Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 7, pp. 2863–2872
DOI : 10.47974/JDMSC-2614

Efficient group ring based post-quantum Niederreiter public key encryption and key encapsulation mechanism

Sandeep Kumar [†]
Gaurav Mittal *
Sunil Sangwan [§]
Defence Research & Development Organisation
Near Metcalfe House
New Delhi 110054
Delhi
India

Abstract

In this work, we present the IND-CPA secure (quantum) dual version of group ring based McEliece public key encryption (PKE) proposed in Mittal et al. (JDMSC, 2023). We show that in comparison to the classical PKE, the dual version is much more efficient. Further, we also present IND-CCA2 secure key encapsulation mechanism and IND-CCA2 secure PKE and show that both of these are quantum secure. Furthermore, we discuss the associated parameters with all the three schemes and also discuss a toy example to showcase their practicality.

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

Keywords: *Code based cryptography, Public key encryption, Key encapsulation mechanism, Group ring, Units.*

1. Introduction

In the last decade, group ring based cryptography has received paramount attention due to being post-quantum and efficient (see [4, 7, 8, 10, 12, 13, 14, 15]). In particular, the discrete logarithm problem in group ring (DLPGR), which is an extension of DLP in groups, is a quantum safe hard problem with small parameter sizes [13]. We refer to [11, 5, 13] for a comprehensive literature on group ring along with few initial works in the direction of group ring cryptography. Further, we also refer to [12, 6, 8, 9] for some of the most recent works that employed group ring to build new quantum secure crypto primitives.

[†] *E-mail:* san.kuwar@gmail.com
[*] *E-mail:* gaurav.mittaltwins@gmail.com (Corresponding Author)
[§] *E-mail:* sunilsangwan6174@gmail.com

© Taru Publications

Recently, Mittal, Kumar, and Kumar [16] proposed group ring analogue of McEliece public key encryption (PKE). Specifically, this PKE employs the generator matrix of Goppa codes [2] and units in group ring to encrypt the data. The main advantage of this PKE over conventional McEliece PKE is that it works with considerably small parameters, which leads to the efficiency and small bandwidth requirement. However, by incorporating the idea of Niederreiter [2], one may further reduce the efficiency of this PKE by employing the dual matrix associated with Goppa codes instead of its generator matrix. Consequently, in this paper, we propose the efficient dual version of McEliece group ring based PKE and show it is IND-CPA secure.

Next, it is well known that one can also construct a secure key encapsulation mechanism (KEM) (i.e., IND-CCA2 secure) from IND-CPA PKE using the Fujisaki-Okamoto (F-O) transform [3]. Additionally, one can also convert IND-CCA2 KEM to IND-CCA2 PKE using a secure symmetric encryption scheme. Using these ideas, we also construct IND-CCA2 KEM and IND-CCA2 PKE from above-mentioned IND-CPA KEM. We emphasize that all the three schemes discussed in this paper are quantum secure or post-quantum.

Organization: We discuss a few preliminaries in Section 2. Section 3 is devoted to construction of PKEs and KEM. The corresponding securities of these schemes are also discussed in this section. Section 4 is devoted to a toy example and last section involves some concluding remarks.

2. Preliminaries

We discuss basic terminologies related to group ring and security models in this section.

Definition 2.1: PKE and KEM: A PKE is an encryption scheme in which public key encrypts the messages and private key decrypts them. A KEM is one in which public key is used to obtain a key and the corresponding ciphertext. The ciphertext is decrypted using private key, which yields the key. Thus, both parties get the same key, which can be used for symmetric encryption.

Definition 2.2: Group Ring [11]: Let $\mathfrak{R}$ be a ring and $\mathbf{G}$ be a group, both finite. We define $\mathfrak{R}\mathbf{G}$ as the set

$$\mathfrak{R}\mathbf{G} = \{(l_1 g_1 + \cdots + l_m g_m) : l_i \in \mathfrak{R}, g_i \in \mathbf{G}\}, |\mathbf{G}| = m.$$

Under canonical addition $+$ and multiplication $*$, respectively, $\mathfrak{R}\mathbf{G}$ is a group and also a ring. We denote its identity by 1.

