Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 7, pp. 2797–2810
DOI : 10.47974/JDMSC-2131

Secure public key encryption and key encapsulation mechanism based on group ring learning with errors problem

Gaurav Mittal *
Sandeep Kumar †
Sunil Kumar §
Defence Research and Development Organization
Near Metcalfe House
New Delhi 110054
India

Shiv Narain ‡
Department of Mathematics
Arya P.G. Collge
Panipat 132103
Haryana
India

Yogesh K. Gupta @
Defence Research and Development Organization
Near Metcalfe House
New Delhi 110054
India

Abstract

In this paper, our main aim is to propose a group ring analogue of the well-known learning with errors problem and discuss its security. Using this novel problem, we construct

* *E-mail:* gaurav.mittaltwins@gmail.com (Corresponding Author)
† *E-mail:* sandeepkumar.hqr@gov.in
§ *E-mail:* sunilkumar.hqr@gov.in
‡ *E-mail:* math.shiv@gmail.com
@ *E-mail:* yogeshg206@gmail.com

IND-CPA secure public key encryption scheme and IND-CCA secure key encapsulation mechanism. We also discuss a toy example relevant to our encryption scheme.

Subject Classification: *(2010) 94A60, 20C05, 20C07.*

Keywords: *Cryptography, Public key encryption, Lattice cryptography, Group ring.*

1. Introduction

Due to the availability of various practical quantum algorithms, the well-known hard mathematical problems such as integer factorization problem, discrete logarithm problem and its elliptic curve analogue will no longer be safe to employ whenever there is an availability of sufficiently large quantum computer [2]. Therefore, researchers around the world are looking to discover new quantum safe hard mathematical problems to construct cryptographic primitives such as encryption schemes, key encapsulation mechanisms, digital signatures etc. Some of the well-known and recently discovered hard problems are learning with errors (LWE), decoding of a general linear code, solving multi-variable equations etc., see [2] for a nice survey. The LWE problem is a well-studied lattice based problem and it is believed to be quantum safe [1]. However, the cryptosystems based on LWE problem are not practical for large scale usage due to large public key size. Consequently, ring learning with errors problem (RLWE) has been discovered, which is LWE in a quotient ring $\frac{\mathbb{Z}_q[x]}{(x^N-1)}$, where q is a prime and N is a positive integer (see [20]).

The cryptosystems based on RLWE problem have a considerably smaller public key size in comparison to cryptosystems based on LWE problem [11], but they offer less security in comparison to the latter [20]. This is due to the fact that the matrix involved in LWE problem is a generalized one. Nevertheless, RLWE problem has many applications in cryptography as the reduced strength does not lead to any practical polynomial time attack or any other vulnerability [11]. In this paper, our main purpose is to propose a generalized version of RLWE problem and consequently, to propose public key encryption (PKE) and key encapsulation mechanism (KEM) based on the generalized problem. More precisely, we propose a group ring analogue of the LWE problem and call it as GRLWE problem.

Group ring based cryptography [6] has gained the attention of many researchers in the recent years. This is due to the fact that the algebraic structure of group ring is a source of many hard (possibly quantum safe)

mathematical problems (see [18]). We refer to [15, 16, 17, 18, 19, 7, 8, 9, 10] for some recent constructions of cryptographic primitives based on group ring.

Our contribution: In this paper, we define the group ring analogue of LWE problem (i.e., GRLWE problem) and discuss its security. Further, by employing this hard problem, we propose a IND-CPA secure public key encryption motivated by the work of [12] and IND-CCA secure key encapsulation mechanism motivated from [3]. To showcase the practicality of our encryption scheme, we also discuss a toy example. Furthermore, we also recommend the values of various parameters involved in our scheme.

This paper is structured in the following way. The discussion on preliminaries is included in Section 2. In Section 3, we propose the novel GRLWE problem and then construct the PKE and KEM based on it. We also discuss the security of our PKE and KEM in the same section. In Section 4, we discuss a toy example and values of the various parameters involved in our scheme for practical usage. Section 5 concludes the paper.

