Research Article

Atul Pandey*, Indivar Gupta, and Dhiraj Kumar Singh

Improved cryptanalysis of a ElGamal Cryptosystem Based on Matrices Over Group Rings

https://doi.org/10.1515/jmc-2019-0054
Received Oct 24, 2019; accepted Sep 08, 2020

Abstract: ElGamal cryptosystem has emerged as one of the most important construction in Public Key Cryptography (PKC) since Diffie-Hellman key exchange protocol was proposed. However, public key schemes which are based on number theoretic problems such as discrete logarithm problem (DLP) are at risk because of the evolution of quantum computers. As a result, other non-number theoretic alternatives are a dire need of entire cryptographic community.
In 2016, Saba Inam and Rashid Ali proposed a ElGamal-like cryptosystem based on matrices over group rings in 'Neural Computing & Applications'. Using linear algebra approach, Jia et al. provided a cryptanalysis for the cryptosystem in 2019 and claimed that their attack could recover all the equivalent keys. However, this is not the case and we have improved their cryptanalysis approach and derived all equivalent key pairs that can be used to totally break the ElGamal-like cryptosystem proposed by Saba and Rashid. Using the decomposition of matrices over group rings to larger size matrices over rings, we have made the cryptanalysing algorithm more practical and efficient. We have also proved that the ElGamal cryptosystem proposed by Saba and Rashid does not achieve the security of IND-CPA and IND-CCA.

Keywords: Group ring decomposition; ElGamal cryptosystem; circulant matrices

2020 Mathematics Subject Classification: 94A60

1 Introduction

The security of ElGamal encryption scheme depends on the difficulty of solving the discrete logarithm problem. The standard security notion for ElGamal encryption scheme is indistinguishability under a chosen plaintext attack (IND-CPA) whereas a stronger notion of security is indistinguishability under a chosen ciphertext attack (IND-CCA).

Due to the inability of resisting quantum attacks, various traditional cryptosystem based on DLP are not considered secure and there has been interest in constructing ElGamal encryption scheme via non-number theoretic platform structures. In this context, Majid Khan et al. [6] proposed two new ElGamal public key encryption schemes based on the large commutative subgroups of general linear groups on the residual ring which was later cryptanalyzed by Jia et al. [4] using structural attack.

In 2016, Inam and Ali improved it [3] and proposed a new ElGamal-like cryptosystem based on matrices over group ring. The authors claimed that the cryptosystem is safe against known plaintext attacks and has the potential to resist quantum attacks. But using a linear algebra attack, this proposed cryptosystem was

***Corresponding Author: Atul Pandey:** Department of Mathematics, University of Delhi, Delhi-110007, India; Email: pandeyatul_ap@yahoo.com
Indivar Gupta: SAG, Metcalfe House, DRDO Complex, Delhi-110054, India
Dhiraj Kumar Singh: Zakir Husain College, University of Delhi, Delhi-110002, India

rendered insecure in [5] where the authors also claimed that they could retrieve all the equivalent keys which can be used for decryption. Inam and Ali also provided a simple fix for their cryptosystem which they claimed that it has the ability to defend chosen ciphertext attacks.

Our Contribution: In this paper, we have proved that the ElGamal cryptosystem proposed by Saba and Rashid does not achieve the security of IND-CPA and IND-CCA which makes the cryptosystem completely insecure. We have developed a cryptanalytic attack and derived all equivalent keys (including the keys generated by authors in [5]) that can be used to totally break the ElGamal-like cryptosystem by Saba and Rashid. We have decomposed group ring elements to matrices over base ring and it makes the proposed cryptanalytic algorithm more efficient and practical.

The rest of this article is organized as follows. The second section provides necessary background for this work. In section 3, we present the ElGamal-like cryptosystem proposed by Saba Inam and Rashid Ali. In section 4 and 5, we prove that the proposed scheme is not secure against IND-CPA and IND-CCA adversary. In section 6, we develop a stronger attack which derives all the equivalent keys for the proposed cryptosystem. We also discuss the computational complexity of the scheme. Conclusions are finally drawn in section 7.

2 Preliminaries

Definition 1 (*Group Ring*). *: Let R be a Commutative ring with unity and $G = \{g_1, g_2, \cdots, g_k\}$ be a finite multiplicative group. The group ring consist of all finite sums of the form*

$$p = \sum_{g \in G} \alpha_g g$$

where $\alpha_g \in R$ and is denoted by GR. Let $q = \sum_{g\in G} \beta_g g$ and $r = \sum_{h\in G} \gamma_h h$ be elements of GR, then the addition and multiplication is defined as follows:

$$p + q = \left(\sum_{g\in G} \alpha_g g\right) + \left(\sum_{g\in G} \beta_g g\right) = \sum_{g\in G} (\alpha_g + \beta_g) g$$

and

$$pr = \left(\sum_{g\in G} \alpha_g g\right)\left(\sum_{h\in G} \gamma_h h\right) = \sum_{g,h\in G} \alpha_g \gamma_h (gh) = \sum_{t\in G} \eta_t t$$

where $gh = t$ and

$$\eta_t = \sum_{gh=t} \alpha_g \gamma_h = \sum_{g} \alpha_g \gamma_{g^{-1}t} = \sum_{h} \alpha_{th^{-1}} \gamma_h.$$