Definition 2.3: Unit: Let $\kappa_1 \in \mathfrak{R}\mathbf{G}$. Then κ_1 is said to be a unit if there exists $\kappa_2 \in \mathfrak{R}\mathbf{G}$ such that $\kappa_1 * \kappa_2 = \kappa_2 * \kappa_1 = 1$.

Definition 2.4: DLPGR [13]: Given $\kappa_1, \kappa_2 \in \mathfrak{R}\mathbf{G}$ such that $\kappa_1 = \kappa_2^{\zeta}$ for $\zeta \in \mathbb{Z}^+$. Find ζ.

The most efficient algorithm to solve DLPGR is a collision algorithm discussed in [13], which is sub-exponential in nature. Consequently, DLPGR is a hard task even for quantum computers. Next, we discuss the IND-CPA (indistinguishability under chosen plaintext attack) and IND-CCA2 (indistinguishability under adaptive chosen ciphertext attack) security models (see [1]).

Definition 2.5: IND-CPA secure [1]: Let $\mathbf{A}$ be an adversary and $\mathbf{C}$ be a challenger. Let M_i be two messages picked by $\mathbf{A}$ for $i = 1,2$. $\mathbf{A}$ submits these to $\mathbf{C}$, which in response, picks $b \in \{0,1\}$ and encrypts M_b and submits it back to $\mathbf{A}$. $\mathbf{A}$ responds with $b' \in \{0,1\}$. If $b \neq b'$, PKE is IND-CPA secure .

Definition 2.6: IND-CCA 2 secure [1]: Let $\mathbf{A}$ be an adversary and $\mathbf{C}$ be a challenger. $\mathbf{A}$ adaptively picks any ciphertext of his choice and gets the corresponding plaintext from $\mathbf{C}$. After querying polynomially many ciphertexts, let M_i be two messages picked by $\mathbf{A}$ for $i = 1,2$. $\mathbf{A}$ submits these to $\mathbf{C}$, which in response, picks $b \in \{0,1\}$ and encrypts M_b and submits it back to $\mathbf{A}$. Again, $\mathbf{A}$ adaptively picks any ciphertext of his choice and get the corresponding plaintext from $\mathbf{C}$ (he cannot submit the challenged one). After polynomially many queries, $\mathbf{A}$ responds with $b' \in \{0,1\}$. If $b \neq b'$, PKE is IND-CCA 2 secure.

We note that IND-CCA2 is highest security (or golden standard) as if any PKE is IND-CCA2 secure, then it is also non-malleable as well as secure against adaptive chosen ciphertext attack (CCA2 secure).

3. IND-CPA and IND-CCA2 Group Ring based PKE and KEM

In this section, we propose group ring based IND-CPA secure PKE based on Niederreiter dual version of McEleice PKE. Furthermore, we also discuss its security and the associated parameters. We also see how to convert our IND-CPA secure PKE to IND-CCA2 secure KEM and PKE.

3.1 *IND-CPA PKE*

The PKE is described in the following three algorithms.

3.1.1 Parameters and Key Generation

Let $\mathbf{G} = \{g_j : 1 \leq j \leq |\mathbf{G}|, g_1 = e\}$ be a finite group. Let $\Re\mathbf{G}$ be a finite group ring and let κ be its unit of large order. Let $\mathcal{G}$ be a (m, l, t)-linear Goppa code. Let $\mathcal{H}$ be its parity check matrix. Its dimension is $(m - l) \times m$. Let N be a non-singular matrix of order $m - l$ and let P be a permutation matrix of order m. Both of these are random. The public key is $(\mathrm{H}' = \mathrm{N}\mathcal{H}\mathrm{P}, \kappa^{\ell}, \kappa^{-1})$ for some secret $\ell \in \mathbb{Z}^{+}$. The private key is $(\mathrm{N}, \mathcal{H}, \mathrm{P}, \ell)$. Note that κ^{-1} is a part of public key as inverse computation is not an easy task in group ring. Let $\Phi: \{0,1\}^{m-l} \rightarrow \Re\mathbf{G}$ be a canonical mapping defined as

$$(c_1, c_2, \cdots, c_{m-l}) \mapsto c_1 g_1 + c_2 g_2 + \cdots + c_{m-l} g_{m-l}$$

where $|\mathbf{G}| \geq m - l$ (otherwise it can be broken into chunks) Note that Φ is a bijection from $\{0,1\}^{m-l}$ to the image of Φ.

