

McEliece and Blum-Goldwasser group rings based probabilistic cryptosystems

Gaurav Mittal *

Defense Research and Development Organisation

Near Metcalfe House

Civil Lines

New Delhi 110054

India

and

Department of Mathematics

Indian Institute of Technology Roorkee

Roorkee

India

Sandeep Kumar [†]

Sunil Kumar [§]

Defense Research and Development Organisation

Near Metcalfe House

Civil Lines

New Delhi 110054

India

Shiv Narain [‡]

Department of Mathematics

Arya P. G. College

Panipat

Haryana

India

* E-mail: gmittal@ma.iitr.ac.in (Corresponding Author)

[†] E-mail: sandeepkumar.hqr@gov.in

[§] E-mail: sunilkumar.hqr@gov.in

[‡] E-mail: math.shiv@gmail.com

Abstract

In this paper, we present two probabilistic public key cryptosystems (PKCs) based on the well known algebraic structure of group rings. The first cryptosystem is based on McEliece cryptosystem and we coin it as McEliece-group-ring based PKC. The second PKC is the extension of Blum-Goldwasser PKC in group rings and we name it as Blum-Goldwasser-group-ring based PKC. We carefully discuss the security analysis of the proposed PKCs and their advantages over the existing PKCs. Additionally, we consider the toy examples for both the cryptosystems in order to show the practicality of both the PKCs.

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

Keywords: Group ring, Units, Cryptography, Public key cryptography.

1. Introduction

In the last decade, the subject of group rings (cf. [13] for an excellent survey on group rings) has received a great attention in cryptography. One of the most influential article in this direction was written by Hurley et al. [8]. This paper along with [9] discussed various advantages of the algebraic structure of group rings that can be used in cryptography. Consequently, many PKCs have been constructed over the years based on group rings. To mention a few, Hanoyamak et al. [6] proposed a PKC based on RSA and group rings. A new ElGamal-like cryptosystem based on matrices over group rings is presented in [10]. Küsmüs et al. [11] proposed a novel PKC by considering Bass cyclic units in integral group rings. Very recently, Mittal et al. [14, 15] constructed secure PKCs based on group rings. Apart from this, various researchers have constructed many authentication protocols based on group rings [18, 5]. All in all, the subject of group rings is source of many hard problems (e.g. DLP in group rings, Inverse computation problem (ICP) [14]) that belong to the complexity class NP.

In this paper, our main motive is to present two novel group rings based PKCs. We first describe the motivation behind the introduction of these PKCs. McEliece PKC (cf. [12]) is a well known PKC based on the NP-hard problem of *decoding a general linear code*. This PKC was proposed way back in 1978 and received little attention at that time due to large public key size. Moreover, other secure PKCs such as RSA, ElGamal etc., were available at that time with considerably smaller key sizes. It is believed that with the advent of a sufficiently large quantum computer, the PKCs based on hardness of integer factorization problem (e.g. RSA, Blum-Goldwasser etc.) and discrete logarithm problem in abelian groups (e.g. ElGamal) will no longer be secure [1]. Consequently, PKCs based on other hard problems

such as decoding of a general linear code, *shortest and closest vector problems in lattices* etc., have received ample attention of the researchers. This is not because they have been proved safe against any attack on a quantum computer, but due to the fact that there is no known practical attack on these problems on a quantum computer, as well as these problems have been well studied by the mathematical community. Therefore, the current research in this direction is mainly focused on the following two aspects: (i) how to improve the security of existing PKCs with small parameters. (ii) how to construct secure (preferably quantum) PKCs based on new hard problems.

In this paper, we focus on the both the above-mentioned aspects. We construct a McEliece-group-ring based PKC based on McEliece PKC and group rings. We show that the security of this PKC depends on a NP-hard problem and Inverse computation problem (ICP) that is a NP-problem. Further, we construct another group rings based PKC that is the extension of Blum-Goldwasser PKC [12]. The security of Blum-Goldwasser PKC depends on integer factorization problem which is insecure in the presence of a sufficiently large quantum computer. Therefore, we propose a secure version of Blum-Goldwasser PKC by extending it to group rings. We show that its security depends on the *discrete logarithm problem in group rings* (DLPGR) that is a considerably hard problem than DLP in groups. Rest of the paper is structured as follows. The Section 2 comprises discussion on McEliece-group-ring based PKC and its security. The extension of Blum-Goldwasser PKC in group rings is proposed in Section 3 along with its security. The Section 4 is related to discussion on toy examples for both the proposed schemes and the last section concludes the paper.

