Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 6, pp. 1839–1849
DOI : 10.47974/JDMSC-1862

New public-key cryptosystem algorithm based on function composition of matrix

Maxrizal *
Department of Information Systems
Institut Sains Dan Bisnis Atma Luhur
Pangkalpinang 33172
Indonesia

Baiq Desy Aniska Prayanti
Department of Mathematics
Universitas Bangka Belitung
Bangka 33172
Indonesia

Amri
Bambang Adiwinoto
Department of Management Information Systems
Institut Sains Dan Bisnis Atma Luhur
Pangkalpinang 33172
Indonesia

Abstract

Experts argue that public key cryptography systems based on commutative groups (abelian groups) are quite vulnerable to quantum algorithms attacks. For this reason, experts have developed a non-commutative group-based public-key cryptosystem. In this study, we propose a public-key cryptosystem using the non-commutative property of the function composition of the matrix. The results of this study indicate that the proposed public-key cryptosystem can work well. Furthermore, the proposed cryptosystem is also safe from various attempted mathematical attacks on the key exchange process at the sender and receiver of the message.

Subject Classification: *11C08, 11T71.*

Keywords: *Matrix of public-key cryptosystem, Cryptosystem matrix, Function composition of the matrix.*

* *E-mail:* **maxrizal@atmaluhur.ac.id**

1. Introduction

Public key cryptosystems such as RSA, ElGamal, and ECC are still quite popular in private data exchange transactions. However, experts argue that this public key cryptography system is quite vulnerable to quantum algorithms attacks because it is based on a commutative group (abelian group). For this reason, experts have developed a non-commutative group-based public-key cryptosystem, namely the concept of a ring matrix [1-7], a special matrix [8-13], and matrix decomposition [14-15]. The structure formed on the matrix is generally non-commutative. Experts are also working on the Affine plane, modifying the Affine Hill Cipher to form public key cryptosystems [16]. As with ECC, experts also use discrete logarithms over group multiplication to construct public key cryptosystems [17].

In [15], Liu Jinhui developed a public-key cryptosystem based on matrix decomposition. They use the concept of a general linear group, a non-commutative matrix group over a field, and a polynomial. The strength of this system lies in the key generation protocol. Even so, there are three types of mathematical attacks, namely direct attacks, linearization equations attacks, and over-defined systems of multivariate polynomial equations attacks that hackers can carry out. Furthermore, in [8], the weakness in Jinhui is corrected by replacing the matrix decomposition with a singular matrix, which is a matrix that does not have an inverse.

In this study, we also propose improvements to the public key cryptosystem developed by Liu Jinhui by using the non-commutative property of the composition of functions on matrices.

2. Material And Methods

The proposed research forms a key exchange protocol algorithm, encryption, and message description, which is studied in mathematical theory. In the first stage, we will analyze the algorithm developed by Liu Jinhui. Liu Jinhui's key exchange protocol involves the concept of a general linear group invertible matrix $n \times n$ over a field $(GL_n(F_q))$, a non-commutative matrix group over a field $(M_n(F_q), \bullet)$, and a polynomial $f(x) \in F_q[x]$. In this cryptosystem [15], the sender and receiver of the message form a public key pair (P, Q) which is used to construct a private key (secret key), provided that $P \in GL_n(F_q)$, $Q \in M_n(F_q)$, and $PQ \neq QP$ (non-commutative). Next, the sender of the message calculates $y = f^a(P)Qf^b(P)$ and sends it to the recipient of the message. Finally, the

message's recipient also calculates $u = h^a(P)\ Qh^b(P)$ and sends it to the message's sender. After the exchange of y and u, the sender and receiver of the message can form the same private key, $K = f^a(P)\ uf^b(P) = h^a(P)\ yh^b(P)$. Note that hackers can find private key K by looking for a matrix $X \in M_n(F_q)$ corresponding to the public key matrix $P \in GL_n(F_q)$.

In the second stage, we duplicate Liu Jinhui's key exchange protocol using the non-commutative property of the composition of functions over the matrix. We also analyze various mathematical attacks on the proposed public-key cryptosystem.

3. Modification of Function Composition

We suppose there is a function $f, g \in F[x]$, and then we can form $f \circ g$ or $g \circ f$. Furthermore, if there are $f(x)$ and $g(x)$, then we can calculate $(f \circ g)(x) = f(g(x))$ or vice versa. In this study, we define a modification operation for a linear combination of a set of functions.