2. Preliminaries

This section contains certain definitions and notions needed in our work. We begin with the definition of group ring.

Definition 2.1: Group Ring [13]: Let G be a finite group of order N. Then a group ring RG is the set of all finite R-linear combinations of the elements of G, where R is a ring. More precisely, we have

$$\mathrm{RG} = \left\{ \sum_{s=1}^{N} r_s g_s : r_s \in \mathrm{R}, g_s \in \mathrm{G} \right\}.$$

Under usual addition and multiplication, RG forms a ring. Let $u_1 \circledast u_2$ denote the product of any two elements $u_1, u_2 \in \mathrm{RG}$. Further, any element $u \in \mathrm{RG}$ is said to be unit in RG, provided $v \in \mathrm{RG}$ exists uniquely such that $u \circledast v = 1$, where 1 is the identity of G.

Next, we discuss the notion of attack models IND-CPA and IND-CCA.

Definition 2.2: IND-CPA security [20]: Let $\mathcal{A}$ be an adversary and let $\mathcal{C}$ be a challenger. The IND-CPA attack model involves a game to be played between $\mathcal{A}$ and $\mathcal{C}$ as follows:

Setup: $\mathcal{C}$ generates the scheme parameters along with the public key and submits these to $\mathcal{A}$.

Challenge: $\mathcal{A}$ picks two random messages M_0, M_1 of his/her choice and submits them to $\mathcal{C}$. In response, $\mathcal{C}$ tosses a coin $c \in \{0,1\}$. Using c, $\mathcal{C}$ encrypts M_c and submits the ciphertext to $\mathcal{A}$.

Guess: $\mathcal{A}$ comes out with $c' \in \{0,1\}$ through some means. $\mathcal{C}$ wins the game if $c \neq c'$.

If $\mathcal{C}$ wins the game, then the scheme is IND-CPA secure.

Definition 2.3: IND-CCA security [20]: Let $\mathcal{A}$ be an adversary and let $\mathcal{C}$ be a challenger. The IND-CCA attack model involves a game to be played between $\mathcal{A}$ and $\mathcal{C}$ as follows:

Setup: Same as described in Definition 2.2.

Practice: $\mathcal{A}$ can submit any message to $\mathcal{C}$ and obtains its ciphertext for any number of times (polynomial queries). When $\mathcal{A}$ attains a certain level of confidence, the next phase begins.

Challenge: Same as described in Definition 2.2 with the additional restriction that M_0 and M_1 should not be queried earlier in practice phase.

Guess: Same as described in Definition 2.2.

If $\mathcal{C}$ wins the game, then the scheme is IND-CCA secure.

Next, we recall the definitions of LWE and RLWE problems.

Definition 2.4: LWE problem [1]: Let q and N be positive integers, let s be a uniformly chosen vector in $\mathbb{Z}_q^N$ and let χ be a probability distribution (PD) on $\mathbb{Z}$. Let L_s^χ be a PD on $\mathbb{Z}_q^N \times \mathbb{Z}_q$ that return $(k, h = \langle k, s\rangle + \varepsilon) \in \mathbb{Z}_q^N \times \mathbb{Z}_q$, where $\varepsilon \in \mathbb{Z}$ is chosen in accordance with χ and $k \in \mathbb{Z}_q^N$ is chosen uniformly at random. Then LWE problem asks to determine s from the polynomial number of samples $(k,h) \in L_s^\chi$.

Definition 2.5: RLWE (ring learning with errors) problem [1]: Let $R_q = \mathbb{Z}_q[x] / (x^n + 1)$ for some positive integers q and n. Let s be a uniformly chosen vector in R_q and let χ be a probability distribution (PD) on $R = \mathbb{Z}[x] / (x^n + 1)$. Let $\tilde{L}_s^\chi$ be a PD on $R_q \times R_q$ that return $(k, h = \langle k, s\rangle + \varepsilon) \in R_q \times R_q$, where $\varepsilon \in \mathbb{Z}$ is chosen in accordance with χ and $k \in R_q$ is chosen uniformly at random. Then RLWE problem asks to determine s from the sample $(k,h) \in \tilde{L}_s^\chi$.

