ADV MATH SCI JOURNAL

Advances in Mathematics: Scientific Journal **12** (2023), no.2, 357–366
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.12.2.4

A NEW PUBLIC KEY CRYPTOSYSTEM BASED ON GROUP RING

Sassia Makhlouf[1] and Kenza Guenda

ABSTRACT. In this paper, we propose a new public key cryptosystem in a non-commutative group over group ring, using a hard problem, Factorization with Discrete Logarithm Problem (FDLP). The security analysis of the proposed scheme is discussed and it is shown that the system is secure.

1. INTRODUCTION

The concept of public key cryptography was first introduced by Deffie and Hellman [3] in 1976. Several systems (PKC) were proposed, based on mathematical hard problems like discrete logarithm problem (DLP)and integer factorization problem (IFP). The most public key cryptosystems are as follows: the RSA cryptosystem, was intrduced in 1978 by Rivest, Shamir and Adelman [16] and its variants, and the Elgamal cryptosystem which was introduced in 1985 [6] and its variants. Many PKCs have been proposed using linear groups, non-commutative groups and rings [1, 2, 8, 10, 11, 14, 17]. Some properties of matrices have been used to develop attacks against schemes which use $GL_n(\mathbb{F}_q)$ [4,12,13]. in order to avoid such attacks, the authors in [7] introduced a new hard problem, Factorzation with Discrete Logarithm Problem (FDLP) over the non-commutative semigroup

[1] *corresponding author*

2020 *Mathematics Subject Classification.* 94A60, 11T71.

Key words and phrases. Encrypion, Decryption, Public key Cryptosystem, Group ring, General Linear Group.

Submitted: 11.01.2023; *Accepted:* 26.01.2023; *Published:* 06.02.2023.

$M_{k\times k}\left(\mathbb{F}_q\left[S_r\right]\right)$, this protocol resists the known attacks, also they proposed an Elgamal cryptosystem [6] over group ring which is based on FDLP, chosen ciphertext attack works on this protocol. We improve the above scheme PKC by proposing a new public key cryptosystem based on the FDLP in general linear group over group ring, the prime advantage of using $GL_n\left(\mathbb{F}_q\left[S_r\right]\right)$ is that the multiplication of matrices is very efficient [18] and the multiply and square algorithm can be used for exponentiation [9]. This group is resistant to attacks such as eigenvalue and determinant attacks [4]. This has been examinad in [9]. The security analysis of the proposed protocol has been provided.

The basic definitions are given in section 2. In section 3 we present the key exchange protocol and the Elgamal cryptosystem proposed in [7]. The proposed PKC; key generation, encryption and decryption is descriped in section 4, analysis is given in section 5. Finally, section 6 gives the conclusion.

2. Preliminaries

In this section, we give some definitions which will be helpful for later.

Definition 2.1 (Factorization with Discrete Logarithm Problem (FDLP)). *Let G be a finite non-abelian group of order n, and $\alpha, \beta \in G$, the factorization with discrete logarithm problem is to find two elements $t \in G$ and $s \in \mathbb{Z}$ such that $\alpha = \beta^s t$ [7].*

The security and complexity of the FDLP are provided in [7]. The well known attacks [4, 13] are not applicable to the FDLP.

Definition 2.2 (Group ring). *Let $\mathbb{F}$ be a field, and G be a group. Then the group ring $\mathbb{F}\left[G\right]$, is defined to be the set of all linear combinations*

$$\gamma = \sum_{g\in G} b_g g,$$

where $b_g \in \mathbb{F}$. The sum and the product in group ring are defined as follows:

$$\begin{aligned}\gamma + \delta &= \left(\textstyle\sum_{g\in G} b_g g\right) + \left(\textstyle\sum_{g\in G} c_g g\right)\\ &= \textstyle\sum_{g\in G}\left(b_g + c_g\right) g\end{aligned}$$

and

$$\begin{aligned}\gamma\sigma &= \left(\textstyle\sum_{g\in G} b_g g\right)\left(\textstyle\sum_{h\in G} d_h h\right)\\ &= \textstyle\sum_{g,h\in G} b_g d_h \,(gh)\\ &= \textstyle\sum_{u\in G} a_u u\end{aligned}$$

where $\delta = \sum_{g\in G} c_g g$, $\sigma = \sum_{h\in G} d_h h$,

$$gh = u$$

and

$$a_u = \textstyle\sum_{gh=u} b_g d_h.$$

For example, consider the group ring $\mathbb{F}_5\,[S_3]$ with identity e and let $a, b \in \mathbb{F}_5\,[S_3]$ such that

$$\begin{aligned} a &= 2\alpha + 4\beta,\\ b &= 3\alpha\beta + \alpha^2 + \beta.\end{aligned}$$