Remark 1. *[Decomposition of group ring] Corresponding to every element $p = \sum_{g\in G} \alpha_g g \in GR$, we can define a matrix $M_p \in M_k(R)$ as*

$$M_p = \begin{bmatrix} \alpha_{g_1 g_1^{-1}} & \alpha_{g_1 g_2^{-1}} & \dots & \alpha_{g_1 g_k^{-1}} \\ \alpha_{g_2 g_1^{-1}} & \alpha_{g_2 g_2^{-1}} & \dots & \alpha_{g_2 g_k^{-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{g_k g_1^{-1}} & \alpha_{g_k g_2^{-1}} & \dots & \alpha_{g_1 g_k^{-1}} \end{bmatrix}$$

which clearly has k entries $\alpha_{g_1}, \alpha_{g_2}, \cdots, \alpha_{g_k}$ in row 1 in some order and rest all other entries are permutation of this row. Thus for each $p \in GR$, the associated matrix M_p can be defined by only k unknowns $\alpha_{g_1}, \alpha_{g_2}, \cdots, \alpha_{g_k}$ and their permutations. Thus, for any matrix $A \in M_n(GR)$, say,

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$$

we can define a corresponding matrix $\overline{A} \in M_{nk}(R)$ *as*

$$\overline{A} = \begin{bmatrix} M_{a_{11}} & M_{a_{12}} & \dots & M_{a_{1n}} \\ M_{a_{21}} & M_{a_{22}} & \dots & M_{a_{2n}} \\ \vdots & \vdots & \ddots & \vdots \\ M_{a_{n1}} & M_{a_{n2}} & \dots & M_{a_{nn}} \end{bmatrix}$$

where $M_{a_{ij}}$ *are* $k \times k$ *matrices corresponding to the elements* $a_{ij} \in GR$*. The previous remark and computations are summarized in Theorem 1.*

Theorem 1. *For a finite group G with k elements and a commutative ring R with unity,* $M_n(GR)$ *can be embedded in* $M_{nk}(R)$ *via the map* $\phi : A \mapsto \overline{A}$ *[9].*

Theorem 2. *For a matrix* $A \in M_n(GR)$*, we have [8]*

$$A \in GL_n(GR) \iff \phi(A) = \overline{A} \in GL_{nk}(R).$$

Definition 2 (Circulant matrices and their properties [1])**.** *let F be a finite field. We define a* $k \times k$ *circulant matrix C over F as*

$$C = circ(c_1, c_2, \dots, c_k) = \begin{bmatrix} c_1 & c_2 & \dots & c_k \\ c_k & c_1 & \dots & c_{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_2 & c_3 & \dots & c_1 \end{bmatrix}$$

where the elements of each row of C are identical to those of the previous row, but are moved one position to the right and wrapped around.

Circulant matrices have the following important properties:

(i) If A and B are two $n \times n$ circulant matrices then so is AB and the matrix product is commutative, that is,

$$AB = BA$$

(ii) If A is circulant matrix, A^{-1} is also circulant (provided it exists).

Corollary 1. *Using Theorem* 1*, for any circulant matrix* $C \in M_n(GR)$ *we have a corresponding block circulant matrix* $\overline{C} \in M_{nk}(R)$ *defined by*

$$\overline{C} = \begin{bmatrix} M_{a_1} & M_{a_2} & \dots & M_{a_n} \\ M_{a_n} & M_{a_1} & \dots & M_{a_{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ M_{a_2} & M_{a_3} & \dots & M_{a_1} \end{bmatrix}_{nk \times nk}$$

which can be defined clearly by nk *elements only of the first row of all* M_{a_i}*.*

3 Description of the public key cryptosystem

In this section, we describe the ElGamal-like cryptosystem proposed by Saba Inam and Rashid Ali [3].

Let $M_n(GR)$ be the set of all $n \times n$ matrices over the group ring GR and $\mathsf{H} \subset M_n(GR)$ be the subgroup of all $n \times n$ invertible circulant matrices over GR. Bob and Alice communicate in the following steps.

Key generation (KeyGen):

(i) Alice Choose random $A, B \in \mathsf{H}$ and compute

$$M_1 = AB^2, M_2 = BA^2$$

(ii) Select a random invertible matrix $N \in GL_n(GR)$ and generate the key pairs (pk, sk) given by

$$pk = (P_1, P_2) = (M_1^{-1}NM_1, M_2^{-1}N^{-1}M_2) \text{ and } sk = (A, B)$$

where pk is public key and sk is secret key.

Encryption ($\mathbf{Enc_{pk}(m)}$):

(i) Bob represents the message m as an element $M \in M_n(GR)$.

