Contemporary Mathematics
http://ojs.wiserpub.com/index.php/CM/

UNIVERSAL WISER PUBLISHER

Research Article

A New Encryption Scheme Based on Groupring

Saba Inam[1*], Shamsa Kanwal[1], Rashid Ali[2]

[1]Department of Mathematical Sciences, Faculty of Science and Technology, Fatima Jinnah Women, The Mall, Rawalpindi, Pakistan
[2]Department of Mathematics, Faculty of Computing, Capital University of Science and Technology, Islamabad, Pakistan
E-mail: saba.inam@fjwu.edu.pk

Received: 25 August 2020; **Revised:** 28 December 2020; **Accepted:** 5 February 2021

Abstract: Security of some present day public key cryptosystem (PKC) is based on general linear groups as it is a good choice for developing such types of cryptosystems. This study presents various public key encryption schemes based on general linear groups. Different techniques including automorphisms in connection with conjugacy search problem and its generalization are used to develop these schemes. Further, the grouprings are chosen as a platform to enhance the security and efficiency. Numerous aspects related to our new proposal are also elaborated.

***Keywords*:** groupring, general linear group, key exchange protocol, public key cryptography

MSC: 94A60, 20G40

1. Introduction

Due to rapid development in the area of information technology, a secure commercial and private communication has become a need. Therefore, faster and more efficient methods enable people to protect their valuable information. Adversaries are also there to penetrate this secret information. The field of cryptography has played a vital role in the secure transformation of important information between two or more people. The main purpose of cryptography is to send information between participants in such a way that the threats from adversaries can be prevented. The history of cryptography is very long and fascinating. It is the study of methods of transforming a secret message in such a way that it can be understood only by an authorized recipient who has been provided with a secret key for deciphering it. In 1985, Magyarik and Wagner [1] proposed a public key cryptography by using the elements of semigroup with undecidable word problems. A review of group based cryptographic methods was discussed by Myasnikov et al. [2] in the book Group-based Cryptography. But Birget et al. [3] told that the public key cryptosystem (PKC) proposed by Magyarik and Wagner [1] actually did not depends on word problem and as a result they developed a new scheme, which was based on finitely generated groups with hard problems. On braid group based cryptography, Anshel et al. [4] proposed a key exchange protocol in 1999 and the hard problem of this protocol was the difficulty of resolving equations over algebraic structures. In this paper [5], they mentioned that for PKC braid groups as a platform were a goodchoice. Later in 2000, Ko et al. [6] developed a new key exchange protocol by using braid groups. The conjugacy search problem (CSP) is the underlying hard problem for this protocol. Furthermore, many successful schemes were proposed in this area by Cha et al. [7] in 2001, Anshel et al [8] in 2003, Dehornoy [9] in 2004 and Anshel et. al [10] in 2006. Paeng et

