Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 8(7): 17307–17334.
DOI:10.3934/math.2023885
Received: 27 January 2023
Revised: 24 April 2023
Accepted: 08 May 2023
Published: 19 May 2023

Research article

Public key exchange protocols based on tropical lower circulant and anti circulant matrices

B. Amutha and R. Perumal[*]

Department of Mathematics, Faculty of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur 603203, Tamilnadu, India

* **Correspondence:** Email: perumalr@srmist.edu.in.

Abstract: In recent years, many efficient key exchange protocols have been proposed based on matrices over the tropical semirings. The tropical addition of two elements is the minimum of the elements, while the tropical multiplication is the sum of the two elements. This paper proposes a novel key exchange protocol based on the min-plus semiring $(\mathbb{Z}\cup\{\infty\},\oplus,\otimes)$ by introducing anti-s-p-circulant matrices, which forms a commutative subset of $M_{n\times n}(\mathbb{Z}\cup\{\infty\})$. We have given further analysis of the protocol in detail using upper or lower-s-circulant matrices. Additionally, we prove that the set of all lower-s-circulant matrices is a sub-semiring of the tropical semiring $M_{n\times n}(\mathbb{Z}\cup\{\infty\})$. We discuss the detailed security analysis of the protocol with upper or lower-s-circulant matrices and provide cryptographic algorithms for both key exchange protocols with detailed explanations. We compare the protocol based on upper or lower-s-circulant matrices and our proposed protocol in terms of time complexity and memory usage. Finally, we analyse the security and show that our protocol is safe against popular attacks of tropical key exchange protocols. The security of these protocols relies on the difficulty of solving tropical non-linear equations.

Keywords: lower-s-circulant matrix; anti-s-p-circulant matrix; tropical semiring; tropical cryptography; key exchange protocol
Mathematics Subject Classification: 11T71, 14G50, 14M25, 15B51, 52B20

1. Introduction

‘Cryptography’ is the process of establishing secure communication between the sender and the receiver of information [1, 2]. The sender uses a method called ‘encryption’ to turn plaintext into a secret message called ‘ciphertext’, while the receiver uses a method called ‘decryption’ to convert the ciphertext back into plaintext [3,4]. A ‘key’ is secret common knowledge shared by both entities. There are two broad types of cryptography: symmetric key cryptography and asymmetric key cryptography.

Symmetric key cryptography uses a single secret key for both encryption and decryption, which is only known by the sender and the receiver [5]. In asymmetric key cryptography, one key is used for encryption, and a different key is used for decryption [3,6]. Many varieties of cryptographic algorithms have been constructed over classical algebra [2]. Cryptographic algorithms over tropical algebra have gained significance in recent years, and tropical cryptography is one of the fields used to construct secure cryptographic algorithms. Martin Hellman and Whitfield Diffie suggested the two-keys cryptosystem in 1976 to overcome the issue of key distribution in symmetric key cryptography [4, 7]. The general protocol that uses semi-direct products of semigroups was introduced in [8], and one of its special cases is the standard Diffie-Hellman protocol based on cyclic groups. This paper gives a conjecture that, when the protocol is used with non-commutative semigroups, it acquires several useful features. They suggest the extension of a particular non-commutative semigroup of matrices over a certain finite group ring by a conjugation automorphism as a suitable platform. However, the protocol introduced in [8] was attacked by the linear algebra attack [9]. The Cramer-Shoup scheme was introduced in [10] and proved to be secure against adaptive chosen ciphertext attacks. Stickel proposed the key exchange protocol based on classical algebra [11], which was then attacked by Shpilrain [12]. Grigoriev and Shpilrain extended Stickel's protocol by using tropical polynomials and showed that solving the system of tropical linear equations was NP-hard [13]. An advantage of using tropical algebras as the platform for building key exchange schemes is that, in tropical schemes, one does not have to perform any classical multiplication since tropical multiplication is classical addition and is not invertible [14–16]. However, the major weakness of the tropical protocol is that the tropical powers of the matrices exhibit a particular pattern, as noted by Kotov and Ushakov. This pattern helps them to attack Grigoriev's key exchange protocol [17]. Grigoriev and Shpilrain's next key exchange protocol was based on semidirect product [18], but it had the weakness that the sequence $(M, H)^l$ is linearly ordered, which was found by Rudy and Monico [19]. Issac and Kahrobaei implemented the linear periodicity attack [20] to attack the same protocol that used semidirect product. These attacks showed that key exchange protocols with matrix powers over the tropical approach are easily attackable. Different attacks of various tropical key exchange protocols were consolidated in [6]. The significance of our research is that our protocols are related to the tropical two sided matrix action problem that can be reduced to a system of non-linear equations, and solving such a system is NP-hard [13].

Our contribution: In this paper, we propose a key exchange protocol over the tropical semiring with min-plus operation. We avoid using power and linearly ordered operations over tropical concepts to ensure the safety of our schemes against popular attacks. We introduce the abelian subset $((\mathfrak{A}(D_p[\mathfrak{C}])_l^u)(s))_n, \oplus, \otimes)$ of the semiring $(M_{n\times n}(\mathfrak{Z}), \oplus, \otimes)$, which is obtained by modifying the set of p-circulant matrices and use it to frame our new protocol. Similarly, the protocol introduced in [21] uses the set of upper-t-circulant matrices, which is also obtained by modifying the set of circulant matrices. We provide a detailed analysis of the protocol using upper-t-circulant matrix [21] replaced by the protocol using lower-s-circulant matrix. We compare the protocols using the lower-s-circulant matrix instead of the upper-t-circulant matrix in the protocol introduced in [21] with our proposed protocol. We also provide some propositions on the commutativity of the set of lower-s-circulant matrices $(\mathfrak{C}_l(s))_n, \oplus, \otimes)$ and the commutative property of the set of anti-s-p-circulant matrices. We also give some propositions on the security of both protocols. We provide the security analysis of our proposed protocol against the existing tropical attacks of Kotov & Ushakov, Rudy & Monico.