(ii) Choose a random invertible matrix $X \in \mathsf{H}$ and η, a unit of the group ring GR and compute the ciphertext as $\mathbf{Enc_{pk}(m)} = \mathbf{C} = (C_1, C_2)$, where

$$C_1 = \eta^{-1}X^{-1}P_2X \text{ and } C_2 = \eta MX^{-1}P_1X.$$

Decryption ($\mathbf{Dec_{sk}(C)}$):

(i) Using her secret keys A, B Alice computes

$$S = AB^{-1}C_1BA^{-1}.$$

(ii) She obtains the message using C_2 and S as

$$C_2S = M$$

Thus, $\mathbf{Dec_{sk}(C)} = M$

Correctness of the protocol: Since $S = AB^{-1}C_1BA^{-1}$, we have

$$\begin{aligned} S &= AB^{-1}\eta^{-1}X^{-1}P_2XBA^{-1} \\ &= \eta^{-1}AB^{-1}X^{-1}M_2^{-1}N^{-1}M_2XBA^{-1} \\ &= \eta^{-1}AB^{-1}X^{-1}A^{-2}B^{-1}N^{-1}BA^2XBA^{-1} \\ &= \eta^{-1}A^{-1}B^{-2}X^{-1}N^{-1}XB^2A \end{aligned}$$

and hence

$$\begin{aligned} C_2S &= \eta MX^{-1}P_1X\eta^{-1}A^{-1}B^{-2}X^{-1}N^{-1}XB^2A \\ &= MX^{-1}M_1^{-1}NM_1XA^{-1}B^{-2}X^{-1}N^{-1}XB^2A \\ &= MX^{-1}B^{-2}A^{-1}NAB^2XA^{-1}B^{-2}X^{-1}N^{-1}XB^2A \\ &= MX^{-1}B^{-2}A^{-1}NXX^{-1}N^{-1}B^2AX \\ &= MX^{-1}B^{-2}A^{-1}B^2AX \\ &= MX^{-1}X \\ &= M \end{aligned}$$

Remark 2. *The authors in [3] have used the commutative circulant matrices over the group ring GR, where R is a commutative ring with unity and G is a finite group. We believe that the authors wanted the group G to be an abelian group, otherwise the circulant matrices will not commute and the proposed cryptosystem will not work. Hence from now onwards we assume that G is a finite abelian group.*

4 Analysis of IND-CPA security of the cryptosystem

Consider the following IND-CPA experiment with the challenger $\mathcal{C}$ and and efficient adversary $\mathcal{A}$:

(i) Challenger $\mathcal{C}$ generates the key pair (pk, sk) and publishes $pk = (P_1, P_2) = (M_1^{-1}NM_1, M_2^{-1}N^{-1}M_2)$ to the adversary $\mathcal{A}$.
(ii) Adversary $\mathcal{A}$ chooses $D_0, D_1 \leftarrow M_n(GR)$ and submits these to $\mathcal{C}$.
(iii) Challenger $\mathcal{C}$ selects a bit $b \leftarrow \{0, 1\}$ uniformly at random and sends the challenge ciphertext

$$\mathbf{C} = (C_1, C_2) = (\eta^{-1}X^{-1}P_2X, \eta D_b X^{-1}P_1X)$$

to the adversary $\mathcal{A}$.
(iv) The adversary $\mathcal{A}$ outputs a bit b'.

The adversary is successful in the above experiment and outputs 1 if and only if $b = b^{'}$

In step two, if the adversary $\mathcal{A}$ chooses two messages D_0 and D_1 such that $det(D_0) \neq det(D_1)$, then it can compute

$$\frac{det(C_1C_2)}{det(P_1P_2)} = \frac{det(\eta^{-1}X^{-1}P_2X\eta D_bX^{-1}P_1X)}{det(P_1P_2)} = det(D_b)$$

and if

$$\frac{det(C_1C_2)}{det(P_1P_2)} = det(D_0) \quad \mathcal{A} \text{ outputs } b' = 0$$

otherwise $\mathcal{A}$ outputs $b' = 1$. Thus the adversary $\mathcal{A}$ succeeds in the above IND-CPA security experiment with probability 1. Hence the proposed scheme is not secure against a chosen plaintext attack.

5 Analysis of IND-CCA security of the cryptosystem

The authors in [3] have presented a chosen cipher text attack for their scheme and they proposed a fix where they replace the one sided ciphertext with the two sided ciphertext as follows:

$$\mathbf{C} = (C_1, C_2) \quad \text{where}$$
$$C_1 = \eta^{-1}X^{-1}P_2X \text{ and } C_2 = \eta^2X^{-1}P_1XMX^{-1}P_1X$$

Consider the following IND-CPA experiment with the challenger $\mathcal{C}$ and and efficient adversary $\mathcal{A}$:

