ARTICLE TEMPLATE

Stickel's Protocol using Tropical Increasing Matrices

Any Muanalifah[a], Zahari Mahad [b], Nurwan [c], Rosalio G Artes [d]

[a]Department of Mathematics, UIN Walisongo Semarang, Indonesia; [b] INSPEM, UPM; [c] Department of Mathematics, Universitas Negeri Gorontalo, Indonesia; [d] Mindanao State University - Tawi-Tawi College of Technology and Oceanography

ARTICLE HISTORY
Compiled February 14, 2024

ABSTRACT
In this paper we introduce new concept of tropical increasing matrices and then prove that two tropical increasing matrices are commute. Using this property, we modified Stickel's protocol. This idea similar to [5] where modified Stickel's protocol using commuting matrices (Linde De La Puente Matrices).

KEYWORDS
tropical algebra, increasing matrices, diffie-hellman, stickel protocol, public key cryptography

1. Introduction

Public Key Cryptography represents a cornerstone in the domain of digital security, enabling secure communication over insecure channels through the use of two separate key for encryption and private key for decryption. Unlike symmetric key cryptography, where the same key is used for both encryption and decryption, public key cryptography allows for the distribution of the public key openly, while keeping the private key secret.

Tropical cryptography is a branch of cryptography that utilizes the principles of tropical algebra that was introduced by Griogriev and Sphilrain [**?**]. This algebraic structure operates on the tropical semiring, which, in its simplest form, involves the operations of taking the maximum (minimum) and addition of real numbers. Unlike traditional cryptographic methods that rely on the arithmetic of numbers or algebraic structures like groups, rings, and fields, tropical cryptography explores encryption and decryption mechanisms through the lens of tropical mathematics.

The applications of tropical cryptography are still being explored but hold promise for developing new encryption schemes that could potentially offer advantages in terms of efficiency, security, and resistance to certain types of cryptographic attacks. This area is particularly interesting for theoretical cryptographers and mathematicians who are seeking to expand the boundaries of what is possible in cryptography.

Some researches have done in tropical cryptography, especially in public key cryotography such as modification of Stickel's protocol [**?**], [5], [10], public key cryptography using tropical semidirect product, tropical cryptography in digital signature [12], and

CONTACT Any Muanalifah. Email: any.muanalifah@walisongo.ac.id

tropical encryption [11]. The attack for tropical cryptography also introduced by [7], [4], [3], and [9]

Some modifications of public protocol using tropical commuting matrices have been conducted by [8], [5], [6]. In their paper, Muanalifah and Sergey studied some classes of commuting matrices in tropical algebra and its application on public key cryptograpy. They modified stickel protocol using tropical quasi-polynomial and Linde De la puente Matrices. However this protocol can be attacked by generalized of Kotov and Ushakov attack [5].

Our aim is to study a new class in tropical commuting matrices and implement into Stickel's protocol. In this paper we introduce a new concept about the tropical increasing matrix and study some properties in tropical increasing matrices.

The paper is organized as follows: We focus on some definitions as fundamental key notions of tropical semiring and tropical matrix algebra in Section 2. In Section 3, we present the Tropical Increasing Matrices. Then, in Section 4, we discuss two modification of Stickel's protocol using tropical increasing matrices. Finally, the conclusion and further research are given in Section 5.

2. Preliminaries

In this section we introduce the basic definition of tropical algebra and public key cryptography.

The tropical (max-plus) semiring $\mathbb{R}_{\max}$ is the set $\mathbb{R} \cup \{\infty\}$, equipped with the addition ($\oplus$) and the multiplication ($\otimes$). For each $a, b \in \mathbb{R}_{\max}$, we set

$$a \oplus b = \max(a, b), \qquad and \qquad a \otimes b = a + b \tag{1}$$

This arithmetic operation can be extended to matrices and vectors as in the following definition.

