DELTA
Jurnal Ilmiah Pendidikan Matematika
p.ISSN: 2303 -3983 e.ISSN:2548-3994
Vol. 10 No. 2 Bulan Juli Hal. 413 – 418
DOI: https://jurnal.unikal.ac.id/index.php/Delta/index

ANALISIS SISTEM KRIPTOGRAFI MATRIKS SINGULAR BERBASIS POLINOMIAL

[1)]Maxrizal
[1)]Jurusan Sistem Informasi, Institut Sains Dan Bisnis Atma Luhur
maxrizal@atmaluhur.ac.id

Received :
01/09/2022

Accepted :
06/09/2022

Published :
09/09/2022

Abstract

Commutative public key cryptosystems are vulnerable to quantum algorithm attacks. For this reason, experts have developed a public key cryptography system that involves matrix algebra with non-commutative multiplication operations. In addition, there is the NTRU public key cryptosystem, which is claimed to be not vulnerable to quantum algorithm attacks. The NTRU system works on a truncated polynomial ring so the resulting key length will be difficult to guess. In addition, encryption and description in NTRU are very fast compared to RSA, ElGamal and ECC because NTRU only involves polynomial multiplication. Researchers have formed a modified public key cryptosystem using a singular matrix in previous research. This study uses non-commutative algebra and a matrix that has no inverse. For this reason, in this study, researchers adopted polynomials in the NTRU public key cryptographic system so that the resulting key length is difficult to predict. The researcher changed the matrix entries in the form of integers into polynomial entries. Meanwhile, the singular matrix entry remains a ring matrix over integers. The results show that the proposed system produces polynomials whose length cannot be guessed, so a brute-force attack is tricky. Apart from that, this system is superior to NTRU because it does not use the inverse principle. If in NTRU, the resulting polynomial does not have an inverse, then another polynomial must be found and repeated until the step is successful.

Keywords: public key, NTRU, singular polynomial, singular matrix

Abstrak

Sistem kriptografi kunci publik yang bersifat komutatif rentan terhadap serangan algoritma kuantum. Untuk itu, para pakar mengembangkan sistem kriptografi kunci publik yang melibatkan aljabar matriks dengan operasi perkaliannya bersifat non-komutatif. Selain itu, terdapat sistem kriptografi kunci publik NTRU yang diklaim tidak rentan terhadap serangan algoritma kuantum. Sistem NTRU bekerja pada ring polinomial terpotong sehingga panjang kunci yang dihasilkan akan sulit ditebak. Selain itu, enkripsi dan deskripsi pada NTRU sangat cepat dibandingkan RSA, ElGamal dan ECC, karena NTRU hanya melibatkan perkalian polinomial. Pada penelitian terdahulu, peneliti telah membentuk suatu modifikasi sistem kriptografi kunci publik menggunakan matriks singular. Penelitian tersebut menggunakan aljabar non-komutatif dan suatu matriks yang tidak memiliki invers (balikan). Untuk itu, pada penelitian ini, peneliti mengadopsi penggunaan polinomial pada sistem kriptografi kunci publik NTRU agar panjang kunci yang dihasilkan sulit ditebak. Peneliti mengubah entri-entri matriks yang berupa integer menjadi entri-entri polinomial. Sedangkan, entri matriks singular tetap berupa ring matriks atas bilangan bulat. Hasil penelitian menunjukkan bahwa sistem yang diusulkan menghasilkan polinomial yang tidak dapat ditebak panjangnya, sehingga *brute force attack* cukup sulit untuk dilakukan. Selain itu, sistem ini lebih unggul dari NTRU karena tidak menggunakan prinsip balikan (invers). Jika pada NTRU, polinomial yang dihasilkan tidak memiliki invers maka harus dicari polinomial yang lain dan diulang sampai langkah itu berhasil.