2. McEliece-group-ring based PKC

In the present section, we propose a McEliece-group-ring based PKC based on the McEliece PKC and group rings. The McEliece PKC uses *Goppa codes* since for these codes a well known decoding algorithm *Patterson algorithm* exists (cf. [3] for a comprehensive survey of McEliece based PKCs and their security). Further, we quickly recall the definition of group rings. If K is a ring with unity and G is a group, then the set $KG = \{\sum_{j=1}^t k_j g_j : k_j \in K, g_j \in G\}$ of all finite sums is known as group ring. For $u_1, u_2 \in KG$, let $u_1 * u_2$ denote the product of u_1 and u_2 . To this end, let us now define our novel group rings based scheme by first defining the various parameters required in the scheme. Let the party B encrypts the message for party A that possess private key.

2.1 Parameters Creation

In order to create the public and private keys and perform the encryption and decryption procedure, the following parameters, matrices and algebraic structures are required. We fix the integers n_1 , n_2 and n_3 . Let G be a generator matrix of order $n_1 \times n_2$ for a binary (n_2, n_1) -linear code for which there exists an efficient decoding algorithm (e.g. Goppa code). The additional requirement is that this code should correct up to n_3 errors. Let S and P be two matrices with respective orders $n_1 \times n_1$ and $n_2 \times n_2$ such that S has binary entries with determinant $\neq 0$ and P be a permutation matrix. Further, let $G = \{g_i : i \in I\}$ be a group for index set $I = \{1, 2, \dots, z\}$ with $z \geq n_2$ and K be a ring or a field. Let u be a unit of group ring KG (i.e. u has inverse with respect to operation $*$ in KG) whose inverse u^{-1} is known. Further, choose a secret positive integer n_4 to obtain $v = u^{n_4}$. Finally, let φ be a map that maps $(\mathbb{Z}_2)^{n_2}$ to an element of KG as $\varphi(c_1, c_2, \dots, c_{n_2}) = \sum_{j=1}^{n_2} c_j g_j$. And φ^{-1} be the inverse of φ defined on the range of φ . Thus, the public parameters are $K, G, n_1, n_2, n_3, \varphi$.

2.2 Public and Private keys creation

The public key is obtained as follows: Multiply the matrices S , G and P to obtain $\mathcal{G}_1 = SGP$ having order $n_1 \times n_2$. This along with n_3 and v is the public key of our PKC, i.e. public key $= (\mathcal{G}_1, n_3, v)$. The corresponding private key is (S, G, P, v^{-1}) .

2.3 Encryption process

The encryption process is discussed as follows:

- (a) B verifies the authenticity of public key of A .
- (b) The binary message m is written as a row vector of length n_1 .
- (c) B chooses a binary vector ε of order $1 \times n_2$ with weight at most n_3 .
- (d) B computes $c' = m\mathcal{G}_1 + \varepsilon = (c_1, c_2, \dots, c_{n_2})$ and apply φ on c' .
- (e) The ciphertext is $c = \varphi(c') * v$.

2.4 Decryption process

The decryption process is discussed as follows:

- (a) A computes $m' = c * v^{-1}$ using a part of private key and check whether the coefficients of m' are in $(\mathbb{Z}_2)^{n_2}$. If not, A reject the

ciphertext c , since it does not belong to ciphertext space of the scheme.

- (b) Otherwise, A applies φ^{-1} on m' and obtain a vector of length n_2 (if the vector has length less than n_2 , then fill the remaining entries with 0) and multiply the result by $\mathcal{P}^{-1}$ to obtain $m'' = \varphi^{-1}(m')\mathcal{P}^{-1}$.
- (c) A uses the decoding algorithm for code with generator matrix $\mathcal{G}$ to decode m'' to $\hat{m}$.
- (d) The plaintext m equals to $\hat{m}\mathcal{S}^{-1}$.