Definition 3.1: We take any $f_1, f_2, g_1, g_2 \in F_q[x]$, a collection of functions over any integer modulo q. We form $F(f_1, f_2)$ and $G(g_1, g_2)$. We define

$$FG = (f_1, f_2)(g_1, g_2) = (f_1 \circ g_1 + f_2 \circ g_2) \tag{1}$$

and

$$F(x) = (f_1, f_2)(x) = \left(f_1(x), f_2(x)\right) \tag{2}$$

Thus, there is a linear transformation of a *2-tuple* function to a *1-tuple* function.

Example 3.2: We take $F(f_1(x) = 2x+1,\ f_2 = 3x+2),\ G(g_1(x) = 9x+4,\ g_2 = x+1),$ and $x = 3$ over. We calculate

$$\begin{aligned} FG = f_1 \circ g_1 + f_2 \circ g_2 &= (21x+14) \bmod 5 = (x+4) \bmod 5 \\ (FG)(3) &= 7 \bmod 5 = 2 \bmod 5 \end{aligned} \tag{3}$$

and

$$\begin{aligned} F(3) &= (f_1(3), f_2(3)) = (7, 11) \bmod 5 = (2, 1) \bmod 5 \\ G(3) &= (g_1(3), g_2(3)) = (31, 4) \bmod 5 = (1, 4) \bmod 5 \end{aligned} \tag{4}$$

Based on Definition 3.1. and Example 3.2, we find that $FG \in F_q[x]$. Thus, trivially applies the property of the function in general, namely $FG(x)$.

Example 3.3: Based on Example 3.2, we get $(FG)(3) = 7 \bmod 5$. We also get $G(3) = (1,4) \bmod 5$. We count

$$(F)(G(3)) = ((2.1+1)+(3.4+2)) \bmod 10 = 17 \bmod 5 = 2 \bmod 5 \quad (5)$$

Thus, applies $(FG)(3) = F(G(3))$.

Theorem 3.4: *We take any* $f_1, f_2, g_1, g_2 \in F_q[x]$. *We form* $F(f_1, f_2)$, *and* $G(g_1, g_2)$. *For every* $x \in \mathbb{R}$ *applies* $(FG)(x) = F(G(x))$.

Proof: We take $F(f_1, f_2)$, and $G(g_1, g_2)$. We calculate

$$\begin{aligned} F(G(x)) &= F((g_1, g_2)(x)) \\ &= F(g_1(x), g_2(x)) \\ &= (f_1, f_2)(g_1(x), g_2(x)) \\ &= (f_1 \circ g_1)(x) + (f_2 \circ g_2)(x) \\ &= ((f_1 \circ g_1) + (f_2 \circ g_2))(x) \\ &= ((f_1, f_1)(g_1, g_2))(x) \\ &= (FG)(x) \end{aligned} \quad (5)$$

Remark 3.5: We take $F(f_1, f_2)$, and $G(g_1, g_2)$, with $f_1, f_2, g_1, g_2 \in F_q[x]$. The following statements apply:

(1) If $g_1 = g_2$ then $f_1 \circ g_1 + f_2 \circ g_1 = (f_1 + f_2) \circ g_1$.
(2) If $f_1 = f_2$ then $f_1 \circ g_1 + f_1 \circ g_2 \neq f_1 \circ (g_1 + g_2)$.

Based on Remark 3.5.a, in this study, we provide an additional condition that for any $g_1, g_2 \in F_q[x]$ applies $g_1 \neq g_2$.

In this study, we replace $x \in \mathbb{R}$ with a matrix $N \in M_n(F_q)$. We choose to use a matrix for the optimal level of security.

Corollary 3.6: *We take any* $f_1, f_2, g_1, g_2 \in F_q[x]$. *We form* $F(f_1, f_2)$, *and* $G(g_1, g_2)$. *For every* $N \in M_n(F_q)$ *applies* $(FG)(N) = F(G(N))$.

We limit the degree of $d(F_q[x]) \geq 2$ or the minimum of the quadratic function to optimize security.

