J. Ris. & Ap. Mat. Vol. 07 No. 01 (2023) pp. 49-55
Jurnal Riset dan Aplikasi Matematika
e-ISSN: 2581-0154
URL: journal.unesa.ac.id/index.php/jram

SUATU MODIFIKASI SISTEM KRIPTOGRAFI KUNCI PUBLIK BERBASIS KOMPOSISI FUNGSI ATAS MATRIKS UNTUK MENINGKATKAN KEAMANAN PENGIRIMAN DATA

MAXRIZAL[1*], TRI SUGIHARTONO[2] , BAIQ DESY ANISKA PRAYANTI[3]

[1]Jurusan Sistem Informasi, Institut Sains Dan Bisnis Atma Luhur, [2,]Jurusan Teknik Informatika, Institut Sains dan Bisnis Atma Luhur, [3,]Jurusan Matematika, Universitas Bangka Belitung

*maxrizal@atmaluhur.ac.id

ABSTRAK

Sistem kriptografi kunci publik berbasis grup komutatif rentan terhadap *quantum algorithms attack*. Untuk itu para pakar mengembangkan sistem kriptografi kunci publik berbasis grup non-komutatif. Salah satu sistem kriptografi kunci publik berbasis grup non-komutatif dikembangkan oleh Liu Jinhui menggunakan konsep dekomposisi matriks. Namun sistem kriptografi kunci publik yang dikembangkannya masih rentan terhadap 3 jenis serangan matematis *yaitu direct attack, linearization equations attack* dan *overdefined systems of multivariate polynomial equations attack*. Untuk itu, Peneliti memperbaiki sistem kriptografi kunci publik yang dikembangkan oleh Liu Jinhui dengan menambahkan konsep komposisi fungsi atas matriks. Penelitian yang diusulkan difokuskan pada algoritma pembentukan protokol pertukaran kunci, enkripsi dan deskripsi pesan. Peneliti juga menganalisis berbagai serangan matematis pada sistem kriptografi kunci publik yang diusulkan. Peneliti juga menguji kebenaran konsep yang diusulkan secara aljabar (matematis). Hasil menunjukkan bahwa algoritma modifikasi yang dihasilkan dapat bekerja dengan baik dalam pengiriman pesan.

Kata Kunci: sistem kriptografi kunci publik; dekomposisi matriks; komposisi fungsi atas matriks, sistem kriptografi non-komutatif

ABSTRACT

Commutative group-based public key cryptosystems are vulnerable to quantum algorithms attacks. For this reason, experts have developed a non-commutative group-based public key cryptosystem. A non-commutative group-based public key cryptosystem developed by Liu Jinhui uses the concept of matrix decomposition. However, the public key cryptosystem he developed is still vulnerable to 3 types of mathematical attacks: direct attacks, linearization equations attacks, and overdefined systems of multivariate polynomial equations attacks. For this reason, the researcher improved the public key cryptosystem developed by Liu Jinhui by adding the concept of function composition to the matrix. The proposed research is focused on key exchange protocol formation algorithms, encryption and message description. The researcher also analyzes various mathematical attacks on the proposed public key cryptosystem. Researchers also tested the truth of the concept proposed algebraically (mathematically). The results show that the resulting modification algorithm can effectively send messages.

2020 *Mathematics Subject Classification*: 81P94
Tanggal Masuk: 23-01-23; direvisi: 29-03-23; diterima: 28-04-23

Keyword: *public key cryptosystem; matrix decomposition; composition of functions over matrices, non-commutative cryptosystems*

1 Pendahuluan

Sistem kriptografi kunci publik telah banyak diimplementasikan pada keamanan pengiriman data dan informasi. Sistem kriptografi kunci publik yang sering digunakan yaitu *RSA, ElGamal* dan sistem kriptografi kurva eliptik yang berbasis grup komutatif. Pada faktanya, semua sistem kriptografi kunci publik berbasis grup komutatif rentan terhadap *quantum algorithms attack*. Untuk itu para pakar mengembangkan sistem kriptografi kunci publik berbasis grup non-komutatif yaitu konsep matriks atas ring dan lapangan [1-8], matriks khusus [9-11], dan dekomposisi matriks [12-13].

