JURNAL FOURIER| Oktober 2023, Vol. 12, No. 2, 51-59 ISSN 2252-763X
DOI: 10.14421/fourier.2023.122.51-59 E-ISSN 2541-5239

Protokol Otentikasi Menggunakan Konstruksi Matriks Komutatif Atas Matriks Aljabar Max-Plus

Mufarij Anna Ziaulhaq[1], Muhamad Zaki Riyanto[2]

[1,2]*Program Studi Matematika, Fakultas Sains dan Teknologi, Uiniversitas Islam Negeri Sunan Kalijaga Yogyakarta, Jl. Marsda Adisucipto No. 1 Yogyakarta 55281, Indonesia*

Korespondensi; Mufarij Anna Ziaulhaq, Email:mufarijanna123@gmail.com

Abstrak

Aljabar max-plus adalah himpunan bilangan real bersama elemen negatif tak hingga yang dilengkapi operasi penjumlahan didefinisikan sebagai operasi maksimum dan operasi perkalian didefinisikan sebagai operasi penjumlahan. Konsep aljabar max-plus diperluas untuk membentuk suatu himpunan matriks atas aljabar max-plus. Lebih lanjut himpunan matriks atas aljabar max-plus merupakan struktur semiring non komutatif. Salah satu penelitian tentang matriks atas aljabar max-plus membahas tentang pengkonstruksian suatu matriks yang bersifat komutatif terhadap operasi perkalian pada matriks atas aljabar max-plus. Salah satu aplikasi dari aljabar max-plus adalah dapat diaplikasikan pada bidang kriptografi, seperti proses enkripsi-dekripsi, protokol pertukaran kunci dan protokol otentikasi. Fungsi protokol otentikasi yaitu untuk memastikan kebenaran identitas pihak pengirim kepada pihak penerima, agar tidak terjadi pemalsuan data pengirim. Artikel ini akan mengembangkan protokol otentikasi menggunakan konstruksi matriks komutatif atas aljabar max-plus. Penggunaan matriks komutatif atas aljabar max-plus dimaksudkan untuk meningkatkan keamanan protokol otentikasi dari pihak yang hendak menyadap protokol otentikasi tersebut.

Kata Kunci: Aljabar max-plus, semiring non komutatif, matriks komutatif, kriptografi, protokol otentikasi

Abstract

The max-plus algebra is a set of real numbers along with infinitely negative element that completed addition operations defined as maximum operations and multiplication operations defined as addition operations. The concept of max-plus algebra is extended to form a matrix set over max-plus algebra. Furthermore, the set of matrices over max-plus algebra is a noncommutative semiring structure. One of the studies of max-plus matrix is discussing about the construction of commutative matrix over multiplication operations in max-plus algebra. One of the applications of max-plus algebra is that it can be applied to the field of cryptography, such as encryption-decryption processes, key exchange protocols and authentication protocols. The function of the authentication protocol is to ensure the correctness of the identity of the sending party to the receiving party, so that falsification of sender data does not occur. This article will develop authentication protocols using construction of commutative matrix over max-plus algebra. The use of commutative matrices over max-plus algebra is intended to increase the security of authentication protocols from those who want to intercept the authentication protocol.

Keywords: Max-plus algebra, non commutative semiring, commutative matrix, cryptography, authentication protocol

Pendahuluan

Komunikasi merupakan proses yang digunakan untuk menyampaikan suatu informasi atau pesan kepada orang lain, tentunya komunikasi merupakan hal penting dalam kehidupan sehari-hari. Seiring berjalannya waktu terlebih di era teknologi seperti saat ini, komunikasi mengalami perkembangan yang sangat pesat, yang dahulu hanya bisa dilakukan dengan menulis surat atau berbicara secara langsung kepada orang lain, menjadi mudah dengan cukup menuliskan pesan yang kita inginkan melalui media internet. Namun seiring perkembangan teknologi, komunikasi juga terdapat dampak negatif, yaitu

rawan terjadi penyadapan atau pemalsuan pesan. Oleh karena itu aspek keamanan sangat diperlukan dalam komunikasi pada era teknologi seperti ini [14].