3.1.2 Encryption

Let plaintext be a vector $\mathrm{M} \in \{0,1\}^m$ of length m and weight $\leq t$ (done via a suitable encoding). Further, compute $\tilde{C} = \mathrm{H}'\mathrm{M} \in \{0,1\}^{m-l}$ and subsequently deduce $\Phi(\tilde{C}) \in \mathfrak{R}\mathbf{G}$. The ciphertext is (C_1, C_2) for

$$C_1 = (\kappa^{-1})^n, C_2 = \Phi(\tilde{C}) * (\kappa^{\ell})^n,$$

where $n \in \mathbb{Z}^+$ is randomly chosen (also known as nonce or ephemeral key).

3.1.3 Decryption

After receiving ciphertext, first compute $C_2 * C_1^{\ell}$ using private key. Further, compute $\widetilde{\Phi} = \Phi^{-1}(C_2 * C_1^{\ell})$ and subsequently compute $\mathrm{N}^{-1}\widetilde{\Phi}$. For code $\mathcal{G}$, apply a syndrome decoding and multiply the result by P^{-1} to obtain the plaintext.

Correctness. In the following result, we discuss the correctness of our PKE.

Theorem 3.1: *The group ring based PKE defined above is Mathematically correct.*

Proof: For decryption, first we need to compute $C_2 * C_1^{\ell}$, which yields

$$C_2 * C_1^{\ell} = \Phi(\tilde{C}) * (\kappa^{\ell})^n * ((\kappa^{-1})^n)^{\ell} = \Phi(\tilde{C}).$$

By computing $\Phi^{-1}(C_2 * C_1^{\ell})$, we get $\tilde{C}$. Further, multiplying this with N^{-1} to get

$$\mathrm{N}^{-1}(\mathrm{H}'\mathrm{M}) = \mathcal{H}\mathrm{PM}.$$

By applying syndrome decoding, we further obtain PM. Finally, we multiply the last quantity by P^{-1} to get M. Thus, result.

3.2 *Security of our PKE*

In this subsection, we discuss the security of our PKE, i.e., we show it is IND-CPA secure. First we show that n should be used to encrypt only one message. Otherwise, there is a catch. Second, we discuss the IND-CPA security of our PKE.

Theorem 3.2: *In our PKE, if same n is used to encrypt more than one messages, then our scheme succumbs to chosen-plaintext attack.*

Proof: Suppose n is used to encrypt two messages $\mathrm{M}_1, \mathrm{M}_2$. The corresponding ciphertexts are

$$C_1 = (\kappa^{-1})^n, C_2 = \Phi(\tilde{C_1}) * (\kappa^{\ell})^n, C_{1,} = (\kappa^{-1})^n, C_{2,} = \Phi(\tilde{C_2}) * (\kappa^{\ell})^n.$$

This means that

$$\frac{C_{2\prime}}{C_2} = \frac{\Phi(\tilde{C_2})}{\Phi(\tilde{C_1})}\frac{\Phi^{-1}(C_{2\prime})}{\Phi^{-1}(C_2)} = \frac{\tilde{C_2}}{\tilde{C_1}} = \frac{\mathrm{H}\prime\mathrm{M}_2}{\mathrm{H}\prime\mathrm{M}_1}.$$

Clearly, if $(\mathrm{M}_1, C_1,)$ is known, then above equality implies that one may obtain M_2. Thus, n should be used only once.