Proof that decryption works: First we mention that what happen in coefficients of m' are not in $(\mathbb{Z}_2)^{n_2}$. If any of the coefficients of m' is different from $\{0, 1\}$, then $m' \notin \text{Range}(\varphi)$. Therefore, $\varphi^{-1}(m')$ is not defined. Consequently, A can identify that c is not a valid ciphertext. Next, if $m' \in \text{Range}(\varphi)$, then $m'' = \varphi^{-1}(m')\mathcal{P}^{-1} = \varphi^{-1}(c * v^{-1})\mathcal{P}^{-1} = \varphi^{-1}((\varphi(c') * v) * v^{-1})\mathcal{P}^{-1} = \varphi^{-1}(\varphi(c'))\mathcal{P}^{-1} = c'\mathcal{P}^{-1} = (m\mathcal{G}_1 + \mathcal{E})\mathcal{P}^{-1} = (m\mathcal{S}\mathcal{G}\mathcal{P} + \mathcal{E})\mathcal{P}^{-1} = (m\mathcal{S})\mathcal{G} + \mathcal{E}\mathcal{P}^{-1}$. Since $\mathcal{P}^{-1}$ is also a permutation matrix, the vector $\mathcal{E}\mathcal{P}^{-1}$ again has weight at most n_3 . Thus, using decoding algorithm on m'' , A can obtain $\hat{m} = m\mathcal{S}$. Finally, $m = \hat{m}\mathcal{S}^{-1}$.

2.5 Security of the scheme

The security of McEliece-group-ring based PKC is discussed in the following points:

- (1) The scheme is probabilistic in nature as corresponding a single m , there can be many different ciphertexts (since $\mathcal{E}$ is randomly chosen for each message).
- (2) The scheme provides an inherent check that can detect improperly constructed ciphertexts. This is an additional check in our scheme which was not there in the original McEliece PKC.
- (3) Hard problems: The task in front of an adversary is either to obtain the private key from the public key or to obtain the plaintext from the ciphertext. In order to obtain the private key, adversary needs to calculate $\mathcal{G}$ from $\mathcal{G}_1$ and v^{-1} from v . There is no practical known way to calculate $\mathcal{G}$ from $\mathcal{G}_1$ (cf. [3]). In order to calculate v^{-1} from v , an adversary needs to solve ICP. There is no known way to solve ICP except the brute force method [8, 14]. We now study the brute force complexity of ICP. Let $u = \sum_{j=1}^z k_j g_j$ be a given unit and $u^{-1} = \sum_{l=1}^z k'_l g_l$ be its corresponding inverse that is unknown. Then, $u * u^{-1} = 1$ implies

that $(\sum_{j=1}^z k_j g_j)(\sum_{l=1}^z k'_l g_l) = 1$ which means $\sum_{j,l=1}^z (k_j k'_l)(g_j g_l) = 1$. Let $|K| = m$ (let it be finite), then via brute force, the last equation can be solved in $O(m^z)$ operations (e.g. if $K = \mathbb{F}_2$, then the equation can be solved via brute force in $O(2^z)$ operations). Since order of K is atleast 2, if we take $|G| \geq 2^7 = 128$, then ICP can not be solved via brute force attack. This is a very small size as compare to group sizes considered in RSA and ElGamal PKCs (as of writing this paper, 2048 bits is the recommendation to attain security equivalent to 112 bits). Therefore, ICP is a hard mathematical problem.

Now, in the following theorem, we discuss the another task (already mentioned above) of adversary that involves deducing the plaintext from the ciphertext without key.

Theorem 2.1 : *The probability of deducing the plaintext from the ciphertext without the knowledge of key is negligibly small in McEliece-group-ring based PKC even if there exists a random oracle that solves ICP.*

Proof : For a given ciphertext c , an adversary can obtain $c * v^{-1}$ by utilizing the random oracle that solves ICP. Moreover as ϕ is open in public domain, adversary can deduce $c' = m\mathcal{G}_1 + \mathcal{E}$ from $c * v^{-1}$. Since $\mathcal{G}_1$ is of order $n_1 \times n_2$, the adversary picks n_1 columns at random to construct an invertible matrix $\widehat{\mathcal{G}}_1$. Accordingly, let c'_{n_1} and $\mathcal{E}_{n_1}$ be the restrictions of c' and $\mathcal{E}$, respectively to the n_1 columns mentioned above. If $\mathcal{E}_{n_1} = 0$ and $\widehat{\mathcal{G}}_1$ is invertible, then m can be recovered by solving $c'_{n_1} = m\widehat{\mathcal{G}}_1$. However, the probability that $\mathcal{E}_{n_1} = 0$ is $\binom{n_2 - n_3}{n_1} / \binom{n_2}{n_1}$ and it is small as comparison to 1. Consequently, there is a small probability that this attack succeed.