Here $S_3 = \langle \alpha, \beta \mid \alpha^3 = 1, \beta^2 = 1\rangle$. Then

$$\begin{aligned} a^2 &= 4\alpha^2 + \alpha\beta + 1,\\ a + b &= \alpha^2 + 3\alpha\beta + 2\alpha,\\ ab &= 2\alpha\beta + 2\alpha + 1.\end{aligned}$$

Consider $GL_2\,(\mathbb{F}_5\,[S_3])$, the group of 2×2 invertible matrices under matrix multiplication. let $A, B \in GL_2\,(\mathbb{F}_5\,[S_3])$ such that

$$A = \begin{pmatrix}\alpha & 0\\ a & 1\end{pmatrix},\ B = \begin{pmatrix} b & 1\\ 0 & b\end{pmatrix}.$$

Then

$$\begin{aligned} AB &= \begin{pmatrix}\alpha b & \alpha\\ ab & a+b\end{pmatrix}\\ &= \begin{pmatrix} 3\alpha^2\beta + \alpha\beta + 1 & \alpha\\ & \\ 2\alpha\beta + 2\alpha + 1 & \alpha^2 + 3\alpha\beta + 2\alpha\end{pmatrix},\end{aligned}$$

where ab and $a + b$ are given above.

For more details on group ring, the reader is referred to [15].

3. A Key Exchange Protocol Based on FDLP

In [7], the authors presented a key exchange protocol. The hard problem of the proposed protocol is the factorization with discrete logarithm problem (FDLP). Let G be a finite non-abelian group and H an abelian sub-group of G. Let $x \in G$ with very large order m and $C_G(x)$ the centralizer of x in G. The group G, H, x, and m are publicly known. The protocol is as follows:

(1) Alice chooses a random secret integer $a \in [2, m-1]$ and a secret element $y \in H \setminus C_G(x)$. She computes $w_1 = x^a y$ and sends it to Bob.
(2) Bob chooses a random secret integer $b \in [2, m-1]$ and a secret element $z \in H \setminus C_G(x)$. He computes $w_2 = x^b z$ and sends it to Alice.
(3) Alice calculates $k_A = x^a w_2 y$ as the shared secret key.
(4) Bob calculates $k_B = x^b w_1 z$ as the shared secret key.

Since $yz = zy$, then common secret key is $x^{a+b} yz$.

The security of this protocol is based on the hardness of the FDLP. The complexity and security analysis of the key exchange protocol are provided in [7], the following attacks were considered: attacks on the DLP and linear algebra, attacks using the decomposition of group rings [5] and attacks using the properties of matrices [4, 13]. The authors in [7] shown that for small sizes of q and r, the complexity is high.

The following is the original cryptosystem given in [7].

3.1. **Elgamal Public Key Cryptosystem.**

Suppose Bob wants to send a message to Alice using Elgamal cryptosystem [6] for encryption and decryption.

(1) Key generation: Alice selects $x \in GL_k(\mathbb{F}_q[S_r])$ of large order m and $y \in H \setminus C_G(x)$ and $a \in [2, m-1]$ and computes $w_1 = x^a y$. Then Alice's public key is $pk = (w_1, x)$ and secret key is $sk = (a, y)$.
(2) Encryption: To encrypte a message, Bob chooses a random secret integer $b \in [2, m-1]$ and a secret element $z \in H \setminus C_G(x)$. He computes $C_1 = x^b z$ and $C_2 = x^b w_1 z M$, where message $M \in GL_k(\mathbb{F}_q[S_r])$ and then sends the ciphertext $C = (C_1, C_2)$ to Alice.
(3) Decryption: On receiving the ciphertext C Alice decrypts it by computing: $M = (x^a C_1 y)^{-1} C_2$.