Definition 2.1 (Tropical Matrix Addition)**.** Let $A = [A_{ij}] \in \mathbb{R}_{\max}, B = [B_{ij}] \in \mathbb{R}_{\max}$. the tropical matrix addition is

$$(A \oplus B) = A_{ij} \oplus B_{ij} = \max\{A_{ij}, B_{ij}\}$$

Definition 2.2 (Tropical Matrix Multiplication)**.** Let $A = [A_{ij}] \in \mathbb{R}_{\max}^{m \times p}$ and $C = [C_{ij}] \in \mathbb{R}_{\max}^{p \times n}$ then

$$A \otimes C = \bigoplus_{k=1}^{n} [A_{ik}] \otimes [C_{kj}] = \max_{1 \le k \le n} \{A_{ik} + C_{kj}\}$$

Definition 2.3. Let $A = [A_{ij}] \in \mathbb{R}_{\max}$ and c be any scalar. Scalar multiplication $c \otimes A$ is obtained by adding c to each entry in A.

$$c \otimes A = c \otimes [A_{ij}] = [c + A_{ij}]$$

Definition 2.4 (Identity matrix)**.** Matrix $I \in \mathbb{R}_{\max}$ is called a tropical identity matrix

if its entries are

$$I_{ij} = \begin{cases} 0 & ; i = j \\ -\infty & ; i \neq j \end{cases}$$

Definition 2.5 (Matrix powers)**.**

$$A^{\otimes k} = \underbrace{A \otimes A \cdots \otimes A}_{\text{k}}$$

Tropical matrix powers are a natural extension of scalar tropical powers

Definition 2.6.

$$a^{\otimes k} = \underbrace{a \otimes a \cdots \otimes a}_{\text{k}} = \underbrace{a + a \cdots + a}_{\text{k}} = k \times a, \forall a \in \mathbb{R}_{\max}, k \in \mathbb{N}.$$

Definition 2.7 (Kleene stars e.g [1])**.** Suppose $A \in \mathbf{R}_{n\times n}^{\max}$ then denote

$$A^* = I \oplus A \oplus A^2 \oplus A^3 \cdots$$

. If this series converges then it is called the Kleene star of A.

As we know the first pioneer of public key cryptography was Diffie-Hellman [13]. They implemented cyclic group to construct public key exchange protocol as below.

Diffie-Hellman Protocol

Alice and Bob agree on public parameter cyclic group Z_p^* where p is prime number and generator g. They exchange public key in the following steps

(1) Alice picks a private integer number r and computes $u = g^r$.
(2) Bob picks a private integer number s and computes $v = g^s$.
(3) Alice and Bob exchange their public keys u and v. Alice sends u to Bob and Bob sends v to Alice, respectively.
(4) Using Bob's public key v, Alice computes her private key $K_A = (v)^r = g^{sr}$.
(5) Bob uses Alice's public key u to construct his private Key $K_B = (u)^s = g^{rs}$

It is clear that Alice and Bob have common secret key.

In 2005, Stickel introduced new concept in public key cryptography by modifying Diffie-Hellman protocol [13]. Here we recall the classic Stickel's protocol.

Stickel's Protocol

Alice and Bob agree on non abelian grup G. Alice and Bob chooses public parameter $a, b, w \in G$ where $ab \neq ba$. They exchange public key as follows.

(1) Alice chooses two random positive integers k, l and sends $u = a^k w b^l$ to Bob.
(2) Bob chooses two random positive integers r, s and sends $v = a^r w b^s$ to Alice.
(3) Alice calculates her private Key $K_A = a^k v b^l$.
(4) Bob calculates his private key $K_B = a^r u b^s$.

Then Alice and Bob end up with the same secret key. This Stickel's protocol version has been attacked by Vladimir Shiplrain using linear algebra attack [15]

3. Tropical Increasing Matrices

In this section we will define increasing matrices in tropical algebra and discuss about the properties of tropical increasing matrices.

First of all, we introduce a new concept of tropical increasing matrix in the following definition.