We end this section by defining the notion of norm of an element in a group ring.

Definition 2.6: Let $\mathrm{G}=\{g_1,g_2,\cdots,g_N\}$ be a finite group of order N and $\mathrm{R}=\mathbb{Z}_q$ be a finite ring. Then for any $u=\sum_{i=1}^{N} r_i g_i \in \mathrm{RG}$, we write

$$\| u \|_\infty = \max\{|r_i|, 1 \le i \le N\}.$$

3. GRLWE and an IND-CPA PKE and IND-CCA KEM based on GRLWE

In this section, we propose a novel group ring learning with errors (GRLWE) problem and discuss its security. Furthermore, we also propose a novel IND-CPA (indistinguishability under chosen plaintext attack) secure public key encryption (PKE) and a novel IND-CCA (indistinguishability under chosen ciphertext attack) secure key encapsulation mechanism (KEM).

3.1 *GRLWE problem and its security*

Let $\mathrm{G}=\{g_1,g_2,\cdots,g_N\}$ be a finite group of order N and $\mathrm{R}=\mathbb{Z}_q$ be a finite ring for $q=2^z$, where $z\ge 3$ is a positive integer. Let RG be the corresponding group ring. Let $|q|$ be the bit size of q. Let $\mathcal{H}:\{0,1\}^* \to \{0,1\}^{|q|\cdot N}$ be a secure hash function. This hash function can be easily constructed using the existing secure hash functions (e.g., SHA-3, SHAKE etc.) by simply concatenating their outputs. Let χ_{RG} be a probability distribution on $\mathrm{R'G}$, where $\mathrm{R'}=\mathbb{Z}_{q'}$ for $q'\le q$. This means that any element of $\mathrm{R'G}$ chosen via probability distribution χ_{RG} (e.g., Gaussian distribution or binomial distribution etc.) gives an element of RG with smaller coefficients that belong to the ring $\mathrm{R'}$. We describe the GRLWE problem as follows:

(a) **Sample** $_{\mathrm{RG}}(\rho)$: This algorithm takes input a random bit string ρ and outputs a uniformly chosen element of the group ring RG. Its work flow is as follows:

Input: $\rho \in \{0,1\}^*$ (bit strings of arbitrary lengths).

- Compute $\mathcal{H}_1=\mathcal{H}(\rho)$.
- Divide $\mathcal{H}_1$ into N equal parts each of length $|q|$. Let these parts be $r_s, 1\le s\le N$.

Output: $\sum_{s=1}^{N} r_s g_s$, where it is evident that $r_s \in \mathrm{R}=\mathbb{Z}_q$.

(b) **GRLWE-Sampling**: Let σ and ρ be two bit strings in $\{0,1\}^*$. Let $\tilde{L}_s^{\chi,\mathrm{RG}}$ be a probability distribution that return $(\alpha,\beta=\alpha\circledast s+e)\in$

$\mathrm{RG}\times\mathrm{RG}$, where $\alpha = \mathrm{Sample}_{\mathrm{RG}}(\sigma)$, $s = \mathrm{Sample}_{\mathrm{RG}}(\rho)$ and $e \in \mathrm{RG}$ is chosen uniformly through the distribution χ_{RG}.

(c) **GRLWE Problem**: Given a GRLWE-Sample $(\alpha, \beta = \alpha \circledast s + e) \in \mathrm{RG}\times\mathrm{RG}$, find s.

Before discussing the security of GRLWE problem, let us first discuss its relationship with RLWE problem.