Theorem 3.3: *Our PKE is IND-CPA secure as per Definition if DLPGR is a hard problem.*

Proof: As per Definition 2.5, **A** picks messages M_i for $i = 0,1$. **C** randomly picks $b \in \{0,1\}$ and sends

$$C_1 = (\kappa^{-1})^n, C_2 = \Phi(\mathrm{H}'\mathrm{M}_b) * (\kappa^{\ell})^n.$$

In response, **C** comes out with $b' \in \{0,1\}$ and **C** wins if

$$(\kappa^{-1})^n = (\kappa^{-1})^{n'} \text{ and } \Phi(\mathrm{H}'\mathrm{M}_b) * (\kappa^{\ell})^n = \Phi(\mathrm{H}'\mathrm{M}_{b'}) * (\kappa^{\ell})^{n'}.$$

This is only possible if $n = n'$, which is a computationally infeasible task as DLPGR is a hard problem. Also, in terms of probability, if order$(\kappa) = \lambda$, where λ is a large positive integer, then probability that $n = n'$ is $\frac{1}{\lambda}$. This is negligible. Hence, our scheme is IND-CPA secure.

We know that DLPGR is a quantum-safe hard problem. Thus, our PKE is IND-CPA secure in quantum sense.

3.3 *IND-CCA2 KEM*

In this subsection, we show that our IND-CPA secure PKE can be easily converted to a IND-CCA2 KEM (key encapsulation mechanism) using the F-O transform (slightly tweaked) provided by Fujisaki and Okamoto [3] as follows. The main purpose of KEM is to produce a key and the corresponding ciphertext.

Let G and H be two hash functions from $\{0,1\}^*$ (arbitrary length bit strings) with outputs $512,256$ bits, respectively. Let pk, sk denote the pubic and private keys, respectively.

3.3.1 Key Generation

Same as that of IND-CPA PKE. Additionally, let **S** be a 256 bit secret binary vector, which is a part of sk.

3.3.2 Encapsulation

Pick $\mathrm{M} \in \{0,1\}^{256}$ randomly. Let $(\hat{\mathrm{S}}, \mathrm{R}) = G(H(\mathrm{pk})||\mathrm{M})$. Deduce $C = (C_1, C_2) =$ Encrypt(M||R) using public key pk of IND-CPA PKE. Further, compute

$$\mathcal{S} = H(H(C)||\hat{\mathrm{S}}).$$

The symmetric key is $\mathcal{S}$ and encapsulated key (or ciphertext) is C. The ciphertext is send to other end.

3.3.3 Decapsulation

After getting C, apply decryption using IND-CPA PKE to get M'. Let $(\hat{\mathrm{S}}', \mathrm{R}') = G(H(\mathrm{pk})||\mathrm{M}')$. Deduce $C' = (C'_1, C'_2) =$ Encrypt($\mathrm{M}'||\mathrm{R}'$) using public key pk of IND-CPA PKE. If $C = C'$, then

$$\mathcal{S} = H(H(C)||\hat{\mathrm{S}}).$$

Otherwise output

$$H(H(C)||\mathbf{S}).$$

3.3.4 Security of our KEM

Fujisaki and Okamoto [3] shown that any IND-CPA Psecure KE can be converted into an IND-CCA2 secure KEM by using F-O transform. Therefore, our KEM is IND-CCA2 secure as per Definition 2.6, provided G and H are strong cryptographic hash functions. This KEM achieves the highest possible security.

3.3.5 Features of our KEM

- KEM provides a shared key of 256 bits. It can be easily changed by using a new hash function that provides outputs of different sizes.
- Note that our KEM never returns *failure*. Instead it outputs $\mathcal{S}$, which is the result of hashing of a secret vector $\mathbf{S}$ that is a part of the private key along with the ciphertext. This protects against *failure boosting attacks*.
- It does not need padding in contrary to PKE scheme.
- It is quantum secure as G and H are strong cryptographic hash functions and PKE is IND-CPA secure.

3.4 *IND-CCA2 PKE*

Finally, we propose the last scheme of our work, which is IND-CCA2 secure PKE. We obtain this by incorporating IND-CCA2 KEM along with CCA2 symmetric encryption scheme (SES), e.g., AES-256. This is defined in the following algorithms.