DOI: https://doi.org/10.37256/cm.222021611

al. [11] in 2001 also proposed a new scheme which was based on finite noncommutative groups. That method consists of the Discrete Log Problem (DLP) in the inner automorphism group. In this era, Magliveras et al. [12] in 2002 gave a remarkable idea about one way function and trapdoors which were generated on finite fields. In the meantime, on finite groups Magliveras et al. anticipated anew PKC scheme using one way function and trapdoors. Consequently, on integer matrices, Grigoriev and Ponomarenko [13-14] extended the difficulty of the membership problem [15] for a fnitely generated group of elements. In 2007, a new proposal was given by Cao et al. [16] on polynomials over noncommutative semigroups or rings. The method was named as Z modular method. As an application of this scheme Kubo [6] in 2008 presented a scheme based on a noncommutative dihedral group of order 6. Reddy et al. [17] in 2008 developed a signature scheme over noncommutative groups and division ring by using Z modular method. The implementation of this scheme was built by Moldovyan and Moldovyan [18]. Another scheme was also formulated by Kanwal and Ali and Inam et. al [19-20] by using noncommutative platform groups. Now let us talk about some PKC schemes of groupring. A cryptosystem based on the structure of a groupring was proposed by Rososhek [21-22]. In 2011, Kahrobaei et al. [23] developed a key exchange protocol based on matrices over groupring. After that many PKC schemes based on groupring were proposed. After that, many PKC schemes were proposed based on groupring [24, 26]. In 2016, S. Inam and R. Ali [25] developed a cryptosystem for which the underlying work structure is groupring. The main idea to apply the grouprings in cryptography depends on the fact that if the cardinality of the finite ring R is fixed, the cardinality of a groupring GR for a finite group is an exponent of the cardinality of a group G. Then cryptographic transformation performed by a legal user separately in the group G and in the ring R using polynomial algorithms and an illegal user has to solve computationally dicult problems in groupring GR. In this article, we would like to suggest a new technique of constructing PKC which is based on a general linear group over a groupring. The rest of the article is summarized as follows: Section 2 will deal with the denition of general linear group as well as groupring which will be helpful in next sections. In Section 3, we present the proposed PKC and an example will help to explain the proposed cryptosystem in detail. Without security, cryptosystems have no value, so in Section 4, a detailed discussion will take place on the security aspects of the proposed cryptosystem.

2. Preliminaries

This section will deal with some notations which will be helpful to develop the new PKC:

Definition 1 (General Linear group) The set of an $m \times m$ invertible matrices of degree m is known as the general linear group. The operation is the same as usual matrix multiplication. Since an invertible matrix has an inverse which is also invertible and also the product of two invertible matrices is again invertible, hence this forms a group. More precisely, the basic necessity is to identify what type of items/objects will come in the matrix entries. For example, if entries of the general linear group come from R (the set of real numbers), then it is represented by $GL_m(R)$ or $GL(m, R)$ is the group of $m \times m$ invertible matrices of real numbers. In general, the general linear group of degree n over a ring R (such as the ring of integers) or any field F (such as the complex numbers), is the set of $m \times n$ invertible matrices with entries from F (or R), again with matrix multiplication as the group operation. Typically, it is denoted by $GL(m, F)$ or $GL_m(F)$ or simply $GL(m)$ if the field is understood.

Here we give some basic concepts of grouprings and units.

Definition 2 (Groupring and Units) Let us consider a ring R and a group G. Then, we can define the groupring [7] GR as the set of all linear combinations

$$\gamma = \sum_{g_1 \in G} b_{g_1} g_1,$$

where $b_{g_1} \in R$ and have only finitely many of the $b'_{g_1}s$ are non-zero. The sum and product in groupring is defined as

$$\gamma + \delta = \sum_{g_1 \in G} b_{g_1} g_1 + \sum_{g_1 \in G} d_{g_1} g_1 = \sum_{g_1 \in G} \left(b_{g_1} + d_{g_1}\right) g_1 \tag{1}$$

$$\gamma\delta = \left(\sum_{g_1 \in G} b_{g_1} g_1\right)\left(\sum_{h \in G} d_h h\right) = \sum_{g_1, h \in G} b_{g_1} d_h g_1 h \tag{2}$$

respectively. The equation (2) can be redefined as:

$$\gamma\delta = \sum_{v \in G} E_v v, \text{ where } E_v = \sum_{g_1 h = v} b_{g_1} d_h.$$

Here we note that groupring GR is a ring with usual addition and multiplication defined in equations (1) and (2). We can also define multiplication as $\gamma \in GR$ and $\rho \in R$, then

$$\rho\gamma = \rho \sum_{g_1 \in G} b_{g_1} g_1 = \sum_{g_1 \in G} (\rho b_{g_1}) g_1.$$

For more details on groupring, see Reference [5]. The invertible elements with respect to the multiplication are said to be units. The set of units under multiplication forms a group, it is denoted by $U(RG)$. For more details, see References [20, 24].

Nevertheless, GR is in general not commutative and therefore $M(n, GR)$ and $GL(n, GR)$ do not make sense in general, that is why we need to be extremely careful while making choices for ground structures of group and ring.