Kata Kunci: kunci publik, NTRU, polynomial singular, matriks singular

1. Pendahuluan

Sistem-sistem kriptografi kunci publik yang dibentuk dari perkalian dua atau lebih bilangan bulat biasanya bersifat komutatif. Sistem-sistem ini dapat ditemukan pada sistem kripto kunci publik Rivest-Shamir-Adleman (RSA), ElGamal dan *Elliptic Curve Cryptography* (ECC). Sistem yang berbasis aljabar komutatif rentan oleh serangan algoritma kuantum. Untuk itu, para pakar mengembangkan sistem kriptografi kunci

publik yang melibatkan aljabar matriks dengan operasi perkaliannya bersifat non-komutatif. Beberapa sistem kriptografi yang dihasilkan berupa sistem kriptografi kunci publik dengan struktur matriks atas ring dan lapangan (Hoffstein, Pipher, & Silverman, 1998; Kahrobaei, Koupparis, & Shpilrain, 2013) dan dekomposisi matriks (Liu et al., 2016; Liu, Zhang, & Jia, 2017; Zeriouh, Chillali, & Boua, 2019).

Selanjutnya, terdapat sistem kriptografi kunci publik *N-th Degree Truncated Polynomial Ring* (NTRU) yang juga di klaim tidak rentan terhadap serangan algoritma kuantum. Sistem NTRU bekerja pada ring polinomial terpotong sehingga panjang kunci yang dihasilkan akan sulit ditebak (Sree Parvathi & Srinivasan, 2020; Yassein, Al-Saidi, & Farhan, 2022). Selain itu, enkripsi dan deskripsi pada NTRU sangat cepat dibandingkan RSA, ElGamal dan ECC, karena NTRU hanya melibatkan perkalian polinomial. Perlu diperhatikan bahwa NTRU menggunakan invers (balikan) polinomial, sehingga jika terpilih suatu polinomial yang tidak memiliki invers maka pemilihan polinomial harus diulang.

Pada penelitian terdahulu (Maxrizal, 2022), peneliti telah membentuk suatu modifikasi sistem kriptografi kunci publik menggunakan matriks singular (matriks yang tidak memiliki invers). Penelitian ini mengembangkan sistem kriptografi kunci publik dengan melibatkan sebuah matriks singular X yang bersifat tidak rahasia (kunci publik) dan sebarang dua matriks A, B sebagai kunci privat. Pada penelitian tersebut, entri-entri matriks berupa integer.

Selanjutnya pada penelitian ini, entri-entri matriks A, B yang berupa integer (grup bilangan bulat mod m) akan diganti dengan entri-entri berupa polinomial. Prinsip polinomial diadopsi dari keunggulan sistem kripto NTRU. Pada bagian akhir, jumlahan atau sigma entri polinomial akan dijadikan kunci privat bersama bagi pengirim dan penerima pesan untuk proses enkripsi dan dekripsi. Tujuannya agar kunci baru yang dibentuk lebih acak dan ruang kunci lebih besar sehingga menyulitkan hacker melakukan peretasan.

2. Metode Penelitian

Penelitian ini merupakan penelitian lanjutan dari penelitian terdahulu tentang sistem kriptografi kunci publik yang berbasis matriks singular (Maxrizal, 2022). Pada tahap awal, peneliti melakukan perubahan pada beberapa entri-entri matriks berupa bilangan bulat menjadi entri-entri polinomial. Matriks-matriks ini merupakan kunci privat yang dipilih sebarang oleh pengirim dan penerima pesan serta mereka merahasiakannya. Peneliti juga membutuhkan sifat-sifat matriks dan polinomial yang di referensi dari buku aljabar linear dan matriks (Anton & Rorres, 2004; Dummit & Foote, 2004). Langkah berikutnya, peneliti merumuskan algoritma untuk pembangkit kunci untuk menghasilkan kunci bersama pada kedua pihak. Selanjutnya, peneliti menambahkan langkah penjumlahan entri polinomial sehingga diperoleh polinomial baru yang semakin acak dan panjangnya sulit ditebak yang berperan sebagai kunci bersama utama. Pada tahap akhir, peneliti dapat melengkapi proses enkripsi dan dekripsi pesan dengan menggunakan penjumlahan dan pengurangan polinomial biasa.