Salah satu solusi sebagai pengamanan pesan yaitu menggunakan kriptografi. Kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berkaitan dengan aspek keamanan informasi meliputi kerahasiaan data, keabsahan data, integritas data, dan otentikasi data. Aspek yang sering dibahas dalam kriptografi yaitu tentang kerahasiaan data [3]. Proses yang dilakukan untuk merahasiakan suatu data atau informasi yaitu menggunakan proses enkripsi dan dekripsi. Enkripsi adalah proses penyandian pesan yang dapat dimengerti (plainteks) menjadi kode-kode yang sulit dimengerti (cipherteks). Sementara dekripsi adalah proses kebalikan dari enkripsi. Proses enkripsi dan dekripsi membutuhkan kunci yang hanya diketahui dan disepakati oleh pihak yang saling berkomunikasi [13]. Salah satu metode untuk menyepakati kunci tersebut menggunakan protokol pertukaran kunci.

Selain aspek kerahasiaan, aspek otentikasi juga merupakan salah satu aspek penting yang digunakan sebagai pengamanan data. Diperlukannya aspek otentikasi untuk mencegah adanya pemalsuan identitas pihak pengirim pesan. Aspek otentikasi dapat diselesaikan menggunakan skema tanda tangan digital. Saat ini skema tanda tangan digital yang dikenal secara luas yaitu skema tanda tangan digital RSA dan DSA. Konsep matematika yang digunakan kedua skema tanda tangan digital tersebut yaitu menggunakan permasalahan faktorisasi bilangan bulat dan logaritma diskrit pada grup komutatif [7]. Namun adanya ancaman komputer kuantum diklaim dapat memecahkan masalah faktorisasi bilangan bulat dan logaritma diskrit dengan cepat, salah satunya yaitu dengan algoritma Shor [9]. Beberapa peneliti pun mencari alternatif efisien lain yang dapat meminimalisir serangan komputer kuantum, salah satunya yaitu menggunakan struktur aljabar max-plus. Struktur aljabar max-plus mempunyai operasi penjumlahan yang didefinisikan operasi maksimum dan operasi perkalian yang didefinisikan operasi penjumlahan biasa [4].

Struktur aljabar max-plus dinilai dapat dijadikan sebagai alternatif lain untuk digunakan dalam bidang kriptografi sebab dinilai efisien dan tergolong masih sulit untuk diserang keamanannya. Pembahasan tentang aljabar max-plus pun mulai banyak dikembangkan oleh para peneliti, diantaranya [1] membahas tentang pengkonstruksian matriks komutatif atas aljabar max-plus, [11] membahas tentang matriks-matriks dalam aljabar max-plus yang mempunyai struktur-struktur khusus, sementara dalam bidang kriptografi aljabar max plus mulai dikembangkan oleh para peneliti, seperti pada [2], [8] dan [15] yang menerapkan aljabar max-plus pada protokol pertukaran kunci. Penelitian ini akan diperkenalkan suatu pengembangan protokol otentikasi baru yang mengaplikasikan konstruksi matriks komutatif atas operasi perkalian aljabar max-plus.

Landasan Teori

Berikut akan dijelaskan tentang teori-teori dasar yang digunakan untuk pembahasan, seperti aljabar max-plus dan matriks atas aljabar max-plus.