In our case, we have taken a cyclic group of order n which is always abelian and ring is $\mathbb{Z}_n$, also a unitary commutative ring. Now in our proposed schemes, the matrices are either circulant or coming from the center of $GL(n, GR)$. There are many units and group rings available of many different types that can be used. These can be non-commutative as well as commutative. Shiplrain et al. [23] used the structure of non-commutative groupring.

Lemma 3 Let R be a ring of order m and G a group of order n. Then, GR is a finite groupring of size $|R|^{|G|} = m^n$.

The very well known two hard problems are defined as follows:

Definition 4 (Discrete Log Problem, DLP) Let G be a multiplicative group such that $|G| = n$, and the generator $g \in G$. Find the unique integer b, $0 < b < n - 1$, such that $g^b = y$, b can be defined as $\log_g y$ and $y \in G$.

Definition 5 (Conjugacy Search Problem) Let us consider a group G and two elements s and t such that $s, t \in G$ and the information that $s^y = t$ for some $y \in G$ to find at least one element y. Here s^y means that ysy^{-1}.

The general structure of proposed cryptosystem is defined in Section 3.

3. Proposed cryptosystem

The key generation, encryption and decryption algorithm will help us to define all the characteristics of the proposed scheme. To understand this scheme, a toy example will also be given in this section.

Alice and Bob agreed on the order of a matrix n and groupring GR.

The implementation of our proposed scheme is elaborated as follows:

Consider the set $M(n, GR)$, which contains all matrices with order n defined over the groupring GR. Take H, the collection of all circulant as well as invertible matrices of order n, with entries from groupring GR. Then $H \leq M(n, GR)$.

Algorithm 6 (Key Generation)

Input: A random matrix $A \in GL(n, GR)$.

Output: A pair of keys public key $K_p = (P_1, P_2, BD)$ and $K_r = (B, D)$.

1. Generate the following matrices

$$B = A^2 \text{ and } D = A^3. \tag{3}$$

2. Compute the matrices

$$M = B^2D \text{ and } N = BD^2, \tag{4}$$

using in step 1, equation (3).

3. Choose a randomly matrix $R \in GL(n, GR)$.
4. Calculate the conjugates of R by M and N

$$P_1 = (R)^M = M^{-1}RM, \tag{5}$$

$$P_2 = ((R)^{-1})^M = M^{-1}(R)^{-1}M, \tag{6}$$

and

$$BD. \tag{7}$$

Algorithm 7 (Encryption)
Input: A plaintext message P and public key K_p.
Output: A ciphertext $C = (c_1, c_2)$.
1. Convert the plaintext P in the form of a matrix $m \in M(n, GR)$.
2. Select a random integer $n_0 \in \mathbb{N}$.
3. Compute a matrix

$$Y = (BD)^{n_0}. \tag{8}$$

4. Find the following conjugates with the help of Y defined in step 3,

$$Q_1 = (P_1)^Y = Y^{-1}P_1Y, \tag{9}$$

$$Q_2 = (P_2)^Y = Y^{-1}P_2Y, \tag{10}$$

$$Q_3 = m(P_1)^Y = mY^{-1}P_1Y. \tag{11}$$

5. Pick any randomly invertible element ρ of groupring and calculates theciphertext

$$c_1 = \rho^{-1}(Q_2) = \rho^{-1}Y^{-1}P_2Y, \tag{12}$$

$$c_2 = \rho m(Q_1) = \rho mY^{-1}P_1Y. \tag{13}$$

Algorithm 8 (Decryption)
Input: A ciphertext C and private key K_R.
Output: A plaintext message P.
1. Compute the inverse matrix D^{-1}.
2. Calculate the conjugate

$$L = (c_1)^B = B^{-1}(c_1)B. \tag{14}$$

3. Use equation (14) in step 2, find t as

$$t = (L)^{D^{-1}} = DLD^{-1}. \tag{15}$$

4. Decrypt the ciphertext to obtain m

$$m = tc_2t. \tag{16}$$

Theorem 9 In view of proposed cryptosystem, the correctness of decryption algorithm is guaranteed.
Proof. We can easily prove by noticing the equation (14) and (15),

