Modified Public Key Cryptosystem Based On Circulant Matrix

Maxrizal¹, I Gusti Nyoman Yudi Hartawan², Padrul Jana³, Baiq Desy Aniska Prayanti⁴

¹Department of Information Systems, STMIK Atma Luhur, Jl. Jendral Sudirman, Pangkalpinang, Bangka Belitung Islands Province, Indonesia
²Department of Mathematics Education, Ganesha University of Education, Pegok, Jl. Raya Sesetan No.196 Sesetan, Pedungan, Denpasar Sel., Denpasar, Bali 80223, Indonesia
³Department of Mathematics Education, University of PGRI Yogyakarta, Jl. IKIP PGRI I Sonosewu No.117, Sonosewu, Ngestiharjo, Kec. Kasihan, Bantul, Daerah Istimewa Yogyakarta 55182, Indonesia
⁴Department of Mathematics, Bangka Belitung University, Gg. IV No.1, Balun Ijuk, Merawang, Bangka Regency, Bangka Belitung Islands Province 33172, Indonesia

Email: maxrizal@atmaluhur.ac.id

Abstract. Experts believe that public key cryptosystems on non-commutative algebraic structures are resistant to the attack of quantum algorithms. In recent years, public key cryptosystems based on Polynomial Symmetrical Decomposition (PSD) on the non-commutative group have been developed. However, they are vulnerable to direct attack, linearization equations attack, and overdefined systems of multivariate polynomial equations attack. This cryptosystem has also been improved by experts. However, the operation of the proposed PSD Improvement still uses complex computing and untested. Therefore in this paper, we replace PSD on a non-commutative group into a non-commutative matrix group. We chose the circulant matrix on the key agreement protocol and the key distribution. The results show that the cryptosystem proposed on the circulant matrix is resistant to direct attack, linearization equations attack, and overdefined systems of multivariate polynomial equations attack.

1. Introduction

In recent years, public-key cryptosystems based on commutative algebraic structures such as RSA, ElGamal, ECC and their modifications have begun to be left behind [1]–[5]. The commutative algebraic structure of the cryptosystem is vulnerable to quantum algorithm attacks [6]. For this reason, experts develop a public-key cryptosystem for non-commutative algebraic structures. This system is claimed to be resistant to quantum algorithm attacks.

In public-key cryptographic systems, the non-commutative algebraic structure used is the concept of matrix, near-ring, and division semiring [7]–[9]. These concepts are still vulnerable to attack [10]. For this reason, experts develop an extension of the polynomial concept of non-commutative algebraic structures [11]–[13].
In the paper by Liu Jinhui explained about the public key cryptosystem on Polynomial Symmetrical Decomposition (PSD) on the non-commutative group. This system presents public key pairs \((P, Q)\) [11]. Jinhui explained that this system can be hacked with direct attacks, linearization equations attacks, and overdefined systems of multivariate polynomial equations attacks. All three of these attacks use public information \(P\), so hackers can generate secret keys from the sender and receiver.

For this reason, in this study, we propose system improvements by eliminating public information \(P\). We only need the matrix \(Q\) as a public key. Thus, the three attacks above cannot be carried out by hackers. Next, we use the concept of a circular matrix [14]–[16] to modify this algorithm. We also need some algebraic structure to modify the proposed algorithm [17], [18].

2. Methods
This research is a type of literature study. The main reference of this paper is Cryptanalysis of Schemes Based on Polynomial Symmetrical Decomposition *. In the main reference, it is explained that the public key cryptosystem on Polynomial Symmetrical Decomposition (PSD) is still vulnerable to 3 types of attacks. All attacks are built on public information \(P\). For this reason, we try to modify the public-key cryptosystem with a circulant matrix. The concept of a circulant matrix is expected to eliminate public information \(P\) and the proposed algorithm is still running well. Thus, the public-key cryptosystem based on the circulant matrix is resistant to the 3 attacks above.

3. Result and Discussion
3.1. Public Key Cryptosystem Based on Polynomial Symmetrical Decomposition
This algorithm works on non-commutative properties on any matrix and commutative properties on matrix decomposition of a general linear group.

3.1.1. Key Generating Algorithm. We choose \(\left\{ M_n\left(F_q\right), a, b \right\}\), where \(a\) and \(b\) are integers. We choose \(P \in GL_n\left(F_q\right)\) and \(Q \in M_n\left(F_q\right)\), where \(PQ \neq QP\) (commutative properties does not apply). Output \((P, Q)\) is a public key pair.

a. Yudy chose any polynomial \(f(x) \in F_q[x]\) and kept it a secret. He counts \(f(P) \in GL_n\left(F_q\right)\).

Next, he counts \(y = f^a(P)Qf^b(P)\) and sends \(y\) to Max.

b. Max chose any polynomial \(h(x) \in F_q[x]\) and kept it a secret. He counts \(h(P) \in GL_n\left(F_q\right)\).

