geometric structure of the ring $R = \mathbb{Z}[x]/(x^N - 1)$. On the other hand, many NTRU-like systems have been presented as shows Table 1. These variant schemes basically are constructed by changing the ring R used in NTRU to various rings including non-commutative rings. In the table, (T)GR means whether or not the ring can be expressed as a (twisted) group ring.

The ring $\mathbb{Z}[x]/(x^N - 1)$ has a simple formula for its multiplication:

$$x^i * x^j = x^{i+j \bmod N} \tag{1}$$

Generally, in the case of NTRU-like scheme using a ring R, a plain text is realized by an element in R. However, there are plain texts which cause decryption failure. The proportion of the subset of such elements in R depends on the formula for

Variant of NTRU	Ring	(T)GR
NTRU [14]	$\mathbb{Z}[x]/(x^N-1)$	GR
pNE [26]	$\mathbb{Z}[x]/(x^{2^n}+1)$	TGR
ETRU [15]	$\mathbb{Z}[\omega][x]/(x^N-1)$, $(\omega^2+\omega=-1)$	GR*
QTRU [20]	$\mathcal{Q}[x]/(x^N-1)$, ($\mathcal{O}$: integer ring of quaternion alg.)	TGR
CTRU [10]	$\mathbb{F}_2[t][x]/(x^N-1)$	-
MaTRU [6, 25]	$\mathbf{M}(m,\mathbb{Z}[x]/(x^N-1))$	-
NNRU [28]	$\mathbf{M}(m,\mathbb{Z})[x]/(x^N-I_{m,m})$	-
Matrix NTRU [22]	$\mathbf{M}(m,\mathbb{Z})$	-
NTWO [5]	$\mathbb{Z}[x,y]/(x^N-1,y^N-1)$	GR
Non-commutative [7, 27]	$\mathbb{Z}[D_n][x]/(x^N-1)$, ($D_n$: dihedral group)	GR

GR* means that the ring can be expressed as a subring of a group ring.
(T)GR means whether or not the ring can be expressed as a (twisted) group ring.

Table 1. Variants of NTRU and relation of them with group rings

multiplication of R and parameters. In case of NTRU, due to the simplicity of (1), the probability of the decryption failure can be easily minimized by turning parameters. An important direction of research about NTRU is the development of variants of NTRU using other rings and their security analysis. Additionally, it is important to choose rings which have a simple multiplication formula like (1) in order to minimize the decryption error.

1.3 Our Contribution

In this paper, we propose a NTRU-like scheme using group ring as a new encryption scheme, and we call GR-NTRU for such scheme. The group ring $\mathbb{Z}[G]$ associated to a finite group G has also a simple formula for its multiplication like (1). Therefore, we can easily minimize the probability of decryption failure in the proposed scheme similarly as the original NTRU. Since $\mathbb{Z}[x]/(x^N-1)$ is isomorphic to a group ring associated to a cyclic group, the original NTRU can be regarded as a special case of GR-NTRU.

Moreover, we propose an attack against GR-NTRU, and analyze the security of GR-NTRU based on the proposed attack. This attack is essentially an extension of the attack proposed by Gentry [11] against NTRU with composite degree.

The underlying idea of the proposed attack is as follows. Using representation theory, $\mathbb{Z}[G]$ is embedded in a certain matrix ring $\mathbf{M}_n(\mathbb{Z})$. Then, GR-NTRU can be embedded in a form of NTRU-like scheme using $\mathbf{M}_n(\mathbb{Z})$. Therefore, the attacks of NTRU-like schemes using $\mathbf{M}_n(\mathbb{Z})$ can be applied to GR-NTRU. The security of NTRU-like scheme using $\mathbf{M}_n(\mathbb{Z})$ was analyzed by Pan and Deng [23]. Simply speaking, the security of NTRU-like scheme using $\mathbf{M}_n(\mathbb{Z})$ is related to the hardness of some lattice problems of dimension $2n$. Therefore, GR-NTRU can be attacked by solving these lattice problems.

We analyze the security of GR-NTRU for several finite groups for which all irreducible representations are known. Concretely, we compare the dimension of lattice problems associated with GR-NTRU for several finite groups. For lattice attack, not only the dimension of lattice, but also an approximation factor are related to the complexity. However, since the choice of a suitable approximation factor is difficult problem for now, we only discuss the dimension of lattice under the assumption of a fixed approximation factor. As a consequence, we show that the original NTRU and multivariate NTRU are the most secure among them if these schemes have the same key size.

1.4 Comparison with Related Works

There are some variants of NTRU which can be expressed as GR-NTRU. The original NTRU and multivariate NTRU [5] are regarded as special case of GR-NTRU. The variant of NTRU defined by the polynomial $x^{2^n}+1$ [26] cannot be seen as a GR-NTRU, but, can be described as a variant of NTRU using a twisted group ring. Similarly, QTRU [20] can also be described as a variant of NTRU using twisted group ring. Twisted group ring is an extension of group ring. The reason why we do not define GR-NTRU using twisted group ring instead of group ring is because the embedding required in our attack cannot be obtained from standard group representation theory. The scheme proposed by Coppersmith [7, 27], against which an efficient attack has been already found, is a variant of NTRU using the group ring with respect to the dihedral groups. However, its design is different from the design of our scheme.

Other than the previously proposed schemes above, we analyze the security of new schemes described as GR-NTRU with respect to Frobenius group, symmetric group. We summarize these security analysis in the appendix.

2 NTRU

We review a simple description of the NTRU cryptosystem [14]. Let N, p, q be integers satisfying $p < q$, and $R = \mathbb{Z}[x]/(x^N - 1)$. Any element f in R can be expressed uniquely as $f = \sum_{i=0}^{N-1} a_i x^i$ $(a_i \in \mathbb{Z})$. The subsets $\mathcal{L}_f, \mathcal{L}_g, \mathcal{L}_r, \mathcal{L}_m$ are defined as follows. First, we define the space of messages,

$$\mathcal{L}_m = \left\{ f = \sum a_i x^i \in R \;\middle|\; -\frac{1}{2}(p-1) < a_i < \frac{1}{2}(p-1),\ \forall i \right\}. \tag{2}$$

For positive integers d_1, d_2,

$$\mathcal{L}(d_1, d_2) = \left\{ f = \sum a_i x^i \in R \;\middle|\; \begin{array}{l} f \text{ has } d_1 \text{ coefficients equal } 1, \\ f \text{ has } d_2 \text{ coefficients equal } -1, \\ \text{the rest are } 0. \end{array} \right\}$$

For three integers d_f, d_g, d,

$$\mathcal{L}_f = \mathcal{L}(d_f, d_f - 1),\ \mathcal{L}_g = \mathcal{L}(d_g, d_g),\ \mathcal{L}_\phi = \mathcal{L}(d, d). \tag{3}$$

Key Generation

Step 1 Choose $f \in \mathcal{L}_f,\ g \in \mathcal{L}_g$ such that there exists $f_q, f_p \in R$ satisfying $f * f_q = 1 \bmod q$ and $f * f_p = 1 \bmod p$.
Step 2 Let $h = f_q * g \bmod q$.
Public Key h, p, q.
Private Key f (and f_p).