Definisi 1. [5] *Diberikan suatu himpunan* $\mathbb{R}_{\max}$ *yang didefinisikan sebagai* $\mathbb{R}_{\max} = \mathbb{R} \cup \{-\infty\}$. *Untuk setiap* $a, b \in \mathbb{R}_{\max}$ *didefinisikan operasi penjumlahan* $(\oplus)$ *dan perkalian* $(\otimes)$ *sebagai*

$$a \oplus b = \max(a, b)$$
$$a \otimes b = a + b.$$

Selanjutnya himpunan $\mathbb{R}_{\max}$ *yang dilengkapi operasi penjumlahan* $(\oplus)$ *dan perkalian* $(\otimes)$ *disebut dengan aljabar max-plus.*

Aljabar max-plus merupakan suatu semifield komutatif terhadap operasi $\oplus$ dan $\otimes$ sebab memenuhi :

1. Himpunan $\mathbb{R}_{\max}$ adalah monoid komutatif dengan elemen netral $-\infty \in \mathbb{R}_{\max}$ terhadap operasi $\oplus$
2. Himpunan $\mathbb{R}_{\max}$ adalah grup komutatif dengan elemen satuan $0 \in \mathbb{R}_{\max}$ terhadap operasi $\otimes$
3. Operasi $\otimes$ bersifat distributif terhadap operasi $\oplus$
4. Elemen netral $-\infty \in \mathbb{R}_{\max}$ merupakan elemen penyerap terhadap operasi $\otimes$, yaitu untuk setiap $a \in \mathbb{R}_{\max}$ berlaku $a \otimes -\infty = -\infty \otimes a = -\infty$

Konsep aljabar max-plus selanjutnya diperluas untuk membentuk sebuah matriks atas aljabar max-plus.

Definisi 2. [10] *Himpunan semua matriks atas aljabar max-plus berukuran* $n \times n$ *dinotasikan dengan* $\mathbb{R}_{\max}^{n \times n}$. *Untuk setiap* $A, B \in \mathbb{R}_{\max}^{n \times n}$ *didefinisikan operasi* $\oplus$ *dan operasi* $\otimes$ *sebagai berikut :*

$$[A \oplus B]_{ij} = \max(a_{ij}, b_{ij})$$
$$[A \otimes B]_{ij} = \max_{k \in \{1,2,\ldots,p\}} (a_{ik} + b_{kj})$$

Hasil dan Pembahasan

Pembahasan pada penelitian ini akan membahas tentang konstruksi matriks komutatif terhadap operasi perkalian atas aljabar max-plus yang selanjutnya diaplikasikan pada protokol otentikasi

Konstruksi Matriks Komutatif atas Aljabar Max-Plus

Himpunan matriks atas aljabar max-plus membentuk suatu struktur aljabar semiring non komutatif. [1] telah mengkonstruksikan sebuah matriks komutatif atas semiring non komutatif tersebut dan [2] memanfaatkan matriks komutatif tersebut untuk diaplikasikan pada protokol pertukaran kunci Stickel. Penggunaan matriks komutatif tersebut diharapkan dapat meningkatkan keamanan dari protokol yang digunakan, sebab menggunakan konstruksi matriks komutatif atas semiring non komutatif. Selanjutnya akan dibahas tentang konstruksi matriks komutatif atas semiring non komutatif.

Dibentuk sebuah matriks atas aljabar max-plus

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \in \mathbb{R}_{\max}^{n \times n},$$

dengan entri $a_{ii} = k$, untuk setiap i dan $2r \le a_{ij} \le r$, dengan $i \neq j$ dan $k, r \in \mathbb{R}$, dengan $k \ge 0$ dan $r \le 0$. Himpunan semua matriks dengan entri-entri tersebut dinotasikan dengan $CM_n(\mathbb{R}_{\max})_k^r$. Teorema selanjutnya akan menjelaskan bahwa matriks-matriks dengan entri-entri yang telah dijelaskan sebelumnya bersifat komutatif terhadap operasi perkalian matriks atas aljabar max-plus.