(4) IND-CPA security of the scheme: In the following theorem, we claim that the scheme is IND-CPA secure if ICP is a hard problem.

Theorem 2.2 : *The McEliece-group-ring based PKC is IND-CPA secure (or semantically secure) if ICP is a hard problem.*

Proof : In order to show this result, we show that McEliece-group-ring based PKC is not IND-CPA secure if there exists a random oracle O that solves ICP. Let m_0 and m_1 be two plaintexts chosen by the adversary A and submit them to challenger C . The challenger picks a random $t \in \{0, 1\}$,

encrypts m_i and sends the ciphertext $c = \phi(m_i \mathcal{G}_1 + \mathcal{E}) * v$ to A . Further, A calls O to solve ICP and calculate $\hat{c} = \phi^{-1}(c * v^{-1}) = m_i \mathcal{G}_1 + \mathcal{E}$. Note that, by construction, $\mathcal{E}$ has weight at most n_3 . A calculates

$$\mathcal{E}_0 = \hat{c} - \hat{c}_0 = m_i \mathcal{G}_1 + \mathcal{E} - m_0 \mathcal{G}_1 = (m_i - m_0) \mathcal{G}_1 + \mathcal{E},$$

$$\mathcal{E}_1 = \hat{c} - \hat{c}_1 = m_i \mathcal{G}_1 + \mathcal{E} - m_1 \mathcal{G}_1 = (m_i - m_1) \mathcal{G}_1 + \mathcal{E}.$$

Since $m_i \in \{m_0, m_1\}$, either $\mathcal{E}_0 = \mathcal{E}$ or $\mathcal{E}_1 = \mathcal{E}$. Note that A knows when this happens since $\mathcal{E}$'s weight is at most n_3 . Moreover, the other $\mathcal{E}_i$ consists of a sum of a non-zero codeword and the error. Since the code considered can correct up to n_3 errors, this means the minimum distance of the code is $\geq 2n_3 + 1$. Consequently, this codeword must have $\geq 2n_3 + 1$ non-zero terms. Now when we minus $\mathcal{E}$ from this codeword, there must be $\geq n_3 + 1$ non-zero terms, so A has the surety that this was not the message. Hence, A has full probability of winning the game. Since, ICP is a hard problem, we conclude that the scheme is semantically secure.

Unlike our scheme, the original McEliece PKC is not semantically secure, see [17]. Also it is proved in [17] that *padding the plaintext with a random bit-string provides the IND-CPA for the McEliece cryptosystem*.

2.6 Why this scheme?

Finally, we discuss the motivation behind the introduction of McEliece-group-ring based PKC. Although, a variant of McEliece PKC (*Classic McEliece*) is believed to be quantum safe, the main concern is the size of parameters required in the scheme. The main motive of McEliece-group-ring based PKC is to improve the security of McEliece PKC by uplifting the scheme in the algebraic structure of group rings (from Euclidean space) and use the hard problems in group rings that are secure for small parameters. The parameters required in our scheme are already discussed in the security subsection of this scheme.

3. Blum-goldwasser-group-ring based PKC

In this section, we present a Blum-Goldwasser-group-ring based PKC that is an extension of the Blum-Goldwasser PKC defined in groups to group rings. The Blum-Goldwasser PKC incorporates *Blum-Blum-Shub* generator to generate a sequence that is pseudorandom and it is an example of PKC that is a *stream cipher*. To this end, let us now define our novel group rings based scheme by first defining the various parameters

required in the scheme as in Section 2. The notations used in this section carry the same meaning as in the previous section, except unless stated.

3.1 Parameters creation

We choose two large primes p_1, p_2 such that $p_i \equiv 3 \pmod{4}$ for each $i = 1, 2$ and $p_1 \neq p_2$. We employ Euclidean division algorithm to obtain integers a_1 and a_2 such that $a_1 p_1 + a_2 p_2 = 1$. Further, let $G = \{g_i : i \in I\}$ be a group for index set $I = \{1, 2, \dots, z\}$ with z to be specified later on and $K = \mathbb{Z}_2$. Let u be a unit of group ring KG whose inverse u^{-1} may be public. Further, let a_3 be a secret positive integer such that $v = u^{a_3}$. Thus, the public parameters are K, G and u .

3.2 Public and Private keys creation

The public key is $(n = p_1 p_2, v)$ and the corresponding private key is $(p_1, p_2, a_1, a_2, a_3)$.