Example 3.7: We take $G(g_1(x) = x^2, g_2 = x^2 + x)$ and $N = \begin{bmatrix} 1 & 3 \\ 2 & 4 \end{bmatrix}$ over $\mathbb{Z}_5[x]$.

$$\begin{aligned} G(N) &= (N^2, N^2 + N) \bmod 5 \\ &= \left(\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 3 & 3 \\ 2 & 1 \end{bmatrix} \right) \bmod 5 \end{aligned} \quad (7)$$

If G and $G(N)$ are public (not secret) and N is secret, hackers will have a hard time finding N because hackers have to find the root of a matrix $N^2 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \bmod 5$ or the factors of the matrix of $N^2 + N = \begin{bmatrix} 3 & 3 \\ 2 & 1 \end{bmatrix} \bmod 5$

4. Proposed Public Key Cryptosystem Algorithm

We choose any $f_1, f_2, g_1, g_2 \in F_q[x]$. We form $F(f_1, f_2)$ and $G(g_1, g_2)$ and take any matrix $N \in M_n(F_q)$. We form

$$F.G = (f_1, f_2).(g_1, g_2) = f_1 \circ g_1 + f_2 \circ g_2 \tag{8}$$

and

$$G(N) = (g_1, g_2)(N) = (g_1(N), g_2(N)) \tag{9}$$

4.1 Key Generation Algorithm

Alice and Bob agree to use any $g_1, g_2 \in F_q[x]$, $g_1 \neq g_2$, and $d(F_q[x]) \geq 2$. They form $G(g_1, g_2)$.

(1) Alice chooses any $f_1, f_2 \in F_q[x]$ and $d(F_q[x]) \geq 2$. She forms a secret $F(f_1, f_2)$. She counts $X = FG \bmod q$ and sends it to Bob.

(2) Bob chooses any matrix $N \in M_n(F_q)$ that is secret. Then, he calculated $Y = G(N) \bmod q$ and sent it to Alice.

(3) After the exchange of X and Y (according to Corollary 3.6.), Bob and Alice can form the same private key i.e.

$$K_{Alice} = F(Y) = F(G(N)) = (FG)(N) = X(N) = K_{Bob} \tag{10}$$

4.2 Message Encryption and Description

Alice and Bob can use any operation for the encryption and decryption process. However, the focus of the proposed algorithm is on the security of the key generation algorithm.

5. Hacking Attack Analysis

5.1 Attack on Alice

In this algorithm, Alice and Bob agree to use any $g_1, g_2 \in F_q[x]$, $g_1 \neq g_2$, and $d(F_q[x]) \geq 2$. They form a $G(g_1, g_2)$. Alice stores any $F(f_1, f_2)$,

with $f_1, f_2 \in F_q[x]$ and $d(F_q[x]) \geq 2$. Consider equation $X = F.G = (f_1, f_2) \cdot (g_1, g_2) = f_1 \circ g_1 + f_2 \circ g_2$, which is a linear combination. Although *G* and *X* are not secret, hackers are very difficult to find *F* because f_1, f_2 is unknown.

5.2 Attack on Bob

Bob stores the matrix $N \in M_n(F_q)$ and computes $Y = G(N) \bmod q$. Notice that Alice and Bob choose $G(g_1, g_2)$ with $g_1, g_2 \in F_q[x]$, $g_1 \neq g_2$, and $d(F_q[x]) \geq 2$. Thus, the matrix *N* is also very difficult to generate mathematically. Based on Example 3.7., it is very difficult for hackers to find $N = \sqrt[2]{\begin{bmatrix} 7 & 5 \\ 0 & 2 \end{bmatrix}}$ or factor $N(N+I) = \begin{bmatrix} 8 & 8 \\ 2 & 6 \end{bmatrix}$.

5.3 Attack if Alice and Bob Ignore Conditions

In the first condition, Alice and Bob choose $g_1 = g_2$. Based on Remark 3.5.a., applies $f_1 \circ g_1 + f_2 \circ g_1 = (f_1 + f_2) \circ g_1$. Note that $X = ((f_1 + f_2) \circ g_1)(x)$. Using the composition property of the function, if g_1^{-1} exists in $F_q[x]$, then the hacker can find $(f_1 + f_2)(x) = (X \circ g_1^{-1})(x)$. Next, the hacker can do

$$\begin{aligned} K &= (X \circ g_1^{-1})(g_1(N)) \\ &= (f_1 + f_2)(g_1(N)) \\ &= ((f_1 + f_2) \circ g_1)(N) \\ &= (f_1 \circ g_1 + f_2 \circ g_1)(N) \\ &= (f_1, f_2)(g_1, g_2)(N) \\ &= (FG)(N) \\ &= X(N) \\ &= K_{Bob} \end{aligned} \tag{11}$$

Since $Y = G(N) = (g_1, g_2)(N) = (g_1(N), g_2(N)) \bmod q$ is public, then $g_1(N)$ is public. In this way, hackers can find the private key *K*.

