Penerapan Aljabar Max-Plus dalam Protokol Autentikasi Menggunakan Matriks Komutatif

Teosofi Hidayah Agung
5002221132

Departemen Matematika
Institut Teknologi Sepuluh Nopember

Senin, 2 Juni 2025

Daftar Isi

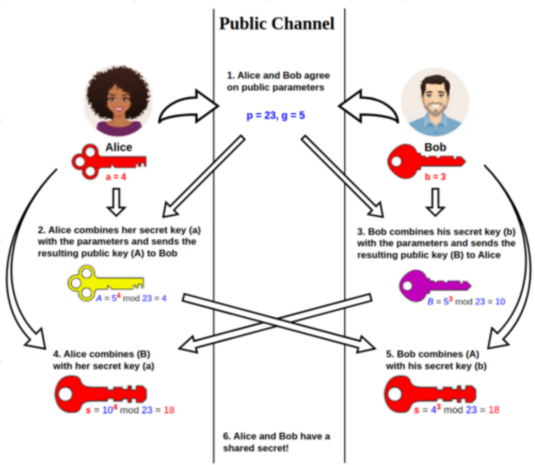
Diffie-Hellman key exchange

Protokol Diffie-Hellman key exchange adalah metode kriptografi yang memungkinkan dua pihak untuk menghasilkan kunci rahasia bersama melalui saluran komunikasi yang tidak aman. Ditemukan oleh Whitfield Diffie dan Martin Hellman pada tahun 1976. Protokol ini didasarkan pada konsep matematika dari grup siklik $(\mathbb{Z}_p^*, \times)$ dengan p adalah bilangan prima.

Kategori	Simbol / Nilai	Keterangan
Parameter Publik	p (bilangan prima), $g \in \mathbb{Z}_p^*$	Dipilih secara umum, diketahui semua pihak termasuk penyerang.
Kunci Privat	$a, b \in \mathbb{Z}_p^*$	Bilangan acak rahasia, **tidak** boleh dibagikan ke siapapun.
Kunci Publik	$A = g^a \mod p$ $B = g^b \mod p$	Dihitung dari kunci privat, lalu dibagikan secara terbuka.
Kunci Bersama	$K = g^{ab} \mod p$	Nilai akhir yang sama, hanya bisa dihitung jika tahu kunci privat.

Tabel: Ringkasan parameter pada protokol Diffie–Hellman

Diffie-Hellman key exchange



Gambar: Protokol Diffie-Hellman key exchange

Definisi 2.1 ([1])

Misalkan $A = (a_{ij})$ dan $B = (b_{ij})$ adalah matriks berukuran $m \times n$ dengan elemen-elemen dari $\mathbb{R} \cup \{\varepsilon\}$. Operasi penjumlahan dan perkalian matriks A dan B didefinisikan sebagai berikut:

$$(A \oplus B)_{ij} = a_{ij} \oplus b_{ij} = \max\{a_{ij}, b_{ij}\},$$
$$(A \otimes B)_{ij} = \bigoplus_{k=1}^{n} a_{ik} \otimes b_{kj} = \max_{1 \le k \le n} (a_{ik} + b_{kj}).$$

Misal:

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix},$$

maka

$$A \oplus B = \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix}, \quad A \otimes B = \begin{pmatrix} 9 & 10 \\ 11 & 12 \end{pmatrix}.$$

Matriks Komutatif Aljabar Max-Plus

Definisi 2.2 (Matriks Linde-de la Puente [2])

Untuk setiap bilangan real $r \leq 0$ dan bilangan real $k \geq 0$, kita definisikan

$$[2r, r]_n^k$$

sebagai himpunan matriks $A_{n\times n}$ sedemikian sehingga $a_{ii} = k$ untuk semua i dan $a_{ij} \in [2r, r]$ untuk $i \neq j$.