3.2 Encryption process

The encryption process for the proposed scheme is as follows:

- (a) B verifies the authentic public key of A .
- (b) Let $l = \lceil \log_2(\log_2 n) \rceil$. B represents message $m = m_1 \cdots m_{a_4}$ for some fixed integer a_4 , where each m_i is a string of 0's and 1's of length l .
- (c) B selects a random q_0 that is a quadratic residue modulo n .
- (d) For $i = 1$ to a_4 , B computes $q_i = q_{i-1}^2 \pmod{n}$ and let r_i be l least significant bits of q_i . Using r_i , B further computes $\widehat{m}_i = m_i \oplus r_i = (M_{(i-1)l+1}, \dots, M_{il})$. Further, after obtaining all the $\widehat{m}_i$'s, B writes $\widehat{M} = \sum_{k=1}^{a_4 l} M_k g_k$. Clearly, $|G| \geq a_4 l$.
- (e) B chooses a one time key a_5 and computes the ciphertext $c = (c_1, c_2, q_{a_4+1})$, where $c_1 = u^{a_5}$, $c_2 = \widehat{M} * v^{a_5}$ and $q_{a_4+1} = q_{a_4}^2$.

3.4 Decryption process : The decryption process is discussed as follows:

- (a) A computes $d_i = ((p_i + 1) / 4)^{a_4+1} \pmod{p_i - 1}$ for $i = 1, 2$.
- (b) Using d_i , A computes $U_i = q_{a_4+1}^{d_i} \pmod{p_i - 1}$ for $i = 1, 2$.
- (c) Using U_i 's, A computes $q'_0 = U_2 a_1 p_1 + U_1 a_2 p_2 \pmod{n}$.

- (d) Next, A utilize c_2, c_1 and the private key to obtain $c_2 * c_1^{-a_3} = \widehat{M}$. Then, A rewrite $\widehat{M}$ as $(\widehat{m}'_1, \dots, \widehat{m}'_{a_4})$, where each $\widehat{m}'_i$ is of length l .
- (e) For $i=1$ to a_4 , A computes $q'_i = (q'_{i-1})^2 \bmod n$ (starting with q'_0) and let r'_i be l least significant bits of q'_i . Using r'_i , A further computes $m'_i = \widehat{m}'_i \oplus r'_i$. This is the decrypted message.

Proof that decryption works: First we show that $q'_0 = q_0$. To see this, note that q_t is a quadratic residue modulo p_1 , since it is a quadratic residue modulo n . Therefore, by definition, $q_{a_4}^{(p_1-1)/2} \equiv 1 \bmod p_1$. By construction, note that $q_{a_4+1}^{(p+1)/4} \equiv (q_{a_4}^2)^{(p+1)/4} \equiv q_{a_4}^{(p-1)/2} q_{a_4} \equiv q_{a_4} \bmod p_1$. Similarly, $q_{a_4-1}^{(p+1)/4} \equiv q_{a_4-1} \bmod p_1$. On continuing similarly, we get $U_1 = q_{a_4+1}^{d_1} \equiv q_0 \bmod p_1$. Further, repeating the above procedure for p_2 implies that $U_2 = q_{a_4+1}^{d_2} \equiv q_0 \bmod p_2$. As $a_1 p_1 + a_2 p_2 = 1$, one can see that $U_2 a_1 p_1 + U_1 a_2 p_2 \equiv q_0 \bmod p_i$ for $i=1, 2$. This means that $q_0 = q'_0$, i.e. A recovers the same seed used by B in encryption. Further, one can see that rest of the proof is easy.

3.5 Why this scheme?

Before discussing the security analysis of Blum-Goldwasser PKC, we discuss the motivation behind the introduction of this scheme since its security analysis heavily depends on its motivation. Blum-Goldwasser PKC is one of the most efficient probabilistic PKC and it is semantically secure, provided integer factorization is intractable. However, it is proved that in order to break RSA-2048, a quantum computer with atleast 4099 qubits is required (using *Shor's algorithm*) (cf. [19]). This means in the presence of a sufficiently large quantum computer, Blum-Goldwasser PKC will no longer serves its purpose. Consequently, we wanted to uplift the group based settings in Blum-Goldwasser PKC to make it a group-ring based PKC so that it can be used as an alternate to Blum-Goldwasser PKC in the presence of a sufficiently large quantum computer. Moreover, we kept its settings in such a manner that its new structure provides the backward compatibility (i.e. if someone needs to use the old version).