The protocol is vulnerable to a chosen ciphertext attack. The attacker can select a random invertible matrix M' and calculates C_2M', in this attack he has capability to make who knows the secret key (Alice) decrypt the ciphertext (C_1, C_2M') and send him back the corresponding plaintext MM'. Then the attacker obtains the initial plaintext $MM'(M')^{-1} = M$.

To remove this attack we propose a new public key cryptosystem.

4. Proposed cryptosystem

The following section explain the proposed PKC: the key generation, encryption and decryption steps. Our protocol based on the group of invertible matrices over a group ring and the FDLP. A simple example will also be given.

Suppose that Bob wants to send a message to Alice over an insecure channal of communication. Let $G = GL_n\left(\mathbb{F}_q\left[S_r\right]\right)$ be the group of $n \times n$ invertible matrices over the group ring $\mathbb{F}_q\left[S_r\right]$ and A an abelian subgroup of G. Let $B \in G$ which has large order m and $C_G(B)$ be the centralizer of B in G. The group G, A, B and m are publicly known.

4.1. Key generation.

Alice chooses $t, s \in \{2, 3, \ldots, m-1\}$ and $U \in A \setminus C_G(B)$. She computes $P_1 = B^tU, P_2 = B^sU^2$ and then takes (t, s, U) as her private key and (P_1, P_2) as her public key.

4.2. Encryption.

a. Bob randomly selects $V \in A\setminus C_G(B)$ and a secret integer $r \in \{2, 3, \ldots, m-1\}$. He then computes $C_1 = B^rV$.

b. Bob convert the message as a matrix M, an element of the semigroup $M_n\left(\mathbb{F}_q\left[S_r\right]\right)$.

c. Bob computes $C_2 = k_1Mk_2^{-1}$, where:

$$\begin{aligned} k_1 &= B^rP_1V \\ k_2 &= B^rP_2V \end{aligned}$$

d. Bob send $C = (C_1, C_2)$ to Alice.

4.3. **Decryption.**

a. Alice computes

$$\begin{aligned} k_1 &= B^t C_1 U \\ k_2 &= B^s C_1 U^2. \end{aligned}$$

b. Then Alice computes

$$k_1^{-1} \, C_2 \, k_2,$$

which is the message M.

Since $U\,V = V\,U$, then

$$B^t C_1 U = B^t B^r V U = B^r \left(B^t U\right) V = B^r P_1 V$$
$$B^s C_1 U^2 = B^s B^r V U^2 = B^r \left(B^s U^2\right) V = B^r P_2 V.$$

Example 1. *Consider* $GL_2(\mathbb{F}_5\left[S_3\right])$*,* $A = \left\{ \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}, b \in \mathbb{F}_5\left[S_3\right] \right\}$*, and let*

$$B = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix},$$

where $m = 6$*.*

4.4. **Key generation.** *Alice chooses* $t = 2, s = 3$ *and* $U = \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}$*, and calculates*

$$P_1 = B^2 U = \begin{pmatrix} \alpha^2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix} = \begin{pmatrix} \alpha^2 & 0 \\ \alpha & 1 \end{pmatrix},$$
$$P_2 = B^3 U^2 = \begin{pmatrix} 1 & 0 \\ 0 & \beta \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2\alpha & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2\alpha\beta & \beta \end{pmatrix}.$$

Then (t, s, U) *is her private key and* (P_1, P_2) *is her public key.*

4.5. **Encryption.** *Bob chooses* $r = 4$ *and* $V = \begin{pmatrix} 1 & 0 \\ \alpha^2 & 1 \end{pmatrix}$*, and computes*

$$C_1 \;=\; B^4 V = \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \alpha^2 & 1 \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ \alpha^2 & 1 \end{pmatrix},$$

$$k_1 \;=\; B^4 P_1 V = \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha^2 & 0 \\ \alpha & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \alpha^2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \alpha + \alpha^2 & 1 \end{pmatrix},$$

and

$$k_2 \;=\; B^4P_2V = \begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 2\alpha\beta & \beta\end{pmatrix}\begin{pmatrix}1 & 0\\ \alpha^2 & 1\end{pmatrix} = \begin{pmatrix}\alpha & 0\\ 2\alpha\beta+\beta\alpha^2 & \beta\end{pmatrix}.$$