3.1.1 Relationship of GRLWE problem with RLWE problem

By Definition 2.5, we know that RLWE problem asks to determine s from the sample $(k,h) \in \tilde{L}_s^{\chi}$. As $R_q = \mathbb{Z}_q[x] \,/\, (x^n+1)$, we may write

$$h = \langle k, s\rangle + e, \text{ where } k = \sum_{i=0}^{n-1} k_i x^i, h = \sum_{i=0}^{n-1} h_i x^i, s = \sum_{i=0}^{n-1} s_i x^i, e = \sum_{i=0}^{n-1} e_i x^i, k_i, h_i, s_i, e_i \in \mathbb{Z}_q.$$

Since $x^n = -1$ in the ring R_q, in terms of matrix representation, we can write

$$H = \begin{bmatrix} h_0 \\ h_1 \\ \vdots \\ h_{n-1} \end{bmatrix} = \begin{bmatrix} k_0 & -k_{n-1} & \cdots & -k_1 \\ k_1 & k_0 & \cdots & -k_2 \\ \vdots & \vdots & \vdots & \vdots \\ k_{n-1} & k_{n-2} & \cdots & k_0 \end{bmatrix} \times \begin{bmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{bmatrix} + \begin{bmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{bmatrix} = K \times S + E.$$

From the above matrix representation, it is known that for the matrix K, only first row is arbitrary and rest of the rows are depending on the first row elements.

In our case, since we are working in a group ring, the matrix involved can not be directly predicted as it depends on the particular choice of the group. We know that GRLWE problem asks to determine s from the sample $(\alpha, \beta = \alpha \circledast s + e) \in \mathrm{RG}\times\mathrm{RG}$. Using Definition 2.1, we may write

$$\beta = \alpha \circledast s + e, \text{ where } \alpha = \sum_{i=0}^{n-1} \alpha_i g_i, \beta = \sum_{i=0}^{n-1} \beta_i g_i, s = \sum_{i=0}^{n-1} s_i g_i, e = \sum_{i=0}^{n-1} e_i g_i, \alpha_i, \beta_i, s_i, e_i \in \mathrm{R}.$$

In terms of matrix representation, we can write

$$\tilde{\beta} = \begin{bmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{n-1} \end{bmatrix} = \begin{bmatrix} \alpha_{0,0} & \alpha_{0,1} & \cdots & \alpha_{0,n-1} \\ \alpha_{1,0} & \alpha_{1,1} & \cdots & \alpha_{1,n-1} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{n-10} & \alpha_{n-1,1} & \cdots & \alpha_{n-1,n-1} \end{bmatrix} \times \begin{bmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{bmatrix} + \begin{bmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{bmatrix} = \tilde{\alpha} \times \tilde{s} + \tilde{e},$$

where $\tilde{\alpha} = [\alpha_{i,j}]_{(n-1)\times(n-1)}$ is a matrix with entries in R but these entries depend on the multiplicative table of the group G. If G is a cyclic group,

then there exists an element $g \in \mathrm{G}$ of order n. This means $g^N = 1$ and one can obtain the matrix $\tilde{\alpha}$ similar to the matrix K computed above. This implies that the GRLWE problem is a generalization of RLWE problem. In the case of LWE problem, if we take m samples from the distribution L_s^χ (see Definition 2.4), then the corresponding matrix is totally random. But this has an obvious drawback as the size of the matrix (or public keys) becomes very large and cryptosystems based on such problems become Impractical [20].

3.1.2 Security of the GRLWE problem

If $e = 0$ and α is a unit of the group ring RG with known inverse, then $s = \alpha^{-1} \circledast \beta$ is the solution of GRLWE problem. Since, in general, the computation of inverse of an element of a group ring is itself a hard problem [18], so it is computationally infeasible to compute s even if e is known. Further, it is known that solving RLWE problem is atleast as hard as solving approximate shortest vector problem on arbitrary ideal lattices for certain parameters (see [12] for a comprehensive discussion). As GRLWE is a generalization of RLWE problem, so one can note that GRLWE problem is also atleast as hard as solving approximate shortest vector problem on arbitrary ideal lattices for certain parameters.