(i) Challenger $\mathcal{C}$ generates the key pair (pk, sk) and publishes $pk = (P_1, P_2) = (M_1^{-1}NM_1, M_2^{-1}N^{-1}M_2)$ to the adversary $\mathcal{A}$.
(ii) Adversary $\mathcal{A}$ has access to a decryption oracle $\mathtt{Dec}_{sk}(.)$. Adversary $\mathcal{A}$ chooses $D_0, D_1 \leftarrow M_n(GR)$ and submits these to $\mathcal{C}$.
(iii) Challenger $\mathcal{C}$ selects a bit $b \leftarrow \{0, 1\}$ uniformly at random and sends the challenge ciphertext

$$\mathbf{C} = (C_1, C_2) = (\eta^{-1}X^{-1}P_2X, \eta^2X^{-1}P_1XMX^{-1}P_1X)$$

to the adversary $\mathcal{A}$.
(iv) A continues to query the decryption oracle except for the challenge ciphertext $\mathbf{C}$.
(v) The adversary $\mathcal{A}$ outputs a bit b'.

The adversary is successful in the above experiment and outputs 1 if and only if $b = b^{'}$

In step two, if the adversary $\mathcal{A}$ chooses two messages D_0 and D_1 such that $det(D_0) \neq det(D_1)$, then it can compute

$$\frac{det(C_1^2C_2)}{det(P_1^2P_2^2)} = \frac{det(\eta^{-2}X^{-1}P_2^2X\eta^2X^{-1}P_1XD_bX^{-1}P_1X)}{det(P_1^2P_2^2)} = det(D_b)$$

and if

$$\frac{det(C_1^2 C_2)}{det(P_1^2 P_2^2)} = det(D_0) \;\; \mathcal{A} \text{ outputs } b' = 0$$

otherwise $\mathcal{A}$ outputs $b' = 1$. Thus the adversary $\mathcal{A}$ succeeds in the above IND-CCA security experiment with probability 1.

Additionally, an adversary can decrypt any plaintext M by playing the following game with the challenger:

Adversary $\mathcal{A}$		Challenger $\mathcal{C}$
$M^\star = dI_n (d \neq 1 \text{ is unit in } GR) \leftarrow M_n(GR)$		
		$M \leftarrow M_n(GR)$
	$\xleftarrow{\mathbf{C}}$	$\mathbf{C} = (C_1, C_2) \leftarrow \mathbf{Enc_{pk}}(\mathbf{M})$
$(C_1, M^\star C_2) = \mathbf{C}^\star \neq \mathbf{C}$	$\xrightarrow{\mathbf{C}^\star}$	
	$\xleftarrow{M^\star M}$	$M^\star M \leftarrow \mathbf{Dec_{sk}}(\mathbf{C}^\star)$
$M = (M^\star)^{-1} M^\star M$		

Hence the proposed fix for the scheme is not secure against a chosen ciphertext attack as claimed by authors in [3].

6 Key recovery attack

In this section, we propose a method where we generate all the equivalent key pairs for the cryptosystem in [3] from the public key pk only.

From the public information any adversary $\mathcal{A}$ has the ability to get the public keys $pk = (P_1, P_2)$. $\mathcal{A}$ find a solution of the following system to obtain all equivalent key pairs (P, Q).

– Choose arbitrary circulant matrices P and Q and hence

$$PX = XP \text{ and } QX = XQ$$

– P and Q satisfies

$$PP_2Q = P_1^{-1} \tag{1}$$

The above system has atleast a solution namely $P = AB^{-1}$ and $Q = A^{-1}B$ as

$$\begin{aligned} PP_2Q &= PM_2^{-1}N^{-1}M_2Q \\ &= PA^{-2}B^{-1}N^{-1}BA^2Q \\ &= AB^{-1}A^{-2}B^{-1}N^{-1}BA^2A^{-1}B \\ &= A^{-1}B^{-2}N^{-1}B^2A \\ &= B^{-2}A^{-1}N^{-1}AB^2 \\ &= M_1^{-1}N^{-1}M_1 \\ &= P_1^{-1} \end{aligned}$$

Theorem 3. *If the adversary is able to find a solution P, Q to the equation (1), then the ElGamal-like cryptosystem proposed by Saba and Rashid is completey broken with equivalent keys P, Q.*

Proof. Using the equivalent keys P and Q, plaintext M can be retrieved from a ciphertext pair (C_1, C_2) as

$$\begin{aligned} C_2PC_1Q &= \eta MX^{-1}P_1XP\eta^{-1}X^{-1}P_2XQ \\ &= \eta\eta^{-1}MX^{-1}P_1PP_2QX \\ &= MX^{-1}X \\ &= M \end{aligned}$$

□

Thus, the proposed scheme is not secure and a total break of the scheme is performed where equivalent key pairs (P, Q) are computed from the public key pair (P_1, P_2).

In Example 1 in appendix, we derive all the equivalent key pairs (P, Q) for the toy example provided in [3] and obtain the plaintext M.