$$t = (L)^{D^{-1}} = Dc_1^B D^{-1}. \tag{17}$$

Now by using equation (13) and equation (17), we have

$$\begin{aligned} c_2t &= \rho^2 P_1^Y m P_1^Y \left(L\right)^{D^{-1}}, \\ &= \rho^2 Y^{-1} P_1 Y.Dc_1^B D^{-1} m Y^{-1} P_1 Y.Dc_1^B D^{-1}, \\ &= \rho^2 P_1 Y.DB^{-1} c_1 BD^{-1} m Y^{-1} P_1 Y.DB^{-1} c_1 BD^{-1}. \end{aligned}$$

Use equation (12) in the last step and follow as

$$\begin{aligned} tc_2t &= \rho m Y^{-1} M^{-1} RMY.DB^{-1} \rho^{-1} Y^{-1} P_2 YBD^{-1} \\ &= \rho m Y^{-1} D^{-1} B^{-2} RB^2 DY.DB^{-1} \rho^{-1} Y^{-1} N^{-1} R^{-1} NYBD^{-1} \\ &= \rho m Y^{-1} D^{-1} B^{-2} RB^2 DY \rho^{-1} D^{-1} B^{-2} Y^{-1} R^{-1} B^2 DY. \end{aligned}$$

Since B, D, B^2D and BD^2 are the integral multiples of A, all the defined matrices commutes.

$$\begin{aligned} tc_2t &= \rho\rho^{-1} m Y^{-1} D^{-1} B^{-2} RYB^2 DD^{-1} B^{-2} Y^{-1} R^{-1} B^2 DY \\ &= m Y^{-1} D^{-1} B^{-2} RYB^2 B^{-2} Y^{-1} R^{-1} B^2 DY \\ &= m Y^{-1} D^{-1} B^{-2} RYY^{-1} R^{-1} B^2 DY \\ &= m Y^{-1} D^{-1} B^{-2} RR^{-1} B^2 DY, && \because YY^{-1} \\ &= m Y^{-1} D^{-1} B^{-2} B^2 DY, && \because RR^{-1} = 1 \\ &= m Y^{-1} D^{-1} DY, && \because B^{-2} B^2 = 1 \end{aligned}$$

$$= mY^{-1}Y, \qquad \because D^{-1}D = 1$$

$$= m.$$

3.1 *A toy example*

This section concludes with a toy-example which illustrates our proposed cryptosystem. For this purpose, let us consider cyclic group $G = C_3$, the ring $R = \mathbb{Z}_2$ where $G = C_3 = \{1, z, z^2\} = \langle z\rangle = \langle z: z^3 = 1\rangle$ and $R = \mathbb{Z}_2 = \{0, 1\}$ Then, one can define

$$\mathbb{Z}_2C_3 = \left\{ \sum_{g\in C_2} a_g g : a_g \in R \right\}$$

$$GR = \mathbb{Z}_2C_3 = \left\{0,\ 1,\ z,\ 1+z,\ z^2,\ 1+z^2,\ z+z^2,\ 1+z+z^2\right\}$$

Let $GL(2, GR)$ be the general linear group of matrices of order 2 over a groupring.
Let us consider the random matrix

$$A = \begin{bmatrix} 1 & 1+z^2 \\ z^2 & z \end{bmatrix} \in GL(2, GR).$$

Next, Alice will compute the following matrices from the equations (3) and (4)

$$B = \begin{bmatrix} 1+z+z^2 & z+z^2 \\ 1+z^2 & z \end{bmatrix},\ D = \begin{bmatrix} z^2 & 1+z^2 \\ z^2 & 1+z+z^2 \end{bmatrix},$$

$$M = \begin{bmatrix} 1+z+z^2 & 1+z \\ 1 & 1 \end{bmatrix} \text{ and } N = \begin{bmatrix} z & z+z^2 \\ 1+z^2 & 1+z+z^2 \end{bmatrix}.$$