Let $M = \begin{pmatrix}\beta & 1\\ 0 & 0\end{pmatrix}$ *be the message. Then Bob computes*

$$\begin{aligned} C_2 &= k_1Mk_2^{-1} = \begin{pmatrix}1 & 0\\ \alpha+\alpha^2 & 1\end{pmatrix}\begin{pmatrix}\beta & 1\\ 0 & 0\end{pmatrix}\begin{pmatrix}\alpha^2 & 0\\ 4\alpha+3 & \beta\end{pmatrix}\\ &= \begin{pmatrix}4\alpha+\beta\alpha^2+3 & \beta\\ \beta+3\alpha+\alpha\beta+2\alpha^2+4 & \alpha\beta+\beta\alpha^2\end{pmatrix},\end{aligned}$$

where: $k_2^{-1} = \begin{pmatrix}\alpha^2 & 0\\ 4\alpha+3 & \beta\end{pmatrix}$. *Then sends* $C = (C_1, C_2)$ *to Alice.*

4.6. **Decryption.** *For decryption, Alice computes*

$$k_1 \;=\; B^2C_1U = \begin{pmatrix}\alpha^2 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}\alpha & 0\\ \alpha^2 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ \alpha & 1\end{pmatrix} = \begin{pmatrix}1 & 0\\ \alpha+\alpha^2 & 1\end{pmatrix},$$

$$k_2 \;=\; B^3C_1U^2 = \begin{pmatrix}1 & 0\\ 0 & \beta\end{pmatrix}\begin{pmatrix}\alpha & 0\\ \alpha^2 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 2\alpha & 1\end{pmatrix} = \begin{pmatrix}\alpha & 0\\ 2\alpha\beta+\beta\alpha^2 & \beta\end{pmatrix},$$

and

$$\begin{aligned} & k_1^{-1}C_2k_2\\ =\; & \begin{pmatrix}1 & 0\\ 4\alpha+4\alpha^2 & 1\end{pmatrix}\begin{pmatrix}4\alpha+\beta\alpha^2+3 & \beta\\ \beta+3\alpha+\alpha\beta+2\alpha^2+4 & \alpha\beta+\beta\alpha^2\end{pmatrix}\begin{pmatrix}\alpha & 0\\ 2\alpha\beta+\beta\alpha^2 & \beta\end{pmatrix},\\ =\; & \begin{pmatrix}\beta & 1\\ 0 & 0\end{pmatrix} = M\end{aligned}$$

where: $k_1^{-1} = \begin{pmatrix}1 & 0\\ 4\alpha+4\alpha^2 & 1\end{pmatrix}$.

Remark 4.1. *Remark that the message is an element of semigroup* $M_n\left(\mathbb{F}_q\left[S_r\right]\right)$ *as the inverse of the matrix* M *is not needed for decryption or encryption.*

5. Security analysis

5.1. **A chiphertext only attack.** Let consider the ciphertext $C = (C_1, C_2)$ of the plaintext $M_{(i)}$, then we get the system:

$$\begin{aligned} C_1 &= B^{r_i} V_i, \\ C_2 &= k_1 M k_2^{-1}. \end{aligned}$$

So to find the plaintext from ciphertext, the attacker needs r and V, but this is so difficult as solving the factorzation with discrete logarithm problem on a non-abelian group [7], no one can obtain (r, V), so he suppose randomly invertible element $V_0 = V$ and get:

$$V_0^{-1} C_1 \;=\; B^{r_i} \;.$$

Here he has a large system of equations, i.e., the solution becomes infeasible.

5.2. **A known-plaintext attack.** Now we will discuss the known plaintext attack. Let the ciphertext plaintext be the pair $(C_i, M_i)\,, (i = 1, 2, 3, \cdots)$. Let us consider an attacker knows the plaintext M_i corresponding to ciphertext C_i. From the pair (C_i, M_i), the attacker wants to find the plaintext M_{i+1} corresponding to the ciphertext C_{i+1}. In our proposed PKC, we choose new private keys (r, V) to get encryption of every new plaintext. This means that the session key (r, V, k_1, k_2) varies in each session. So, knowing an past ciphertext plaintext pair will not provide any information to find the next unknown ciphertext plaintext pair. Thus our protocol is secure against this attack.