The rest of the sections are organized as follows. In Section 2, we discuss some basic definitions and notations. Section 3 contains an analysis of key exchange protocol 1, which uses the lower-s-circulant matrix, the key generation scheme of protocol 1 with cryptographic algorithm, and an example. Similarly, in Section 4, we discuss our proposed key exchange protocol, the key generation scheme with the algorithm and an example. We also provide the security analysis of proposed protocol 2 in Section 4. Section 5 contains a comparative analysis of the protocol based on upper or lower-s-circulant matrices and our proposed protocol with the experimental results like time complexity, memory usage and possible attacks for both protocols.

2. Preliminaries

Definition 1. [22] A non-empty set S with two binary operations addition $(+)$ and multiplication $(\cdot)$ is called a semiring, if it satisfies the following axioms:

1) S is an abelian monoid under the operation addition with '0' as the unique identity element,
2) S is a monoid under the operation multiplication with a unique identity element denoted by '1',
3) $u \cdot (v + w)$ is equal to $u \cdot v + u \cdot w$ and $(v + w) \cdot u$ is equal to $v \cdot u + w \cdot u \ \forall\ u, v, w \in S$,
4) Both $u \cdot 0$ and $0 \cdot u$ are equal to $0 \ \forall\ u \in S$,
5) The identities under the two operations should not be the same element.

Example 2.1. The set $\mathbb{N} \cup \{0\}$ forms a semiring under the operations classical addition and classical multiplication where, $\mathbb{N}$ is the set of all natural numbers.

Definition 2. The following are the two tropical binary operations.

- $x \oplus y = max(x, y)$ (or) $x \oplus y = min(x, y)$.
- $x \odot y = x + y$.

Definition 3. [22] A set $R = S \cup \{\infty\}$ under the operations '$\oplus$' (tropical addition, (min)) and '$\otimes$' (tropical multiplication) is called a min-plus semiring if,

1) $u \oplus v = v \oplus u \ \forall\ u, v \in R$,
2) $(u \oplus v) \oplus w = u \oplus (v \oplus w)$ and $(u \otimes v) \otimes w = u \otimes (v \otimes w) \ \forall\ u, v, w \in R$,
3) $u \otimes (v \oplus w) = (u \otimes v) \oplus (u \otimes w) \ \forall\ u, v, w \in R$,
4) $\exists\ e \in R\ \forall\ u \in R$ such that $e \oplus u = u \oplus e = u$ (Here, the additive identity is '∞'),
5) inverse does not exist.

Let $\mathbb{Z}$ denote the set of all integers and $\mathfrak{Z} = \mathbb{Z} \cup \{\infty\}$. In this paper, we have concentrated on the min-plus semiring $R = (\mathfrak{Z}, \oplus, \otimes)$.

We know that $(\mathfrak{Z}, \oplus, \otimes)$ is a commutative semiring with additive identity and multiplicative identity '∞' and '0' respectively. Let $M_{n\times n}(\mathfrak{Z})$ denote the set of all $n \times n$ matrices over $\mathfrak{Z}$.

2.1. Matrices over the min-plus semiring

The collection of all matrices over the semiring S with 'm' rows and 'n' columns is denoted by $M_{m\times n}(R)$. Let $A \in M_{m\times n}(R)$. Every ij^{th} element of A is denoted by 'a_{ij}'. Let $P = (p_{ij}) \in M_{m\times n}(R)$, $Q = (q_{ij}) \in M_{m\times n}(R)$, $T = (t_{ij}) \in M_{n\times l}(R)$ and $\alpha \in R$.

In min-plus algebra [14–16] addition of two matrices is calculated by

$$P \oplus Q = (\min((p_{ij}), (q_{ij})))_{m\times n}$$

and multiplication of two matrices is calculated by

$$P \otimes T = \min\{((p_{ik}) + (t_{kj}))\}_{m\times l}$$

where, $k \in \{1, 2, \cdots, n\}$

$$\alpha \otimes P = \alpha \otimes p_{ij} = \alpha + p_{ij}$$

Example 2.2. The following is an example of tropical addition, tropical multiplication of two matrices and the tropical addition, tropical multiplication of a matrix.

$$\text{Let } A = \begin{bmatrix} 2 & -11 \\ 4 & 9 \end{bmatrix}, B = \begin{bmatrix} 15 & 21 \\ -18 & 34 \end{bmatrix}, \alpha = 9$$

$$A \oplus B = \begin{bmatrix} 2 & -11 \\ -18 & 9 \end{bmatrix}$$

$$A \otimes B = \begin{bmatrix} -29 & 23 \\ -9 & 25 \end{bmatrix}$$

$$\alpha \otimes A = \begin{bmatrix} 9 & \infty \\ \infty & 9 \end{bmatrix} \otimes \begin{bmatrix} 2 & -11 \\ 4 & 9 \end{bmatrix} = \begin{bmatrix} 11 & -2 \\ 13 & 18 \end{bmatrix}$$

$$\alpha \oplus A = \begin{bmatrix} 2 & -11 \\ 4 & 9 \end{bmatrix}$$

Definition 4. A matrix $T \in M_{n\times n}(\mathfrak{Z})$ is said to be circulant $C_{n\times n}$ with entries $c_1, c_2, \cdots, c_n$ if it is of the form

$$\begin{bmatrix} c_1 & c_n & c_{n-1} & \cdots & c_2 \\ c_2 & c_1 & c_n & \cdots & c_3 \\ c_3 & c_2 & c_1 & \cdots & c_4 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_n & c_{n-1} & c_{n-2} & \cdots & c_1 \end{bmatrix}$$

Definition 5. A matrix $T \in M_{n\times n}(\mathfrak{Z})$ is said to be lower-s-circulant if the matrix is of the form

$$\begin{bmatrix} c_1 & c_n & c_{n-1} & \cdots & c_2 \\ s \otimes c_2 & c_1 & c_n & \cdots & c_3 \\ s \otimes c_3 & s \otimes c_2 & c_1 & \cdots & c_4 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s \otimes c_n & s \otimes c_{n-1} & s \otimes c_{n-2} & \cdots & c_1 \end{bmatrix}$$

where $c_1, c_2, \cdots, c_n, s \in \mathfrak{Z}$. The set of all lower-$s$-circulant matrix of order 'n' is denoted by $(\mathfrak{C}_l(s))_n$. Here, 'l' denotes that the element 's' is added in all the 'lower diagonal' entries.