Remark 3. *Out of* 16 *choices for the solution set in appendix, 8 are non-invertible and remaining* 8 *invertible choices are listed in Example* 1. *Equations A4-A7 are solutions to equation 1 which satisfy* $P = Q^{-1}$ *and these solutions can also be recovered by the method of cryptanalysis of Jia et al. They claim that they can obtain all equivalent keys by their cryptanalysis but their method only allows them to obtain those equivalent key pairs* (P, Q) *which satisfies* $P = Q^{-1}$ *in equation 1. But our cryptanlysis is more of a generic kind and it allows us to obtain all the equivalent key pairs* (P, Q) *which can be used along with Theorem 3 to retrieve the plaintext* M.

6.1 Algorithm for deriving the private keys and decrypting ciphertexts

Remark 4. *Equation 1 can be rewritten as*

$$PP_2 - P_1^{-1}Q^{-1} = 0$$

and then using the Theorem 1 we can embed P, P_1, P_2 *and* Q *in* $M_{nk}(R)$ *and rewrite the corresponding equation as*

$$\overline{P}\,\overline{P}_2 - \overline{P}_1^{-1}\overline{Q}^{-1} = 0 \tag{2}$$

which is a system of n^2k^2 *linear equations in* $2nk$ *unknowns over the commutative ring* R *and it can further be written as*

$$AX = 0 \tag{3}$$

where $A \in M_{n^2k^2\times 2nk}(R)$ *and* $X \in M_{2nk\times 1}(R)$ *is the unknwon vector.*

Algorithm 1 Generating equivalent key pairs and retrieving plaintext

Step 1: Input public information (P_1, P_2, C_1, C_2)

Step 2: Choose random elements $(a_1, a_2, \cdots, a_n), (b_1, b_2, \cdots, b_n) \in GR^n$ and form corresponding circulant matrices P and Q^{-1} respectively.

Step 3: Using the embedding of Theorem 1 obtain the matrices $\overline{P}$, $\overline{Q}^{-1}$, $\overline{P_1}$, $\overline{P_2}$, $\overline{C_1}$ and $\overline{C_2}$.

Step 4: Solve for a system of equations over ring R

$$\overline{P}\,\overline{P}_2 - \overline{P}_1^{-1}\overline{Q}^{-1} = 0$$

using equation 3 and formulate the invertible matrices $\overline{P}$ and $\overline{Q}^{-1}$.

Step 5: Find a_i and b_j using $\overline{P}$, $\overline{Q}^{-1}$ and formulate key pairs P, Q.

Step 6: Compute $M = C_2PC_1Q$

In example 2 in appendix, we execute our proposed algorithm to cryptanalyze the toy example provided in [3]. We decompose the elements of group ring to matrices over same ring and use it to obtain equivalent key pairs and the corresponding plaintext from the given public key pairs and ciphertext.

6.2 Computational complexity of the proposed algorithm over finite field $\mathbb{F}_p$

In this section, we compute the complexity of Algorithm 1 where the commutative ring R is a prime field, that is, $R = \mathbb{F}_p$.

- The number of bit operations required to compute product of two $m \times m$ matrices is $\mathcal{O}(m^\omega)$, where $\omega \approx 2.3755$.
- Inverse of a $m \times m$ matrix can be found using complexity $\mathcal{O}(m^\omega)$.
- Inverses in finite field $\mathbb{F}_p$ can be computed using $(\log p)^3$ bit operations [7].
- Solving a system of p equation in r unknowns over $\mathbb{Z}_n$ has complexity [11] of $\mathcal{O}(pr^{\omega-1})$.

Using above complexity results, we have the following complexity:

(i) The embedding in step 3 is nothing but the rearrangement of the coefficients of the elements of the group ring GR and hence its complexity is neglected.

(ii) In step 4 we need to perform 2 matrix multiplications, 1 matrix inversion and 1 subtraction and then solve the system given in equation 3. Hence the complexity of step 3 is $\mathcal{O}((nk)^\omega(\log p)^3 + 2(nk)^\omega(\log p)^2 + (nk)^2(2nk)^{\omega-1}(\log p)^3) = \mathcal{O}((nk)^{\omega+1}(\log p)^3)$.

(iii) In step 5, the complexity of matrix inversion to find $\overline{Q}$ from $\overline{Q}^{-1}$ is $\mathcal{O}((nk)^\omega(\log p)^3)$. We then rearrange to obtain P and Q from $\overline{P}$ and $\overline{Q}$ respectively. .

(iv) Step 6 requires 3 matrix multiplications with complexity $\mathcal{O}((nk)^\omega(\log p)^2)$.

Thus the overall complexity of Algorithm 1 is $\mathcal{O}((nk)^{\omega+1}(\log p)^3)$, which is polynomial in the size of the entry of the matrices.

Remark 5. *Jia et al. have also computed the complexity of their attack which is not exactly correct as they have computed it over matrices over group rings but the complexity results of $\mathbb{Z}_n$ are used.*

7 Conclusion

We have presented a generic kind of cryptanalysis of a new ElGamal-like cryptosystem based on matrices over group ring. Though the author claimed that their cryptographic protocol seems to be resistant to known plaintext attacks, ciphertext only attacks and chosen plaintext attacks, we have proved that the proposed

scheme is not even secure against the weaker security notion IND-CPA and also against IND-CCA of ElGamal cryptosystem. We then designed a strong linear algebra attack which requires polynomial time to compute all the equivalent keys for a given public key pair.