In the second condition, Alice and Bob choose any $g_1, g_2 \in F_q[x]$ and $d(F_q[x]) < 2$. If this condition occurs, the hacker will easily guess or factor the matrix on the linear equation over the matrix. We assume that given $G(g_1(x) = 2x + 1, g_2(x) = x + 2)$, and, which are public. We are given $Y = G(N) = \left(\begin{bmatrix} 3 & 4 \\ 6 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 2 \\ 3 & 3 \end{bmatrix} \right) \bmod 11$. The hacker can find the matrix $N \in M_2(\mathbb{Z}_{11})$ by calculating

$$\begin{aligned} g_1(N) &= 2N + I \\ 2N &= \begin{bmatrix} 2 & 4 \\ 6 & 2 \end{bmatrix} \\ N &= \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} \end{aligned} \tag{12}$$

or the hacker can solve $g_2(N) = \begin{bmatrix} 3 & 2 \\ 3 & 3 \end{bmatrix} \Leftrightarrow N + 2I = \begin{bmatrix} 3 & 2 \\ 3 & 3 \end{bmatrix}$. Since matrix N is found, the hacker can calculate $X(N) = K_{Bob}$. In this way, hackers can discover the private key K.

6. Generalization of the Proposed Public Key Cryptosystem Algorithm

The proposed algorithm uses the $2-tuple$ of F and G. To further secure messages from hacking attacks mathematically, this algorithm will be generalized to $n-tuple$. However, the computational complexity will also increase.

We choose any $f_i, g_i \in F_q[x]$, with $i = 1, 2, \ldots, k$. We form $F(f_1, f_2, \cdots, f_k)$ and $G(g_1, g_2, \ldots, g_k)$ and take any matrix $N \in M_n(F_q)$. We form

$$F.G = (f_1, f_2, \ldots, f_n).(g_1, g_2, \ldots, g_n) = \sum_{i=1}^{k} f_i \circ g_i \tag{13}$$

and

$$G(N) = (g_1, g_2, \ldots, g_k)(N) = (g_1(N), g_2(N), \ldots, g_k(N)) \tag{14}$$

6.1 Key Generation Algorithm

Alice and Bob agree to use any $g_1, g_2, \ldots, g_k \in F_q[x]$, existing $g_i \neq g_j$, and $d(F_q[x]) \geq 2$. They form $G(g_1, g_2, \ldots, g_k)$.

(1) Alice chooses any $f_1, f_2, \ldots, f_k \in F_q[x]$ and $d(F_q[x]) \geq 2$. She forms a secret $F(f_1, f_2, \ldots, f_k)$. She counts $X = FG \bmod q$ and sends it to Bob.

(2) Bob chooses any matrix $N \in M_n(F_q)$ that is secret. Then, he calculated $Y = G(N) \bmod q$ and sent it to Alice.

(3) After the exchange of X and Y (according to Corollary 3.6.), Bob and Alice can form the same private key i.e.

$$K_{Alice} = F(Y) = F(G(N)) = (FG)(N) = X(N) = K_{Bob} \tag{15}$$

Note that $n-tuple$ make this algorithm even more difficult to hack. This algorithm can improve security by choosing a large matrix size $N \in M_n(F_q)$. We can also select a large modulo m to be more secure.

7. A Toy Example

Alice and Bob will be sending a secret message. First, they agreed to use any $g_1, g_2 \in \mathbb{Z}_7[x]$, $g_1 \neq g_2$, and $d(\mathbb{Z}_7[x]) \geq 2$. Next, they formed $G(g_1(x) = 2x^3 - x + 1,\ g_2(x) = x^2 - 3x)$.