3. Hasil dan Pembahasan

1.1. Sistem Kunci Publik Yang Diusulkan

Pada penelitian ini, pengirim dan penerima pesan juga masih menggunakan sebarang matriks singular $X \in M_n(\mathbb{Z}_m)$ yaitu grup matriks atas bilangan bulat $\bmod m$. Selanjutnya, masing-masing pihak membangkitkan sebarang matriks dengan entri-entri polinomial yaitu $A, B \in M_n(\mathbb{Z}_m(x))$ yaitu grup matriks atas polinomial bilangan bulat $\bmod m$. Peneliti memodifikasi entri-entri integer menjadi polinomial. Berikut algoritma modifikasi yang diusulkan:

Pengirim dan penerima pesan memilih sebarang matriks singular $X \in M_n(\mathbb{Z}_m)$ melalui jalur yang mungkin tidak aman *(not secure line)*.

1. Pengirim pesan memilih sebarang matriks

$$A = \begin{bmatrix} a_{11}(\mathbb{Z}_m(x)) & a_{12}(\mathbb{Z}_m(x)) & \dots & a_{1n}(\mathbb{Z}_m(x)) \\ a_{21}(\mathbb{Z}_m(x)) & a_{22}(\mathbb{Z}_m(x)) & \dots & a_{2n}(\mathbb{Z}_m(x)) \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}(\mathbb{Z}_m(x)) & a_{n2}(\mathbb{Z}_m(x)) & \dots & a_{nn}(\mathbb{Z}_m(x)) \end{bmatrix} \in M_n(\mathbb{Z}_m(x)).$$

   Selanjutnya, ia menghitung $Y = AX$ dan mengirimkan matriks singular Y ke penerima pesan.

2. Penerima pesan memilih sebarang matriks

$$B = \begin{bmatrix} b_{11}(\mathbb{Z}_m(x)) & b_{12}(\mathbb{Z}_m(x)) & \dots & b_{1n}(\mathbb{Z}_m(x)) \\ b_{21}(\mathbb{Z}_m(x)) & b_{22}(\mathbb{Z}_m(x)) & \dots & b_{2n}(\mathbb{Z}_m(x)) \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1}(\mathbb{Z}_m(x)) & b_{n2}(\mathbb{Z}_m(x)) & \dots & b_{nn}(\mathbb{Z}_m(x)) \end{bmatrix} \in M_n(\mathbb{Z}_m(x)).$$

   Selanjutnya, ia menghitung $U = XB$ dan mengirimkan matriks singular U ke pengirim pesan.

3. Setelah terjadi pertukaran matriks Y dan U, penerima pesan membentuk $K_A = AU$ dan penerima pesan membentuk $K_B = YB$. Perhatikan bahwa kunci keduanya sama yaitu $K = K_A = AU = A(XB) = (AX)B = YB = K_B$. Misalkan matriks $K = \begin{bmatrix} k_{11}(\mathbb{Z}_m(x)) & k_{12}(\mathbb{Z}_m(x)) & \dots & k_{1n}(\mathbb{Z}_m(x)) \\ k_{21}(\mathbb{Z}_m(x)) & k_{22}(\mathbb{Z}_m(x)) & \dots & k_{2n}(\mathbb{Z}_m(x)) \\ \vdots & \vdots & \ddots & \vdots \\ k_{n1}(\mathbb{Z}_m(x)) & k_{n2}(\mathbb{Z}_m(x)) & \dots & k_{nn}(\mathbb{Z}_m(x)) \end{bmatrix} \in M_n(\mathbb{Z}_m(x))$.

   Selanjutnya, pada masing-masing pihak, mereka membentuk kunci akhir bersama yaitu $K^* = \sum_{i,j=1}^{n} k_{ij}$.

Pada faktanya kunci K^* berbentuk polinomial dan pengirim pesan harus mengubah pesan asli menjadi polinomial. Pengirim pesan dapat menggunakan operasi penjumlahan polinomial biasa untuk melakukan enkripsi pesan dan penerima pesan dapat membaca pesan kembali (dekripsi) dengan cara melakukan pengurangan polinomial biasa.