3.2 *IND-CPA PKE scheme based on GRLWE problem*

Let $\mathrm{G} = \{g_1, g_2, \cdots, g_N\}$ be a finite abelian group of order N and $\mathrm{R} = \mathbb{Z}_q$ be a finite ring for $q = 2^z$, where z is a positive integer. Let RG be the corresponding group ring. Let $\mathrm{M} = \{0,1\}^N$ be the message space. Let χ_{RG} be a probability distribution on $\mathrm{R'G}$, where $\mathrm{R'} = \mathbb{Z}_{q'}$ for $q' \le q$. The PKE is described through the following three algorithms:

Key Generation:

(i) Let $\rho, \sigma \in \{0,1\}^*$ be chosen randomly.

(ii) Let $\alpha = \mathrm{Sample}_{\mathrm{RG}}(\sigma)$ and $s = \mathrm{Sample}_{\mathrm{RG}}(\rho)$.

(iii) Let $e \in \mathrm{RG}$ be chosen uniformly through the distribution χ_{RG}.

(iv) Return $(\alpha, \beta = \alpha \circledast s + e) \in \mathrm{RG} \times \mathrm{RG}$ as the public key and s as the private key.

Encryption $(M \in \mathrm{M} = \{0,1\}^N)$:

(i) Represent M as $M = \sum_{i=1}^N m_i g_i$, where m_i is the i th bit of M.

(ii) Choose $e_1, e_2, e_3 \in \mathrm{RG} \times \mathrm{RG} \times \mathrm{RG}$ through the distribution $\chi_{\mathrm{RG}} \times \chi_{\mathrm{RG}} \times \chi_{\mathrm{RG}}$.

(iii) Compute $c_1 = \alpha \circledast e_1 + e_2 \in \mathrm{RG}$.

(iv) Compute $c_2 = \beta \circledast e_1 + e_3 + 2^{z-1} \cdot M \in \mathrm{RG}$.

(v) Ciphertext is $(c_1, c_2) \in \mathrm{RG} \times \mathrm{RG}$.

Decryption $((c_1, c_2) \in \mathrm{RG} \times \mathrm{RG})$:

(i) Compute $\tilde{m} = c_2 - s \circledast c_1$.

(ii) Rounding each coefficient $\tilde{m}_i$ of $\tilde{m}$ to nearest integer.

(iii) If $\tilde{m}_i < 2^{z-1}$ then $m_i = 0$, otherwise $m_i = 1$. Here m_i is the ith bit of M.

3.2.1 Correctness of the PKE scheme

Next, we discuss the correctness of our PKE.

Theorem 3.1: Let e_1, e_2, e_3 be such that

$$\delta := \| e \circledast e_1 + e_3 - s \circledast e_2 \|_\infty < 2^{z-2}.$$

The PKE described in subsection 3.2 is correct.

Proof: To decrypt $(c_1, c_2) \in \mathrm{RG} \times \mathrm{RG}$, decryptor needs to compute

$$\tilde{m} = c_2 - s \circledast c_1$$

$$= (\beta \circledast e_1 + e_3 + 2^{z-1} \cdot M) - s \circledast (\alpha \circledast e_1 + e_2)$$

$$= ((\alpha \circledast s + e) \circledast e_1 + e_3 + 2^{z-1} \cdot M) - s \circledast (\alpha \circledast e_1 + e_2)$$

$$= (e \circledast e_1 + e_3 - s \circledast e_2) + 2^{z-1} \cdot M.$$

Further, as $\delta < 2^{z-2}$, we note that the ith coefficient of $\tilde{m}$ is

$$\tilde{m}_i < 2^{z-2} + 2^{z-1} \cdot M.$$

If $\tilde{m}_i < 2^{z-1}$, then this means $m_i = 0$ and if $\tilde{m}_i \geq 2^{z-1}$, then $m_i = 1$. This shows that our scheme is mathematically correct.

3.2.2 IND-CPA security of the PKE scheme

In this subsection, we show that our novel PKE is IND-CPA secure provided GRLWE is a hard problem.