Example 2.3. An example of lower-2-circulant matrix is given below.

$$\text{Let} \quad \mathfrak{C} = \begin{bmatrix} 4 & 17 & 23 & 12 \\ 12 & 4 & 17 & 23 \\ 23 & 12 & 4 & 17 \\ 17 & 23 & 12 & 4 \end{bmatrix}$$

Then,

$$\mathfrak{C}_l(2)_4 = \begin{bmatrix} 4 & 17 & 23 & 12 \\ 14 & 4 & 17 & 23 \\ 25 & 14 & 4 & 17 \\ 19 & 25 & 14 & 4 \end{bmatrix}$$

Proposition 2.4. *If $A \in (\mathfrak{C}_l(s))_n$, $B \in (\mathfrak{C}_l(t))_n$ and $s \neq t$, then $A \otimes B \neq B \otimes A$.*

Proof. Let $A \in (\mathfrak{C}_l(s))_n$ and $B \in (\mathfrak{C}_l(t))_n$

$$A = \begin{bmatrix} a_1 & a_n & a_{n-1} & \cdots & a_2 \\ a_2 + s & a_1 & a_n & \cdots & a_3 \\ a_3 + s & a_2 + s & a_1 & \cdots & a_4 \\ a_4 + s & a_3 + s & a_2 + s & \cdots & a_5 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n + s & a_{n-1} + s & a_{n-2} + s & \cdots & a_1 \end{bmatrix}, B = \begin{bmatrix} b_1 & b_n & b_{n-1} & \cdots & b_2 \\ b_2 + t & b_1 & b_n & \cdots & b_3 \\ b_3 + t & b_2 + t & b_1 & \cdots & b_4 \\ b_4 + t & b_3 + t & b_2 + s & \cdots & b_5 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_n + t & b_{n-1} + t & b_{n-2} + t & \cdots & b_1 \end{bmatrix}$$

To prove the non-commutativity of $\mathfrak{C}_l(s)_n$ and $\mathfrak{C}_l(t)_n$, it is enough to prove that $(A \otimes B)_{ij} \neq (B \otimes A)_{ij}$ for some $1 \leq i, j \leq n$.

Let us calculate the value of $(A \otimes B)_{11}$ and $(B \otimes A)_{11}$. We get,

$$(A \otimes B)_{11} = \min\{a_1 + b_1, a_n + b_2 + t, a_{n-1} + b_3 + t, a_{n-2} + b_4 + t, \cdots, a_2 + b_n + t\}$$

$$(B \otimes A)_{11} = \min\{b_1 + a_1, b_n + a_2 + s, b_{n-1} + a_3 + s, b_{n-2} + a_4 + s, \cdots, b_2 + a_n + s\}$$

Since $s \neq t$, we have $(A \otimes B)_{11} \neq (B \otimes A)_{11}$. Thus, $A \otimes B \neq B \otimes A$. □

Definition 6. A matrix $T \in M_{n \times n}(\mathfrak{Z})$ is said to be an anti-s-circulant $(\mathfrak{A}\mathfrak{C}_l^u(s))_n$ matrix with entries $c_1, c_2, \cdots, c_n, s$ if it is of the form

$$\begin{bmatrix} s \otimes c_1 & s \otimes c_n & \cdots & s \otimes c_3 & c_2 \\ s \otimes c_2 & s \otimes c_1 & \cdots & c_4 & s \otimes c_3 \\ s \otimes c_3 & s \otimes c_2 & \cdots & s \otimes c_5 & s \otimes c_4 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s \otimes c_{n-1} & c_{n-2} & \cdots & s \otimes c_1 & s \otimes c_n \\ c_n & s \otimes c_{n-1} & \cdots & s \otimes c_2 & s \otimes c_1 \end{bmatrix}$$

where $c_1, c_2, \cdots, c_n, s \in \mathfrak{Z}$ and set of all anti-s-circulant matrix of order 'n' is denoted by $(\mathfrak{A}\mathfrak{C}_l^u(s))_n$. Here, '$l$' and '$u$' denote that '$s$' is added to both upper and lower anti-diagonals.

Definition 7. A matrix $T \in M_{n\times n}(\mathfrak{Z})$ is said to be an anti-s-p-circulant with entries $c_1, c_2, \cdots, c_n, s$ if it is of the form

$$\begin{bmatrix} s\otimes c_1 & s\otimes c_n & \cdots & s\otimes c_3 & c_2 \\ s\otimes c_2 & s\otimes c_1 & \cdots & c_4 & s\otimes c_3 \\ s\otimes c_3 & s\otimes c_2 & \cdots & s\otimes c_5 & s\otimes c_4 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s\otimes c_{n-1} & c_{n-2} & \cdots & s\otimes c_1 & s\otimes c_n \\ c_n & s\otimes c_{n-1} & \cdots & s\otimes c_2 & s\otimes c_1 \end{bmatrix}$$

where, $c_k - c_{k+1} = p \ \forall\ 1 \le k \le n$ and $p \in \mathbb{Z}$ and the set of all anti-s-p-circulant matrix of order 'n' is denoted by $(\mathfrak{A}(D_p[\mathfrak{C}])^u_l)(s))_n$.