Teorema 2.3 (Komutativitas Matriks LdlP [2])

Misalkan $A \in [2r, r]_n^{k_1}$, $B \in [2s, s]_n^{k_2}$ untuk setiap $r, s \leq 0$ dan $a_{ii} = k_1 \geq 0$, $b_{ii} = k_2 \geq 0$. Maka

$$A \otimes B = B \otimes A = k_2 \otimes A \oplus k_1 \otimes B.$$

Protokol Tropical Stickel Berbasis Matriks LdIP [3]

1. Alice dan Bob menyepakati sebuah matriks publik $W \in \mathbb{R}_{\max}^{n \times n}$.
2. Alice memilih dua matriks acak A_1 dan A_2, di mana $A_1 \in [2a_1, a_1]_n^{k_1}$ dan $A_2 \in [2a_2, a_2]_n^{k_2}$ sedemikian sehingga $a_1, a_2 \leq 0$ dan $k_1, k_2 \geq 0$ dan mengirimkan $U = A_1 \otimes W \otimes A_2$ kepada Bob.
3. Bob memilih dua matriks acak B_1 dan B_2, di mana $B_1 \in [2b_1, b_1]_n^{l_1}$ dan $B_2 \in [2b_2, b_2]_n^{l_2}$ sedemikian sehingga $b_1, b_2 \leq 0$ dan $l_1, l_2 \geq 0$ dan mengirimkan $V = B_1 \otimes W \otimes B_2$ kepada Alice.
4. Alice menghitung kunci rahasianya menggunakan kunci publik V yang diperoleh dari Bob, yaitu $K_a = A_1 \otimes V \otimes A_2$.
5. Bob juga menghitung kunci rahasianya menggunakan kunci publik Alice, U, yaitu $K_b = B_1 \otimes U \otimes B_2$.

Protokol Autentikasi Menggunakan Matriks Komutatif

Perhatikan bahwa

$$
\begin{aligned}
K_a &= A_1 \otimes V \otimes A_2 \\
&= A_1 \otimes (B_1 \otimes W \otimes B_2) \otimes A_2 \\
&= (A_1 \otimes B_1) \otimes W \otimes (B_2 \otimes A_2) \\
&= (B_1 \otimes A_1) \otimes W \qquad\qquad\qquad = B_1 \otimes (A_1 \otimes W \otimes A_2) \otimes B_2 \\
&= B_1 \otimes U \otimes B_2 = K_b.
\end{aligned}
$$

Kedua pihak berakhir dengan kunci yang identik karena sifat asosiatif dan komutatif dari matriks Linde-de la Puente.

Contoh Permasalahan

Ziaulhaq **and** Riyanto mencotohkan sebuah permasalahan berikut:

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

$$A_1 = \begin{pmatrix} 24 & -12 & -18 \\ -24 & 24 & -15 \\ -17 & -13 & 24 \end{pmatrix} \in [-24, -12]_3^{24} \quad \text{dan} \quad A_2 = \begin{pmatrix} 21 & -15 & -30 \\ -18 & 21 & -22 \\ -24 & -27 & 21 \end{pmatrix} \in [-30, -15]_3^{21}$$

Contoh Permasalahan

selanjutnya Alice menghitung

$$
\begin{aligned}
U &= A_1 \otimes W \otimes A_2 \\
&= \begin{pmatrix} 24 & -12 & -18 \\ -24 & 24 & -15 \\ -17 & -13 & 24 \end{pmatrix} \otimes \begin{pmatrix} 30 & 24 & 26 \\ 12 & -18 & 34 \\ 34 & -21 & -20 \end{pmatrix} \otimes \begin{pmatrix} 21 & -15 & -30 \\ -18 & 21 & -22 \\ -24 & -27 & 21 \end{pmatrix} \\
&= \begin{pmatrix} 54 & 48 & 50 \\ 36 & 6 & 58 \\ 58 & 7 & 21 \end{pmatrix} \otimes \begin{pmatrix} 21 & -15 & -30 \\ -18 & 21 & -22 \\ -24 & -27 & 21 \end{pmatrix} \\
&= \begin{pmatrix} 75 & 69 & 71 \\ 57 & 31 & 79 \\ 79 & 43 & 42 \end{pmatrix}.
\end{aligned}
$$

Contoh Permasalahan

Selanjutnya Alice mengirimkan U kepada Bob. Pada lain pihak, Bob menerima U. Langkah selanjutnya Bob memilih secara rahasia dua buah matriks

$$B_1 = \begin{pmatrix} 32 & -40 & -36 \\ -37 & 32 & -29 \\ -25 & -21 & 32 \end{pmatrix} \in [-40, -20]_3^{32}, \quad \text{dan} \quad B_2 = \begin{pmatrix} 29 & -17 & -18 \\ -19 & 29 & -20 \\ -33 & -34 & 29 \end{pmatrix} \in [-34, -17]_3^{29}.$$