Definition 3.1. Matrix $A = (a_{ij}) \in \mathbb{R}_{\max}^{n\times n}$ is called tropical increasing matrix if it satisfies the following condition :

(1) **row-wise increasing**
for every element a_{ij} then $a_{ij+1} = a_{ij} + 1$ for all j such that $1 \leq j < n$ where n is the dimension of matrix.
(2) **column-wise increasing**
for every element a_{ij} then $a_{i+1j} = a_{ij} + n$ for all i such that $1 \leq i < n$ where n is the dimension of matrix.

We denote tropical increasing matrices by $\mathcal{I}_n$ for all $n \in \mathbf{N}$.

It can be seen that $a_{12} = a_{11} + 1, a_{13} = a_{11} + 2 + ... + a_{11} + (n-1)$. Hence, we can express the entries of tropical increasing matrices by the generator of tropical increasing matrices, i.e a_{11} as in this below definition.

Definition 3.2 (deformation of tropical increasing matrices)**.** Let A be a tropical increasing matrices then each entry a_{ij} of matrix A can be written as the following formula

$$a_{ij} = a_{11} + (i-1)n + (j-1) \tag{2}$$

Example 3.3. Matrix $A = \begin{bmatrix} -1 & 0 & 1 \\ 2 & 3 & 4 \\ 5 & 6 & 7 \end{bmatrix}$ is a tropical increasing matrices with $n = 3$.
We can write $a_{21} = 2$ where $i = 2, j = 1$ and $n = 3$. Using equation (2) a_{21} can be expressed as

$$a_{21} = a_{11}+(i-1)n+(j-1) = a_{11}+(2-1)3+(1-1) = -1+(2-1)3+(1-1) = -1+3+0 = 2.$$

$$a_{23} = a_{11}+(i-1)n+(j-1) = a_{11}+(2-1)3+(3-1) = -1+(2-1)3+(3-1) = -1+3+2 = 4.$$

$$a_{32} = a_{11}+(i-1)n+(j-1) = a_{11}+(3-1)3+(2-1) = -1+(3-1)3+(2-1) = -1+6+1 = 6.$$

It is clear that the eigenvalues of matrix $A \in \mathcal{I}_n$ is equal to a_{nn} since a_{nn} is the largest entry of matrix A.

In the term of classical algebra, two increasing matrices A and B are not commute. Here we give the counter example

Example 3.4. Let $A = \begin{bmatrix} -2 & -1 & 0 \\ 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 3 & 4 \\ 5 & 6 & 7 \\ 8 & 9 & 10 \end{bmatrix}$ be two square increasing matrices then we have

$$A \times B = \begin{bmatrix} -9 & -12 & -15 \\ 36 & 42 & 48 \\ 81 & 96 & 111 \end{bmatrix} \neq B \times A = \begin{bmatrix} 15 & 24 & 33 \\ 24 & 42 & 60 \\ 33 & 60 & 87 \end{bmatrix}$$

However, in the term of tropical algebra we can show that two tropical increasing matrices are commute as in the following theorem

Theorem 3.5. *Let $A, B \in \mathcal{I}_n$ then $A \otimes B = B \otimes A$*

Proof. By definition (2.2) and equation (2), for all i, j we have

$$\begin{aligned} A \otimes B &= \max_k(a_{ik} + b_{kj}) \\ &= \max_k(a_{i1} + b_{1j}, \max_k(a_{i(k-1)} + 1 + b_{(k-1)j} + 1) \\ &= \max_k(a_{11} + b_{11} + (i-1)n + j - 1, \max_k(a_{11} + b_{11} + (i-n)n + (k-2)n + (k+j-1)) \end{aligned}$$

and

$$\begin{aligned} B \otimes A &= \max_k(b_{ik} + a_{kj}) \\ &= \max_k(b_{i1} + a_{1j}, \max_k(b_{i(k-1)} + 1 + a_{(k-1)} + 1) \\ &= \max_k(b_{11} + a_{11} + (i-1)n + (j-1), \max_k(b_{11} + a_1 + (i-1)n + (k-2)n + (k+j-1))) \end{aligned}$$