Teorema 3. [2] Diberikan matriks $A \in CM_n(\mathbb{R}_{\max})_k^r$ dan $B \in CM_n(\mathbb{R}_{\max})_l^s$, dengan $r, s \le 0$ dan $a_{ii} = k \ge 0,\ b_{ii} = l \ge 0$, maka berlaku

$$A \otimes B = B \otimes A = l \otimes A \oplus k \otimes B.$$

Bukti. Diambil sebarang $A \in CM_n(\mathbb{R}_{\max})_k^r$ dan $B \in CM_n(\mathbb{R}_{\max})_l^s$, dengan $r, s \le 0$ dan $a_{ii} = k \ge 0,\ b_{ii} = l \ge 0$, diperoleh

$$\begin{aligned}(A \otimes B)_{ij} &= a_{ii} \otimes b_{ij} \oplus a_{ij} \otimes b_{jj} \oplus \bigoplus_{p \notin \{i,j\}} a_{ip} \otimes b_{pj} \\ &= k \otimes b_{ij} \oplus l \otimes a_{ij} \oplus \bigoplus_{p \notin \{i,j\}} a_{ip} \otimes b_{pj}\end{aligned}$$

Selanjutnya akan dibuktikan bahwa $a_{ip} \otimes b_{pj} \le k \otimes b_{ij} \oplus l \otimes a_{ij}$. Karena $2r \le a_{ij} \le r$ dan $2s \le b_{ij} \le s$, untuk setiap $i \ne j$, diperoleh

$$a_{ip} \otimes b_{pj} \le r \otimes s \le 2r \oplus 2s \le a_{ij} \oplus b_{ij} \le k \otimes b_{ij} \oplus l \otimes a_{ij}.$$

Dengan demikian diperoleh

$$\begin{aligned}(A \otimes B)_{ij} &= k \otimes b_{ij} \oplus l \otimes a_{ij} \oplus \bigoplus_{p \notin \{i,j\}} a_{ip} \otimes b_{pj} \\ &= k \otimes b_{ij} \oplus l \otimes a_{ij} \\ &= l \otimes a_{ij} \oplus k \otimes b_{ij} \\ &= (l \otimes A \oplus k \otimes B)_{ij} \\ &= (B \otimes A)_{ij}.\end{aligned}$$

Untuk setiap i dan j. ■

Selanjutnya diberikan teorema bahwa perkalian antara konstruksi matriks komutatif dengan sebarang matriks atas aljabar max-plus dengan syarat tertentu juga berlaku sifat komutatif.

Teorema 4. [2] Diberikan matriks $A \in CM_n(\mathbb{R}_{\max})_k^r$ dan $B \in \mathbb{R}_{\max}^{n \times n}$, dengan $r \le 0$ dan $k \ge 0$. Jika $0 \le b_{ij} \le k$ untuk setiap i dan j, maka $A \otimes B = B \otimes A$.

Bukti. Diberikan $A \in CM_n(\mathbb{R}_{\max})_k^r$ dan $B \in \mathbb{R}_{\max}^{n \times n}$, dengan $r \le 0$ dan $k \ge 0$. Diketahui $0 \le b_{ij} \le k$ untuk setiap i dan j, maka berlaku $a_{ij} \le 0 \le b_{ij} \le k$, sehingga diperoleh

$$\begin{aligned}(A \otimes B)_{ij} &= a_{ii} \otimes b_{ij} \oplus a_{ij} \otimes b_{jj} \oplus \bigoplus_{p \notin \{i,j\}} a_{ip} \otimes b_{pj} \\ &= k \otimes b_{ij} \\ (B \otimes A)_{ij} &= b_{ii} \otimes a_{ij} \oplus b_{ij} \otimes a_{jj} \oplus \bigoplus_{p \notin \{i,j\}} b_{ip} \otimes a_{pj} \\ &= b_{ij} \otimes k.\end{aligned}$$

Untuk setiap i dan j. Dengan demikian $A \otimes B = B \otimes A$. ■

Protokol Pertukaran Kunci dan Protokol Otentikasi

Proses enkripsi dan dekripsi pesan membutuhkan suatu kunci rahasia yang disepakati oleh kedua belah pihak yang melakukan komunikasi. Salah satu metode untuk menentukan kunci yaitu

menggunakan protokol pertukaran kunci.Protokol pertukaran kunci yang sering sekali digunakan yaitu protokol pertukaran kunci Diffie-Hellman. Dalam protokol pertukaran kunci tersebut, tingkat keamanan didasarkan pada masalah logaritma diskrit pada grup siklik terhadap operasi perkalian modulo p. Berikut skema dari protokol pertukaran kunci Diffie-Hellman [12].