Encryption To encrypt a message $m \in \mathcal{L}_m$, we first choose randomly a $\phi \in \mathcal{L}_\phi$, then compute the cipher text:

$$c \equiv ph * \phi + m \bmod q.$$

Decryption First, we compute

$$a \equiv f * c \bmod q.$$

Next, we choose the coefficients of a in the interval from $-q/2$ to $q/2$. Then, we can recover the message m by computing $f_p * a \bmod p$.

3 New System using Group Ring

In this section, we propose a new NTRU-based cryptosystem using group ring, as an extension of NTRU.

3.1 Group Ring

Let G be a finite group.

Definition 1 ([4]). $\mathbb{Z}[G]$ *is defined as the set*

$$\mathbb{Z}[G] = \left\{ \sum_{g \in G} a_g[g] \;\middle|\; a_g \in \mathbb{Z} \ (\forall g \in G) \right\}$$

Here, $[g]$ *is a formal element associated to* $g \in G$*, and* $\{[g] \mid g \in G\}$ *becomes a basis of* $\mathbb{Z}[G]$*. The addition and multiplication in* $\mathbb{Z}[G]$ *are defined as follows:*

(1) The addition is defined by component-wise addition.

(2) For any $g, h \in G$*,* $[g] * [h] = [gh]$*. The multiplication of any two elements in* $\mathbb{Z}[G]$ *is defined by* $\mathbb{Z}$*-linear extension of the above formula.*

By these addition and multiplication, $\mathbb{Z}[G]$ *becomes a ring, which is called the group ring with respect to* G*.*

Example 1 Let $C_N = \langle \sigma \rangle$ be a cyclic group of order N. Then $\mathbb{Z}[C_N]$ is isomorphic to $\mathbb{Z}[x]/(x^N - 1)$. In fact, the $\mathbb{Z}$-linear map below is a ring isomorphism.

$$\begin{array}{ccc} \mathbb{Z}[C_N] & \xrightarrow{\sim} & \mathbb{Z}[x]/(x^N - 1) \\ \Cup & & \Cup \\ \sigma^i & \mapsto & x^i. \end{array} \tag{4}$$

3.2 GR-NTRU

Let p, q be integers satisfying $p < q$, G a finite group, and $R = \mathbb{Z}[G]$. Any element f in R can be expressed uniquely as $f = \sum_{g \in G} a_g[g]$ $(a_g \in \mathbb{Z})$. The subsets $\mathcal{L}_f, \mathcal{L}_g, \mathcal{L}_\phi, \mathcal{L}_m$ of R are defined as follows. First, we define

$$\mathcal{L}_m = \left\{ f = \sum_g a_g[g] \in R \;\middle|\; -\frac{1}{2}(p-1) < a_i < \frac{1}{2}(p-1), \ \forall i \right\}.$$

For positive integers d_1, d_2,

$$\mathcal{L}(d_1, d_2) = \left\{ f = \sum_g a_g[g] \in R \;\middle|\; \begin{array}{l} f \text{ has } d_1 \text{ coefficients equal } 1, \\ f \text{ has } d_2 \text{ coefficients equal } -1, \\ \text{the rest are } 0. \end{array} \right\}$$

For three integers d_f, d_g, d,

$$\mathcal{L}_f = \mathcal{L}(d_f, d_f - 1),\ \mathcal{L}_g = \mathcal{L}(d_g, d_g),\ \mathcal{L}_\phi = \mathcal{L}(d, d).$$

Key Generation

Step 1 Choose $f \in \mathcal{L}_f,\ g \in \mathcal{L}_g$ such that there exists $f_q, f_p \in R$ satisfying $f * f_q = 1 \bmod q$ and $f * f_p = 1 \bmod p$.
Step 2 Let $h = f_q * g \bmod q$.
Public Key h, p, q.
Private Key f (and f_p).

Encryption To encrypt a message $m \in \mathcal{L}_m$, we first choose a $\phi \in \mathcal{L}_\phi$, then compute the cipher text:

$$c \equiv ph * \phi + m \bmod q.$$

Decryption First, we compute

$$a \equiv f * c \bmod q.$$

Next, we choose the coefficients of a in the interval from $-q/2$ to $q/2$. Then, we can recover the message m by computing $f_p * a \bmod p$.

We call this new scheme *GR-NTRU* in this paper. We remark that in the case of $G = C_N$ (cyclic group), the corresponding GR-NTRU is equivalent to the original NTRU through the isomorphism (4).

We remark that GR-NTRU has a malleability, which is not discussed in this paper: In fact, writing $E(\phi, m)$ for the cipher text $ph * \phi + m \bmod q$, we have

$$E(\phi * a, m * a) = E(\phi, m) * a,$$

for some element $a \in \mathbb{Z}[G]$.

4 Lattice Attack against GR-NTRU

For NTRU, several attacks have been known, e.g. the brute-force attack, the meet-in-the-middle attack [14]. These attacks can be extended to those against GR-NTRU. The side channel attack against NTRU also has been proposed [17]. However, in this paper, we focus on only the security for lattice attack.

4.1 Lattice

We denote a lattice spanned by n linear independent vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n \in \mathbb{Z}^n$ by

$$\mathcal{L}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n) = \left\{ \sum_{i=1}^{n} c_i \mathbf{b}_i \mid c_i \in \mathbb{Z} \right\}.$$

The shortest vector problem (SVP) refers to the question of finding the shortest non-zero vectors. It is known to be NP-hard under random reduction. The closest vector problem (CVP) is to find a lattice vector which is closest to a given vector. Denote by $\|\mathbf{v}\|$ the Euclidean l_2-norm of a vector $\mathbf{v}$ and by $\lambda_1(\mathcal{L})$ the length of the shortest non-zero vector in the lattice $\mathcal{L}$. By the Gaussian Heuristic, $\lambda_1(\mathcal{L}) \approx \sqrt{\frac{n}{2\pi e}}\det(\mathcal{L})^{1/n}$ in an n-dimensional random lattice $\mathcal{L}$. Similarly, most closest vector problems for $\mathcal{L}$ have a solution whose size is approximately $\lambda_1(\mathcal{L}) \approx \sqrt{\frac{n}{2\pi e}}\det(\mathcal{L})^{1/n}$. If we want to find a short vector $\mathbf{v}$ in $\mathcal{L}$, or a vector $\mathbf{v}$ such that $\mathbf{t} - \mathbf{v}$ is the vector in $\mathcal{L}$ close to the target vector $\mathbf{t}$, then experience tells us that the smaller $\|\mathbf{v}\|/\left(\sqrt{\frac{n}{2\pi e}}\det(\mathcal{L})^{1/n}\right)$ is, the more easily we will find $\mathbf{v}$ in practice.