3.4.1 Key Generation

Same as that of KEM.

3.4.2 Encryption

Let $\mathrm{M} \in \{0,1\}^*$ be the message to be signed. We run IND-CCA2 KEM to generate $(\mathcal{S}, C)$, where $\mathcal{S}$ is 256-bit key and C is the ciphertext. Further, we encrypt message M using key $\mathcal{S}$ via CCA2 SES (i.e., AES-256). The corresponding ciphertext is C'. The overall ciphertext is (C, C').

3.4.3 Decryption

First, decapsulate C via IND-CCA2 KEM to get $\mathcal{S}$. Use this $\mathcal{S}$ to decrypt C' using CCA2 SES. This provides M.

3.4.4 Security

It is well-known that combining IND-CCA2 KEM with a CCA2 SES yields IND-CCA2 PKE. Thus, our PKE is IND-CCA2. It is also quantum secure as both

KEM and SES are.

4. Parameters for our schemes and Comparison Analysis

4.1 *Recommended Parameters*

From [13], we know that $|\mathbf{G}|$ should be atleast 512 to attain 128 bits of security via DLPGR. Further, we may take $\mathfrak{R} = GF(2)$ (Galois field of order 2). For Goppa codes, current recommendations are $m = 6960, l = 5413, t = 119$. This gives $m - l = 1547$. So, we may take any group of order 520. Accordingly, to encrypt m bits, we utilize IND-CCA2 PKE, which is the most secure. This uses IND-CCA2 KEM as well as SES. The ciphertext size of SES is m bits (if its block size divides m). The size of the ciphertext (or encapsulated key) provided by IND-CCA2 KEM is as follows. We note that the total length of the message that can be encrypted in one go has length $m = 6960$. We need to encrypt 512 bits via our IND-CCA2 KEM (which further uses IND-CPA PKE) (256 bits randomly picked and 256 bits pseudorandom vector, which is output of hash function), which means that size of $\mathbf{G}$ should be atleast 1547. Consequently, size of ciphertext of IND-CPA PKE becomes 3094 bits. Thus, total ciphertext size becomes $m + 3094$ bits. We take $m = 256$, which means the size is 3360. This is very small in comparison to Classic-McEliece ciphertext size, which is in several hundred bytes.

4.2 *Comparison with scheme of [16]*

A group ring based PKE was designed in [16] that depends on McEliece PKE. For encryption, one can see that IND-CCA2 secure PKE scheme of this paper is very fast in comparison to [16]. This is because of usage of KEM (or AES for bulk encryption) as well as syndrome computation, both of which are lightweight. Especially, matrix multiplication in McEliece is slower than syndrome computation. Thus, in terms of computational complexity of encryption algorithm, our IND-CCA2 PKE is much faster than that of [16]. The complexity of decryption is almost same.

5. Toy example

We consider $\mathfrak{R} = GF(2)$ and $\mathbf{G} = D_{10}$ (dihedral group having 10 elements). We may represent D_{10} as

$$D_{10} = \{e, f \mid e^5 = f^2 = 1, fef = e^4\}.$$

We consider the Goppa code $(6,3,2)$ and its parity check matrix as

$$\mathcal{H} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

We consider matrices N and P as

$$\mathrm{N} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \mathrm{P} = \begin{bmatrix} 0_4 & 1 & 0 \\ I_4 & 0 & 0 \\ 0_4 & 0 & 1 \end{bmatrix}_{6\times 6}, \text{where } 0_4 = [0 \quad 0 \quad 0 \quad 0].$$

Here I_4 is a 4×4 identity matrix. This means that

$$\mathrm{H}' = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Let $\kappa = f + e^2 + e^4$ with

$$\kappa^{-1} = 1 + e + fe + e^3 + e^4 + fe^4 + f.$$

The public key is $(\mathrm{H}' = \mathrm{N}\mathcal{H}\mathrm{P}, \kappa^7, \kappa^{-1})$ for $\ell = 7$, where

$$\kappa^7 = 1 + f + e + e^2 + fe^2 + e^3 + fe^3.$$

The private key is $(\mathrm{N}, \mathcal{H}, \mathrm{P}, \ell)$.