Salah satu sistem kriptografi kunci publik berbasis dekomposisi matriks adalah sistem kriptografi kunci publik yang dikembangkan oleh Liu Jinhui [12]. Kekuataan sistem kriptografi Liu Jinhui terletak pada protokol pembentukan kunci. Mereka menggunakan konsep *general linear group* pada matriks *invertible* $n\times n$ atas lapangan $GL_n\left(F_q\right)$, grup matriks non-komutatif atas lapangan $M_n\left(F_q\right)$ dan suatu polinomial $f\left(x\right)\in F_q\left[x\right]$. Pada sistem kriptografi ini, pengirim dan penerima pesan membentuk pasangan kunci publik $\left(P,Q\right)$ yang digunakan untuk membangun kunci privat (kunci rahasia), dengan syarat $P\in GL_n\left(F_q\right)$, $Q\in M_n\left(F_q\right)$ dan $PQ\neq QP$ (non-komutatif). Selanjutnya, pengirim pesan menghitung $y=f^a\left(P\right)Qf^b\left(P\right)$ dan mengirimkan y ke penerima pesan. Penerima pesan juga menghitung $u=h^a\left(P\right)Qh^b\left(P\right)$ dan mengirimkan u ke pengirim pesan. Setelah terjadi pertukaran y dan u, pengirim dan penerima pesan dapat membentuk kunci privat yang sama yaitu $K=f^a\left(P\right)uf^b\left(P\right)=h^a\left(P\right)yh^b\left(P\right)$. Perhatikan bahwa kunci K digunakan untuk mengenkripsi dan mendeskripsi pesan (data). Berdasarkan [12], sistem kriptografi kunci publik yang dikembangkan Liu Jinhui masih rentan terhadap 3 jenis serangan matematis yaitu *direct attack, linearization equations attack* dan *overdefined systems of multivariate polynomial equations attack.* Ketiga serangan ini dapat menemukan kunci privat K dengan mencari pasangan matriks $X,Y\in M_n\left(F_q\right)$ yang bersesuaian dengan matriks kunci publik $P,Q\in GL_n\left(F_q\right)$.

Untuk itu, pada penelitian ini, Peneliti mengusulkan perbaikan pada sistem kriptografi kunci publik yang dikembangkan oleh Liu Jinhui. Peneliti menggantikan konsep *general linear group* pada matriks *invertible* $n\times n$ atas lapangan $GL_n\left(F_q\right)$ dengan konsep komposisi fungsi atas matriks $\left(f\circ h\right)\left(N\right)$, dengan $f,h\in F_q\left[x\right]$ dan $N\in M_n\left(F_q\right)$. Peneliti mempunyai hipotesis bahwa dengan menghilangkan $P\in GL_n\left(F_q\right)$ maka 3 jenis serangan matematis tidak dapat dilakukan oleh peretas. Selain itu, operasi komposisi fungsi bersifat non-komutatif $\left(f\circ h\neq h\circ f\right)$ sehingga menjamin keamanan dari *quantum algorithms attack*. Secara umum, Peneliti menggunakan konsep grup matriks non-komutatif atas lapangan $N\in M_n\left(F_q\right)$ dan polinomial $f\left(x\right)\in F_q\left[x\right]$.

2 Metode

Literatur pada penelitian ini merujuk pada beberapa jurnal yang berkaitan sistem kriptografi kunci publik berbasis grup non-komutatif atas matriks dan dekomposisinya. Referensi utama penelitian ini adalah artikel karya LIU Jinhui, ZHANG Huanguo, dan JIA Jianwei dengan judul "*Cryptanalysis of Schemes Based on Polynomial Symmetrical Decomposition*$*$". Pada artikel tersebut, kita disajikan 3 serangan matematis yang merupakan masalah utama yang diselesaikan pada usulan penelitian ini.

Selanjutnya, untuk memperbaiki sistem kriptografi kunci publik yang dikembangkan oleh Jinhui, Peneliti mempelajari sistem-sistem kriptografi kunci publik yang telah dimodifikasi menggunakan matriks atas ring, matriks atas lapangan, dan matriks atas ring sisa. Selain itu, Peneliti juga mempelajari referensi yang berhubungan dengan dekomposisi matriks, dan matriks cyclotomic. Peneliti juga mempelajari sifat-sifat komposisi fungsi atas matriks secara aljabar teoritis [14-15].