Now, she again chooses a random matrix

$$R = \begin{bmatrix} 1 & z \\ 1+z+z^2 & 1+z \end{bmatrix} \in GL(2, GR).$$

and computes the matrices defined in equations (5), (6) and (7)

$$R^{-1} = \begin{bmatrix} z+z^2 & z^2 \\ 1+z+z^2 & z \end{bmatrix},$$

$$P_1 = \begin{bmatrix} 0 & 1 \\ z^2 & z \end{bmatrix} \text{ and } P_2 = \begin{bmatrix} 1+z^2 & 1+z+z^2 \\ 1+z+z^2 & 1 \end{bmatrix},$$

$$BD = \begin{bmatrix} z^2 & 0 \\ 1+z+z^2 & z^2 \end{bmatrix}.$$

So Alice's public key is K_p.

Next Bob will do the following steps:

He presents a plaintext as a matrix

$$m = \begin{bmatrix} 0 & 1 \\ z^2 & z \end{bmatrix} \in M(2, GR)$$

First he chooses a natural number $n_0 = 3$ and then computes the matrix

$$Y = \begin{bmatrix} 1 & 0 \\ 1+z+z^2 & 1 \end{bmatrix},$$

and its inverse is

$$Y^{-1} = \begin{bmatrix} 1 & 0 \\ 1+z+z^2 & 1 \end{bmatrix}.$$

He calculates the conjugates using equations (9) and (10)

$$Q_1 = \begin{bmatrix} 1+z+z^2 & 1 \\ z^2 & 1+z^2 \end{bmatrix} \text{ and } Q_2 = \begin{bmatrix} z & 1+z+z^2 \\ 1+z+z^2 & 1+z^2 \end{bmatrix}.$$

Let $\rho = z^2 \in GR$ be the invertible element of groupring. The inverse is

$$\left(z^2\right)^{-1} = z.$$

Finally he computes the matrices using equations (12) and (13)

$$c_1 = \begin{bmatrix} z^2 & 1+z+z^2 \\ 1+z+z^2 & 1+z^2 \end{bmatrix} \text{ and } c_2 = \begin{bmatrix} z & z+z^2 \\ 1+z & 1+z+z^2 \end{bmatrix},$$

to get the ciphertext $C = (c_1, c_2)$.

To obtain the original plaintext, Alice will perform the following steps:

First she calculates the matrix

$$t = (L)^{D^{-1}} = \begin{bmatrix} z+z^2 & z^2 \\ z & 1+z+z^2 \end{bmatrix}.$$

She finally obtains original plaintext/message as

$$m = \begin{bmatrix} 0 & 1 \\ z^2 & z \end{bmatrix}.$$

4. Security analysis of proposed cryptosystem

In Section 3, we have proposed the PKC. It is not enough to propose the new cryptosystems but the security aspects are very important. The security of proposed PKC against different attacks are discussed in this section.

Let us consider that, an attacker only knows the ciphertext c_1 and c_2 as defined in equations (12) and (13) respectively. An adversary knows only the matrices P_1, P_2 and BD which are publicly announced and defined in equations (5), (6) and (7) respectively. To find the plaintext m, he has to find unknown matrix Y and invertible element ρ of groupring. Here he has a large system of nonlinear equations for the ciphertext corresponding to plaintext. For this, he assumes randomly invertible element $\rho_0 = \rho$ and gets

$$\rho_0 c_1 = Q_1, \tag{18}$$

$$c_2 = \rho_0 m Q_2. \tag{19}$$

Then he put each solution by letting $Y = Y_0$ in the above equations (18) and (19) and get

$$c_2 = \rho_0 m (Y_0)^{-1} P_1 Y_0.$$

He finds the corresponding solution $m = m_0$. Thus, for each fixed $\rho_0 = \rho$, an attacker receives number of forms (Y_0, m_0). Here we have a large system of equations with a large number of unknowns as the adversary has to solve firstly the DLP then he has to find the conjugators and in the end he will solve the system of nonlinear equations. No matter how an adversary rearranges these equations, the problem of having a product of two unknown matrices cannot be avoided which leads to a large system of nonlinear equations in the large number of unknown entries. This solution becomes infeasible.