1.2. Analisis Keamanan Skema

Sistem kriptografi kunci publik yang diusulkan menghasilkan kunci polinomial seperti pada sistem kripto NTRU. Berikut perbandingan sistem yang diusulkan dengan NTRU.

Tabel 1. Perbandingan NTRU dan Sistem kriptografi yang diusulkan

Aspek yang dibandingkan	NTRU	Sistem kriptografi yang diusulkan
Parameter yang digunakan	polinomial	matriks
Kunci akhir yang dihasilkan	polinomial	polinomial
Teknik pembangkitan kunci	Membutuhkan invers polinomial, sehingga memerlukan modulo p prima	Tidak membutuhkan invers matriks, sehingga bisa menggunakan sebarang modulo m
Brute force attack	Sulit dilakukan karena panjang polinomial kuncinya tidak diketahui	Sulit dilakukan karena panjang polinomial kuncinya tidak diketahui

Perhatikan bahwa sistem kriptografi kunci publik yang diusulkan lebih unggul dari sistem kripto NTRU karena tidak menggunakan prinsip balikan (invers). Jika pada NTRU, polinomial yang dihasilkan tidak memiliki invers maka harus dicari polinomial yang lain dan diulang sampai langkah itu berhasil. Pada sistem yang dikembangkan, kita sengaja menggunakan prinsip matriks singular.

1.3. Simulasi Skema Pengiriman Pesan

Alice akan berkirim pesan ke Bob. Mereka berdua sepakat menggunakan matriks singular $X = \begin{bmatrix} 1 & 3 \\ 2 & 6 \end{bmatrix} \in M_2\left(\mathbb{Z}_8\right)$.

Algoritma pembangkit kunci

1. Alice memilih sebarang matriks $A = \begin{bmatrix} 2x+1 & x^2 \\ x-1 & 2-x \end{bmatrix} \in M_2\left(\mathbb{Z}_8\left(x\right)\right)$. Ia menghitung $Y = AX = \begin{bmatrix} 1+2x+2x^2 & 3+6x+6x^2 \\ 3+7x & 1+5x \end{bmatrix}$ dan mengirimkan matriks singular Y ke Bob.

2. Bob memilih sebarang matriks $B=\begin{bmatrix}1+x+x^3 & 2x\\ x+2x & x^5\end{bmatrix}\in M_2\left(\mathbb{Z}_8\left(x\right)\right)$. Ia menghitung $U=XB=\begin{bmatrix}1+2x+x^2 & 2x+3x^5\\ 2+4x+2x^2 & 4x+6x^2\end{bmatrix}$ dan mengirimkan matriks singular U ke Alice.
3. Setelah terjadi pertukaran Y dan U, Alice membentuk $K_A=AU$ dan Bob membentuk $K_B=YB$. Perhatikan bahwa kunci keduanya sama yaitu $K=K_A=K_B=\begin{bmatrix}1+4x+6x^2+5x^3+2x^4+2x^5 & 2x+4x^2+4x^3+3x^5+6x^6+6x^7\\ 3+5x+6x^2+3x^3+7x^4 & 6x+6x^2+x^5+5x^6\end{bmatrix}$
Selanjutnya, mereka membentuk kunci akhir bersama yaitu $K^*=\sum_{i,j=1}^{n}k_{ij}=4+x+2x^2+4x^3+x^4+6x^5+3x^6+6x^7$.

Enkripsi

Misalkan Alice yang telah memiliki pesan yang telah diubah menjadi polinomial yaitu $P=3+4x+x^2+6x^3+7x^4+x^5$. Alice melakukan enkripsi dengan menghitung $C=K+P \bmod p$. Selanjutnya, Alice mengirimkan C ke Bob.

Dekripsi

Bob menerjemahkan kembali $P=C-K \bmod p$ sehingga diperoleh pesan semula dalam bentuk polinomial.