4.2 Lattice Attack by Coppersmith and Shamir

The lattice attack [9] by Coppersmith and Shamir against NTRU can be extended to GR-NTRU naturally. Here, we give the brief analysis of the attack.

Let $N = \sharp G$. Given an ordering for elements in G, let us write

$$G = \{g_1, g_2, \ldots, g_N\}.$$

Any element in $\mathbb{Z}[G]$ is identified with a row vector:

$$\sum_{i=1}^{N} a_{g_i}[g_i] \longleftrightarrow (a_{g_1}, a_{g_2}, \ldots, a_{g_N}).$$

In what follows, we identify the secret key, public key, plain text, etc. with the corresponding row vectors. For the public key $h = (h_{g_1}, h_{g_2}, \ldots, h_{g_N})$, consider the $2N$-by-$2N$ matrix as follows:

$$\left(\begin{array}{ccccc|ccccc}
1 & 0 & \cdots & 0 & 0 & h_1 & h_{g_1^{-1}g_2} & \cdots & h_{g_1^{-1}g_{N-1}} & h_{g_1^{-1}g_N} \\
0 & 1 & \cdots & 0 & 0 & h_{g_2^{-1}g_1} & h_1 & \cdots & h_{g_2^{-1}g_{N-1}} & h_{g_2^{-1}g_N} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 1 & 0 & h_{g_{N-1}^{-1}g_1} & h_{g_{N-1}^{-1}g_2} & \cdots & h_1 & h_{g_{N-1}^{-1}g_N} \\
0 & 0 & \cdots & 0 & 1 & h_{g_N^{-1}g_1} & h_{g_N^{-1}g_2} & \cdots & h_{g_N^{-1}g_{N-1}} & h_1 \\
\hline
0 & 0 & \cdots & 0 & 0 & q & 0 & \cdots & 0 & 0 \\
0 & 0 & \cdots & 0 & 0 & 0 & q & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & q & 0 \\
0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & q
\end{array}\right)$$

Let L be the lattice generated by the rows of this matrix. Then, the lattice L contains the vector $\tau = (f, g) \in \mathbb{Z}^{2N}$ because $h = f^{-1}g \bmod q$. By the Gaussian Heuristic, the expected shorter vector in L has length approximately $\sqrt{2N/(2\pi e)} \cdot \det(L)^{1/(2N)} = \sqrt{qN/(\pi e)}$. The smaller $\|(f, g)\|/\sqrt{qn/(\pi e)}$ is, the more easily (f, g) may be found by solving technique for SVP.

4.3 Security Analysis through NTRU-like Scheme Using Matrix Ring

In order to analyze the security of GR-NTRU, we make use of a NTRU-like scheme relying on a matrix ring and its cryptanalysis. We will explain the scheme and its cryptanalysis in this section. We remark that the scheme using matrix ring is not new, in fact, it is regarded as a part of a general NTRU-Like framework proposed by Pan and Deng [23].

NTRU-like System Using Matrix Ring Let $R = \mathbf{M}_n(\mathbb{Z})$. A subset $\mathcal{L}_{\mathbf{m}}$ of $\mathbb{Z}^n$ is defined similarly as $\mathcal{L}_m$ in (2). For a positive integer d, a subset $\mathcal{L}_\phi$ of $\mathbb{Z}^n$ is defined similarly as $\mathcal{L}_\phi$ in (3). For positive integers d_1, d_2, we define

$$\mathcal{D}(d_1,d_2) = \left\{ A = (a_{ij}) \in R \;\middle|\; \begin{array}{l} \text{Each row of } A \text{ has } d_1 \text{ coefficients equal } 1, \\ \text{Each row of } A \text{ has } d_2 \text{ coefficients equal } -1, \\ \text{the rest are } 0. \end{array} \right\}$$

For two integers d_F, d_G, subsets $\mathcal{D}_F, \mathcal{D}_G$ of R are defined by

$$\mathcal{D}_F = \mathcal{D}(d_F, d_F - 1), \; \mathcal{D}_G = \mathcal{D}(d_G, d_G),$$

Key Generation

Step 1 Choose $F \in \mathcal{D}_F$, $G \in \mathcal{D}_G$ such that there exists $F_q, F_p \in R$ satisfying $F * F_q = 1 \bmod q$ and $F * F_p = 1 \bmod p$.

Step 2 Let $H = F_q * G \bmod q$.

Output H, p, q (public key) and F (secret key).

The encryption and decryption are similar to those of the original NTRU, therefore we omit the explanation. We call this scheme *M-NTRU* in this paper.

Some Lattice-Based Attacks against M-NTRU Pan and Deng [23] have described some lattice-based attacks against M-NTRU (by setting it inside in a more general framework). We summarize these attacks.

Since each row of F and of G have small norm, we expect to be able to be recover F and G by finding n short vectors in the lattice spanned by

$$B = \left(\begin{array}{c|c} \mathbf{1}_n & \mathbf{0}_n \\ \hline H^T & q \cdot \mathbf{1}_n \end{array} \right),$$

since every column of $[F|G]^T$ is in the lattice.

By the Gaussian Heuristic, the size of the solution of the shortest vector problems is approximately $\sqrt{2n/(2\pi e)} \cdot \det(\mathcal{L}(B))^{1/(2n)} = \sqrt{qn/(\pi e)}$. For $1 \le i \le n$, the smaller $c_i = \|[F|G]_i^T\| / \sqrt{qn/(\pi e)}$ is, the more easily $[F|G]_i^T$ may be found by solving technique for SVP. As it gets closer to 1, finding $[F|G]_i^T$ becomes more difficult.

4.4 Proposed Attack against GR-NTRU

As explained in the previous subsection, GR-NTRU can be attacked by solving a lattice problem of dimension $\sharp G$. However, we found an attack against GR-NTRU which is reduced to solving a lattice problem of dimension lower than $\sharp G$.