It clear that $A \otimes B = B \otimes A$ □

This commutativity property only holds on tropical increasing matrices in Definition (3.1). Here, we provide a counter example where we take any two tropical increasing matrices ($a_{ij} < a_{(i+1)j}, a_{ij} < a_{i(j+1)}$

Example 3.6. $A = \begin{bmatrix} -2 & -1 & 0 \\ 2 & 3 & 4 \\ 7 & 8 & 9 \end{bmatrix}$ and $B = \begin{bmatrix} -1 & 0 & 1 \\ -2 & -1 & 0 \\ 2 & 3 & 4 \end{bmatrix}$

$$A \otimes B = \begin{bmatrix} 2 & 3 & 4 \\ 6 & 7 & 8 \\ 11 & 12 & 13 \end{bmatrix}, \qquad B \otimes A = \begin{bmatrix} 8 & 9 & 10 \\ 7 & 8 & 9 \\ 11 & 12 & 13 \end{bmatrix}$$

$A \otimes B \neq B \otimes A$

We can also show that this commutativity property holds even if we add any tropical matrix in the middle as in the theorem below.

Theorem 3.7. *Let $A, B \in \mathcal{I}_n$ and $W \in M_n(\mathbb{Z})$ then $A \otimes W \otimes B = B \otimes W \otimes A$*

Proof. We have

$$\begin{aligned} A \otimes W \otimes B &= \max_{k,l}(a_{il} + w_{lk} + b_{kj}) \\ &= \max_{k,l}(a_{11} + (i-1)n + (l-1) + w_{lk} + b_{11} + (k-1)n + (j-1)) \\ &= \max_{k,l}(a_{11} + b_{11} + w_{lk} + (i-1)n + (l-1) + (k-1)n + (j-1)) \end{aligned}$$

$$\begin{aligned} B \otimes W \otimes A &= \max_{k,l}(b_{il} + w_{lk} + a_{kj}) \\ &= \max_{k,l}(b_{11} + (i-1)n + (l-1) + w_{lk} + a_{11} + (k-1)n + (j-1)) \\ &= \max_{k,l}(a_{11} + b_{11} + w_{lk} + (i-1)n + (l-1) + (k-1)n + (j-1) \end{aligned}$$

We prove that $A \otimes W \otimes B = B \otimes W \otimes A$ □

Corollary 3.8. *Suppose that matrices $A, B \in \mathcal{I}_n$ and $W \in M_n(\mathbb{Z})$ such that*

$$A \otimes W \otimes B \otimes W = B \otimes W \otimes A \otimes W$$

Since tropical increasing matrices has a unique eigenvalue and $\lambda = a_{nn}$ then we have $A^k = a_{nn} \otimes A^{k-1}$.

Increasing tropical matrices also has unique property for conjugate tropical matrices. First, we define tropical matrix conjugate $A^* = -A^T = -(a)_{ji}$ for all i, j. We can show that $A \otimes A^* \otimes A = A$ and $A^* \otimes A \otimes A^* = A^*$, respectively as in the following theorem.

Theorem 3.9. *Let $A \in \mathcal{I}_n$, then $A \otimes (-A)^T \otimes A = A$ and $-A^T \otimes A \otimes (-A^T) = -A^T$*

Proof.

$$\begin{aligned} (A \otimes A^* \otimes A)_{ij} &= \max_{k,l}(a_{il} + a^*_{lk} + a_{kj}) \\ &= \max_{k,l}(a_{11} + (i-1)n + (l-1) - (a_{11} + (k-1)n + (l-1)) + a_{11} + (k-1)n + (j-1)) \\ &= \max_{k,l}(a_{11} + (i-1)n + (l-1) - a_{11} - ((k-1)n) - (l-1) + a_{11} + (k-1)n + (j-1)) \\ &= \max(a_{11} + (i-1)n + (j-1)) \\ &= (a_{ij}) \\ &= (A)_{ij}. \end{aligned}$$