Example 2.5. An example of lower-13-circulant matrix and anti-13-circulant matrix of order 4 is given below.

$$\text{Let} \quad \mathfrak{C} = \begin{bmatrix} 5 & 21 & 7 & -4 \\ -4 & 5 & 21 & 7 \\ 7 & -4 & 5 & 21 \\ 21 & 7 & -4 & 5 \end{bmatrix}$$

The lower-13-circulant matrix of $\mathfrak{C}$ is,

$$(\mathfrak{C}_l(13))_4 = \begin{bmatrix} 5 & 21 & 7 & -4 \\ -4\otimes 13 & 5 & 21 & 7 \\ 7\otimes 13 & -4\otimes 13 & 5 & 21 \\ 21\otimes 13 & 7\otimes 13 & -4\otimes 13 & 5 \end{bmatrix} = \begin{bmatrix} 5 & 21 & 7 & -4 \\ 9 & 5 & 21 & 7 \\ 20 & 9 & 5 & 21 \\ 34 & 20 & 9 & 5 \end{bmatrix}$$

The anti-13-circulant matrix of $\mathfrak{C}$ is,

$$(\mathfrak{A}\mathfrak{C}^u_l(13))_4 = \begin{bmatrix} 5\otimes 13 & 21\otimes 13 & 7\otimes 13 & -4 \\ -4\otimes 13 & 5\otimes 13 & 21 & 7\otimes 13 \\ 7\otimes 13 & -4 & 5\otimes 13 & 21\otimes 13 \\ 21 & 7\otimes 13 & -4\otimes 13 & 5\otimes 13 \end{bmatrix} = \begin{bmatrix} 18 & 34 & 20 & -4 \\ 9 & 18 & 21 & 20 \\ 20 & -4 & 18 & 34 \\ 21 & 20 & 9 & 18 \end{bmatrix}$$

An example of anti-13-5-circulant matrix is,

$$\mathfrak{A}(D_5[\mathfrak{C}])^u_l)(13))_4 = \begin{bmatrix} 5\otimes 13 & 20\otimes 13 & 15\otimes 13 & 10 \\ 10\otimes 13 & 5\otimes 13 & 20 & 15\otimes 13 \\ 15\otimes 13 & 10 & 5\otimes 13 & 20\otimes 13 \\ 20 & 15\otimes 13 & 10\otimes 13 & 5\otimes 13 \end{bmatrix} = \begin{bmatrix} 18 & 33 & 28 & 10 \\ 23 & 18 & 20 & 28 \\ 28 & 10 & 18 & 33 \\ 20 & 28 & 23 & 18 \end{bmatrix}$$

Proposition 2.6. *If $A \in ((\mathfrak{A}(D_p[\mathfrak{C}])^u_l)(s))_n, B \in ((\mathfrak{A}(D_p[\mathfrak{C}])^u_l)(t))_n$, then $A\otimes B \neq B\otimes A \ \forall\ s \neq t$.*

Proof. Let $A \in ((\mathfrak{A}(D_p[\mathfrak{C}])^u_l)(s))_n, B \in ((\mathfrak{A}(D_p[\mathfrak{C}])^u_l)(t))_n$

$$A = \begin{bmatrix} a_1+s & a_n+s & a_{n-1}+s & \cdots & a_2 \\ a_2+s & a_1+s & a_n+s & \cdots & a_3+s \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ a_{n-1}+s & a_{n-2} & a_{n-3}+s & \cdots & a_n+s \\ a_n & a_{n-1}+s & a_{n-2}+s & \cdots & a_1+s \end{bmatrix}, B = \begin{bmatrix} b_1+t & b_n+t & b_{n-1}+t & \cdots & b_2 \\ b_2+t & b_1+t & b_n+t & \cdots & b_3+t \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ b_{n-1}+t & b_{n-2} & b_{n-3}+t & \cdots & b_n+t \\ b_n & b_{n-1}+t & b_{n-2}+t & \cdots & b_1+t \end{bmatrix}$$

To prove the non-commutativity of the set $((\mathfrak{A}(D_p[\mathfrak{C}])^u_l)(s))_n$ and $((\mathfrak{A}(D_p[\mathfrak{C}])^u_l)(t))_n$, it is enough to prove that $(A \otimes B)_{ij} \neq (B \otimes A)_{ij}$ for some $1 \leq i, j \leq n$.
Let us compare $(A \otimes B)_{12}$ and $(B \otimes A)_{12}$,

$$(A \otimes B)_{12} = \min\{a_1 + s + b_n + t, a_n + s + b_1 + t, a_{n-1} + s + b_2 + t, \cdots, a_3 + s + b_{n-2}, a_2 + b_{n-1} + t\}$$

$$(B \otimes A)_{12} = \min\{b_1 + t + a_n + s, b_n + t + a_1 + s, b_{n-1} + t + a_2 + s, \cdots, b_3 + t + a_{n-2}, b_2 + a_{n-1} + s\}$$

since $s \neq t$, it implies $(A \otimes B)_{12} \neq (B \otimes A)_{12}$ and hence $A \otimes B \neq B \otimes A$. □

Proposition 2.7. $(\mathfrak{C}_l(s))_n$ *(set of all lower-s-circulant matrices over* $\mathfrak{Z}$*) is a commutative tropical semiring and a subsemiring of* $M_{n\times n}(\mathfrak{Z})$*.*

Proof. 1) To prove that $(\mathfrak{C}_l(s))_n$ is a subsemiring of $M_{n\times n}(\mathfrak{Z})$ it is enough to prove that it is closed under tropical addition and tropical multiplication. Let $A, B \in (\mathfrak{C}_l(s))_n$ with entries $a_1, a_2, \cdots, a_n, a_1 + s, a_2 + s, \cdots, a_n + s$ and $b_1, b_2, \cdots, b_n, b_1 + s, b_2 + s, \cdots, b_n + s$ respectively.