5.3. **Chosen ciphertext attack.** In a chosen ciphertext attack, the adversary can obtain the corresponding plaintext of the ciphertext $C = (C_1, C_2)$, he can take a random invertible matrix $M' \in M_n(\mathbb{F}_q[S_r])$ and calculate $C' = (C_1, C_2 M')$ which is MM'. Then the attacker compute $MM'(M')^{-1} = M$ the initial plaintext.

However, in our proposed system we have:

$$C_2 \;=\; k_1 M k_2^{-1} = B^4 P_1 V M \; (B^4 P_2 V)^{-1} \,.$$

Since the matrices B and V are not commutative, so this attack is not possible.

6. Conclusion

In this paper we proposed a new public key cryptosystem, our protocol is based on the FDLP using the group of invertible matrices over the group ring $\mathbb{F}_q\left[S_r\right]$. We have shown that our scheme is secure against many well know attacks on protocols.

References

[1] R. Alvarez, F. Martinez, J. Vicent, A. Zamora: *A new public key cryptosystem based on matrices*, In WSEAS Int. Conf. on Inform. Security and Privacy, 2007, 36–39.

[2] J.J. Climent, P.R. Navarro, L. Tortosa: *Key exchange protocols over noncommutative rings. The case of End$(Zp \times Zp2)$*, Int. J. Comput. Math. **89**(13-14) (2012), 1753–1763.

[3] W. Diffie, M. Hellman: *New directions in cryptography*, IEEE Trans. Inform. Theory. **22**(6) (1976), 644–654.

[4] M. Eftekhari: *A Diffie–Hellman key exchange protocol using matrices over non-commutative rings*, Groups Complex. Cryptol. **4**(1) (2012), 167–176.

[5] M. Eftekhari: *Cryptanalysis of some protocols using matrices over group rings*, In Int. Conf. on Cryptology in Africa, Springer Cham, Switzerland, 2017, 223–229.

[6] T. ElGamal: *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Trans. Inf. Theory. **31**(4) (1985), 469–472.

[7] I. Gupta, A. Pandey, M.K. Dubey: *A key exchange protocol using matrices over group ring*, Asian-Eur. J. Math. **12**(05) (2019), 1950075.

[8] S. Inam, S. Kanwal, A. Zahid, M. Abid: *A novel public key cryptosystem and digital signatures*, Eur.J.Eng.Sci.Technol. **3**(1) (2020), 22–30.

[9] D. Kahrobaei, C. Koupparis, V. Shpilrain: *Public key exchange using matrices over group rings*, Groups Complex. Cryptol. **5**(1) (2013), 97–115.

[10] S. Kanwal, R. Ali:*A cryptosystem with noncommutative platform groups*, Neural Computing and Appli. **29**(11) (2018), 1273–1278.

[11] C.M. Koupparis: *Non-commutative cryptography: Diffie-Hellman and CCA secure cryptosystems using matrices over group rings and digital signatures*, City University of New York 2012.

[12] Menezes, J. Alfred, Y.H. Wu: *The discrete logarithm problem in $GL(n,q)$*, Ars Combinatoria. **47** (1997), 23–32.

[13] G. Micheli: *Cryptanalysis of a non-commutative key exchange protocol*, Adv. Math. Comm. **9**(2) (2015), 247–253.

[14] G. Mittal, S. Kumar, S. Narain, S. Kumar: *Group ring based public key cryptosystems*, J. Discrete.Math.Sci.Crypto, (2021) 1–22.

[15] D. S. Passman: *The Algebraic Structure of Group Rings*, Wiley, New York, NY, USA, 1977.

[16] R. L. Rivest, A. Shamir, L. Adleman: *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM. **21** (2) (1978), 120–126.

[17] S. K. Rososhek: *Cryptosystems in automorphism groups of group rings of Abelian groups*, J.Math.Sci. **154**(3) (2008), 386–391.

[18] J. H. Silverman: *Fast multiplication in finite fields GF(2^N)*, In International Workshop on Cryptographic Hardware and Embedded Systems, LNCS. 1717 (1999), 122–134.

Faculty of Economic, Commercial and Management Sciences
University of Batna 1
Batna, Algeria.
Email address: sassia.makhlouf@univ-batna.dz

Department of Electrical and Computer Engineering
University of Victoria
PO Box 1700, STN CSC, Victoria, BC, Canada V8W 2Y2,
Canada.
Email address: kguenda@uvic.ca