Analisis Percobaan Serangan

Perhatikan bahwa penyadap *(hacker)* dapat menyerang melalui sisi Alice dan Bob. Pada sisi Alice, diperoleh persamaan $Y=AX=\begin{bmatrix}1+2x+2x^2 & 3+6x+6x^2\\ 3+7x & 1+5x\end{bmatrix}$. Walaupun matriks X dapat diketahui siapapun (termasuk penyadap) tetapi persamaan $A=YX^{-1}$ tidak dapat dilakukan karena X berupa matriks singular. Kasus ini juga tidak dapat dikerjakan oleh penyadap di pihak Bob. Selain itu, penggunaan entri polinomial mempersulit penyadap untuk melakukan *brute force attack* (percobaan serangan secara brutal) karena panjang polinomial yang sulit ditebak.

Satu celah lagi yang bisa dilakukan oleh penyadap yaitu dengan melakukan *brute force attack* pada kunci bersama yang dibangkitkan yaitu K^*. Dengan alasan yang sama, penyadap tidak dapat melakukan *brute force attack* karena panjang polinomial yang sulit ditebak, sehingga membutuhkan waktu yang lama untuk melakukan *hacking* dan mendapatkan kunci bersama yang tepat.

4. Kesimpulan dan Saran

Sistem yang diusulkan menghasilkan polinomial yang tidak dapat ditebak panjangnya, sehingga *brute force attack* cukup sulit untuk dilakukan. Selain itu, sistem ini lebih unggul dari NTRU karena tidak menggunakan prinsip balikan (invers). Jika pada NTRU, polinomial yang dihasilkan tidak memiliki invers maka harus dicari polinomial yang lain dan diulang sampai langkah itu berhasil.

Pustaka

Anton, H., & Rorres, C. (2004). *Elementary Linear Algebra: Applications Version*. Wiley eGrade.

Dummit, D. S., & Foote, R. M. (2004). *Abstract Algebra* (3rd ed.). John Wiley & Sons Inc.

Hoffstein, J., Pipher, J., & Silverman, J. H. (1998). NTRU: A ring-based public key cryptosystem. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *1423*, 267–288. https://doi.org/10.1007/bfb0054868

Kahrobaei, D., Koupparis, C., & Shpilrain, V. (2013). Public Key Exchange Using Matrices Over Group Rings. *Groups, Complexity, Cryptology*, *5*(1), 97–115. https://doi.org/10.1515/gcc-2013-0007

Liu, J., Zhang, H., & Jia, J. (2017). Cryptanalysis of Schemes Based on Polynomial Symmetrical Decomposition. *Chinese Journal of Electronics*, *26*(6), 1139–1146. https://doi.org/10.1049/cje.2017.05.005

Liu, J., Zhang, H., Jia, J., Wang, H., Mao, S., & Wu, W. (2016). Cryptanalysis of an Asymmetric Cipher Protocol Using a Matrix Decomposition Problem. *Science China Information Sciences*, *59*(5). https://doi.org/10.1007/s11432-015-5443-2

Maxrizal, M. (2022). Public Key Cryptosystem Based on Singular Matrix. *Trends in Sciences*, *19*(3), 2147. https://doi.org/10.48048/tis.2022.2147

Sree Parvathi, P. M., & Srinivasan, C. (2020). Matrix Lie Group as an Algebraic Structure for NTRU Like Cryptosystem. *Journal of Discrete Mathematical Sciences and Cryptography*, *23*(7), 1455–1464. https://doi.org/10.1080/09720529.2020.1753302

Yassein, H. R., Al-Saidi, N. M. G., & Farhan, A. K. (2022). A new NTRU cryptosystem outperforms three highly secured NTRU-analog systems through an innovational algebraic structure. *Journal of Discrete Mathematical Sciences and Cryptography*, *25*(2), 523–542. https://doi.org/10.1080/09720529.2020.1741218

Zeriouh, M., Chillali, A., & Boua, A. (2019). Cryptography Based on the Matrices. *Bol. Soc. Paran. Mat*, *3*(3), 75–83. https://doi.org/10.5269/bspm.v37i3.34542