$$A = \begin{bmatrix} a_1 & a_n & a_{n-1} & \cdots & a_2 \\ a_2 + s & a_1 & a_n & \cdots & a_3 \\ a_3 + s & a_2 + s & a_1 & \cdots & a_4 \\ a_4 + s & a_3 + s & a_2 + s & \cdots & a_5 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n + s & a_{n-1} + s & a_{n-2} + s & \cdots & a_1 \end{bmatrix}, B = \begin{bmatrix} b_1 & b_n & b_{n-1} & \cdots & b_2 \\ b_2 + s & b_1 & b_n & \cdots & b_3 \\ b_3 + s & b_2 + s & b_1 & \cdots & b_4 \\ b_4 + s & b_3 + s & b_2 + s & \cdots & b_5 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_n + s & b_{n-1} + s & b_{n-2} + s & \cdots & b_1 \end{bmatrix}$$

(a) Clearly $(\mathfrak{C}_l(s))_n$ is closed under tropical addition.

$$A \oplus B = \begin{bmatrix} \min\{a_1, b_1\} & \min\{a_n, b_n\} & \min\{a_{n-1}, b_{n-1}\} & \cdots & \min\{a_2, b_2\} \\ \min\{a_2, b_2\} + s & \min\{a_1, b_1\} & \min\{a_n, b_n\} & \cdots & \min\{a_3, b_3\} \\ \min\{a_3, b_3\} + s & \min\{a_2, b_2\} + s & \min\{a_1, b_1\} & \cdots & \min\{a_4, b_4\} \\ \min\{a_4, b_4\} + s & \min\{a_3, b_3\} + s & \min\{a_2, b_2\} + s & \cdots & \min\{a_5, b_5\} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \min\{a_n, b_n\} + s & \min\{a_{n-1}, b_{n-1}\} + s & \min\{a_{n-2}, b_{n-2}\} + s & \cdots & \min\{a_1, b_1\} \end{bmatrix} \in (\mathfrak{C}_l(s))_n$$

(b) Let the entry $(A \otimes B)_{ij}$ denotes the ij^{th} entry of the matrix $A \otimes B$. $(C)_k$ and $(D)_k$, $1 \leq k \leq n$ be the entries of circulant matrices to generate the lower-s-circulant matrices $A \otimes B$ and $B \otimes A$ respectively. Assume that $A, B \in (\mathfrak{C}_l(s))_n$. To prove that the set of all lower-s-circulant matrices are closed under the tropical multiplication, it is enough to prove that the matrix $A \otimes B$ is also in the following form

$$\begin{bmatrix} (C)_1 & (C)_n & (C)_{n-1} & (C)_{n-2} & \cdots & (C)_2 \\ (C)_2 + s & (C)_1 & (C)_n & (C)_{n-1} & \cdots & (C)_3 \\ (C)_3 + s & (C)_2 + s & (C)_1 & (C)_n & \cdots & (C)_4 \\ (C)_4 + s & (C)_3 + s & (C)_2 + s & (C)_1 & \cdots & (C)_5 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ (C)_n + s & (C)_{n-1} + s & (C)_{n-2} + s & (C)_{n-3} + s & \cdots & (C)_1 \end{bmatrix}$$

The diagonal entries of the tropical multiplication $A \otimes B$ of the matrices A and B are,

$$(A \otimes B)_{11} = \min\{a_1 + b_1, a_n + b_2 + s, a_{n-1} + b_3 + s, a_{n-2} + b_4 + s, \cdots, a_2 + b_n + s\}$$
$$(A \otimes B)_{22} = \min\{a_2 + b_n + s, a_1 + b_1, a_n + b_2 + s, a_{n-1} + b_3 + s, \cdots a_3 + b_{n-1} + s\}$$
$$\vdots$$
$$(A \otimes B)_{nn} = \min\{a_n + b_2 + s, a_{n-1} + b_3 + s, a_{n-2} + b_4 + s, a_{n-3} + b_5 + s, \cdots a_1 + b_1\}$$

By rearranging the terms, it is clear that $(A \otimes B)_{kk}$ are equal for all $1 \leq k \leq n.$ In general, let us call these entries as $(C)_1$.

$$(A \otimes B)_{11} = (A \otimes B)_{22} = \cdots = (A \otimes B)_{nn} = (C)_1$$

$$(C)_1 = \min\{a_1 + b_1, a_n + b_2 + s, a_{n-1} + b_3 + s, a_{n-2} + b_4 + s, \cdots, a_2 + b_n + s\}$$

Now, the upper off diagonal entries are obtained as follows,

$$(A \otimes B)_{12} = \min\{a_1 + b_n, a_n + b_1, a_{n-1} + b_2 + s, a_{n-2} + b_3 + s, \cdots, a_2 + b_{n-1} + s\}$$
$$(A \otimes B)_{23} = \min\{a_2 + b_{n-1} + s, a_1 + b_n, a_n + b_1, a_{n-1} + b_2 + s, \cdots, a_3 + b_{n-2} + s\}$$
$$\vdots$$
$$(A \otimes B)_{(n-1)n} = \min\{a_{n-1} + b_{n-(n-2)} + s, a_{n-2} + b_{n-3} + s, , \cdots, a_1 + b_n, a_n + b_1\}$$

By rearranging the terms, we can see that the entries $(A \otimes B)_{(k-1)k}$ are equal for all $2 \leq k \leq n.$ We denote this value as $(C)_n$ in general

$$(A \otimes B)_{12} = (A \otimes B)_{23} = \cdots = (A \otimes B)_{(n-1)n} = (C)_n$$

