Nonsingular matrix as private key on ElGamal cryptosystem

Maxrizal¹, Syafrul Irawadi²

¹Department of Information Systems, Institut Sains Dan Bisnis Atma Luhur, Jl. Jendral Sudirman, Pangkalpinang, Bangka Belitung Islands Province, Indonesia
²Department of Informatics Management, Institut Sains Dan Bisnis Atma Luhur, Jl. Jendral Sudirman, Pangkalpinang, Bangka Belitung Islands Province, Indonesia

Corresponding author’s e-mail: maxrizal@atmaluhur.ac.id

Abstract. The ElGamal cryptosystem is an asymmetric cryptosystem using commutative algebra. Currently, applications of commutative algebra are very vulnerable to attack. For this reason, some experts have developed a public-key cryptosystem based on non-commutative algebra. This study proposes the ElGamal cryptosystem using a matrix as the private key to guarantee the non-commutative algebra concept. The result of the cryptosystem is still working on a matrix of a specific size. The results show that we can modify the key generating algorithm, encryption, and description algorithms so that the proposed system can work.

1. Introduction

The ElGamal cryptosystem is a public key cryptosystem using commutative algebra. This cryptosystem has been improved [1], [2], and has been combined with other cryptosystems [3]. The proposed improvements for the ElGamal cryptosystem is vulnerable in the encryption process [4]. For this reason, experts developed the ElGamal cryptosystem using the concept of non-commutative algebra [5], [6].

Generally, asymmetric cryptosystems (ElGamal, RSA, ECC) use an integer as a private key. Ordinary multiplication or addition operations on two integers usually form commutative groups or rings. Therefore, experts develop public-key cryptosystems based on the concept of matrix and non-commutative ring [7]–[12], decomposition problem in the near ring [13], quasi-polynomials over non-commutative groups [14] dan, and non-commutative division semirings [15], [16]. However, the proposed public-key cryptosystem can be attacked through the matrix decomposition problem [17], [18].

The traditional ElGamal cryptosystem applied the discrete logarithmic equation $y = g^x \mod p$, with the public key $(y, g, p)$ and the private key $(x)$. Note that the element $g$ is an integer. Next, we convert the element $g$ to a matrix $G$ of size $n \times n$ [6]. We obtain the discrete logarithmic equation $Y = G^x \mod p$, with the public key $(Y, G, p)$ and the private key $(x)$. We used the concept of a matrix, which is a non-commutative ring [6]. In this study, we will use the discrete logarithmic equation $Y = G^x \mod p$, with the matrix $G$ as the private key and the public key $(Y, x, p)$. We need a lot of modifications to the concept of non-commutative algebra for the matrix $G$ to be inverted and the proposed ElGamal cryptosystem to remain secure [19]–[21].
2. Methods
This research was a literature study. This research will examine the key generating algorithm, encryption process, and message description for the proposed ElGamal cryptosystem. The stages are as follows:

2.1. Modify the key generating algorithm
The traditional ElGamal cryptosystem uses a key generator algorithm \( y = g^x \mod p \), with the private key \((x)\) and the public key \((y, g, p)\). In the proposed ElGamal cryptosystem, the logarithmic equation is converted into a matrix equation \( Y = G^x \mod p \), with the public key \((Y, x, p)\) and the private key \((G)\). We need an algebraic modification so that the matrix \( G \) is reversible or has an inverse.

2.2. Modify plaintext and encryption
The size of the matrix \( G \) (private key) impacts the size plaintext of the message \( M \). In the traditional ElGamal cryptosystem, we have plaintexts \( m_1, m_2, \ldots, m_n \). While in the proposed ElGamal cryptosystem is in the form of a matrix of size \( k \times k \) \((k \leq \sqrt{n})\). Note that the matrix \( M \) in the proposed modification of the ElGamal cryptosystem becomes

\[
\begin{bmatrix}
m_1 & m_2 & \cdots & m_k \\
m_{k+1} & m_{k+2} & \cdots & m_{2k} \\
\vdots & \vdots & \ddots & \vdots \\
m_{(k-1)} & m_{k-2} & \cdots & m_{nk}
\end{bmatrix}
\]

The aim is to make it difficult to solve the keys by tapping (cryptanalyst).

2.3. Modify the description
We have to prove that there is an inverse of the matrix \( G \) so that the ciphertext can be converted back into plaintext.

To validate the proposed theory, we have to prove it with algebra's existing mathematical concepts [19]–[21]. Also, we use Mathematica 5.0 software to simulate the three stages above.

3. Result and discussion

3.1. Advantages of the matrix as a private key in the proposed ElGamal cryptosystem
The traditional ElGamal cryptosystem uses the discrete logarithmic equation \( y = g^x \mod p \), with \( x \) as the private key. This system works on prime numbers \( p \) and generator \( g \) over modulo \( p \), which constructs all nonzero elements of the field \( F_q^* \). Thus, this system's strength depends on the selection of a large integer \( p \), so brute force attacks take a long time.