Theorem 3.2: *The novel PKE proposed in subsection* 3.2 *is IND-CPA secure provided GRLWE is a hard problem.*

Proof: For the scheme to be IND-CPA secure, a game needs to be played between the challenger $\mathcal{C}$ and the adversary $\mathcal{A}$ as discussed in Definition 2.2. $\mathcal{A}$ picks messages M_0, M_1 and submits them to $\mathcal{C}$. In response, $\mathcal{C}$ tosses a coin $c \in \{0,1\}$. Using c, $\mathcal{C}$ encrypts M_c and submits the ciphertext to $\mathcal{A}$. This means $\mathcal{A}$ gets the ciphertext

$$(c_1, c_2) = (\alpha \circledast e_1 + e_2, \beta \circledast e_1 + e_3 + 2^{z-1} \cdot M_c).$$

Suppose $\mathcal{A}$ wins the game by predicting that $c' = c$. As a result, $\mathcal{A}$ calculates

$$c_2 - 2^{z-1} \cdot M_c = s \circledast c_1 + c_3,$$

where $c_3 \in \mathrm{RG}$ and $\| c_3 \|_\infty < 2^{z-2}$. By rounding the coefficients of $c_2 - 2^{z-1} \cdot M_c$, $\mathcal{A}$ can also obtain the coefficients of s since that of c_1 are known. This means that $\mathcal{A}$ can solve GRLWE problem. So, our PKE scheme is IND-CPA secure if GRLWE problem is hard.

3.3 *IND-CCA KEM scheme based on GRLWE problem*

In this subsection, we propose the IND-CCA KEM (key encapsulation mechanism) using the IND-CPA PKE proposed in the Section 3.2 (we call it as GRLWE.PKE and its encryption and decryption algorithms as GRLWE.PKE.ENC and GRLWE.PKE.DEC, respectively). Let pk and sk denote the public and private keys of GRLWE.PKE. Let H be a 256 bit hash function. The KEM scheme involves applying KEM with the Fujisaki-Okamoto transform [4]. We use the same notations as used in the previous subsection unless stated otherwise. The KEM is described through the following three algorithms:

Key Generation: It is same as the key generation algorithm described in Section 3.2.

Encapsulation:

(i) Let $M \in \{0,1\}^{256}$ be chosen randomly.

(ii) Compute $\tilde{K} = H(pk), R = H(m)$.

(iii) Compute $C =$ GRLWE.PKE.Enc$(M; R)$ with pk as the public key.

(iv) Compute $K = H(H(C), \tilde{K})$.

(v) Ciphertext is C and key is K.

Decapsulation:

(i) $M' =$ GRLWE.PKE.Dec(C) with sk as the secret key

(ii) Compute $\tilde{K}' = H(pk)$ and $R' = H(M')$.

(iii) $C' =$ GRLWE.PKE.Enc$(M'; R')$ with pk as the public key.

(iv) If $C' = C$, then return $K = H(H(C), \tilde{K}')$. Otherwise return $\perp$.

3.3.1 Correctness of the KEM scheme

Next, we discuss the correctness of our KEM.

Theorem 3.3: *If the proposed GRLWE.PKE is mathematically correct, then the KEM described in subsection* 3.3 *is correct.*

Proof: The ciphertext is *C* and the key is *K*. After dercrypting *C* with the secret key *sk*, we get $M' =$ GRLWE.PKE.Dec(C). Since GRLWE.PKE is mathematically correct, $M' = M$. This means that $C' = C$ and both the parties get the same key *K*.

3.3.2 IND-CCA security of the KEM scheme

For the construction of our KEM scheme, we have utilized Fujisaki-Okamoto transform (with implicit rejection). Therefore, by using [5], it can be shown that our KEM is IND-CCA secure.

4. Example and Scheme Parameters

In this section, we discuss a toy example related to our scheme to show its practicality. Moreover, we also discuss the parameters to securely implement our scheme.

Example 4.1: Let $\mathrm{G} = C_6 = \langle G \rangle = \{g_i = g^i : 1 \le i \le 6\}$ (cyclic group of order 6 having generator g) and $\mathrm{R} = \mathbb{Z}_8 = \{0,1,2,\cdots,7\}$. Let $\mathrm{M} = \{0,1\}^6$ be the message space and $q' = 2$, which means $R' = \mathbb{Z}_q = \{0,1\}$. Also $z = 3$. We remark that all the following results are verified using the software GAP [14].