Now we will talk about the known plaintext attack. Let us consider an attacker knows the ciphertext $C = (c_1, c_2)$ corresponding to plaintext $m(i = 2, 3, 4, ..., j)$. Let the plaintext ciphertext be the pair (m, C). From this plainte-ciphertext pair, he wants to find the next plaintext m_{j+1} corresponding to the ciphertext C_{j+1}. In the above proposed PKC, these types of attacks are impossible because of choosing dierent Y to get encryption of every new plaintext. Hence, it does not provide any information to find the next unknown plaintext ciphertext pair. As a consequence, we have shown that our proposed cryptosystem is secured against known plaintext attack.

In the structure of groupring, the units form a group, so it is impossible to decide which invertible element used in the cryptosystem. In groupring structure, to find the units and their inverses is one such a big problem named as the unit problem in applications. In cryptography, units are very useful by the said property. Due to this reason, researchers move to develop the cryptosystem based on algebraic structures specially groupring. Many authors think that units of groupring have the similar properties just like the properties of prime numbers. By using Lemma 3, with the choice of large n and m we have a large structure of groupring. So for the parameter m, we suggest that $n \sim 10^{100}$. With the choice of said m, brute force attack is not possible.

5. Conclusion

The successful of quantum algorithm radiate doubts on many PKCs based on discrete logarithm and integer factorization problem. We have shown in Section 4 that the proposed scheme is secure against known plaintext attack. In the given example, we have considered the fix groupring and fix unit for encryption and decryption and observes that to find the units and their inverses is such a big problem itself. Our main aim is to construct a variant of ElGamal public

key cryptosystem based on a general linear group over a groupring. As we know that for the general linear group, we have more options for the matrix entries, for example $GL_n(z_n[C_m]) = (n.m)^n(n^m)^n$. In view of the example, it will be valuable to say that the complex parametric structure of units provide indeterministic peculiarities. As a result, this scheme is more secured than the others.

Conflict of interest statement

This is an original manuscript. This manuscript is neither submitted nor accepted anywhere. All authors declared that we have no competing interests.

References

[1] Magyarik R, Wagner NR. A public key cryptosystem based on the word problem. *Workshop on the Theory and Application of Cryptographic Techniques CRYPTO 1984: Advances in Cryptology.* 1985; 196: 19-36.

[2] Myasnikov A, Shpilrain V, Ushakov A. Group-based cryptography. *Advanced Courses in Mathematics-CRM Barcelona*. 2007. Available from: doi:10.1007/978-3-7643-8827-0.

[3] Birget JC, Magliveras SS, Sramka M. On public key cryptosystems based on combinatorial group theory. *Tatra Mountains Mathematical Publications*. 2006; 33: 137-148.

[4] Anshel I, Anshel M, Goldfeld D. An algebraic method for public-key cryptography. *Mathematical Research Letters*. 1999; 6: 287-291.

[5] Ko KH, Lee SJ, Cheon JH, Han JH, Kang JS, Park C. New public-key cryptosystem using braid groups. *CRYPTO'00 Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology*. 2000. p.166-183. Available from: doi:10.1007/3-540-44598-6_10.

[6] Kubo, J. The dihedral group as a family group. *Quantum Field Theory and Beyond.* World Science Publication; 2008. p.46-63. Available from: doi:10.1142/9789812833556_0004.

[7] Cha JC, Ko KH, Lee SJ, Han JW, Cheon JH. An efficient implementation of braid groups. *Lecture Notes in Computer Science*. 2001; 2248: 144-156. Available from: doi:10.1007/3-540-45682-1_9.