Reduction of GR-NTRU to M-NTRU Assume that there is an embedding,

$$\tau : \mathbb{Z}[G] \hookrightarrow \mathbf{M}_{n_1}(\mathbb{Z}) \oplus \mathbf{M}_{n_2}(\mathbb{Z}) \oplus \cdots \oplus \mathbf{M}_{n_l}(\mathbb{Z}).$$

Then, a GR-NTRU scheme $\mathfrak{Sch}_G$ over $\mathbb{Z}[G]$ corresponds to a set $S_\tau = \{\mathfrak{Sch}_i \,|\, i = 1, \ldots, l\}$ of M-NTRU schemes, where $\mathfrak{Sch}_i$ is a M-NTRU scheme over $\mathbf{M}_{n_i}(\mathbb{Z})$. We will describe the secret and public key of $\mathfrak{Sch}_i$ for each i. We write $\tau_i : \mathbb{Z}[G] \to \mathbf{M}_{n_i}(\mathbb{Z})$ for the projection of τ into the i-th component. Let $f, h \in \mathbb{Z}[G]$ be the secret and public key of the GR-NTRU scheme $\mathfrak{Sch}_G$. We define $F_i, H_i \in \mathbf{M}_{n_i}(\mathbb{Z})$ by $F_i = \tau_i(f), H_i = \tau_i(h)$. Then, F_i and H_i are the secret and public key of the scheme $\mathfrak{Sch}_i$, respectively. From the injectivity of τ, we have

Proposition 1. *Information of all F_i (resp. H_i) for $i = 1, \ldots, l$ recovers F (resp. H).*

Let $m, c \in \mathbb{Z}[G]$ be a message and cipher text for $\mathfrak{Sch}_G$. For $i = 1, \ldots, l$ and $j = 1, \ldots, n$, $\mathbf{m}_{ij}$ and $\mathbf{c}_{ij}$ are defined by the j-th column of $\tau_i(m)$ and $\tau_i(c) \in \mathbf{M}_{n_i}(\mathbb{Z})$, respectively. In this way, $\mathbf{m}_{i1}, \ldots, \mathbf{m}_{in}$ are regarded as the message of the scheme for $\mathfrak{Sch}_i$. From the injectivity of τ, we also have

Proposition 2. *Information of all $\mathbf{m}_{ij}$ (resp. $\mathbf{c}_{ij}$) for $i = 1, \ldots, l$, $j = 1, \ldots, n$ recovers m (resp. c).*

Remark 1. In order that $F_i \in \mathbf{M}_{n_i}(\mathbb{Z})$ defined above becomes the secret of a certain M-NTRU scheme, F_i must have sufficiently small coefficients. Similarly, all $\mathbf{m}_{ij}$ ($j = 1, \ldots, n$) must have sufficiently small coefficients, too. Such conditions are not always satisfied. However, we checked that these conditions are satisfied in the case where G are dihedral groups and Frobenius groups, from the point of view of the Gaussian Heuristic. In what follows, we assume that these conditions are always satisfied.

Lattice Attack Against GR-NTRU From the last subsection, the following attack works well for GR-NTRU. Let $\mathfrak{Sch}_G$ be a GR-NTRU scheme over $\mathbb{Z}[G]$.

Step 1 Find an injective ring homomorphism,

$$\tau : \mathbb{Z}[G] \hookrightarrow \mathbf{M}_{n_1}(\mathbb{Z}) \oplus \mathbf{M}_{n_2}(\mathbb{Z}) \oplus \cdots \mathbf{M}_{n_l}(\mathbb{Z}).$$

Step 2 Using τ, compute the set $\{H_i\}$, or $\{\mathbf{c}_{ij}\}$ defined as in § 4.4 from the public key H, or a cipher text c for $\mathfrak{Sch}_G$.

Step 3 Apply lattice-based attacks to all $\mathfrak{Sch}_i$ ($i = 1, \ldots, l$), and reveal the secret keys F_i or messages $\mathbf{m}_i$.

Step 4 Recover f or m using τ.

From § 4.3, the dimension of the lattice used in the lattice-based attacks against $\mathfrak{Sch}_i$ coincides with n_i. Therefore, the complexity of the attack is determined dominantly by the maximal number among $n_1, \ldots, n_l$.

Remark 2. From the above observation, it is better for adversary to choose an embedding τ with smaller n_i. In the appendix, we explain how to find such embedding. Generally, the decomposition of group ring can be obtained using group representation theory. We apply this fact to finding a good embedding.

5 Relation of GR-NTRU and Previous Variants of NTRU

There are several variants of NTRU previously proposed, where the ring can be described by a (twisted) group ring. Our attack can be applied to such schemes. In this section, these schemes are reconsidered from the point of view of GR-NTRU, and we consider the effect of our attack to these schemes.

5.1 NTRU with composite degree

Gentry analyzed the security of NTRU with a composite degree N [11]. He shows that in case of composite N, NTRU can be associated with a lattice problem of a smaller dimension than that of lattice used in the attack by Coppersmith and Shamir. He makes use of a ring homomorphism,

$$\theta : \mathbb{Z}[x]/(x^N - 1) \to \mathbb{Z}[x]/(x^d - 1) \quad \text{for a divisor } d \text{ of } N \tag{5}$$

From this map, the NTRU system on $\mathbb{Z}[x]/(x^N - 1)$ can be transfered to that of $\mathbb{Z}[x]/(x^d - 1)$. Since the latter ring has smaller dimension than the former, the latter NTRU system is easier to break than the former. If one can gather information about secret keys on NTRU system for all factors, the secret key of the original NTRU can be recovered by the chinese remainder theorem.

Let us explain that the attack above is essentially same as our proposed attack in the case of cyclic group with composite order. As explained in § 3.1, we have the following isomorphism:

$$\mathbb{Z}[C_N] \simeq \mathbb{Z}[x]/(x^N - 1).$$

Therefore, the original NTRU is expressed as a GR-NTRU for $G = C_N$. On the other hand, $\mathbb{Z}[C_N]$ has following decomposition.

$$\mathbb{Z}[C_N] \simeq \bigoplus_{d|N} \mathbb{Z}[\zeta_d],$$

where ζ_d is a primitive root of 1 in $\mathbb{C}$. This isomorphism induces an injective homomorphism,

$$\tau : \mathbb{Z}[C_N] \hookrightarrow \bigoplus_{d|N} \mathbf{M}_{\phi(d)}(\mathbb{Z}). \tag{6}$$