□

4. Public Key Cryptography Based on Tropical Increasing Matrices

In this section, we discuss two modification of Stickel's protocol using tropical increasing matrices

Protocol 1

Alice and Bob agree on public parameter matrix $W \in M_n(\mathbb{Z})$

(1) Alice chooses two random private topical matrices A_1, A_2.
(2) Bob chooses two random private tropical matrices B_1, B_2.
(3) Alice computes $U = A_1 \otimes W \otimes A_2$ and sends U to Bob.
(4) Bob computes $V = B_1 \otimes W \otimes B_2$ and send V to Alice.
(5) Alice calculates her private key $K_A = A_1 \otimes V \otimes A_2$
(6) Bob calculates his private key $K_B = B_1 \otimes U \otimes B_2$.

We can prove that $K_A = K_B$ as in the following equation

$$\begin{aligned} K_A &= A_1 \otimes V \otimes A_2 \\ &= A_1 \otimes B_1 \otimes W \otimes B_2 \otimes A_2 \\ &= B_1 \otimes A_1 \otimes W \otimes A_2 \otimes B_2 \\ &= B_1 \otimes U \otimes B_2 \\ &= K_B \end{aligned} \tag{3}$$

This protocol can be attacked easyly even the attacker does not know matrices A_1, A_2, B_1, B_2 because K_A and K_B in the form of tropical increasing matrices.

We can see in the following toy example

Example 4.1. Alice and Bob agree on public matrix $W = \begin{bmatrix} 34 & -36 & -6 \\ 26 & -34 & -16 \\ 46 & 11 & -43 \end{bmatrix}$. Then they exchange public key as in the following steps.

(1) Alice chooses two tropical increasing matrices $A_1 = \begin{bmatrix} 23 & 24 & 25 \\ 26 & 27 & 28 \\ 29 & 30 & 31 \end{bmatrix}$ and $A_2 = \begin{bmatrix} 86 & 87 & 88 \\ 89 & 90 & 91 \\ 92 & 93 & 94 \end{bmatrix}$.

(2) Bob chooses two tropical increasing matrices $B_1 = \begin{bmatrix} 82 & 83 & 84 \\ 85 & 86 & 87 \\ 88 & 89 & 90 \end{bmatrix}$ and $B_2 = \begin{bmatrix} 67 & 68 & 69 \\ 70 & 71 & 72 \\ 73 & 74 & 75 \end{bmatrix}$

(3) Alice sends $U = \begin{bmatrix} 157 & 158 & 159 \\ 160 & 161 & 162 \\ 163 & 164 & 165 \end{bmatrix}$ to Bob

(4) Bob sends $V = \begin{bmatrix} 197 & 198 & 199 \\ 200 & 201 & 202 \\ 203 & 204 & 205 \end{bmatrix}$ to Alice

(5) Alice has private key $K_A = \begin{bmatrix} 322 & 323 & 324 \\ 325 & 326 & 327 \\ 328 & 329 & 330 \end{bmatrix}$

(6) Bob has private key $K_B = \begin{bmatrix} 322 & 323 & 324 \\ 325 & 326 & 327 \\ 328 & 329 & 330 \end{bmatrix}$

From this example, we can see that $K_A = \lambda(U) \otimes U$

Therefore we construct another protocol as below

Protocol 2

Alice and Bob agree on matrix $W \in M_n(\mathbb{Z})$. They exchange public key in the following steps

(1) Alice chooses two random increasing tropical matrices A_1 and A_2 and makes them private.
(2) Bob chooses two random increasing tropical matrices B_1 and B_2 and makes them private.
(3) Alice computes and sends $U = A_1 \otimes W \otimes A_2 \otimes W$ to Bob
(4) Bob computes and sends $V = B_1 \otimes W \otimes B_2 \otimes W$ to Alice.
(5) Alice computes $K_A = A_1 \otimes V \otimes A_2$
(6) Bob computes $K_B = B_1 \otimes U \otimes B_2$

We can see that $K_A = K_B$ as follows.

$$\begin{aligned} K_A = A_1 \otimes V \otimes A_2 & \\ &= A_1 \otimes B_1 \otimes W \otimes B_2 \otimes W \otimes A_2 \\ &= B_1 \otimes A_1 \otimes W \otimes A_2 \otimes B_2 \\ &= K_B \end{aligned} \tag{4}$$

We suggest the parameters for this protocol

- the dimension of matrices of matrices 30×30.
- the entries of matrices in the interval $[-10^5, 10^5]$.