3.6 Security of the scheme

The security of Blum-Goldwasser-group-ring based PKC is discussed in the following points:

- (1) The scheme is probabilistic in nature since corresponding a single m , there are different ciphertexts (since both q_0 and a_5 are randomly chosen for each message).
- (2) Hard problems: The task in front of an adversary is either to obtain the private key from the public key or to obtain the plaintext from the ciphertext. In order to obtain the private key, adversary needs to solve ICP and integer factorization problem (IFP). The hardness of ICP is already discussed in the last section and the hardness of IFP is well studied in the literature. Moreover, it seems infeasible for an adversary to deduce the plaintext from the ciphertext without the knowledge of key without solving ICP. To this end, we now study the security of Blum-Goldwasser-group-ring based PKC by assuming that IFP is solvable.
- (3) IND-CPA security of the scheme: In the following theorem, we claim that the scheme is IND-CPA secure if ICP is a hard problem.

Theorem 3.1 : *The Blum-Goldwasser-group-ring based PKC is IND-CPA secure (or semantically secure) if ICP is a hard problem.*

Proof : Since we have assumed that IFP is solvable, the only security in this scheme is due to ICP. As in Theorem 2.2, we show that Blum-Goldwasser-group-ring based PKC is not IND-CPA secure if there exists a random oracle O that solves ICP. Let m_0 and m_1 be two plaintexts chosen by the adversary A and submit them to challenger C . The challenger picks a random $t \in \{0, 1\}$, encrypts m_t and sends the ciphertext $c = (c_1, c_2, q_{a_4+1})$, where $c_1 = u^{a_5}$, $c_2 = \widehat{M} * v^{a_5}$ and $q_{a_4+1} = q_{a_4}^2$ to A . Further, A calls O to solve ICP and calculate $c_2 * v^{-a_5} = \widehat{M}$ and indeed $\hat{m}_i = m_{ti}$ for all $i = 1$ to a_4 . Since IFP is solvable, A can find out the initial seed q_0 . Consequently, A has full probability of winning the game. Since, ICP is a hard problem, we conclude that the scheme is semantically secure.

4. Examples

In this section, we discuss two toy examples related to both the schemes. The results used in both the examples are computed using GAP (Groups, Algorithm and Programming) version 4.10.2 (cf. [4]).

4.1 Toy example of McEliece-group-ring based PKC

We consider the following generator matrix $\mathcal{G}$ of $(7,4)$ -Hamming code having order 4×7 , a random invertible 4×4 matrix $\mathcal{S}$ with binary entries and the 7×7 permutation matrix $\mathcal{P}$:

$$\mathcal{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}, \mathcal{S} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}, \mathcal{P} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

Therefore, the matrix $\mathcal{G}_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$. We consider the integral

group ring of dihedral group $G = D_{10}$. To be more precise, we have $K = \mathbb{Z}$ and

$$G = \langle \alpha, \beta \mid \alpha^5 = 1 = \beta^2, \beta\alpha = \alpha^4\beta \rangle = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta, \alpha^4\beta\}.$$

Consider the element $\bar{u} = 1 - 2\alpha - 2\alpha^2 + \alpha^3 + 3\alpha^4$ of $\mathbb{Z}D_{10}$. One can see that $\bar{u}$ is a unit of $\mathbb{Z}D_{10}$ with $\bar{u}^{-1} = -2 + 3\alpha - 2\alpha^2 + \alpha^3 + \alpha^4$. Therefore, the public key is $(\mathcal{G}_1, n_3 = 1, v = \bar{u}^8)$, where $v = \bar{u}^8 = -1576239 + 602070\alpha + 1948339\alpha^2 + 602070\alpha^3 - 1576239\alpha^4$. The private key is $(\mathcal{S}, \mathcal{G}, \mathcal{P})$ and $v^{-1} = \bar{u}^{-8} = 602070 + 602070\alpha - 1576239\alpha^2 + 1948339\alpha^3 - 1576239\alpha^4$. Let the message $m = [1 \ 1 \ 0 \ 1]$ need to be encrypted. Accordingly, B consider the binary vector $\mathcal{E} = [0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0]$. Clearly, weight of $\mathcal{E}$ is 1. Therefore, B computes $c' = m\mathcal{G}_1 + \mathcal{E} = [0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0] + [0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0] = [0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0]$. At this stage, B apply φ on c' to obtain $\varphi(c') = \alpha + \alpha^2 + \alpha^4 + \beta$. Finally, the ciphertext is

$$\begin{aligned} c = \varphi(c') * v = & -372099 - 1204139\alpha - 372099\alpha^2 + 974170\alpha^3 + 974170\alpha^4 \\ & - 1576239\beta - 1576239\alpha\beta \\ & + 602070\alpha^2\beta + 1948339\alpha^3\beta + 602070\alpha^4\beta. \end{aligned}$$