Then,

$$(C)_n = \min\{a_1 + b_n, a_n + b_1, a_{n-1} + b_2 + s, a_{n-2} + b_3 + s, \cdots, a_2 + b_{n-1} + s\}$$

The next upper off diagonal elements are obtained as,

$$(A \otimes B)_{13} = \min\{a_1 + b_{n-1}, a_n + b_n, a_{n-1} + b_1, a_{n-2} + b_2 + s, \cdots, a_2 + b_{n-2} + s\}$$

$$(A \otimes B)_{24} = \min\{a_2 + b_{n-2} + s, a_1 + b_{n-1}, a_n + b_n, a_{n-1} + b_1, \cdots, a_3 + b_{n-3} + s\}$$
$$\vdots$$
$$(A \otimes B)_{(n-2)n} = \min\{a_{n-1} + b_{n-(n-3)} + s, a_{n-2} + b_{n-4} + s, , \cdots, a_1 + b_1, a_n + b_n\}$$

Again by rearranging the terms, it is clear that the entries $(A \otimes B)_{(k-2)k}$ are equal $\forall\ 3 \leq k \leq n.$ We name these entries as $(C)_{n-1}$ in general.

$$(A \otimes B)_{13} = (A \otimes B)_{24} = \cdots = (A \otimes B)_{(n-2)n} = (C)_{n-1}$$

Then,

$$(C)_{n-1} = \min\{a_1 + b_{n-1}, a_n + b_n, a_{n-1} + b_1, a_{n-2} + b_2 + s, \cdots, a_2 + b_{n-2} + s\}$$

The entries $(A \otimes B)_{1(n-1)}, (A \otimes B)_{2n}$ are obtained as,

$$(A \otimes B)_{1(n-1)} = \min\{a_3 + b_1, a_2 + b_2 + s, a_1 + b_3, a_n + b_4, \cdots, a_3 + b_1\}$$

$$(A \otimes B)_{2n} = \min\{a_2 + b_2 + s, a_1 + b_3, a_n + b_4, a_{n-1} + b_5 + s, \cdots, a_3 + b_1\}$$

In general, we denote it as $(C)_3$. Then,

$$(C)_3 = \min\{a_2 + b_2 + s, a_1 + b_3, a_n + b_4, a_{n-1} + b_5 + s, \cdots, a_3 + b_1\}$$

By continuing this process, finally we end up with the entry $(A \otimes B)_{1n}$. We name this entry as $(C)_2$

$$(A \otimes B)_{1n} = (C)_2 = \min\{a_1 + b_2, a_n + b_3, a_{n-1} + b_4, a_{n-2} + b_5, \cdots, a_2 + b_1\}$$

Similarly, we obtained the lower off diagonal elements with following values

$$(A \otimes B)_{21} = \min\{a_2 + b_1 + s, a_1 + b_2 + s, a_n + b_3 + s, a_{n-1} + b_4 + s, \cdots, a_3 + b_n + s\}$$

$$(A \otimes B)_{32} = \min\{a_3 + b_n + s, a_2 + b_1 + s, a_1 + b_2 + s, a_1 + b_3 + s, \cdots, a_5 + b_{n-1} + s\}$$

$$\vdots$$

$$(A \otimes B)_{n(n-1)} = \min\{a_n + b_3 + s, a_{n-1} + b_4 + s, a_{n-2} + b_5 + s, a_{n-3} + b_6 + s, \cdots, a_1 + b_2 + s\}$$

By rearranging the above terms, we can see that $(A \otimes B)_{k(k-1)}$ are equal for all $2 \leq k \leq n.$ That is, $(A \otimes B)_{21} = (A \otimes B)_{32} = \cdots = (A \otimes B)_{n(n-1)}$

$$= \min\{a_2 + b_1 + s, a_1 + b_2 + s, a_n + b_3 + s, a_{n-1} + b_4 + s, \cdots, a_3 + b_n + s\}$$

$$= \min\{a_1 + b_2, a_n + b_3, a_{n-1} + b_4, a_{n-2} + b_5, \cdots, a_2 + b_1\} + s = (C)_2 + s$$

Now, the second lower off diagonal entries are obtained as,

$$(A \otimes B)_{31} = \min\{a_3 + b_1 + s, a_2 + b_2 + 2s, a_1 + b_3 + s, a_n + b_4 + s, \cdots, a_4 + b_n + s\}$$

$$(A \otimes B)_{42} = \min\{a_4 + b_n + s, a_3 + b_1 + s, a_2 + b_2 + 2s, a_1 + b_3 + s, \cdots, a_5 + b_{n-1} + s\}$$

$$\vdots$$

$$(A \otimes B)_{n(n-2)} = \min\{a_2 + b_2 + 2s, a_1 + b_3 + s, a_n + b_4 + s, a_{n-1} + b_5 + s, \cdots, a_3 + b_1 + s\}$$

Again, second lower off diagonal elements $(A \otimes B)_{k(k-2)}$ are equal for all $3 \leq k \leq n.$ Which can be denoted as

$$(A \otimes B)_{31} = (A \otimes B)_{42} = \cdots = (A \otimes B)_{(n+2)n}$$

$$= \min\{a_3 + b_1 + s, a_2 + b_2 + 2s, a_1 + b_3 + s, a_n + b_4 + s, \cdots, a_4 + b_n + s\}$$

$$= \min\{a_2 + b_2 + s, a_1 + b_3, a_n + b_4, a_{n-1} + b_5 + s, \cdots, a_3 + b_1\} + s = (C)_3 + s$$

Again by continuing this process, the final lower off diagonal entry is obtained as,

$$\begin{aligned}(A \otimes B)_{n1} &= \min\{a_n + b_1 + s, a_{n-1} + b_2 + 2s, a_{n-2} + b_3 + 2s, a_{n-3} + b_4 + 2s, \cdots, a_1 + b_n + s\}\\ &= \min\{a_1 + b_n, a_n + b_1, a_{n-1} + b_2 + s, a_{n-2} + b_3 + s, \cdots, a_2 + b_{n-1} + s\} + s\\ &= (C)_n + s\end{aligned}$$