Here, $\phi(d)$ is the Euler's totient function. Since we obtain an embedding, our attack can be applied to NTRU. The homomorphism (5) can be rewritten by

$$\theta : \mathbb{Z}[C_N] \to \bigoplus_{d'|d} \mathbb{Z}[\zeta_{d'}].$$

Therefore, considering θ's for all factors of N is essentially equivalent to considering τ above. From the embedding (6), we have

Proposition 3. *The proposed attack against NTRU is reduced to a lattice attack of dimension $\phi(N)$.*

5.2 Multivariate NTRU of Two Variables

NTWO (refered as GB-NTRU in [5]) is a multivariate variant of NTRU using two variables. The used ring is $\mathbb{Z}[x_1, x_2]/(x_1^N - 1, x_2^N - 1)$. The degrees of ideal generating functions are equal. Here, we consider NTWO as a more general case using

$\mathbb{Z}[x_1, x_2]/(x_1^{N_1} - 1, x_2^{N_2} - 1)$. We have the following isomorphism,

$$\mathbb{Z}[x_1, x_2]/(x_1^{N_1} - 1, x_2^{N_2} - 1) \simeq \mathbb{Z}[C_{N_1} \times C_{N_2}].$$

Similarly as we obtained (6), we have an embedding,

$$\tau : \mathbb{Z}[C_{N_1} \times C_{N_2}] \hookrightarrow \bigoplus_{d_1|N_1, d_2|N_2} \mathbf{M}_{\phi(d_1)\phi(d_2)}(\mathbb{Z}).$$

Among the matrix size appearing in the direct summands in the right hand side, the largest number is $\phi(N_1)\phi(N_2)$. Therefore, we have the following.

Proposition 4. *The proposed attack against NTWO is reduced to a lattice attack of dimension $\phi(N_1)\phi(N_2)$.*

5.3 NTRU ring defined by $x^{2^n} + 1$

There is a variant of NTRU using $x^{2^n} + 1$ instead of $x^N - 1$ [16, 26]. The polynomial $x^{2^n} + 1$ is always irreducible and $R = \mathbb{Z}[x]/(x^{2^n} + 1)$ is isomorphic to the integer ring of a cyclotomic field for any n. The security of NTRU using $x^{2^n} + 1$ is related to not only SVP, but also Ring-LWE problem [26], which is described over an integer ring of a cyclotomic field.

Unfortunately, the ring R cannot be described as a group ring, but can be described as a twisted group ring [8]. In short, a twisted group ring has the same set as group ring, but the product generally is defined as

$$[g] * [h] = c_{gh}[gh] \quad \text{for some integer } c_{gh} \quad (\forall g, h \in G).$$

When c_{gh} is always one, the twisted group ring coincides with a group ring. For the cyclic group $C_{2^n} = \{1, \sigma, \sigma^2, \ldots, \sigma^{2^n-1}\}$, if a product as a twisted group ring is defined by

$$[\sigma^i] * [\sigma^j] = c_{i+j}[\sigma^{i+j}] \quad (0 \leq i, j < 2^n),$$

where $c_{i+j} = -1$ if $i + j = 2^n$, and $c_{i+j} = 1$ otherwise. The twisted group ring is isomorphic to R.

As explained above, NTRU using $x^{2^n} + 1$ is not described by a GR-NTRU, but the proposed attack in § 4.4 can be applied to this scheme. The reason why we do not define GR-NTRU using twisted group ring instead of group ring is because the embedding τ with small image required in the algorithm in § 4.4 cannot be obtained using the theory of group representation. However, in the case of NTRU using $x^{2^n} + 1$, we have that

$$\tau : \mathbb{Z}[x]/(x^{2^n} + 1) \hookrightarrow \mathbf{M}_{2^n}(\mathbb{Z})$$

is the embedding with the smallest matrix size because $\mathbb{Z}[x]/(x^{2^n} + 1)$ is an integral domain. Therefore, when we apply the proposed attack to NTRU using $x^{2^n} + 1$, the dimension of a lattice attack is equal to 2^{n+1}.

5.4 Non-commutative NTRU

Non-commutative NTRU by Coppersmith Coppersmith proposed a variant of NTRU using $\mathbb{Z}[D_N]$ where D_N is the dihedral group of order $2N$ [7, 27]. However, the design of the scheme is different from that of GR-NTRU. Coppersmith also proposed an efficient attack against its own scheme. However, the attack cannot be applied to GR-NTRU with respect to D_N. On the other hand, our attack can be applied to the scheme by Coppersmith. In § A.2 appendix, we analyze our attack against GR-NTRU with respect to D_N.

QTRU: Quaternionic Variant of NTRU Let Q be the Hamilton's quaternion algebra, and $\mathcal{O}_Q$ its integer ring:

$$\mathcal{O}_Q = \mathbb{Z}.1 \oplus \mathbb{Z}.i \oplus \mathbb{Z}.j \oplus \mathbb{Z}.k,$$
$$i^2 = j^2 = k^2 = -1,\ ij = -ji = k.$$

$\mathcal{O}_Q$ can be described as a twisted group ring with respect to $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. QTRU is a variant of NTRU using $\mathcal{O}_Q[x]/(x^N - 1)$ [20]. $\mathcal{O}_Q[x]/(x^N - 1)$ is also described as a twisted group ring with respect to $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times C_N$. The paper [20] where QTRU is proposed analyzes the lattice attack by Coppersmith and Shamir. Our attack can be applied to QTRU. However, since $\mathcal{O}_Q[x]/(x^N - 1)$ cannot be described as a group ring, we cannot find the best choice of embedding τ using group representation theory. Therefore, the complexity of our attack cannot be estimated for now.

6 Comparison

For finite groups G_1, G_2 of equal order $\sharp G_1 = \sharp G_2$, GR-NTRU over $\mathbb{Z}[G_1]$ and that over $\mathbb{Z}[G_2]$ have secret key of the same size. For GR-NTRU over $\mathbb{Z}[G]$, the dimension of lattice problem associated with the lattice attack by Coppersmith and Shamir is equal to $2 \cdot \sharp G$. On the other hand, the dimension of lattice problem associated with our attack is $2n_G$. In the appendix, for the product of cyclic groups $C_{N_1} \times \cdots \times C_{N_k}$, the dihedral groups D_N, the Frobenius groups F_p, we analyze the proposed attack against GR-NTRU. Table 2 shows the dimension of lattice problem associated with the lattice attack by Coppersmith and Shamir (Dimension(C&S)) and that of our attack (Dimension(Our attack)) against GR-NTRU over $\mathbb{Z}[C_N]$, $\mathbb{Z}[C_{N_1} \times \cdots \times C_{N_k}]$, $\mathbb{Z}[D_n]$, $\mathbb{Z}[F_p]$.