Tabel 1. Protokol Pertukaran Kunci Diffie-Hellman

Alice dan Bob menyepakati secara publik bilangan prima p dan generator g dari grup siklik G	
Alice	Bob
1. Alice memilih secara rahasia bilangan bulat $1 < a < p-1$ 2. Alice menghitung $u = g^a \bmod p$ 3. Alice mengirimkan u kepada Bob 4. Alice menghitung $K_A = v^a \bmod p$	1. Bob memilih secara rahasia bilangan bulat $1 < b < p-1$ 2. Bob menghitung $v = g^b \bmod p$ 3. Bob mengirimkan v kepada Alice 4. Bob menghitung $K_B = u^b \bmod p$
Alice dan Bob menyepakati kunci yang sama, yaitu $K = K_A = K_B$	

Berdasarkan protokol pertukaran kunci Diffie-Hellman, dapat dikembangkan menjadi protokol otentikasi.Protokol otentikasi bertujuan sebagai alat pembuktian Alice sebagai pihak user untuk membuktikan identitasnya kepada Bob sebagai pihak verifikator atau sebagai server.Berikut skema protokol otentikasi Diffie-Hellman.

Tabel 2. Protokol Otentikasi Diffie-Hellman

Alice dan Bob menyepakati secara publik bilangan prima p dan generator g dari grup siklik G	
Alice	Bob
1. Alice memilih secara rahasia bilangan bulat $1 < a < p-1$ 2. Alice menghitung $u = g^a \bmod p$ 3. Alice mengirimkan u kepada Bob	
	4. Bob menerima u dari Alice 5. Bob memilih secara rahasia bilangan bulat $1 < b < p-1$ 6. Bob mengirimkan tantangan $v = g^b \bmod p$ kepada Alice
7. Alice menerima v dari Bob 8. Alice merespon dengan mengirimkan $P = v^a \bmod p$ kepada Bob	
	9. Bob memverifikasi dengan menghitung apakah $u^b \bmod p = P$

Beberapa peneliti mengembangkan protokol pertukaran kunci yang diharapkan keamanannya kuat terhadap serangan komputer kuantum. Salah satu protokol pertukaran kunci tersebut, yaitu protokol pertukaran kunci Stickel yang menggunakan grup non komutatif [6]. Berikut skema protokol pertukaran kunci Stickel.

Tabel 3. Protokol Pertukaran Kunci Stickel

Alice dan Bob menyepakati secara publikgrup non komutatif G dan $a,b \in G$	
Alice	Bob
1. Alice memilih secara rahasia bilangan bulat m dan n 2. Alice menghitung $u = a^m b^n$ 3. Alice mengirimkan u kepada Bob 4. Alice menghitung $K_A = a^m v b^n$	1. Bob memilih secara rahasia bilangan bulat r dan s 2. Bob menghitung $v = a^r b^s$ 3. Bob mengirimkan v kepada Alice 4. Bob menghitung $K_B = a^r u b^s$
Alice dan Bob menyepakati kunci yang sama, yaitu $K = K_A = K_B$	

Untuk meningkatkan keamanan, [2] menggunakan konstruksi matriks komutatif untuk mengembangkan protokol pertukaran kunci Stickel. Berikut skema protokol pertukaran kunci Stickel yang dimodifikasi menggunakan konstruksi matriks komutatif atas aljabar max-plus.