(1) Alice chooses any $f_1, f_2 \in \mathbb{Z}_7[x]$ and $d(\mathbb{Z}_7[x]) \geq 2$. She forms a secret $F(f_1(x) = 4x^2 + 5x,\ f_2(x) = x^3 - 4)$. He counts

$$\begin{aligned} X &= FG \bmod 7 \\ &= (f_1, f_2).(g_1, g_2) \bmod 7 \\ &= (f_1 \circ g_1 + f_2 \circ g_2) \bmod 7 \\ &= [4(2x^3 - x + 1)^2 + 5(2x^3 - x + 1)] + [(x^2 - 3x)^3 - 7] \bmod 7 \\ &= 17x^6 - 9x^5 + 11x^4 - x^3 + 4x^2 - 13x + 5 \bmod 7 \\ &= 3x^6 + 5x^5 + 4x^4 + 6x^3 + 4x^2 + x + 5 \bmod 7 \end{aligned} \tag{16}$$

and sends it to Bob.

(2) Bob chooses any matrix $N = \begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix} \in M_2(\mathbb{Z}_7[x])$ that is secret. Then, he calculated

$$\begin{aligned} Y &= G(N) \bmod 7 \\ &= (g_1, g_2)(N) \bmod 7 \\ &= (g_1(N), g_2(N)) \bmod 7 \\ &= \left(2\begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix}^3 - \begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix}^2 - 3\begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix} \right) \bmod 7 \\ &= \left(\begin{bmatrix} 86 & 209 \\ 146 & 378 \end{bmatrix}, \begin{bmatrix} 4 & 9 \\ 6 & 16 \end{bmatrix} \right) \bmod 7 \\ &= \left(\begin{bmatrix} 2 & 2 \\ 6 & 0 \end{bmatrix}, \begin{bmatrix} 4 & 2 \\ 6 & 2 \end{bmatrix} \right) \bmod 7 \end{aligned} \tag{17}$$

and sent it to Alice.

(3) After exchanging X and Y, Alice generates the private key

$$
\begin{aligned}
K_{Alice} &= F(Y) \\
&= (4x^2 + 5x, x^3 - 4)\left(\begin{bmatrix} 2 & 2 \\ 6 & 0 \end{bmatrix}, \begin{bmatrix} 4 & 2 \\ 6 & 2 \end{bmatrix}\right) \bmod 7 \\
&= \left(\left(4\begin{bmatrix} 2 & 2 \\ 6 & 0 \end{bmatrix}^2 + 5\begin{bmatrix} 2 & 2 \\ 6 & 0 \end{bmatrix}\right) + \left(\begin{bmatrix} 4 & 2 \\ 6 & 2 \end{bmatrix}^3 - 4\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right)\right) \bmod 7 \\
&= \begin{bmatrix} 254 & 106 \\ 318 & 148 \end{bmatrix} \bmod 7 \\
&= \begin{bmatrix} 2 & 1 \\ 3 & 1 \end{bmatrix} \bmod 7
\end{aligned} \tag{18}
$$

and Bob generates

$$
\begin{aligned}
K_{Bob} &= X(N) \\
&= (3x^6 + 5x^5 + 4x^4 + 6x^3 + 4x^2 + x + 5)\left(\begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix}\right) \bmod 7 \\
&= 3\begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix}^6 + 5\begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix}^5 + 4\begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix}^4 + 6\begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix}^3 + 4\begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix}^2 \\
&\quad + \begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix} + 5\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod 7 \\
&= \begin{bmatrix} 39706 & 102474 \\ 68316 & 176338 \end{bmatrix} \bmod 7 \\
&= \begin{bmatrix} 2 & 1 \\ 3 & 1 \end{bmatrix} \bmod 7
\end{aligned} \tag{19}
$$

Let's say that Alice has a message $P = \begin{bmatrix} 3 & 7 \\ 1 & 1 \end{bmatrix}$. Alice and Bob agree to use encryption $C = E(P) = P + K \bmod 7$ and decryption $P = D(C) = C - K \bmod 7$. Bob and Alice's encryption and decryption are very easy to do.

Based on this example, Alice and Bob meet all the algorithm requirements, so it is very difficult for hackers to carry out an attack mathematically.

8. Conclusion

In this study, we propose a public-key cryptosystem using the non-commutative property of the function composition of the matrix. The results of this study indicate that the proposed public-key cryptosystem can work well. Furthermore, the proposed cryptosystem is also safe from

various attempted mathematical attacks on the key exchange process at the sender and receiver of the message.