For $G = C_N, C_{N_1} \times \cdots \times C_{N_k}, D_n, F_p$, let us compare $2 \cdot \sharp G$ and the minimum values of $2n_G$. In any case, n_G does not exceed $\sharp G$. However, if N is prime then the ratio of $n_{C_N} = \phi(N)$ and $\sharp C_N = N$ is almost 1. Similarly, for $G = C_{N_1} \times \cdots \times C_{N_k}$ if $N_1, \ldots, N_k$ are all prime, the ratio of $n_G = \phi(N_1) \cdots \phi(N_k)$ and $\sharp G = N_1 \cdots N_k$ is almost 1. On the other hand, in other cases than cyclic groups and their product, the ratio of n_G by the group order is properly less than 1. If we make the orders of groups (i.e. the secret key sizes) even, we can compare the security of GR-NTRU by the number $2n_G$. As a result, we have that the original NTRU and multivariate NTRU are most secure among these GR-NTRUs.

7 Conclusion

We propose an extension of NTRU cryptosystem using group ring, which is called GR-NTRU. We also propose an attack against GR-NTRU. Based on the attack, we investigate the security of GR-NTRU. In particular, we compare the security of GR-NTRU in the case of cyclic groups (original NTRU case), products of cyclic groups,

Group	Order	Dimension(C&S)	Dimension(Our attack)
C_N	N	$2N$	$2\phi(N)$
$C_{N_1} \times \cdots \times C_{N_k}$	$N_1 \cdots N_k$	$2N_1 \cdots N_k$	$\phi(N_1) \cdots \phi(N_k)$
D_n	$2n$	$4n$	$2n$
F_p	$p(p-1)$	$2p(p-1)$	$2p$

Table 2. Comparison of Attacks against GR-NTRU over $\mathbb{Z}[C_N]$, $\mathbb{Z}[C_{N_1} \times \cdots \times C_{N_k}]$, $\mathbb{Z}[D_n]$, $\mathbb{Z}[F_p]$

dihedral groups, Frobenius groups. We show that at the same secret key size, the original NTRU and multivariate NTRU are most secure among these schemes. It is important to understand why (multivariate) NTRU is most secure. From this point of view, we contribute to the safety of NTRU.

GR-NTRU has a possibility to extend to a functional encryption. If it is possible, GR-NTRU's other than the original NTRU and multivariate NTRU may also be usable. Moreover, GR-NTRU can be extended to a variant of NTRU using twisted group ring, which includes NTRU defined by $x^N + 1$ and QTRU. It is an important future work to study the security of variant of NTRU in the widely framework.

Acknowledgements

This research is commissioned by" Strategic Information and Communications R&D Promotion Programme (SCOPE), no. 0159-0016 ", Ministry of Internal Affairs and Communications, JAPAN.

References

1. W.D. Banks and I.E. Shparlinski, "A Variant of NTRU with Non-Invertible Polynomials", INDOCRYPT'02. Springer LNCS, vol. 2551, pp. 62–70, 2002.
2. K. Bagheri and M.-R. Sadeghi, "A new non-associative cryptosystem based on NTOW public key cryptosystem and octonions algebra", ACM Communications in Computer Algebra 2015, vol. 49, no. 1, pp. 13-13, 2015.
3. D.J. Bernstein, J. Buchmann, E. Dahmen, "Post-Quantum Cryptography", Springer-Verlag Berlin Heidelberg, p. 245, 2008.
4. A. A. Bovdi, "Group algebra", in Hazewinkel, Michiel, Encyclopedia of Mathematics, Springer, 2001.
5. M. Caboara, F. Caruso, C. Traverso, "Gröbner bases for public key cryptography ,International Symposium, ISSAC'08.
6. M. Coglianese and B.-M. Goi, "MaTRU: A New NTRU-Based Cryptosystem", INDOCRYPT'05. Springer LNCS, vol. 3797, pp. 232–243, 2005.
7. D. Coppersmith. "Attacking non-commutative NTRU", IBM Research Report, page 5, April 1997.
8. C. W. Curtis, I. Reiner, "Methods of representation theory I", Wiley, 1981.
9. D. Coppersmith, A. Shamir, "Lattice Attacks on NTRU", Eurocrypt'97, Springer LNCS, vol. 1223, pp. 52–61, 1997.
10. P. Gaborit, J. Ohler and P. Sole, "CTRU, a polynomial analogue of NTRU", INRIA, Rapport de recherche 4621, INRIA, 2002, `ftp://ftp.inria.fr/INRIA/publication/publi-pdf/RR/RR-4621.pdf`
11. C. Gentry, "Key Recovery ans Message Attachs on NTRU-Composit", Eurocrypt'01, Springer LNCS, vol. 2045, pp. 182–194, 2001.

12. J. Hoffstein, N. Howgrave-Graham, J. Pipher, J.H. Silverman, and W. Whyte, "Hybrid Lattice Reduction and Meet in the Middle Resistant Parameter Selection for NTRUEncrypt", `grouper.ieee.org/groups/1363/lattPK/submissions/ChoosingNewParameters.pdf`.
13. J. Hoffstein, N. Howgrave-Graham, J. Pipher, W. Whyte, "Practical Lattice-Based Cryptography: NTRUEncrypt and NTRUSign". The LLL Algorithm'10, pp. 349–390, 2010.
14. J. Hoffstein, J. Pipher, and J.H. Silverman, "NTRU: a ring based public key cryptosystem". ANTS-III, Springer LNCS vol. 1423, pp. 267–288, 1998.
15. K. Jarvis, M. Nevins, "ETRU: NTRU over the Eisenstein integers", Designs, Codes and Cryptography, vol. 74, no. 1, pp. 219–242, 2015.
16. K. Xagawa and K. Tanaka "NFALSE: Another Ring-Based Public Key Cryptosystem with Faster Encryption", The 28th Symposium on Cryptography and Information Security (SCIS'09), 2009.
17. M.-k. Lee , J. E. Song , D. Choi, D.-g. Han, "Countermeasures against Power Analysis Attacks for the NTRU Public Key Cryptosystem", IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, vol. E93-A, no.1, pp. 153–163. 2010.
18. A. Lopez-Alt, E. Tromer, V. Vaikuntanathan, "On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption", STOC'12, ACM disital library, pp. 1219–1234, 2012.
19. E. Malekian, A. Zakerolhosseini, "Ntru-like Public Key Cryptosystems beyond Dedekind Domain Up to Alternative Algebra", `http://eprint.iacr.org/2009/446`
20. E. Malekian, A. Zakerolhosseini, A. Mashatan, "QTRU: Quaternionic Version of the NTRU Public-Key Cryptosystems", ISeCure'11, vol. 3, no. 1, pp. 29–42, 2011.
21. M. Nevins , C. KarimianPour, A. Miri, "NTRU over rings beyond $\mathbb{Z}$", Designs, Codes and Cryptography, vol. 56, no. 1, pp. 65–78, 2010.
22. R. Nayak, C. Sastry, and J. Pradhan, "A matrix formulation for NTRU cryptosystem", ICON'08, IEEE, pp.1–5, 2008.
23. Y. Pan and Y. Deng, "A General NTRU-Like Framework for Constructing Lattice-Based Public-Key Cryptosystems", WISE'11, Springer LNCS vol. 7115, pp. 109–120, 2012.
24. J.-P. Serre, "Linear Representations of Finite Groups", Springer, Graduate Texts in Mathematics, vol. 42.
25. J.E. Song, T.Y. Han, M.-L. Lee, "Analysis and Improvement of MaTRU Public Key Cryptosystem", IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, E98.A(4), pp. 982–991, 2015
26. D. Stehl, R. Steinfeld, "Making NTRU as Secure as Worst-Case Problems over Ideal Lattices", EUROCRYPT'11, Springer LNCS vol. 6632, pp. 27–47, 2011.
27. K. R. Truman: Analysis and extension of non-commutative NTRU. (Ph.D Thesis, University of Maryland).
28. N. Vats, "NNRU, a noncommutative analogue of NTRU", `http://arxiv.org/abs/0902.1891`
29. "IEEE P1363: Standard Specifications For Public Key Cryptography", Grouper.ieee.org. Retrieved 7 December 2014.