In [6], the ElGamal cryptosystem works on general linear groups \( GL_n(F_p) \), namely a matrix equation \( Y = G^x \mod p \), with \( G \in GL_n(F_p) \) and \( x \) as private keys. Note that the key is a matrix, resulting in more complex ciphertext randomization. This cryptosystem also still relies on selecting a large integer \( p \).

The proposed improvement of the ElGamal cryptosystem uses the equation \( Y = G^x \mod p \), where \( G \in GL_n(F_p) \) is the private key. The strength of the traditional ElGamal cryptosystem and its improvements lies in the difficulty of solving discrete logarithms. Meanwhile, the power of the
The proposed ElGamal cryptosystem lies in the complexity of factoring the matrix \( G \) from the equation \( Y = G^x \mod p \). If we are given \( Y = G^{100} \mod 11 = \begin{bmatrix} 7 & 3 \\ 10 & 6 \end{bmatrix} \), then we will have trouble finding the private key \( G \).

Furthermore, the brute force attack on the proposed cryptosystem will be more difficult to work with because of the many possible trials and errors in the matrix \( G \). The possible private key on the proposed ElGamal cryptosystem is \( \prod_{k=0}^{n-1} (p^n - p^k) = (p^n - 1)(p^{n-1} - p) \cdots (p^1 - p) \) [19]–[21]. Whereas the traditional ElGamal cryptosystem and its improvements only have \( p \) possibilities of brute force attack.

Another advantage of the proposed ElGamal cryptosystem is that it can work on prime numbers \( p \) that don't need to be large (don't need to be up to 200 or 300 digits). If we choose \( p = 11 \), then the attack on the private key on the traditional ElGamal cryptosystem and its variations is 11 attempts to brute force attack. Thus, the selection of prime \( p = 11 \) is so insecure that we are advised to have large prime numbers \( p \). Furthermore, if \( p = 11 \) and \( G_{4x4} \in GL_4 \left( F_p \right) \) are selected to work on the proposed ElGamal cryptosystem, then there is a brute force attack experiment. Thus, the proposed ElGamal cryptosystem can work on relatively small prime numbers (2 digit numbers, i.e., \( p = 11 \)). However, it has power on par with the traditional ElGamal cryptosystem and improves upon the prime number \( p \) close to 41393302251840000 (11 digit numbers).

Another advantage of the proposed ElGamal cryptosystem lies in selecting the matrix \( G \) (private key). Note that \( G \) is a matrix, so the plaintext must also be a matrix of the same size. Thus, the resulting ciphertext is the result of multiplying the key matrix \( G \) and plaintext, so that plaintext randomization becomes more complicated and more resistant (safer) to chosen-plaintext attacks.

### 3.2. The proposed ElGamal cryptosystem

In this paper, we are presenting the use of a matrix of a specific size in the proposed ElGamal cryptosystem. We need equation \( Y = G^x \mod p \) [6], where \( G \in GL_4 \left( F_p \right) \) is the general linear group over the field \( F_p \).

#### 3.2.1. Key generating algorithm.

At this stage, the message's recipient and the sender will generate the public key and private key for each party.

**Message recipient:**

a. Bob selects \( G_{4x2} \) and forms \( G_{4x4} = \begin{bmatrix} G_{3x2} & O_{2x2} \\ O_{1x2} & I_{2x2} \end{bmatrix} \), where \( O_{2x2} \) is the null matrix and \( I_{2x2} \) is the identity matrix.

b. Bob chooses any \( x \) and forms \( Y_{4x4} = (G_{4x4})^x \).

c. Bob chooses any \( S_{2x4} \).

Bob gets the private key \( G_{3x2} \) and the public key \( \{ x, Y_{4x4}, S_{2x4} \} \). Then, Bob sends the public key to Alice.

**Message Sender:**

a. Alice chooses any \( K_{4x3} \).
b. Alice selects $H_{2 \times 2}$ and forms $H_{4 \times 4} = \begin{bmatrix} H_{2 \times 2} & O_{2 \times 2} \\ O_{2 \times 2} & I_{2 \times 2} \end{bmatrix}$.

c. Alice calculates $T_{4 \times 3} = H_{4 \times 4} Y_{4 \times 4} K_{4 \times 3}$.

Alice gets the private keys $H_{2 \times 2}$ and the public key $\{K_{4 \times 3}, T_{4 \times 3}\}$. Then, Alice sends the public key to Bob.

Message recipient:

Bob calculates $P_{2 \times 2} = S_{2 \times 4} T_{4 \times 3} G_{3 \times 2}$ and sends it to Alice.

3.2.2. Encryption. Alice calculates $Q_{2 \times r} = H_{2 \times 2} P_{2 \times 2} M_{2 \times r}$, and $U_{2 \times 4} = H_{2 \times 2} S_{2 \times 4} H_{4 \times 4}$. Alice sends $\{Q_{2 \times r}, U_{2 \times 4}\}$ to Bob.