For decryption, A utilize the second part of private key, i.e. v^{-1} to obtain $m' = \alpha + \alpha^2 + \alpha^4 + \beta$. Further, A verifies that the coefficients of m' are in $(\mathbb{Z}_2)^{n_2}$ and apply φ^{-1} on m' to obtain $\varphi^{-1}(m') = [0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0]$.

After this, A calculates $m'' = \varphi^{-1}(m')\mathcal{P}^{-1} = [1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1]$. Furthermore, using the fast decoding algorithm, A decodes m'' as $\hat{m}$ and multiply the result with $\mathcal{S}^{-1}$ to obtain the plaintext.

4.2 Toy example of Blum-Goldwasser-group-ring based PKC :

Let $p_1 = 19, p_2 = 7$. Note that $l = \lceil \log_2(\log_2(133)) \rceil = 3$. Let the message to be encrypted be $m = 101001$. As $l = 3$, break m in 2 blocks m_1 and m_2 of length 3, where $m_1 = 101, m_2 = 001$. Clearly, $a_4 = 2$. The group ring under consideration is $K = \mathbb{F}_2$, $G = D_{10}$ with the similar presentation as considered in the last subsection. Consider the unit element $u = \alpha^2 + \alpha^4 + \beta$ of KG with inverse $u^{-1} = 1 + \alpha + \alpha^3 + \alpha^4 + \beta + \alpha\beta + \alpha^4\beta$. The public key is $(n = p_1p_2 = 133, v)$ and the corresponding private key is $(19, 7, 3, -8, 8)$, since $a_1p_1 + a_2p_2 = 1$, where $v = u^8 = 1 + \alpha + \alpha^2 + \alpha\beta + \alpha^2\beta + \alpha^3\beta + \alpha^4\beta$. Now, in order to encrypt, B selects a random $r = 36$ and use this to compute $q_0 = 36^2 \bmod 133 = 99$. By choice, it is clear that q_0 is a quadratic residue modulo $n = 133$. Using this, B calculates $q_1 = 99^2 \bmod 133 = 92$, $q_2 = 92^2 \bmod 133 = 85$, $q_3 = 85^2 \bmod 133 = 43$ and write these numbers in base 2 as $q_1 = 1011100, q_2 = 1010101$. The $l = 3$ least significant bits of these are $r_1 = 100$ and $r_2 = 101$. Using r_i 's, B further computes $\widehat{m}_1 = m_1 \oplus r_1 = 001$, $\widehat{m}_2 = m_2 \oplus r_2 = 100$. After that, B writes $\widehat{M} = \sum_{k=1}^{a_4l} M_k g_k = \sum_{k=1}^6 0 = 0 + 0\alpha + \alpha^2 + \alpha^3 + 0\alpha^4 + 0\beta = \alpha^2 + \alpha^3$. Finally, B chooses $a_5 = 2$ to obtain the ciphertext $c = (c_1, c_2, q_3)$, where $c_1 = u^2 = 1 + \alpha^3 + \alpha^4 + \alpha\beta + \alpha^2\beta + \alpha^3\beta + \alpha^4\beta$ and $c_2 = \widehat{M} * v^2 = 1 + \alpha + \alpha^2 + \alpha^4 + \alpha^2\beta + \alpha^3\beta$.

In order to decrypt, A computes $d_1 = 5^3 \bmod 18 = 17$, $d_2 = 2^3 \bmod 6 = 2$. Accordingly, $U_1 = 43^{17} \bmod 19 = 4$ and $U_2 = 43^2 \bmod 7 = 1$. Consequently, $q_0 = q'_0 = 1(3)(19) + 4(-8)(7) \bmod 133 = 99$ which is the initial seed. Next, A utilize c_2, c_1 and the private key to obtain $c_2 * c_1^{-8} = \widehat{M}$. Then, A rewrite $\widehat{M}$ as $(\widehat{m}'_1, \widehat{m}'_2)$, where each $\widehat{m}'_i$ is of length 3. For $i = 1$ to 2, A computes $q'_i = (q'_{i-1})^2 \bmod n$ (starting with q'_0) and consider r'_i as the 3 least significant bits of q'_i . Using r'_i , A further computes $m'_i = \widehat{m}'_i \oplus r'_i$ to obtain the message.