A Security of GR-NTRU for Some Groups

A.1 The Case of Product of Cyclic Group

Let $G = C_{N_1} \times \cdots \times C_{N_k}$, where C_{N_i} is the cyclic group of order N_i $(i = 1, \ldots, k)$. For this group, the corresponding GR-NTRU is multivariate NTRU. In fact, $R = \mathbb{Z}[G]$ is realized by

$$R = \mathbb{Z}[x_1, \ldots, x_k]/(x_1^{N_1} - 1, \ldots, x_k^{N_k} - 1).$$

Therefore, a secret and public keys, plain and cipher texts are described in the form,

$$\sum_{0 \le i_1 < N_1, \ldots, 0 \le i_k < N_k} a_{i_1,\ldots,i_k} x_1^{i_1} \cdots x_k^{i_k} \qquad (a_{i_1,\ldots,i_k} \in \mathbb{Z}).$$

Using the result in the case of a cyclic group, we have

$$\tau : R \hookrightarrow \bigoplus_{d_1|N_1,\dots,d_k|N_k} \mathbf{M}_{\phi(d_1)\cdots\phi(d_k)}(\mathbb{Z}).$$

As a result,

Proposition 5. *The proposed attack against GR-NTRU over $\mathbb{Z}[C_{N_1} \times \cdots \times C_{N_k}]$ is reduced to a lattice attack of dimension $\phi(N_1) \times \cdots \phi(N_k)$.*

A.2 The Case of Dihedral Group

The dihedral group $D_n = C_n \rtimes \mathbb{Z}/2\mathbb{Z}$ is a group of order $2n$. D_n is embedded in n-symmetric group $\mathfrak{S}_n$. In fact, a generator of C_N corresponds to a cyclic permutation $(2, 3, \dots, n, 1)$, and the non-trivial element of $\mathbb{Z}/2\mathbb{Z}$ corresponds to

$$\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & n-1 & \cdots & 2 & 1 \end{pmatrix}.$$

Using this embedding and the expression of permutation, we have a ring homomorphism,

$$\Phi_1 : \mathbb{Z}[D_n] \to \mathbf{M}_n(\mathbb{Z}).$$

Moreover, a group homomorphism $D_n = C_n \rtimes \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ induces a ring homomorphism,

$$\Phi_2 : \mathbb{Z}[D_n] \to \mathbb{Z}.$$

If n is even, there is a group homomorphism, $D_n = C_n \rtimes \mathbb{Z}/2\mathbb{Z} \to (C_n \rtimes \mathbb{Z}/2\mathbb{Z})/(C_{n/2} \rtimes \mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$, and this induces

$$\Phi_3 : \mathbb{Z}[D_n] \to \mathbb{Z}.$$

Thus, we have

Lemma 1. *1. If n is odd, $\Phi_1 \oplus \Phi_2 : \mathbb{Z}[D_n] \to \mathbf{M}_n(\mathbb{Z}) \oplus \mathbb{Z}$ is injective.*
2. If n is even, $\Phi_1 \oplus \Phi_2 \oplus \Phi_3 : \mathbb{Z}[D_n] \to \mathbf{M}_n(\mathbb{Z}) \oplus \mathbb{Z} \oplus \mathbb{Z}$ is injective.

Consequently, the following proposition holds:

Proposition 6. *The proposed attack against GR-NTRU over $\mathbb{Z}[D_n]$ is reduced to a lattice attack of dimension n.*

A.3 The Case of Frobenius Group

The Frobenius group is defined by $F_p = (\mathbb{Z}/p\mathbb{Z}) \rtimes (\mathbb{Z}/p\mathbb{Z})^\times$ (p: prime). From the classification of irreducible representations of F_p, we have an injection,

$$\tau : \mathbb{Z}[F_p] \hookrightarrow \mathbb{Z}[x]/(x^{p-1} - 1) \oplus \mathbf{M}_p(\mathbb{Z})$$

From this map and the result of the case for $G = C_N$, we have

Proposition 7. *The proposed attack against GR-NTRU over $\mathbb{Z}[F_p]$ is reduced to a lattice attack of dimension p.*

We remark that the injection τ can be used to realize secret and public keys, and plain and cipher texts. In fact, the image of $\mathbb{Z}[F_p]$ is expressed as follows,

$$(\sum_{i=0}^{p} c_i x^i,\ (a_{k,l})_{1 \le k,l \le p}).$$

A.4 The Case of Symmetric Group

We also analyze the security of our scheme for symmetric groups. However, we cannot estimate the exact order of the complexity with regard to the degree of symmetric group. Therefore, we describe the result of the security analysis in the case of the symmetric groups, separately here.

We denote by $\mathfrak{S}_n$ n-th symmetric group. To investigate the decomposition of $\mathbb{Z}[\mathfrak{S}_n]$, we quote general results of group representation theory.