Let the message to be encrypted be

$$\mathrm{M} = [1,0,0,0,1,0]^t.$$

Clearly, its weight is 2. We note that

$$\tilde{C} = \mathrm{H}'\mathrm{M} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Further, we may see that the mapping Φ is such that

$$\Phi(c_1, c_2, \cdots, c_{10}) = c_1 + c_2 f + c_3 f^2 + c_4 f^3 + c_5 f^4 + c_6 e + c_7 fe + c_8 fe^2 + c_9 fe^3 + c_{10} fe^4.$$

The above mapping implies that $\Phi(\tilde{C}) = c_1 = 1$.

Encryption: We pick $n = 4$ and accordingly, we get

$C_1 = (\kappa^{-1})^4 = fe^2 + f^3 + fe^3, C_2 = \Phi(\tilde{C}) * (\kappa^7)^4 = f + fe + fe^4.$

Thus, the ciphertext is (C_1, C_2).

Decryption: First, we obtain $C_2 * C_1^{\ell} = C_2 * C_1^7$ and subsequently

$$\widetilde{\Phi} = \Phi^{-1}(C_2 * C_1^7) = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Next, we derive $\mathrm{N}^{-1}\widetilde{\Phi}$. Finally, for code $\mathcal{G}$, we apply a syndrome decoding and multiply the result by P^{-1} to obtain the plaintext.

6. Discussion

We have put forward three post-quantum schemes in this paper. First one is IND-CPA PKE based on group ring and Niederreiter PKE. Further, using this PKE, we have proposed an IND-CCA2 KEM. Finally, using this KEM and CCA2 SES, we have proposed a IND-CCA2 PKE. We have discussed the security of these schemes and shown their advantages in comparison to the McEliece version of group ring based PKE. We have also discussed a toy example along with the parameters sizes to showcase the validity of our IND-CPA PKE scheme. This also implies the validity of our IND-CCA2 PKE and IND-CCA2 KEM schemes.

References

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

[2] D. Engelbert, R. Overbeck, and A. Schmidt, "A summary of McEliece-type cryptosystems and their security," *J. Math. Cryptol.*, vol. 1, no. 2, pp. 151–199 (2007).

[3] E. Fujisaki and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes," in Advances in Cryptology – CRYPTO'99, pp. 537–554 (1999).

[4] N. Goel, I. Gupta, and M. Dubey, "Undeniable signature scheme based over group ring," *Appl. Algebra Eng. Commun. Comput.*, vol. 27, pp. 523–535 (2016).

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

[6] S. Kumar, G. Mittal, and A. Yadav, "A novel and provably secure identity-based blind signature scheme for online transactions," *Sādhanā*, vol. 50, no. 2, pp. 1–12 (2025).

[7] S. Kumar, G. Mittal, and S. Kumar, "Digital signature schemes based on group ring," *SN Comput. Sci.*, vol. 3, article 398 (2022).

[8] S. Kumar, G. Mittal, and A. Yadav, "An efficient ID-based cryptographic encryption based on group ring," *J. Discrete 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. Singapore: Springer Nature, pp. 1–15 (2023).

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

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

[12] G. Mittal, S. Kumar, S. Kumar, and S. Mittal, "A novel and efficient undeniable signature scheme based on group ring," *Soft Comput.*, vol. 28, no. 23, pp. 13053–13070 (2024).

[13] G. Mittal, S. Kumar, and S. Kumar, "A quantum secure ID-based cryptographic encryption based on group rings," *Sādhanā*, vol. 47, article 35, pp. 1–16 (2022).

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

[15] 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).

[16] G. Mittal, S. Kumar, and S. Kumar, "McEliece and Blum–Goldwasser group rings based probabilistic cryptosystems," *J. Discrete Math. Sci. Cryptogr.,* vol. 26, no. 8, pp. 2229–2242 (2023).

Received June, 2025