Next, he counts \(u = h^a(P)Qh^b(P)\) and sends \(u\) to Yudy.

c. After exchanging \(y\) and \(u\), Yudy counts \(K_1 = f^a(P)uf^b(P)\) and Max calculates \(K_2 = h^a(P)yh^b(P)\). Note that

\[
K_1 = f^a(P)uf^b(P) = f^a(P)h^a(P)Qh^b(P)f^b(P) = h^a(P)f^a(P)Qf^b(P)h^b(P) = h^a(P)yh^b(P) = K_2
\]

Yudy and Max have the same key. The public info on this algorithm is \((P, Q, u, y, a, b)\).
3.1.2. **Encryption and Description.** After having the same key, the sender and recipient can send messages. Furthermore, encryption and description are based on the agreement of the sender and receiver. For example, we choose the usual matrix addition operation scheme for encryption, namely \( E(\text{P}) = \text{P} + \text{K} = \text{C} \), with plaintext \( \text{P} \), key \( \text{K} \) and ciphertext \( \text{C} \). To describe the ciphertext, we do description \( D(\text{C}) = \text{C} - \text{K} = \text{P} \). Next, change the alphabet (message) into numbers using the agreement of the sender and receiver of the message. We can use the ASCII code or use the Hill Cipher conversion barrel to convert messages into numbers.

3.2. **Attacks on public-key cryptosystem Based on Polynomial Symmetrical Decomposition**

The attacks on public-key cryptosystem on Polynomial Symmetrical Decomposition was built by public information \( \text{P} \). The attack on the direct attack starts with the assumption that

\[
\begin{align*}
XP &= PX \\
YP &= PY \\
y &= XQY
\end{align*}
\]

(2)

In the linearization equation attack, the matrix \( P \) constructs a system of linear equations

\[
\begin{align*}
X^{-1} &= \sum_{i=0}^{n-1} h_i P_i \\
Y &= \sum_{j=0}^{n-1} g_j P_j \\
X^{-1}y &= QY
\end{align*}
\]

(3)

Meanwhile, in overdefined systems of multivariate polynomial equations attack, the matrix \( P \) constructs the system of equation

\[
\begin{align*}
X &= \sum_{i=0}^{n-1} h_i P_i \\
Y &= \sum_{j=0}^{n-1} g_j P_j \\
y &= XQY
\end{align*}
\]

(4)

Furthermore, the three systems of equations above produce \( XuY = K \) [11]. Thus, the secret key matrix \( K \) can be owned by the hacker.

Note that the three attacks above focus on public information \( \text{P} \). If the matrix \( P \) is unknown, the algorithm is safe. For this reason, in this study, we will omit public information \( \text{P} \).

3.3. **Modified Public Key Cryptosystem Based on Circulant Matrix**

The proposed improvement algorithm is to replace \( f(P) \in GL_n(F_q) \) with a circulant matrix \( F \in \text{circ}(c_0,c_1,\ldots,c_{n-1}) \). Basically, this algorithm still uses the non-commutative algebra structure of any matrix.

3.3.1. **Key Generating Algorithm.** We choose \( \{M_n(F_q),a,b\} \), where \( a \) and \( b \) are integers. We choose \( Q \in M_n(F_q) \). Output \( (Q) \) is a public key.

a. Yudy chose any matrix \( F \in \text{circ}(c_0,c_1,\ldots,c_{n-1}) \), with \( FQ \neq QF \) and kept it a secret. He counts \( y = F^aQF^b \) and sends \( y \) to Max.

b. Max chose any matrix \( H \in \text{circ}(c_0,c_1,\ldots,c_{n-1}) \), with \( HQ \neq QH \) and kept it a secret. He counts \( u = H^aQH^b \) and sends \( u \) to Yudy.
c. After exchanging \( y \) and \( u \), Yudy counts \( K_1 = F^a u F^b \) and Max calculates \( K_2 = H^a y H^b \).

Note that
\[
K_1 = F^a u F^b \\
= F^a H^a Q H^b F^b \\
= H^a F^a Q F^b H^b \\
= H^a y H^b \\
= K_2
\]

Yudy and Max have the same key. The public info on this algorithm is \((Q,u,y,a,b)\).

### Table 1. Table of Algorithm Comparison

| Public Key Cryptosystem Based on Polynomial Symmetrical Decomposition | Public Key Cryptosystem Based on Circulant Matrix |
|---------------------------------------------------------------------|-----------------------------------------------|
| Output \((P,Q)\) as the public key pair.                           | Output \((Q)\) as the public key.               |
| The public information on this algorithm is \((P,Q,u,y,a,b)\).       | The public information on this algorithm is \((Q,u,y,a,b)\). |
| Polynomial Symmetrical Decomposition (PSD) uses complex the key agreement protocol. | Circulant Matrix uses more simple the key agreement protocol. |
| Public key \(P\) causes direct attack,                             | No public key \(P\) so there are no direct     |
| linearization equations attack, and                               | attack, linearization equations attack, and   |
| overdefined systems of multivariate                                | overdefined systems of multivariate           |
| polynomial equations attack.                                       | polynomial equations attack.                  |
| The form of the matrix \(K\) is not patterned, so it's not easy to remember | The form of matrix \(K\) is patterned, so it's easier to remember. |