Tabel 4. Protokol Pertukaran Kunci Stickel Menggunakan Konstruksi Matriks Komutatif

Alice dan Bob menyepakati secara publik matriks $W \in \mathbb{R}_{\max}^{n\times n}$	
Alice	Bob
1. Alice memilih secara rahasia matriks $A \in CM_n(\mathbb{R}_{\max})_k^r$ dan $B \in CM_n(\mathbb{R}_{\max})_l^s$ dengan $r,s<0$ dan $k,l \geq 0$ 2. Alice menghitung $U = A \otimes W \otimes B$ 3. Alice mengirimkan U kepada Bob 4. Alice menghitung $K_A = A \otimes V \otimes B$	1. Bob memilih secara rahasia matriks $C \in CM_n(\mathbb{R}_{\max})_x^a$ dan $D \in CM_n(\mathbb{R}_{\max})_y^b$ dengan $a,b<0$ dan $x,y \geq 0$ 2. Bob menghitung $V = C \otimes W \otimes D$ 3. Bob mengirimkan V kepada Alice 4. Bob menghitung $K_B = C \otimes U \otimes D$
Alice dan Bob menyepakati kunci yang sama, yaitu $K = K_A = K_B$	

Protokol Otentikasi Menggunakan Konstruksi Matriks Komutatif

Berdasarkan protokol pertukaran kunci menggunakan konstruksi matriks komutatif, dapat dikembangkan menjadi protokol otentikasi. Berikut skema dari protokol otentikasi tersebut.

Tabel 5. Protokol OtentikasiMenggunakan Konstruksi Matriks Komutatif

Alice dan Bob menyepakati secara publik matriks $W \in \mathbb{R}_{\max}^{n\times n}$	
Alice	Bob
1. Alice memilih secara rahasia matriks $A \in CM_n(\mathbb{R}_{\max})_k^r$ dan $B \in CM_n(\mathbb{R}_{\max})_l^s$ dengan $r,s<0$ dan $k,l \geq 0$ 2. Alice menghitung $U = A \otimes W \otimes B$ 3. Alice mengirimkan U kepada Bob	

	4. Bob menerima U dari Alice 5. Bob memilih secara rahasia matriks $C \in CM_n(\mathbb{R}_{\max})_x^a$ dan $D \in CM_n(\mathbb{R}_{\max})_y^b$ dengan $a, b < 0$ dan $x, y \geq 0$ 6. Bob mengirimkan tantangan $V = C \otimes W \otimes D$ kepada Alice
7. Alice menerima V dari Bob 8. Alice merespon dengan mengirimkan $P = A \otimes V \otimes B$ kepada Bob	
	9. Bob memverifikasi dengan menghitung apakah $C \otimes U \otimes D = P$

Contoh. Alice dan Bob mempublikasikan matriks $W = \begin{pmatrix} 30 & 24 & 26 \\ 12 & -18 & 34 \\ 34 & -21 & -20 \end{pmatrix} \in \mathbb{R}_{\max}^{3\times 3}$. Alice memilih secara rahasia dua buah matriks $A = \begin{pmatrix} 24 & -12 & -18 \\ -24 & 24 & -15 \\ -17 & -13 & 24 \end{pmatrix} \in CM_3(\mathbb{R}_{\max})_{24}^{-12}$ dan $B = \begin{pmatrix} 21 & -15 & -30 \\ -18 & 21 & -22 \\ -24 & -27 & 21 \end{pmatrix} \in CM_3(\mathbb{R}_{\max})_{21}^{-15}$ selanjutnya Alice menghitung