3 Hasil dan Pembahasan

Penelitian yang diusulkan oleh Peneliti difokuskan pada algoritma pembentukan protokol pertukaran kunci, enkripsi dan deskripsi pesan. Peneliti juga menganalisis berbagai serangan matematis pada sistem kriptografi kunci publik yang diusulkan. Peneliti juga menguji kebenaran konsep yang diusulkan secara aljabar (matematis) dan menguji secara komputasi dengan bantuan software Mathematica 5.0.

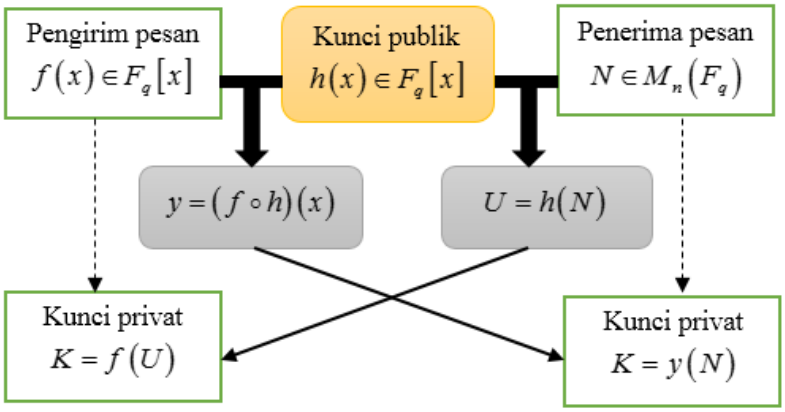
3.1. Modifikasi pembentukan protokol pertukaran kunci

Peneliti memperbaiki sistem kriptografi kunci publik yang dikembangkan Liu Jinhui dkk menggunakan konsep grup matriks non-komutatif atas lapangan $N \in M_n\left(F_q\right)$ dan polinomial $f\left(x\right) \in F_q\left[x\right]$, dengan derajat lebih dari 2.

Secara umum, pada protokol pertukaran kunci, pengirim dan penerima pesan akan memilih sebarang $h\left(x\right) \in F_m\left[x\right]$ sebagai kunci publik, dengan derajat lebih dari 2.

1. Pengirim pesan memilih sembarang polinomial $f\left(x\right) \in F_q\left[x\right]$ dan merahasiakannya. Selanjutnya, pengirim pesan menghitung $y = \left(f \circ h\right)\left(x\right)$ dan mengirimkan y ke penerima pesan.
2. Penerima pesan memilih sebarang matriks non-komutatif atas lapangan $N \in M_n\left(F_q\right)$ dan merahasiakannya. Selanjutnya penerima pesan menghitung matriks $U = h\left(N\right)$ dan mengirimkan U ke pengirim pesan.
3. Setelah terjadi pertukaran y dan U, pengirim dan penerima pesan dapat membentuk kunci privat yang sama yaitu $K = f\left(U\right) = y\left(N\right)$. Hal ini berlaku karena $K = K_A = f\left(U\right) = f\left(h\left(N\right)\right) = \left(f \circ h\right)\left(N\right) = y\left(N\right) = K_B$

Gambar 1. Digram pembentukan protokol pertukaran kunci yang diusulkan



Kekuatan modifikasi algoritma ini terletak pada algoritma pembentukan protokol pertukaran kunci. Selanjutnya untuk melakukan enkripsi dan deskripsi pesan, pengirim dan penerima pesan dapat menggunakan operasi penjumlahan dan pengurangan biasa pada bilangan bulat.

3.2. Analisis serangan peretasan dan perbandingan sistem kriptografi Liu Jinhui

Pada pengirim pesan disimpan polinomial $f(x) \in F_q[x]$ (kunci privat) dan dihitung $y = (f \circ h)(x)$. Agar polinomial f tidak bisa ditemukan dengan mudah walaupun (y, h) bersifat publik (dapat diketehaui peretas), penerima pesan harus memilih suatu polinomial $f(x) \in F_q[x]$ dengan derajat lebih dari 2. Hal ini dikarenakan f^{-1} akan lebih sukar dihitung pada kondisi seperti ini, sehingga f tetap aman dari peretasan dari hacker.