Key Generation: For two randomly chosen strings $\rho, \sigma \in \{0,1\}^*$, let

$$\alpha = g_1 + 7g_2 + 3g_3 + 6g_4 + 4g_5, \quad s = 2g_2 + 7g_6.$$

Let the error vector be

$$e = g_1 + g_2 + g_4 + g_5 \in \mathrm{R'G}.$$

Using these values, the public key is (α, β), where α is already computed and

$$\beta = \alpha \circledast s + e = 2g_2 + 7g_3 + g_4 + 3g_5 + 4g_6.$$

The private key is $s = 2g_2 + 7g_6$.

Encryption $(M = (101101) \in \{0,1\}^6)$:

We represent the message M as

$$M = g_1 + g_3 + g_4 + g_6.$$

Let the error vectors $e_1, e_2, e_3 \in \mathrm{RG} \times \mathrm{RG} \times \mathrm{RG}$ chosen through the distribution $\chi_{\mathrm{RG}} \times \chi_{\mathrm{RG}} \times \chi_{\mathrm{RG}}$ be

$$e_1 = g_1 + g_4,\ e_2 = g_1 + g_6,\ e_3 = g_1 + g_2 + g_3.$$

We compute $c_1 = \alpha \circledast e_1 + e_2$ and $c_2 = \beta \circledast e_1 + e_3 + 2^{z-1} \cdot M$ as

$$c_1 = (g_1 + 7g_2 + 3g_3 + 6g_4 + 4g_5) \circledast (g_1 + g_4) + (g_1 + g_6)$$

$$= 4g_1 + 7g_2 + 3g_3 + 3g_4 + 7g_5 + 4g_6,$$

$$c_2 = (2g_2 + 7g_3 + g_4 + 3g_5 + 4g_6) \circledast (g_1 + g_4) + (g_1 + g_2 + g_3) + 4 \circledast (g_1 + g_3 + g_4 + g_6)$$

$$= 2g_2 + 2g_3 + 7g_4 + g_5 + g_6.$$

The ciphertext is (c_1, c_2).

Decryption $((c_1, c_2) \in \mathrm{RG} \times \mathrm{RG})$:

We compute $\tilde{m} = c_2 - s \circledast c_1$ as follows

$$\tilde{m} = (2g_2 + 2g_3 + 7g_4 + g_5 + g_6) - (2g_2 + 7g_6) \circledast (4g_1 + 7g_2 + 3g_3 + 3g_4 + 7g_5 + 4g_6)$$

$$= 6g_1 + g_2 + 5g_3 + 4g_4 + 2g_5 + 7g_6.$$

Further, we have $\tilde{m}_i < 4$ for $i = 2,5$. This means the message is $M = (1,0,1,1,0,1)$. This matches with the original message. This shows that our scheme is practical.

4.2 *Secure Parameters*

The parameters involved are discussed as follows:

(1) The ring R can be taken as $\mathbb{Z}_{7681}$ as recommended in [3].

(2) The group G can be any abelian group of order 256.
(3) Hash function $\mathcal{H}$ can be taken as SHA-3-256 or SHA-3-512.
(4) q' can be taken as 5 or 7, which means $R' = \mathbb{Z}_5$ or $\mathbb{Z}_7$.

This completes the description of secure parameters involved in our scheme.

5. Discussion

We have proposed a novel group ring learning with errors (GRLWE) problem and discussed its hardness. Using this problem, we have constructed a IND-CPA public key encryption (PKE) scheme. Further, using the PKE scheme, we have constructed a IND-CCA key encapsulation mechanism (KEM). To show the practicality of our scheme, we have discussed an example. Finally, as an extension of this work, researchers can look for constructions of other cryptographic primitives based on GRLWE problem. Moreover, it is interesting to take G as any non-abelian group and then build the cryptographic primitives based on GRLWE problem.