Acknowledgement

This research is supported by University Grants Commission (UGC), reference number-1100 (DEC-2016).

References

[1] P. J. Davis, *Circulant matrices*, Chelsea (1994).
[2] T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Trans Inf Theory 31, (1985), 469–472.
[3] S. Inam and R. Ali, *A new ElGamal-like cryptosystem based on matrices over group ring*, Neural Comput. Appl. 29(11), (2018), 1279–1283.
[4] J. Jia, J. Liu and H. Zhang, *Cryptanalysis of cryptosystems based on general linear group*, China Commun. 13(6), (2016), 217–224.
[5] J. Jia, H. Wang, H. Zhang, S. Wang and J. Liu, *Cryptanalysis of an ElGamal-Like Cryptosystem Based on Matrices Over Group Rings*, In: Zhang H., Zhao B., Yan F. (eds) Trusted Computing and Information Security. CTCIS 2018. Communications in Computer and Information Science, vol 960. Springer, Singapore (2019).
[6] M. Khan and T. Shah, *A novel cryptosystem based on general linear group*, 3D Res. 6(1), (2015), 1–8.
[7] N. Koblitz, *A course in Number Theory and Cryptography*, 2nd edn. springer, New York (1994).
[8] M. Kreuzer, A. D. Myasnikov and A. Ushakov, *A linear algebra attack to group-ring-based key exchange protocols*, Applied Cryptography and Network Security (ACNS 2014), Lecture Notes in Comput. Sci. 8479, Springer, Berlin, (2014), 37–43.
[9] A. D. Myasnikov and A. Ushakov: *Quantum algorithm for the discrete logarithm problem for matrices over finite group rings*, Groups, Complexity, Cryptology 6, (2014), 31–36.
[10] D. S. Passman, *The Algebraic structure of Group Ring*, Wiley, New York (1977).
[11] A. Storjohann and T. Mulders, *Fast algorithms for linear algebra modulo N.*, Proceedings of Algorithms—ESA'98. Springer Berlin Heidelberg, 1461, (1998), 139-150.

Appendix

Example 1. *Consider the ring* $R = \mathbb{Z}_2 = \{0, 1\}$ *and the cyclic group* $G = C_2 = \{1, y\} = \langle y \rangle$*, then the group ring is defined as*

$$GR = \left\{ \sum_{g \in C_2} a_g g : a_g \in R \right\} = \{0, 1, y, 1 + y\}$$

The addition and multiplication table for the group ring GR are provided in Table A1 and Table A2 respectively:

Table A1: Addition table for group ring

+	0	1	y	1+y
0	0	1	y	1+y
1	1	0	1+y	y
y	y	1+y	0	1
1+y	1+y	y	1	0

Table A2: Multiplication table for group ring

·	0	1	y	1+y
0	0	0	0	0
1	0	1	y	1+y
y	0	y	1	1+y
1+y	0	1+y	1+y	0

In the 2×2 *matrix semi group* $M_2(GR)$*, consider the public key elements*

$$P_1 = \begin{bmatrix} 1 & 0 \\ 1+y & y \end{bmatrix} \text{ and } P_2 = \begin{bmatrix} 1 & 0 \\ 1+y & y \end{bmatrix}$$

and for some plaintext M, the ciphertext pair (C_1, C_2) *given by*

$$C_1 = \begin{bmatrix} y & 0 \\ 1+y & 1 \end{bmatrix} \text{ and } C_2 = \begin{bmatrix} y & 1 \\ 1 & y \end{bmatrix}$$

Suppose P and Q^{-1} *be arbitrary invertible circulant matrices with elements in GR, then*

$$P = \begin{bmatrix} a & b \\ b & a \end{bmatrix} \text{ and } Q^{-1} = \begin{bmatrix} c & d \\ d & c \end{bmatrix}$$

and $PP_2Q = P_1^{-1}$ *can be written as*

$$PP_2 = P_1^{-1}Q^{-1}$$

which implies

$$\begin{bmatrix} a & b \\ b & a \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1+y & y \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1+y & y \end{bmatrix} \begin{bmatrix} c & d \\ d & c \end{bmatrix}$$

which results in the following system of 4 *linear equations in* 4 *variables* a, b, c *and* d.

$$\begin{aligned} a + b(1+y) + c &= 0 \\ yb + d &= 0 \\ a(1+y) + b + (1+y)c + yd &= 0 \\ ay + cy + d(1+y) &= 0 \end{aligned}$$

which can further be written as

$$\begin{aligned} c &= a + b(1+y) \\ d &= by \end{aligned}$$

where a, b *are free parameters. Hence, a solution to the above system is given by*

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \left\{ s \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + t \begin{pmatrix} 0 \\ 1 \\ 1+y \\ y \end{pmatrix} \middle| s, t \in GR \right\}$$