$$
\begin{aligned}
U &= A \otimes W \otimes B \\
&= \begin{pmatrix} 24 & -12 & -18 \\ -24 & 24 & -15 \\ -17 & -13 & 24 \end{pmatrix} \otimes \begin{pmatrix} 30 & 24 & 26 \\ 12 & -18 & 34 \\ 34 & -21 & -20 \end{pmatrix} \otimes \begin{pmatrix} 21 & -15 & -30 \\ -18 & 21 & -22 \\ -24 & -27 & 21 \end{pmatrix} \\
&= \begin{pmatrix} 54 & 48 & 50 \\ 36 & 6 & 58 \\ 58 & 7 & 21 \end{pmatrix} \otimes \begin{pmatrix} 21 & -15 & -30 \\ -18 & 21 & -22 \\ -24 & -27 & 21 \end{pmatrix} \\
&= \begin{pmatrix} 75 & 69 & 71 \\ 57 & 31 & 79 \\ 79 & 43 & 42 \end{pmatrix}.
\end{aligned}
$$

Selanjutnya Alice mengirimkan $U=\begin{pmatrix}75 & 69 & 71\\ 57 & 31 & 79\\ 79 & 43 & 42\end{pmatrix}$ kepada Bob. Pada lain pihak, Bob menerima $U=\begin{pmatrix}75 & 69 & 71\\ 57 & 31 & 79\\ 79 & 43 & 42\end{pmatrix}$. Langkah selanjutnya Bob memilih secara rahasia dua buah matriks $C=\begin{pmatrix}32 & -40 & -36\\ -37 & 32 & -29\\ -25 & -21 & 32\end{pmatrix}\in CM_3(\square_{\max})_{32}^{-20}$ dan $D=\begin{pmatrix}29 & -17 & -18\\ -19 & 29 & -20\\ -33 & -34 & 29\end{pmatrix}\in CM_3(\square_{\max})_{29}^{-17}$ Selanjutnya Bob menghitung

$$\begin{aligned}V &= C\otimes W\otimes D\\ &=\begin{pmatrix}32 & -40 & -36\\ -37 & 32 & -29\\ -25 & -21 & 32\end{pmatrix}\otimes\begin{pmatrix}30 & 24 & 26\\ 12 & -18 & 34\\ 34 & -21 & -20\end{pmatrix}\otimes\begin{pmatrix}29 & -17 & -18\\ -19 & 29 & -20\\ -33 & -34 & 29\end{pmatrix}\\ &=\begin{pmatrix}62 & 56 & 58\\ 44 & 14 & 66\\ 66 & 11 & 13\end{pmatrix}\otimes\begin{pmatrix}29 & -17 & -18\\ -19 & 29 & -20\\ -33 & -34 & 29\end{pmatrix}\\ &=\begin{pmatrix}91 & 85 & 87\\ 73 & 43 & 95\\ 95 & 49 & 48\end{pmatrix}.\end{aligned}$$

Setelah menghitung V, Bob mengirimkan tantangan tersebut kepada Alice. Selanjutnya Alice menerima tantangan V dari Bob dan mengirimkan respon kepada Bob yaitu

$$\begin{aligned}P &= A\otimes V\otimes B\\ &=\begin{pmatrix}24 & -12 & -18\\ -24 & 24 & -15\\ -17 & -13 & 24\end{pmatrix}\otimes\begin{pmatrix}91 & 85 & 87\\ 73 & 43 & 95\\ 95 & 49 & 48\end{pmatrix}\otimes\begin{pmatrix}21 & -15 & -30\\ -18 & 21 & -22\\ -24 & -27 & 21\end{pmatrix}\\ &=\begin{pmatrix}115 & 109 & 111\\ 97 & 67 & 119\\ 119 & 73 & 82\end{pmatrix}\otimes\begin{pmatrix}21 & -15 & -30\\ -18 & 21 & -22\\ -24 & -27 & 21\end{pmatrix}\\ &=\begin{pmatrix}136 & 130 & 132\\ 118 & 92 & 140\\ 140 & 104 & 103\end{pmatrix}.\end{aligned}$$