References

[1] M. Albrecht, R. Player, and S. Scott, "On the concrete hardness of Learning with Errors," *J. Math. Cryptol.*, vol. 9, no. 3, pp. 169–203 (2015).

[2] D. Bernstein, J. Buchmann, and E. Dahmen, *Post-Quantum Cryptography*, Springer, Berlin Heidelberg (2009).

[3] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. Schanck, P. Schwabe, G. Seiler, and D. Stehle, "CRYSTALS - Kyber: a CCA-secure module-lattice-based KEM," in *European Symposium on Security and Privacy*, pp. 33–367, IEEE (2018).

[4] E. Fujisaki and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes," in *Crypto'99*, LNCS, vol. 1666, Springer-Verlag, Berlin, pp. 537–554 (1999).

[6] D. Hofheinz, K. Hövalmanns, and E. Kitlz, "A modular analysis of Fujisaki-Okamoto transform," in *TCC 2017*, pp. 341–371 (2017).

[6] B. Hurley and T. Hurley, "Group ring cryptography," *Int. J. Pure Appl. Math.*, vol. 69, no. 1, pp. 67–86 (2011).

[7] S. Kumar, G. Mittal, and S. Kumar, "Digital signature schemes based on group ring," *SN Comput. Sci.*, vol. 3, Article no. 398 (2022).

[9] S. Kumar, G. Mittal, and A. Yadav, "An efficient ID-based cryptographic encryption based on group ring," *J. Discret. Math. Sci. Cryptogr.*, vol. 27, no. 6, pp. 1851–1866 (2024).

[9] S. Kumar, G. Mittal, and A. Yadav, "A Group Ring-Based Provably Secure and Efficient Identity-Based Signature Scheme," in *Congress on Smart Computing Technologies, CSCT 2023*, Smart Innovation, Systems and Technologies, vol. 395, J.C. Bansal, H. Sharma, and A. Chakravorty, Eds., Springer, Singapore, pp. 1–15 (2024). doi: 10.1007/978-981-97-5081-8_1.

[10] O. Küsmüs and T. Hanoymak, "A novel public-key encryption scheme based on Bass cyclic units in integral group rings," *J. Discret. Math. Sci. Cryptogr.*, vol. 25, no. 2, pp. 579–589 (2023).

[11] V. Lyubashevsky, C. Peikert, and O. Regev, "A toolkit for R-LWE cryptography," in *EUROCRYPT*, pp. 35–43 (2013).

[12] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," *J. ACM*, vol. 60, no. 6, pp. 1–43 (2013).

[13] C. P. Milies and S. K. Sehgal, *An Introduction to Group Rings*, Springer, Dordrecht (2002).

[14] GAP: Groups, Algorithms, Programming, Ver 4.12.2 (2022). [Online]. Available: https://www.gap-system.org.

[15] G. Mittal, S. Kumar, S. Narain, and S. Kumar, "Group rings based public key cryptosystems," *J. Discret. Math. Sci. Cryptogr.*, vol. 25, no. 6, pp. 1683–1704 (2022).

[16] G. Mittal, S. Kumar, S. Kumar, and S. Narain, "McEliece and Blum-Goldwasser group rings based probabilistic cryptosystems," *J. Discret. Math. Sci. Cryptogr.*, Online first (2022).

[17] G. Mittal, S. Kumar, and S. Kumar, "Novel public-key cryptosystems based on NTRU and algebraic structure of group rings," *J. Info. Opti. Sci.*, vol. 42, no. 7, pp. 1507–1521 (2021).

[18] G. Mittal, S. Kumar, and S. Kumar, "A quantum secure ID-based cryptographic encryption based on group rings," *Sadhana*, vol. 47, Article no. 35, pp. 1–16 (2022).

[19] G. Mittal, S. Kumar, and S. Kumar, "An efficient procedure for online/offline ID-based signature using extended chaotic maps and group ring," *Security and Privacy*, vol. 6, no. 3, e279 (2023).

[20] J. Zhang and Z. Zhang, Lattice-Based Cryptosystems: A Design Perspective, Springer Nature Singapore (2020).

Received December, 2023