5. Conclusion

We have presented two probabilistic PKCs based on the structure of group rings. We have discussed the advantages of both the PKCs over the existing PKCs as well as the reasons behind the introduction of these systems. In terms of security, we have shown that the security of these PKCs depend on hard problems in group rings. We emphasize the fact that in both the PKCs, units of group rings are required in the public as well as private keys. We refer to articles [2, 16] for a method to construct of units of group algebras. Further, as of writing this paper, to the best of our knowledge, there is no known polynomial time algorithm to solve these hard problems in group rings. Therefore, both the schemes can be very useful in the near future.

References

- [1] D. Bernstein, J. Buchmann, E. Dahmen, Post-Quantum cryptography, Springer, 2009.
- [2] C. Dietzel, G. Mittal, Summands of finite group algebras, *Czechoslovak Mathematical Journal*, 71(4), 1011-1014, 2021.
- [3] D. Engelbert, R. Overbeck, A. Schmidt, A summary of McEliece-type cryptosystems and their security, *Journal of Mathematical Cryptology*, 1(2), 151-199, 2007.
- [4] GAP, Groups, Algorithms, Programming, A system for computational discrete algebra, Version 4.11.1, www.gap-system.org
- [5] N. Goel, I. Gupta, M. Dubey, B. K. Dass, Undeniable signature scheme based over group ring, *Applicable Algebra in Engineering, Communication and Computing*, 27(6), 523-535, 2016.
- [6] T. Hanoymak, Ö. Küsmüs, On construction of cryptographic systems over units of group rings, *International Electronic Journal of Pure and Applied Mathematics*, 9(1), 37-43, 2015.
- [7] J. Hoffstein, J. Pipher, J. H. Silverman, An introduction of mathematical cryptography, Springer, 2008.
- [8] B. Hurley, T. Hurley, Group ring cryptography, *International Journal of Pure and Applied Mathematics*, 69(1), 67-86, 2011.
- [9] T. Hurley, Group rings for communications, *International Journal of Group Theory*, 4(4), 1-23, 2015.

- [10] S. Inam, R. Ali, A new ElGamal-like cryptosystem based on matrices over group ring, *Neural Computations and Applications*, 29(11), 1279-1283, 2018.
- [11] Ö. Küsmüs, T. Hanoyamak, A novel public-key encryption scheme based on Bass cyclic units in integral group rings, *Journal of Discrete Mathematical Sciences and Cryptography*, Online first, 1-11, 2020, DOI: 10.1080/09720529.2020.1756042.
- [12] A. Menezes, P. Oorschot, S. Vanstone Handbook of applied cryptography, CRC press, 1997.
- [13] C. P. Milies, S. K. Sehgal, An Introduction to Group Rings, Klumer, 2002.
- [14] G. Mittal, S. Kumar, S. Narain, S. Kumar, Group rings based public key cryptosystems, *Journal of Discrete Mathematical Sciences and Cryptography*, Online first, 1-22, 2021, DOI:10.1080/09720529.2020.1796868.
- [15] G. Mittal, S. Kumar, S. Kumar, Novel public key cryptosystems based on NTRU and algebraic structure of group rings, *Journal of Information and Optimization Sciences*, 42, 1507-1521, 2021.
- [16] G. Mittal, R. K. Sharma, Unit group of semisimple group algebras of some non-metabelian groups of order 120, *Asian-European Journal of Mathematics*, Online first, 1-11, 2021, DOI:10.1142/S1793557122500590.
- [17] R. Nojima, H. Imai, K. Kobara, K. Morozov, Semantic security for the McEliece cryptosystem without random oracles, *Designs, Codes and Cryptography*, 49, 289-305, 2008.
- [18] A. Pandey, I. Gupta, A new undeniable signature scheme on general linear group over group ring, *Journal of Information and Optimization Sciences*, Online first, 1-13, 2020, DOI:10.1080/09720529.2020.1744814.
- [19] The deal with quantum computing and cryptography, accessed on 2020-01-13. [Online]. Available: www.infosecurity-magazine.com/opinions/quantum-computing-cryptography-1-1-1

Received June, 2021

Revised November, 2021