Pada penerima pesan, disimpan matriks $N \in M_n(F_q)$ dan dihitung $U = h(N)$. Perhatikan bahwa jika h polinomial berderajat lebih dari satu maka belum ada algoritma untuk mengakarkan pangkat matriks. Misalkan diberikan $h = x^3$ dan diperoleh $U = h(N) = N^3 = \begin{bmatrix} 108 & 135 \\ 108 & 81 \end{bmatrix}$, untuk suatu matriks N yang dirahasiakan. Dengan demikian, kita tidak bisa menghitung $N = \sqrt[3]{\begin{bmatrix} 108 & 135 \\ 108 & 81 \end{bmatrix}}$ dengan mudah. Dengan demikian, kondisi ini sudah mengindikasikan bahwa peretasan pada sisi penerima pesan menjadi sangat sulit untuk dilakukan.

Selain itu, sistem kriptografi yang diusulkan tidak dapat diserang melalui serangan matematis yaitu *direct attack, linearization equations attack* dan *overdefined systems of multivariate polynomial equations attack* yang bergantung pada pasangan kunci publik (P, Q) [12]. Ketiga serangan ini dapat menemukan kunci privat K dengan mencari sebarang pasangan matriks $X, Y \in M_n(F_q)$ yang bersesuaian dengan matriks kunci publik $P, Q \in GL_n(F_q)$. Hasil penelitian yang diusulkan hanya menggunakan satu kunci publik $h(x) \in F_m[x]$. Dengan

demikian, tidak mungkin dilakukan ketiga serangan tersebut, karena kunci publik menjadi lebih sedikit diketahui, dan struktur algoritma menjadi lebih efisien dan berbeda.

Berikut ini perbandingan sistem kriptografi yang diusulkan dengan sistem kriptografi kunci publik Jinhui dkk.

Tabel : Perbandingan Sistem Kriptografi yang Diusulkan Dengan Sistem Kriptografi Jinhui

Aspek yang dibandingkan	Sistem Kriptografi Kunci Publik	
	Jinhui, dkk	Yang Diusulkan
Parameter yang digunakan	Matriks $GL_n(F_q)$, matriks $M_n(F_q)$ dan polinomial $f(x) \in F_q[x]$	Matriks $M_n(F_q)$ dan polinomial $f(x) \in F_q[x]$
Kunci publik	pasangan kunci publik (P,Q)	sebarang $h(x) \in F_m[x]$
Algoritma protokol pertukaran kunci	$K = f^a(P)uf^b(P)$ $= h^a(P)yh^b(P)$	$K = f(U)$ $= y(N)$
Kemungkinan 3 serangan peretasan	Bisa diserang dengan mencari sebarang pasangan matriks $X, Y \in M_n(F_q)$ yang bersesuaian dengan matriks kunci publik $P, Q \in GL_n(F_q)$.	Tidak mungkin dilakukan ketiga serangan tersebut, karena kunci publik menjadi lebih sedikit diketahui, dan struktur algoritma menjadi lebih efisien dan berbeda.

3.3. Contoh Penerapan Algoritma Yang Diusulkan

Alice dan Bob akan berkirim pesan. Mereka sepakat memilih sebarang $h(x) = x^3 + 1 \in F_5[x]$ sebagai kunci publik.

1. Alice memilih sembarang polinomial $f(x) = 2x + x^2 \in F_5[x]$ dan merahasiakannya. Selanjutnya, Alice menghitung

$$\begin{aligned} y &= (f \circ h)(x) \\ &= f(h(x)) \\ &= f(x^3+1) \\ &= 2(x^3+1) + (x^3+1)^2 \\ &= 2x^3 + 2 + x^6 + 2x^3 + 1 \\ &= 4x^3 + x^6 + 3 \in F_5[x] \end{aligned}$$

   dan mengirimkan $y = 4x^3 + x^6 + 3 \in F_5[x]$ ke Bob.