Bob menerima respon $P=\begin{pmatrix}136 & 130 & 132\\ 118 & 92 & 140\\ 140 & 104 & 103\end{pmatrix}$ dari Alice. Untuk melakukan otentikasi Bob menghitung apakah $C\otimes U\otimes D=P$, diperoleh

$$C \otimes U \otimes D = \begin{pmatrix} 32 & -40 & -36 \\ -37 & 32 & -29 \\ -25 & -21 & 32 \end{pmatrix} \otimes \begin{pmatrix} 75 & 69 & 71 \\ 57 & 31 & 79 \\ 79 & 43 & 42 \end{pmatrix} \otimes \begin{pmatrix} 29 & -17 & -18 \\ -19 & 29 & -20 \\ -33 & -34 & 29 \end{pmatrix}$$
$$= \begin{pmatrix} 107 & 101 & 103 \\ 89 & 63 & 111 \\ 111 & 75 & 74 \end{pmatrix} \otimes \begin{pmatrix} 29 & -17 & -18 \\ -19 & 29 & -20 \\ -33 & -34 & 29 \end{pmatrix}$$
$$= \begin{pmatrix} 136 & 130 & 132 \\ 118 & 92 & 140 \\ 140 & 104 & 103 \end{pmatrix}.$$

Bob memperoleh hasil bahwa $C \otimes U \otimes D = P$, sehingga proses otentikasi berhasil.

Kesimpulan

Adanya pengembangan protokol otentikasi menggunakan struktur aljabar semiring non komutatif diharapkan tingkat keamanannya lebih tinggi terhadap serangan computer kuantum di masa mendatang, terlebih lagi menggunakan konstruksi matriks komutatif atas aljabar max-plus berukuran besar, hal ini diharapkan pihak yang melakukan otentikasi lebih efisien dan pihak penyerang mengalami kesulitan karena harus memecahkan masalah aljabar linear dalam aljabar max-plus.

Referensi

[1] J. Linde and M. J. de la Puente, "Matrices commuting with a given normal tropical," *Linear Algebra and its Applications*, pp. 101-121, 2015.

[2] Any Muanalifah and Sergei Sergeev, "Modifying The Tropical Version Of Stickel's Key," *Applications of Mathematics*, pp. 727-753, 2020.

[3] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton: CRC Press, 1996.

[4] Subiono, *Aljabar Max-Plus dan Terapannya*. Surabaya: Matematika FMIPA ITS, 2013.

[5] M. Andy Rudhito, *Aljabar Max-Plus dan Penerapannya*. Yogyakarta: Program Studi Pendidikan Matematika FKIP Universitas Sanata Dharma, 2016.

[6] E. Stickel, "A New Method for Exchanging Secret Keys," *Third International Conference on Information Technology and Applications (ICITA'05)*, 2005.

[7] Johannes A.Buchmann, *Introduction to Cryptography*. New York: Springer New York, 2004.

[8] Dima Grigoriev and Vladimir Shpilrain, "Tropical Cryptography," *Communications in Algebra*, pp. 2624–2632, 2014.

[9] Peter W. Shor, "Polynomial-time Algorithms for Prime Factorization and Discrete Logarithm on a Quantum Computer," *SIAM Journal on Computing*, pp. 1484-1509, 1997.

[10] Kasie G. Farlow, *Max-Plus Algebra*.: Virginia Polytechnic Institute, 2009.

[11] Daniel Jones, *Special and Structured Matrices in Max-Plus Algebra*.: The University of Birmingham, 2017.

[12] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, pp. 644-654, 1976.

[13] Douglas R. Stinson and Maura B. Paterson, *Textbooks in Mathematics Cryptography Theory and Practice Fourth Edition*.: CRC Press, Inc, 2019.

[14] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, *An Introduction to Mathematical Cryptography Second Edition*.: Springer-Verlag New York, Inc, 2014.

[15] Musthofa, "An Application of Max-Plus Algebra in Criptography," in *International Seminar on Innovation in Mathematics and Mathematics Education*, 2014.