3.4. Protocol Agreement Simulation

3.4.1. Key Generating Algorithm. Max and Yudy will send a message. They agreed to choose \( a = 2, \)

\[
b = 3, \begin{bmatrix} 1 & 2 & 3 \\ 4 & 15 & 6 \\ 71 & 8 & 9 \end{bmatrix}
\]

and the non-commutative matrix \( Q = \begin{bmatrix} 41 & 5 & 6 \\ 17 & 5 & 6 \\ 21 & 6 & 4 \end{bmatrix} \).

a. Max chooses a circulant matrix \( F = \begin{bmatrix} 6 & 41 & 5 \\ 6 & 41 & 5 \\ 5 & 6 & 41 \end{bmatrix} \). Max also checks \( FQ \neq QF \). Next, he counted

\[
y = F^a Q F^b = \begin{bmatrix} 6464380 & 84434864 & 48466581 \\ 2293688 & 14416825 & 70772283 \\ 92905863 & 68667135 & 83572866 \end{bmatrix}
\]

b. Yudy chooses a circulant matrix \( H = \begin{bmatrix} 1 & 17 & 6 \\ 6 & 1 & 17 \\ 17 & 6 & 1 \end{bmatrix} \). Yudy also checks \( HQ \neq QH \). Next, he counted
3.4.2. **Encryption.** Suppose Max has a secret message "YOURS". Matrix $K$ has the size of $3 \times 3$ so Max forms a plaintext $P_{3 \times 1}$. The message "YOURS" consists of 5 characters so we need 4 dummy elements to complete the matrix entry. Max chooses the dummy element A so the message becomes "YOURSAAAA". Max and Yudy agreed to use the Hill Cipher conversion table algorithm.

| Table 2. Letter conversion table. |
|-----------------------------------|
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 0 |

The message "YOURSAAAA" becomes "25-15-21-18-19-1-1-1-1". Next, Max calculates $C(P) = K + P_i$, with $P_i = \begin{bmatrix} 25 & 15 & 21 \\ 18 & 19 & 1 \\ 1 & 1 & 1 \end{bmatrix}$. Max gets the ciphertext.

$$C(P) = K + P_i = \begin{bmatrix} 37156569 & 40102446 & 47378418 \\ 106860974 & 114023870 & 93824832 \\ 59875066 & 51553375 & 41020859 \end{bmatrix}$$

Max sends ciphertext $C$ to Yudy.

3.4.3. **Description.** Yudy received the ciphertext $C$ and counted $D(C) = C - K = P = \begin{bmatrix} 25 & 15 & 21 \\ 18 & 19 & 1 \\ 1 & 1 & 1 \end{bmatrix}$. Yudy uses the letter conversion table and gets the message "YOURSAAAA". Yudy understands that Max's original message is just "YOURS" because there are dummy elements.

### 4. Conclusions

In this study, we modified the public key cryptosystem on polynomial symmetrical decomposition with a circulant matrix. The results show that we can eliminate the public information $P$ and the proposed algorithm can work well. Thus, the public key cryptosystem proposed on the circulant matrix is resistant to direct attacks, linearization equations attacks, and overdefined systems of multivariate polynomial equations attacks.
References

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

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

[3] 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.

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

[5] Lu Y Peng L and Sarkar S, 2017 Cryptanalysis of an RSA variant with moduli N = p r q l J. Math. Cryptol. 11, 2 p. 117–130.

[6] Hiroki T Eleni D Rob T and Zhiliang Y, 2015 Introduction to the Issue on Quantum Communication and Cryptography IEEE J. Sel. Top. Quantum Electron. 21, 3 p. 3–4.

[7] Ezhilmaran D and Muthukumaran V, 2016 Key Exchange Protocol Using Decomposition Problem In Near Ring Gazi Univ. J. Sci. 29, 1 p. 123–127.

[8] 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.

[9] Andrecut M, 2015 A Matrix Public Key Cryptosystem p. 1–18.

[10] 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 Sciene China. Inf. Sci. 59, May p. 1–11.

[11] Liu J Zhang H and Jia J, 2017 Cryptanalysis of Schemes Based on Polynomial Symmetrical Decomposition* Chinese J. Electron. 26, 6 p. 1139–1146.

[12] 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.

[13] 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.

[14] Fuyong L, 2011 The inverse of circulant matrix Appl. Math. Comput. 217, 21 p. 8495–8503.

[15] Fan Y and Liu H, 2017 Double circulant matrices Linear Multilinear Algebr. 66, 10 p. 2119–2137.

[16] Reddy K A Vishnuvardhan B Madhuvishwanatham and Krishna A V N, 2012 A Modified Hill Cipher Based on Circulant Matrices Procedia Technol. 4 p. 114–118.

[17] Lang S, 1993 Linear Algebra New York: Springer.

[18] Anton H and Rorres C, 2013 Elementary Linear Algebra: Applications Version, 11th Edition Wiley eGrade.