5. Conclusion

In this paper, we introduced new concept of tropical increasing matrices and showed that if A, B are increasing tropical matrices then $A \otimes B = B \otimes A$. We also proved that $A \otimes A^* \otimes A = A$ and $A^* \otimes A \otimes A^*$ for $A \in \mathcal{I}_n$ and $A*$ is a tropical conjugate matrices. We constructed two new Stickel's protocol using tropical increasing matrices. For further research we can analyse the security of the protocols.

Funding

This research is funding by Indonesian Mathematics Society (INDOMS)

6. References

References should be listed at the end of the main text in the order in which they are first cited in the text. The following list shows some sample references prepared in Taylor & Francis' Reference Style Q.

References

[1] P. Butkovi˘c, *Max-linear systems: theory and algorithms*, Springer Science & Business Media, 2010

[2] D. Grigoriev and V. Shpilrain. *Tropical cryptography II. extensions by homomorphisms.* Communications in Algebra, 47 (2018). pp. 4224–4229.

[3] D. Rudy and C. Monico. *Remarks on a tropical key exchange system.* International Journal of Mathematical Cryptology 15(2020), pp. 280–283.

[4] A. Muanalifah and S. Sergeev *On the tropical discrete logarithm problem and security of a protocol based on tropical semidirect product*, Communications in Algebra. 50 (2022),pp. 861–879

[5] A. Muanalifah and S. Sergeev *Modifying the tropical version of stickel's key exchange protocol*, Applications of Mathematics, Springer. 65 (2020), pp. 727–753.

[6] H. Huang, C. Li, and L. Deng. *Public-key cryptography based on tropical circular matrices.* Applied Sciences, 12(2022).

[7] M. Kotov and A. Ushakov. *Analysis of a key exchange protocol based on tropical matrix algebra.* Journal of Mathematical Cryptology, 12(2018). pp. 137—141.

[8] B. Amutha and R. Perumal. *Public key exchange protocols based on tropical lower circulant and anti circulant matrices.* AIMS Mathematics, 8(2023). pp. 17307— 17334.

[9] S. Isaac and D. Kahrobaei. *A closer look at the tropical cryptography.* International Journal of Computer Mathematics: Computer Systems Theory, 6(2021):pp. 137— 142.

[10] S. Alhussaini, C. Collett and S. Sergeev *On the tropical two-sided discrete logarithm and a key exchange protocol based on the tropical algebra of pairs*, Cryptology ePrint Archive, (2024).

[11] A. Muanalifah, A. Riana, R. Artes Jr., and N. Nurwan. *The tropical version of El Gamal Encryption*, Journal of Natural Sciences and Mathematics Research, 9(2023),pp. 151–157.

[12] J. Chen, J, D. Grigoriev, D. and V. Shpilrain, *Tropical cryptography III: digital signatures*, arXiv preprint arXiv:2309.11256, 2023.

[13] W. Diffie and M. E. Hellman *New Directions in Cryptography*, IEEE Transaction on Information Theory, VOL. IT-22(2008), pp. 644—654.

[14] E. Stickel *A New Method for Exchanging Secret Keys.* Third International Conference on Information Technology and Applications (ICITA'05), 2(2005), pp. 426–430.

[15] V. Shpilrain *Cryptanalysis of Stickel's key exchange scheme.* In: E.A. Hirsch et al. (eds.) Proceedings of the 3rd international computer science symposium in Russia, LNCS 5010 (2008), Zbl 1142.94360, MR 2475176, pp. 283—288.