2. Bob memilih sebarang matriks non-komutatif atas lapangan $N = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \in M_2(F_5)$ dan merahasiakannya. Selanjutnya Bob menghitung matriks

$$
\begin{aligned}
U &= h(N) \\
&= h\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right) \\
&= \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^3 + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 4 & 2 \\ 2 & 2 \end{bmatrix} \in M_2(F_5)
\end{aligned}
$$

dan mengirimkan $U = \begin{bmatrix} 4 & 2 \\ 2 & 2 \end{bmatrix} \in M_2(F_5)$ ke Alice.

3. Setelah terjadi pertukaran y dan U, Alice dan Bob dapat membentuk kunci privat yang sama yaitu

$$
\begin{aligned}
K_{Alice} &= f(U) \\
&= 2\begin{bmatrix} 4 & 2 \\ 2 & 2 \end{bmatrix} + \begin{bmatrix} 4 & 2 \\ 2 & 2 \end{bmatrix}^2 \\
&= \begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix} \in F_5[x]
\end{aligned}
$$

$$
\begin{aligned}
K_{Bob} &= y(N) \\
&= 4\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^3 + \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^6 + 3\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix} \in F_5[x]
\end{aligned}
$$

Perhatikan bahwa Alice dan Bob telah memiliki kunci yang sama. Alice dan Bob dapat melakukan enkripsi dan deskripsi pesan dengan kunci yang sama.

4 Kesimpulan

Penelitian yang diusulkan difokuskan pada algoritma pembentukan protokol pertukaran kunci, enkripsi dan deskripsi pesan. Peneliti juga menganalisis berbagai serangan matematis pada sistem kriptografi kunci publik yang diusulkan. Peneliti juga menguji kebenaran konsep yang diusulkan secara aljabar (matematis). Hasil menunjukkan bahwa algoritma modifikasi yang dihasilkan dapat bekerja dengan baik dalam pengiriman pesan.

Referensi

1. Kahrobaei D Koupparis C and Shpilrain V, 2013 Public Key Exchange Using Matrices over Group Rings Groups, Complexity, Cryptol. 5, 1 p. 97–115.
2. Zeriouh M Chillali A and Boua A, 2019 Cryptography Based on the Matrices Bol. Soc. Paran. Mat 3, 3 p. 75–83.
3. 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.

4. Andrecut M, 2015, A Matrix Public Key Cryptosystem.
5. Yumman M Shah T and Hussain I, 2021 Asymmetric Cryptosystem on Matrix Algebra over a Chain Ring Symmetry (Basel). 13, 1 p. 1–11.
6. Maxrizal M, 2022 Public Key Cryptosystem Based on Singular Matrix Trends Sci. 19, 3 p. 2147.
7. Rososhek S K, 2013 New Practical Algebraic Public-Key Cryptosystem and Some Related Algebraic and Computational Aspects Appl. Math. 4, 7 p.1043–1049.
8. Y. Z Luy E and Gonen B, 2019 Public Key Cryptosystem based on Matrices Int. J. Comput. Appl. 182, 42 p. 47–50.
9. Helal Ahmed M Tanti J and Pushp S, 2021 A Public Key Cryptosystem Using Cyclotomic Matrices Coding Theory - Recent Adv. New Perspect. Appl.[Working Title] p. 1–9.
10. Sree Parvathi P M and Srinivasan C, 2020 Matrix Lie Group as an Algebraic Structure for NTRU Like Cryptosystem J. Discret. Math. Sci. Cryptogr. 23, 7 p. 1455–1464.
11. Maxrizal Gusti Nyoman Yudi Hartawan I Jana P and Desy Aniska Prayanti B, 2020 Modified Public Key Cryptosystem Based on Circulant Matrix J. Phys. Conf. Ser. 1503, 1.
12. Liu J Zhang H and Jia J, 2017 Cryptanalysis of Schemes Based on Polynomial Symmetrical Decomposition Chinese J. Electron. 26, 6 p. 1139–1146.
13. 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 Sci. China Inf. Sci. 59, 5.
14. Dummit D S and Foote R M, 2004 Abstract Algebra 3rd ed. John Wiley & Sons Inc.
15. Anton H and Rorres C, 2004 Elementary Linear Algebra: Applications Version Wiley eGrade