The following are the invertible key pairs obtained by these solutions

$$P_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } Q_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{A4}$$

$$P_2 = \begin{bmatrix} y & 0 \\ 0 & y \end{bmatrix} \text{ and } Q_2 = \begin{bmatrix} y & 0 \\ 0 & y \end{bmatrix} \tag{A5}$$

$$P_3 = \begin{bmatrix} 1 & 1+y \\ 1+y & 1 \end{bmatrix} \text{ and } Q_3 = \begin{bmatrix} 1 & 1+y \\ 1+y & 1 \end{bmatrix} \tag{A6}$$

$$P_4 = \begin{bmatrix} y & 1+y \\ 1+y & y \end{bmatrix} \text{ and } Q_4 = \begin{bmatrix} y & 1+y \\ 1+y & y \end{bmatrix} \tag{A7}$$

$$P_5 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } Q_5 = \begin{bmatrix} 1+y & y \\ y & 1+y \end{bmatrix} \tag{A8}$$

$$P_6 = \begin{bmatrix} 0 & y \\ y & 0 \end{bmatrix} \text{ and } Q_6 = \begin{bmatrix} 1+y & 1 \\ 1 & 1+y \end{bmatrix} \tag{A9}$$

$$P_7 = \begin{bmatrix} 1+y & y \\ y & 1+y \end{bmatrix} \text{ and } Q_7 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{A10}$$

$$P_8 = \begin{bmatrix} 1+y & 1 \\ 1 & 1+y \end{bmatrix} \text{ and } Q_8 = \begin{bmatrix} 0 & y \\ y & 0 \end{bmatrix} \tag{A11}$$

Using any of these possible pairs, say

$$P = \begin{bmatrix} 0 & y \\ y & 0 \end{bmatrix} \text{ and } Q = \begin{bmatrix} 1+y & 1 \\ 1 & 1+y \end{bmatrix}$$

we can obtain the plaintext M *as*

$$\begin{aligned} C_2PC_1Q &= \begin{bmatrix} y & 1 \\ 1 & y \end{bmatrix} \begin{bmatrix} 0 & y \\ y & 0 \end{bmatrix} \begin{bmatrix} y & 0 \\ 1+y & 1 \end{bmatrix} \begin{bmatrix} 1+y & 1 \\ 1 & 1+y \end{bmatrix} \\ &= \begin{bmatrix} y & 1 \\ 1 & y \end{bmatrix} \begin{bmatrix} 1+y & y \\ 1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} y & 1 \\ 1 & y \end{bmatrix} \\ &= M \end{aligned}$$

which is the original plaintext which was encrypted in toy example in [3].

Example 2. *Consider the ring* $R = \mathbb{Z}_2 = \{0, 1\}$ *and the cyclic group* $G = C_2 = \{g_1 = 1, g_2 = y\} = \langle y \rangle$*, then the group ring is defined as*

$$GR = \left\{ \sum_{g \in C_2} a_g g : a_g \in R \right\} = \{0, 1, y, 1 + y\}$$

Also, $g_1 g_1^{-1} = 1 = g_1, g_1 g_2^{-1} = y = g_2$ *and* $g_2 g_1^{-1} = y = g_2, g_2 g_2^{-1} = 1 = g_1$*. Then the embedding of the group ring elements are given by*

$$0 \leftrightarrow \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad 1 \leftrightarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad y \leftrightarrow \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \quad 1 + y \leftrightarrow \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

Step 1: *Now consider the public key elements*

$$P_1 = \begin{bmatrix} 1 & 0 \\ 1 + y & y \end{bmatrix} \text{ and } P_2 = \begin{bmatrix} 1 & 0 \\ 1 + y & y \end{bmatrix}$$

and for some plaintext M*, the ciphertext pair* (C_1, C_2) *given by*

$$C_1 = \begin{bmatrix} y & 0 \\ 1 + y & 1 \end{bmatrix} \text{ and } C_2 = \begin{bmatrix} y & 1 \\ 1 & y \end{bmatrix}$$

Step 2: *Choose arbitrary* $(a, b), (c, d) \in GR^2$ *and form circulant matrices* P *and* Q^{-1} *as*

$$P = \begin{bmatrix} a = a_1 g_1 + a_2 g_2 & b = b_1 g_1 + b_2 g_2 \\ b = b_1 g_1 + b_2 g_2 & a = a_1 g_1 + a_2 g_2 \end{bmatrix}$$

and

$$Q^{-1} = \begin{bmatrix} c = c_1 g_1 + c_2 g_2 & d = d_1 g_1 + d_2 g_2 \\ d = d_1 g_1 + d_2 g_2 & c = c_1 g_1 + c_2 g_2 \end{bmatrix}$$

Step 3: *Then the embedded matrices are*

$$\overline{P} = \begin{bmatrix} a_1 & a_2 & b_1 & b_2 \\ a_2 & a_1 & b_2 & b_1 \\ b_1 & b_2 & a_1 & a_2 \\ b_2 & b_1 & a_2 & a_1 \end{bmatrix} \quad \overline{Q}^{-1} = \begin{bmatrix} c_1 & c_2 & d_1 & d_2 \\ c_2 & c_1 & d_2 & d_1 \\ d_1 & d_2 & c_1 & c_2 \\ d_2 & d_1 & c_2 & c_1 \end{bmatrix}$$