By placing all obtained elements in the following matrix of order n we get the form of lower-s-circulant matrix

$$A \otimes B = \begin{bmatrix} (C)_1 & (C)_n & (C)_{n-1} & (C)_{n-2} & \cdots & (C)_2 \\ (C)_2 + s & (C)_1 & (C)_n & (C)_{n-1} & \cdots & (C)_3 \\ (C)_3 + s & (C)_2 + s & (C)_1 & (C)_n & \cdots & (C)_4 \\ (C)_4 + s & (C)_3 + s & (C)_2 + s & (C)_1 & \cdots & (C)_5 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ (C)_n + s & (C)_{n-1} + s & (C)_{n-2} + s & (C)_{n-3} + s & \cdots & (C)_1 \end{bmatrix}$$

Hence, it is proved that the set of all lower-s-circulant matrix is closed under tropical multiplication.

2) To show that $(\mathfrak{C}_l(s))_n$ is commutative, it is enough to show that $(C)_k = (D)_k$ and $(C)_k + s = (D)_k + s$ for all $1 \leq k \leq n$.
Since we found the entries of $A \otimes B$ in the previous proof, it is enough to find the entries of $B \otimes A$.

$$(D)_1 = \min\{b_1 + a_1, b_n + a_2 + s, b_{n-1} + a_3 + s, b_{n-2} + a_4 + s, \cdots, b_2 + a_n + s\}$$

By rearranging the terms we get,

$$\begin{aligned} (D)_1 &= \min\{a_1 + b_1, a_n + b_2 + s, a_{n-1} + b_3 + s, a_{n-2} + b_4 + s, \cdots, a_2 + b_n + s\} \\ &= (C)_1 \end{aligned}$$

Similarly,

$$\begin{aligned} (D)_2 &= \min\{b_1 + a_2, b_n + a_3, b_{n-1} + a_4, b_{n-2} + a_5, \cdots, b_2 + a_1\} \\ &= \min\{a_1 + b_2, a_n + b_3, a_{n-1} + b_4, a_{n-2} + b_5, \cdots, a_2 + b_1\} \\ &= (C)_2 \end{aligned}$$

Also,

$$\begin{aligned} (D)_3 &= \min\{b_2 + a_2 + s, b_1 + a_3, b_n + a_4, b_{n-1} + a_5 + s, \cdots, b_3 + a_1\} \\ &= \min\{a_2 + b_2 + s, a_1 + b_3, a_n + b_4, a_{n-1} + b_5 + s, \cdots, a_3 + b_1\} \\ &= (C)_3 \end{aligned}$$

By continuing this process, we obtain the entry $(B \otimes A)_{n-1}$ as,

$$\begin{aligned} (D)_{n-1} &= \min\{b_1 + a_{n-1}, b_n + a_n, b_{n-1} + a_1, b_{n-2} + a_2 + s, \cdots, b_2 + a_{n-2} + s\} \\ &= \min\{a_1 + b_{n-1}, a_n + b_n, a_{n-1} + b_1, a_{n-2} + b_2 + s, \cdots, a_2 + b_{n-2} + s\} \\ &= (C)_{n-1} \end{aligned}$$

Finally, the term $(B \otimes A)_n$ is obtained as,

$$\begin{aligned} (D)_n &= \min\{b_1 + a_n, b_n + a_1, b_{n-1} + a_2 + s, b_{n-2} + a_3 + s, \cdots, b_2 + a_{n-1} + s\} \\ &= \min\{a_1 + b_n, a_n + b_1, a_{n-1} + b_2 + s, a_{n-2} + b_3 + s, \cdots, a_2 + b_{n-1} + s\} \\ &= (C)_n \end{aligned}$$

Now the next entry is obtained as,

$$\begin{aligned} (D)_2 + s &= \min\{b_2 + a_1 + s, b_1 + a_2 + s, b_n + a_3 + s, b_{n-1} + a_4 + s, \cdots, b_3 + a_n + s\} \\ &= \min\{b_1 + a_2, b_n + a_3, b_{n-1} + a_4, b_{n-2} + a_5, \cdots, b_2 + a_1\} + s \\ &= \min\{a_1 + b_2, a_n + b_3, a_{n-1} + b_4, a_{n-2} + b_5, \cdots, a_2 + b_1\} + s \\ &= (C)_2 + s \end{aligned}$$

Similarly,

$$\begin{aligned}(D)_3 + s &= \min\{b_3 + a_1 + s, b_2 + a_2 + 2s, b_1 + a_3 + s, b_n + a_4 + s, \cdots, b_4 + a_n + s\}\\ &= \min\{b_2 + a_2 + s, b_1 + a_3, b_n + a_4, b_{n-1} + a_5 + s, \cdots, b_3 + a_1\} + s\}\\ &= \min\{a_2 + b_2 + s, a_1 + b_3, a_n + b_4, a_{n-1} + b_5 + s, \cdots, a_3 + b_1\} + s\\ &= (C)_3 + s\end{aligned}$$

Also,

$$\begin{aligned}(D)_{n-1} + s &= \min\{b_1 + a_{n-1} + s, b_n + a_n + s, b_{n-1} + a_1 + s, b_{n-2} + a_2 + 2s, \cdots, b_2 + a_{n-2} + 2s\}\\ &= \min\{b_1 + a_{n-1}, b_n + a_n, b_{n-1} + a_1, b_{n-2} + a_2 + s, \cdots, b_2 + a_{n-2} + s\} + s\\ &= \min\{a_1 + b_{n-1}, a_n + b_n, a_{n-1} + b_1, a_{n-2} + b_2 + s, \cdots, a_2 + b_{n-2} + s\} + s\\ &= (C)_{n-1} + s\end{aligned}$$