[8] Anshel I, Anshel M, Goldfeld D. Non-abelian key agreement protocols. *Discrete Applied Mathematics*. 2003; 130(1): 3-12.

[9] Dehornoy P. Braid-based cryptography. *AMS eBooks: Contemporary Mathematics*. 2004; 360: 1-29.

[10] Anshel I, Anshel M, Goldfeld D. A linear time matrix key agreement protocol over small finite fields. *Applicable Algebra in Engineering, Communication and Computing.* 2006; 17: 195-203.

[11] Paeng SH, Ha KC, Kim JH, Chee S, Park C. New public key cryptosystem using finite non abelian groups. *Advances in Cryptology-CRYPTO of Lecture Notes in Computer Science*. 2001. p.470-485.

[12] Magliveras SS, Stinson DR, Trung TV. New approaches to designing public key cryp-tosystems using one way functions and trapdoors infinite groups. *Journal of Cryptology*. 2002; 15: 285-297.

[13] Grigoriev D, Ponomarenko I. On non-Abelian homomorphic public-key cryptosystems. *Journal of Mathematical Sciences*. 2002; 126: 1158-1166.

[14] Grigoriev D, Ponomarenko I. *Homomorphic public-key cryptosystems over groups and rings*. 2001. Available from: https://arxiv.org/abs/cs/0309010v1.

[15] Shpilrain V, Ushakov A. Thompsons group and public key cryptography. *ACNS'05 Proceedings of the Third international conference on Applied Cryptography and Network Security.* 2005. p.151-163.

[16] Cao Z, Dong X, Wang L. New public key cryptosystems using polynomials over noncommutative rings. *Journal of Cryptology-IACR*. 2007; 9: 1-35.

[17] Reddy V, Gsgn A, Reddy VR, Mokkala P. New digital signature scheme using polynomials over noncommutative groups. *International Journal of Computer Science and Network Security*. 2008; 8: 245-250.

[18] Moldovyan DN, Moldovyan NA. A new hard problem over noncommutative finite groups for cryptographic protocols. *Computer Network Security: 5th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security, MMM-ACNS 2010, St. Petersburg, Russia, September 8-10, 2010. Proceedings, vol. 6258 of Lecture Notes in Com-puter Science*. 2010. p.183-194.

[19] Inam S, Kanwal S, Zahid A, Abid M. A novel public key cryptosystem and digital signatures. *European Journal of*

Engineering Science and Technology. 2020; 3: 22-30. Available from: https://doi.org/10.33422/ejest.v3i1.157.
[20] Kanwal S, Ali R. A cryptosystem with noncommutative platform groups. *Neural Computing and Applications*. 2018; 29: 1273-1278.
[21] Rososhek SK. Cryptosystems in automorphism groups of grouprings of abelian groups. *Fundamentalnaya i Prikladnaya Matematika*. 2007; 13: 157-164.
[22] Rososhek SK. Cryptosystems in automorphism groups of grouprings of abelian groups. *Journal of Mathematical Sciences*. 2008; 154: 386-391. Available from: doi:10.1007/s10958-008-9168-2.
[23] Kahrobaei D, Koupparis C, Shpilrain V. A CCA secure cryptosystem using matrices over groupring. *American Mathematical Society*. 2015; 633: 73-80. Available from: doi:http://dx.doi.org/10.1090/conm/633.
[24] Charalambos M, Koupparis C. Non-commutative cryptography: Diffie Hellman and CCA secure cryptosystems using matrices over group rings and digital signatures. Pro Quest LLC, Ann Arbor, Thesis (Ph.D), City University of New York. 2012.
[25] Inam S, Ali R. A new ElGamal-like cryptosystem based on matrices over groupring. *Neural Computing and Applications*. 2018; 29: 1279-1283.
[26] Mittal G, Kumar S, Narain S, Kumar S. Jan 2020 group ring based public key cryptosystems. *ArXiv* [Preprint]. 2020. Available from: https://arxiv.org/abs/1909.07262 [Accessed 10th July 2020].