Proposition 8 (Maschke). *For a finite group G, $\mathbb{Q}[G]$ is semi-simple.*

Proposition 9 (Wedderburn-Artin). *If A is an algebra over a field K and is semi-simple, A is uniquely decomposed into a direct sum of matrix ring over a (skew) field:*

$$A \simeq \mathbf{M}_{n_1}(D_1) \oplus \mathbf{M}_{n_2}(D_2) \oplus \cdots \oplus \mathbf{M}_{n_l}(D_l)$$

Here, D_i is a (skew) field over F.

From the above two propositions, $\mathbb{Q}[G]$ is decomposed into a direct sum of matrix ring over a (skew) field.

Moreover, in case of $\mathbb{C}[G]$, the following is well-known.

Theorem 1.

$$\mathbb{C}[G] \simeq \bigoplus_{\sigma \in \hat{G}} \mathbf{M}_{n_\sigma}(\mathbb{C}). \tag{7}$$

Here, $\hat{G}$ is the set of isomorphism classes of irreducible representations of G, and n_σ is the degree of an irreducible representations σ.

In addition, if $G = \mathfrak{S}_n$, it is known that $\mathbb{Q}[G]$ has the same decomposition as (7):

$$\mathbb{Q}[G] \simeq \bigoplus_{\sigma \in \hat{G}} \mathbf{M}_{n_\sigma}(\mathbb{Q}). \tag{8}$$

Therefore, it suffices to investigate $\hat{\mathfrak{S}_n}$ and n_σ for an irreducible representation σ. From Proposition 10, it is necessary to know all conjugate classes of $\mathfrak{S}_n$. In case of $G = \mathfrak{S}_n$, any conjugate class has one-to-one correspondence to a type of permutation.

Example 2 The type of $\pi = (1,2)(3,4,5)(6,7,8) \in \mathfrak{S}_8$ is $(2,3,3)$.

Moreover, any type of permutation has a one-to-one correspondence to a partition of n.

Example 3 A class of irreducible representation of $\mathfrak{S}_8$ has one-to-one correspondence to a partition of 8. There are 22 partitions of 8:

$$8 = [1^8] = [2, 1^6] = \cdots = [8].$$

For any irreducible representation of $\mathfrak{S}_8$, its degree is also known. The pair of the degree of irreducible representation and its multiplicity is described as follows.

$$[1,2],\ [7,2],\ [14,2],\ [20,2],\ [21,2],\ [28,2],$$
$$[35,2],\ [42,1],\ [56,2],\ [64,2],\ [70,2],\ [90,1]$$

From this, $\mathbb{Q}[\mathfrak{S}_8]$ is decomposed as follows.

$$\mathbb{Q}[\mathfrak{S}_8] \simeq \mathbf{M}_1(\mathbb{Q})^{\oplus 2} \oplus \mathbf{M}_7(\mathbb{Q})^{\oplus 2} \oplus \cdots \oplus \mathbf{M}_{90}(\mathbb{Q}).$$

This implies that in order to break GR-NTRU associated to $\mathfrak{S}_8$, one must solve a lattice-based problem of dimension 90.

Similarly as $\mathfrak{S}_8$, we can compute the minimum value of n_G.

Degree n	Dimension (minimum of n_G)
8	90
9	216
10	768
11	2310
12	7700
13	21450
14	69498
15	292864
16	1153152
17	4873050
18	16336320
19	64664600
20	249420600
21	1118939184

Table 3. Dimension of lattice attack against GR-NTRU over $\mathbb{Z}[\mathfrak{S}_n]$

B How To Find an Embedding $\boldsymbol{\tau}$

In the algorithm in § 4.4, it is better for adversary to choose an embedding τ with smaller n_i. Group representation theory tells information of τ which minimizes the maximum number n_G among $n_1, \ldots, n_l$.

B.1 Linear Representation of Group

Here, we review fundamental facts about group representation theory. For more details, we refer the reader to the book [24].

Let G be a finite group. A group homomorphism $\sigma : G \to GL(n, \mathbb{C})$ for some positive integer n is called a representation of G (of finite degree). Here, n is called the degree of the representation σ. In this case, G acts on the vector space $\mathbb{C}^n$ via σ:

$$g.v = \sigma(g).v \ (\forall g \in G, v \in \mathbb{C}^n)$$

Conversely, if a vector space $V = \mathbb{C}^n$ endowed with an action of G is given, V provides a representation of G. In what follows, we call V a representation of G, simply.

Definition 2. *Let V be a representation of G of degree n.*

1. *For a subspace W of V, if the action of G is stable, we say that W is a subrepresentation of V.*
2. *If V has only $\{0\}$ and itself as subrepresentations, we say that V is irreducible.*
3. *For a representation W of G, if there exists an isomorphism $\phi : V \to W$ as vector spaces such that*
$$\phi(g.v) = g.(\phi(v)) \quad (\forall g \in G, v \in V),$$
we say that V and W are isomorphic as representation of groups.

As for representations of finite groups, the following fact is well-known.

Proposition 10. *The number of isomorphism classes of representations of G is equal to the number of conjugate classes in G. In particular, this number is finite.*

Next, we describe a known relation between group representation and group ring.

Lemma 2. *A group representation $\sigma : G \to GL(n, \mathbb{C})$ is naturally extended to a homomorphism between group rings, $\tilde{\sigma} : \mathbb{C}[G] \to \mathbf{M}(n, \mathbb{C})$. Conversely, a homomorphism between group rings, $\tilde{\sigma} : \mathbb{C}[G] \to \mathbf{M}(n, \mathbb{C})$ provides a group representation $\sigma : G \to GL(n, \mathbb{C})$ by restriction.*

Consider a ring homomorphism
$$\tau : \mathbb{Z}[G] \to \mathbf{M}_{n_1}(\mathbb{Z}) \oplus \mathbf{M}_{n_2}(\mathbb{Z}) \oplus \cdots \oplus \mathbf{M}_{n_l}(\mathbb{Z}) \tag{9}$$
which is not necessary injective. The scalar extension '$\otimes_{\mathbb{Z}}\mathbb{C}$' on τ, yields the following ring homomorphism,
$$\tau_{\mathbb{C}} : \mathbb{C}[G] \to \mathbf{M}_{n_1}(\mathbb{C}) \oplus \mathbf{M}_{n_2}(\mathbb{C}) \oplus \cdots \oplus \mathbf{M}_{n_l}(\mathbb{C}) \tag{10}$$
The map (10) can be regarded as a representation of degree $n_1 + \cdots + n_l$. Then, from representation theory, we have

Proposition 11. *A ring homomorphism* (9) *is injective if and only if the group representation given by* (10) *includes all irreducible representations of G as a subrepresentation.*