The embedded public key elements are given by

$$P_1 \leftrightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} = \overline{P_1} \quad P_2 \leftrightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} = \overline{P_2}$$

and the embedded ciphertext matrices are

$$C_1 \leftrightarrow \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} = \overline{C_1} \quad C_2 \leftrightarrow \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} = \overline{C_2}$$

Step 4: *The equation* $\overline{P}\,\overline{P}_2 - \overline{P}_1^{-1}\overline{Q}^{-1} = 0$ *can be written as*

$$\begin{bmatrix} a_1 + b_1 + b_2 - c_1 & a_2 + b_1 + b_2 - c_2 & b_2 - d_1 & b_1 - d_2 \\ a_2 + b_2 + b_1 - c_2 & a_1 + b_2 + b_1 - c_1 & b_1 - d_2 & b_2 - d_1 \\ b_1 + a_1 + a_2 - (c_1 + c_2 + d_2) & b_2 + a_1 + a_2 - (c_2 + c_1 + d_1) & a_2 - (d_1 + d_2 + c_2) & a_1 - (d_2 + d_1 + c_1) \\ b_2 + a_2 + a_1 - (c_1 + c_2 + d_1) & b_1 + a_2 + a_1 - (c_2 + c_1 + d_2) & a_1 - (d_1 + d_2 + c_1) & a_2 - (d_2 + d_1 + c_2) \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

This can be written as a new system of equations given by

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ b_1 \\ b_2 \\ c_1 \\ c_2 \\ d_1 \\ d_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

which is equivalent to

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ b_1 \\ b_2 \\ c_1 \\ c_2 \\ d_1 \\ d_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

which corresponds to the following system of equations

$$\begin{aligned} a_1 &= c_1 + d_1 + d_2 \\ a_2 &= c_2 + d_1 + d_2 \\ b_1 &= d_2 \\ b_2 &= d_1 \end{aligned}$$

Step 5: *Thus for different values of* $(c_1, c_2, d_1, d_2) \in \mathbb{Z}_2^4$ *we get 16 pairs of different matrices* $(\overline{P}, \overline{Q}^{-1})$. *The choices of tuple which makes the matrix Q invertible are:*

(i) $(1, 0, 0, 0)$*:*

$$\overline{Q} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \leftrightarrow Q_1 \quad \overline{P} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \leftrightarrow P_1$$

(ii) $(0, 1, 0, 0)$*:*

$$\overline{Q} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \leftrightarrow Q_2 \quad \overline{P} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \leftrightarrow P_2$$

(iii) $(1, 0, 1, 1)$*:*

$$\overline{Q} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} \leftrightarrow Q_3 \quad \overline{P} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} \leftrightarrow P_3$$

(iv) $(0, 1, 1, 1)$*:*

$$\overline{Q} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \leftrightarrow Q_4 \quad \overline{P} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \leftrightarrow P_4$$

(v) $(1, 1, 0, 1)$*:*

$$\overline{Q} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \leftrightarrow Q_5 \quad \overline{P} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \leftrightarrow P_5$$

(vi) $(1, 1, 1, 0)$*:*

$$\overline{Q} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \leftrightarrow Q_6 \quad \overline{P} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \leftrightarrow P_6$$

(vii) $(0, 0, 1, 0)$*:*

$$\overline{Q} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \leftrightarrow Q_7 \quad \overline{P} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \leftrightarrow P_7$$

(viii) $(0, 0, 0, 1)$*:*

$$\overline{Q} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \leftrightarrow Q_8 \quad \overline{P} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \leftrightarrow P_8$$

Hence the equivalent key pairs are given by $(\overline{P_i}, \overline{Q_i})$ *or* (P_1, Q_i), $1 \leq i \leq 8$ *which are exactly the same as extracted in Example* 1.

Step 6: *Using any of these possible pairs, say*

$$P = \begin{bmatrix} 0 & y \\ y & 0 \end{bmatrix} \text{ and } Q = \begin{bmatrix} 1+y & 1 \\ 1 & 1+y \end{bmatrix}$$

we can obtain the plaintext M as

$$\begin{aligned} C_2PC_1Q &= \begin{bmatrix} y & 1 \\ 1 & y \end{bmatrix} \begin{bmatrix} 0 & y \\ y & 0 \end{bmatrix} \begin{bmatrix} y & 0 \\ 1+y & 1 \end{bmatrix} \begin{bmatrix} 1+y & 1 \\ 1 & 1+y \end{bmatrix} \\ &= \begin{bmatrix} y & 1 \\ 1 & y \end{bmatrix} \begin{bmatrix} 1+y & y \\ 1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} y & 1 \\ 1 & y \end{bmatrix} \\ &= M \end{aligned}$$

which is the original plaintext which was encrypted in toy example in [3].