Selanjutnya Bob menghitung

$$
\begin{aligned}
V &= B_1 \otimes W \otimes B_2 \\
&= \begin{pmatrix} 32 & -40 & -36 \\ -37 & 32 & -29 \\ -25 & -21 & 32 \end{pmatrix} \otimes \begin{pmatrix} 30 & 24 & 26 \\ 12 & -18 & 34 \\ 34 & -21 & -20 \end{pmatrix} \otimes \begin{pmatrix} 29 & -17 & -18 \\ -19 & 29 & -20 \\ -33 & -34 & 29 \end{pmatrix} \\
&= \begin{pmatrix} 62 & 56 & 58 \\ 44 & 14 & 66 \\ 66 & 11 & 13 \end{pmatrix} \otimes \begin{pmatrix} 29 & -17 & -18 \\ -19 & 29 & -20 \\ -33 & -34 & 29 \end{pmatrix} \\
&= \begin{pmatrix} 91 & 85 & 87 \\ 73 & 43 & 95 \\ 95 & 49 & 48 \end{pmatrix}.
\end{aligned}
$$

Contoh Permasalahan

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

$$P = A_1 \otimes V \otimes A_2$$

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

Contoh Permasalahan

Bob menerima respon P dari Alice. Untuk melakukan autentikasi, Bob menghitung apakah $B_1 \otimes U \otimes B_2 = P$. Setelah dicek ternyata

$$\begin{aligned}
B_1 \otimes U \otimes B_2 &= \begin{pmatrix} 32 & -40 & -36 \\ -37 & 32 & -29 \\ -25 & -21 & 32 \end{pmatrix} \otimes \begin{pmatrix} 75 & 69 & 71 \\ 57 & 31 & 79 \\ 79 & 43 & 42 \end{pmatrix} \otimes \begin{pmatrix} 29 & -17 & -18 \\ -19 & 29 & -20 \\ -33 & -34 & 29 \end{pmatrix} \\
&= \begin{pmatrix} 107 & 101 & 103 \\ 89 & 63 & 111 \\ 111 & 75 & 74 \end{pmatrix} \otimes \begin{pmatrix} 29 & -17 & -18 \\ -19 & 29 & -20 \\ -33 & -34 & 29 \end{pmatrix} \\
&= \begin{pmatrix} 136 & 130 & 132 \\ 118 & 92 & 140 \\ 140 & 104 & 103 \end{pmatrix}.
\end{aligned}$$

Bob memperoleh hasil bahwa $B_1 \otimes U \otimes B_2 = P$, sehingga proses autentikasi berhasil.

Berikut adalah link website *demo* dari protokol autentikasi menggunakan matriks komutatif:

https://tetewheroez.github.io/Tugas-Kuliah/Semester%207/Aljabar%20Max-Plus/Kripto%20Max-Plus/index.html

Referensi

[1] Subiono, *Aljabar Min-Max Plus dan Terapannya*. Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia: Jurusan Matematika, Institut Teknologi Sepuluh Nopember, 2015, Available at: subiono2008@matematika.its.ac.id.

[2] J. Linde **and** M. J. de la Puente, *Matrices commuting with a given normal tropical matrix*, 2014. arXiv: 1209.0660 [math.RA]. **url**: https://arxiv.org/abs/1209.0660.

[3] S. Alhussaini **and** S. Sergeev, *On implementation of Stickel's key exchange protocol over max-min and max-T semirings*, Cryptology ePrint Archive, Paper 2024/519, 2024. **url**: https://eprint.iacr.org/2024/519.

[4] M. A. Ziaulhaq **and** M. Z. Riyanto, **?**Protokol Otentikasi Menggunakan Konstruksi Matriks Komutatif Atas Matriks Aljabar Max-Plus,**?** *Jurnal Fourier*, **jourvol** 12, **number** 2, **pages** 51–59, **october** 2023. DOI: 10.14421/fourier.2023.122.51-59. **url**: https://fourier.or.id/index.php/FOURIER/article/view/182.