3.2.3. Description. Bob forms $X_{2 \times 2} = U_{2 \times 4} Y_{4 \times 4} K_{4 \times 3} G_{3 \times 2}$ and calculates the matrix $M_{2 \times r} = (X_{2 \times 2})^{-1} Q_{2 \times r}$.

So, Bob can read plaintext $M_{2 \times r}$.

4. Conclusions

In this study, we propose the ElGamal cryptosystem using a matrix as the private key. The resulting system is still working on a matrix of a specific size. The results show that we can modify the key generating algorithms, encryption, and description algorithms so that the proposed system can work.

5. Acknowledgments

This research is a Grant of Penelitian Dosen Pemula (PDP) 2020 funded by the Ministry of Research and Technology / National Agency for Research and Technology (Kemenristek / BRIN). We would like to express our gratitude to the Ministry of Research and Technology/ National Agency for Research and Technology to provide financial support and opportunities. We would also like to thank the Institut Sains Dan Bisnis (ISB) Atma Luhur for motivating us to conduct research.

References

[1] Joye M, 2016 Secure ElGamal-Type Cryptosystems Without Message Encoding Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics) 9100 p. 470–478.

[2] Rao F-Y, 2015 On the Security of a Variant of ElGamal Encryption Scheme IEEE Trans. Dependable Secur. Comput. 14, 8 p. 1–4.

[3] Bharathi C R, 2018 Improved ELGAMAL Encryption for Elliptic Curve Cryptography Int. J. Pure Appl. Math. 118, 17 p. 341–353.

[4] Chang T-Y Hwang M-S and Yang W-P, 2013 Cryptanalysis on an Improved Version of ElGamal-Like Public-Key Encryption Scheme for Encrypting Large Messages Inform. 0, 0 p. 1–30.

[5] Mahalanobis A, 2012 A Simple Generalization of the ElGamal Cryptosystem to Non-Abelian Groups II Commun. Algebr. 40, 9 p. 3583–3596.

[6] Maxrizal Safftari M Marna and Sujono, 2019 Generalisasi Sistem Kriptografi ElGamal Menggunakan Konsep Matriks Nonsingular in Seminar Nasional Sistem Informasi dan Teknik Informatika (SENSITIF) p. 21–26.

[7] Maxrizal Nyoman I G Hartawan Y Jana P and Aniska B D, 2020 Modified Public Key Cryptosystem Based On Circulant Matrix.

[8] Karatas Z Y Luy E and Gonen B, 2019 A Public Key Cryptosystem Based on Matrices Int. J. Comput. Appl. 182, 42 p. 47–50.
[9] Zeriouh M Chillali A and Boua A, 2019 Cryptography Based on the Matrices Bol. Soc. Paran. Mat 3, 3 p. 75–83.
[10] Krishna A V N Narayana A H and Vani K M, 2017 A Novel Approach with Matrix Based Public Key Cryptosystems J. Discret. Math. Sci. Cryptogr. 20, 2 p. 407–412.
[11] Andrecut M, 2015, A Matrix Public Key Cryptosystem.
[12] Kahrobaei D Koupparis C and Shpilrain V, 2013 Public Key Exchange Using Matrices Over Group Rings Groups, Complexity, Cryptol. 5, 1 p. 97–115.
[13] Ezhilmaran D and Muthukumaran V, 2016 Key Exchange Protocol Using Decomposition Problem In Near Ring Gazi Univ. J. Sci. 29, 1 p. 123–127.
[14] Valluri M R, 2014 Zero-Knowledge Authentication Schemes Using Quasi-Polynomials over Non-Commutative Groups Open J. Inf. Secur. Appl. 1, 1 p. 43–50.
[15] Anjaneyulu G S G N and Sanyasirao A, 2014 Distributed Group Key Management Protocol over Non-commutative Division Semirings Indian J. Sci. Technol. 7, 6 p. 871–876.
[16] Dwivedi A Ojha D B Sharma A and Mishra A, 2011 A Model of Key Agreement Protocol using Polynomials over Non-Cummutative Division Semirings J. Glob. Res. Comput. Sci. 2, 3 p. 40–43.
[17] Liu J Zhang H Jia J Wang H Mao S and Wu W, 2016 Cryptanalysis of an Asymmetric Cipher Protocol Using a Matrix Decomposition Problem Science China. Inf. Sci. 59, 11 p. 1–11.
[18] Liu J Zhang H and Jia J, 2017 Cryptanalysis of Schemes Based on Polynomial Symmetrical Decomposition Chinese J. Electron. 26, 6 p. 1139–1146.
[19] Lang S, 1993 Linear Algebra New York: Springer.
[20] Dummit D S and Foote R M, 2004 Abstract Algebra 3rd ed. John Wiley & Sons Inc.
[21] Anton H and Rorres C, 2013 Elementary Linear Algebra: Applications Version, 11th Edition Wiley eGrade.