9. Acknowledgment

The authors would like to thank the Institut Sains dan Bisnis Atma Luhur and Universitas Bangka Belitung for financial support and computing laboratories in this research.

Disclosure statement

The author reported no potential conflict of interest.

References

[1] D. Ezhilmaran and V. Muthukumaran, "Key Exchange Protocol Using Decomposition Problem In Near Ring," *Gazi Univ. J. Sci.*, vol. 29, no. 1, pp. 123–127 (2016).

[2] A. V. N. Krishna, A. H. Narayana, and K. M. Vani, "A Novel Approach with Matrix Based Public Key Cryptosystems," *J. Discret. Math. Sci. Cryptogr.*, vol. 20, no. 2, pp. 407–412 (2017).

[3] M. Andrecut, "A Matrix Public Key Cryptosystem," *https://arxiv.org/abs/1506.00277v1*, pp. 1–18 (2015).

[4] Z. Y., E. Luy, and B. Gonen, "Public Key Cryptosystem based on Matrices," *Int. J. Comput. Appl.*, vol. 182, no. 42, pp. 47–50 (2019).

[5] D. Kahrobaei, C. Koupparis, and V. Shpilrain, "Public Key Exchange Using Matrices Over Group Rings," *Groups, Complexity, Cryptol.*, vol. 5, no. 1, pp. 97–115 (2013).

[6] M. Yumman, T. Shah, and I. Hussain, "Asymmetric Cryptosystem on Matrix Algebra over a Chain Ring," *Symmetry (Basel).*, vol. 13, no. 1, pp. 1–11 (2021).

[7] M. Zeriouh, A. Chillali, and A. Boua, "Cryptography Based on the Matrices," *Bol. Soc. Paran. Mat*, vol. 3, no. 3, pp. 75–83 (2019).

[8] M. Maxrizal, "Public Key Cryptosystem Based on Singular Matrix," *Trends Sci.*, vol. 19, no. 3, p. 2147 (2022).

[9] M. Helal Ahmed, J. Tanti, and S. Pushp, "A Public Key Cryptosystem Using Cyclotomic Matrices," *Coding Theory - Recent Adv. New Perspect. Appl. [Working Title]*, pp. 1–9 (2021).

[10] M. Kumari, "A model of Public key cryptography using multinacci matrices," *https://arxiv.org/abs/2003.08634v1*, pp. 1–12 (2020).

[11] P. M. Sree Parvathi and C. Srinivasan, "Matrix Lie Group as an Algebraic Structure for NTRU Like Cryptosystem," *J. Discret. Math. Sci. Cryptogr.*, vol. 23, no. 7, pp. 1455–1464 (2020).

[12] K. A. Reddy, B. Vishnuvardhan, Madhuviswanatham, and A. V. N. Krishna, "A Modified Hill Cipher Based on Circulant Matrices," *Procedia Technol.*, vol. 4, pp. 114–118 (2012).

[13] Maxrizal, I. Gusti Nyoman Yudi Hartawan, P. Jana, and B. Desy Aniska Prayanti, "Modified Public Key Cryptosystem Based on Circulant Matrix," *J. Phys. Conf. Ser.*, vol. 1503, no. 1 (2020).

[14] J. Liu, H. Zhang, J. Jia, H. Wang, S. Mao, and W. Wu, "Cryptanalysis of an Asymmetric Cipher Protocol Using a Matrix Decomposition Problem," *Sci. China Inf. Sci.*, vol. 59, no. 5 (2016).

[15] J. Liu, H. Zhang, and J. Jia, "Cryptanalysis of Schemes Based on Polynomial Symmetrical Decomposition," *Chinese J. Electron.*, vol. 26, no. 6, pp. 1139–1146 (2017).

[16] P. Sundarayya and G. Vara Prasad, "A public key cryptosystem using Affine Hill Cipher under modulation of prime number," *J. Inf. Optim. Sci.*, vol. 40, no. 4, pp. 919–930 (2019).

[17] C. Meshram and X. Li, "New efficient key authentication protocol for public key cryptosystem using DL over multiplicative group," *J. Inf. Optim. Sci.*, vol. 39, no. 2, pp. 391–400 (2018).

Received May, 2023