And the final entry of $B \otimes A$ is obtained as,

$$\begin{aligned}(D)_n + s &= \min\{b_n + a_1 + s, b_{n-1} + a_2 + 2s, b_{n-2} + a_3 + 2s, b_{n-3} + a_4 + 2s, \cdots, b_1 + a_n + s\}\\ &= \min\{b_1 + a_n, b_n + a_1, b_{n-1} + a_2 + s, b_{n-2} + a_3 + s, \cdots, b_2 + a_{n-1} + s\} + s\}\\ &= \min\{a_1 + b_n, a_n + b_1, a_{n-1} + b_2 + s, a_{n-2} + b_3 + s, \cdots, a_2 + b_{n-1} + s\} + s\\ &= (C)_n + s\end{aligned}$$

Hence, it is proved that $(C)_k = (D)_k \ \forall\ 1 \leq k \leq n$ and $(C)_k + s = (D)_k + s \ \forall\ 2 \leq k \leq n$.
Thus,

$$A \otimes B = B \otimes A.$$

□

Proposition 2.8. $((\mathfrak{A}(D_p[\mathfrak{C}])^u_l)(s))_n$ *(set of all anti-s-p-circulant matrices) is a commutative subset of the tropical semiring* $M_{n\times n}(\mathfrak{Z})$*.*

Proof.

$$\text{Let } A = \begin{bmatrix} a_1 + s & a_n + s & a_{n-1} + s & \cdots & a_2 \\ a_2 + s & a_1 + s & a_n + s & \cdots & a_3 + s \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ a_{n-1} + s & a_{n-2} & a_{n-3} + s & \cdots & a_n + s \\ a_n & a_{n-1} + s & a_{n-2} + s & \cdots & a_1 + s \end{bmatrix} \ \& \ B = \begin{bmatrix} b_1 + s & b_n + s & b_{n-1} + s & \cdots & b_2 \\ b_2 + s & b_1 + s & b_n + s & \cdots & b_3 + s \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ b_{n-1} + s & b_{n-2} & b_{n-3} + s & \cdots & b_n + s \\ b_n & b_{n-1} + s & b_{n-2} + s & \cdots & b_1 + s \end{bmatrix}$$

To prove the commutativity of $((\mathfrak{A}(D_p[\mathfrak{C}])^u_l)(s))_n$, it is enough to prove that $(A \otimes B)_{ij} = (B \otimes A)_{ij}$, $\forall$ $1 \leq i, j \leq n$.

Let $A, B \in ((\mathfrak{A}(D_p[\mathfrak{C}])^u_l)(s))_n$, then we have $a_{k_1} \otimes b_{k_2} = b_{k_1} \otimes a_{k_2} \forall\ 1 \leq k_1, k_2 \leq n$.

By using this property we get,

$$\begin{aligned}
(A \otimes B)_{11} &= \min\{a_1 + b_1 + 2s, a_n + b_2 + 2s, \cdots, a_3 + b_{n-1} + 2s, a_2 + b_n\} \\
&= \min\{b_1 + a_1 + 2s, b_n + a_2 + 2s, \cdots, b_3 + a_{n-1} + 2s, b_2 + a_n\} \\
&= (B \otimes A)_{11} \\
(A \otimes B)_{12} &= \min\{a_1 + b_n + 2s, a_n + b_1 + 2s, \cdots, a_3 + b_{n-2} + s, a_2 + b_{n-1} + s\} \\
&= \min\{b_1 + a_n + 2s, b_n + a_1 + 2s, \cdots, b_3 + a_{n-2} + s, b_2 + a_{n-1} + s\} \\
&= (B \otimes A)_{12} \\
&\ \ \vdots \\
(A \otimes B)_{1n} &= \min\{a_1 + b_2 + s, a_n + b_3 + 2s, \cdots, a_3 + b_n + 2s, a_2 + b_1 + s\} \\
&= \min\{b_1 + a_2 + s, b_n + a_3 + 2s, \cdots, b_3 + a_n + 2s, b_2 + a_1 + s\} \\
&= (B \otimes A)_{1n}
\end{aligned}$$

Similarly,

$$\begin{aligned}
(A \otimes B)_{21} &= \min\{a_2 + b_1 + 2s, a_1 + b_2 + 2s, \cdots, a_4 + b_{n-1} + 2s, a_3 + b_n + s\} \\
&= \min\{b_2 + a_1 + 2s, b_1 + a_2 + 2s, \cdots, b_4 + a_{n-1} + 2s, b_3 + a_n + k\} \\
&= (B \otimes A)_{21} \\
(A \otimes B)_{22} &= \min\{a_2 + b_n + 2s, a_1 + b_1 + 2s, \cdots, a_4 + b_{n-2}, a_3 + b_{n-1} + 2s\} \\
&= \min\{b_2 + a_n + 2s, b_1 + a_1 + 2s, \cdots, b_4 + a_{n-2}, b_3 + a_{n-1} + 2s\} \\
&= (B \otimes A)_{22}
\end{aligned}$$

By continuing the process, we get,

$$\begin{aligned}
(A \otimes B)_{2n} &= \min\{a_2 + b_2 + s, a_1 + b_3 + 2s, \cdots, a_4 + b_n + s, a_3 + b_1 + 2s\} \\
&= \min\{b_2 + a_2 + s, b_1 + a_3 + 2s, \cdots, b_4 + a_n + s, b_3 + a_1 + 2s\} \\
&= (B \otimes A)_{2n} \\
(A \otimes B)_{(n-1)1} &= \min\{a_{n-1} + b_1 + 2s, a_{n-2} + b_2 + s, \cdots, a_1 + b_{n-1} + 2s, a_n + b_n + s\} \\
&= \min\{b_{n-1} + a_1 + 2s, b_{n-2} + a_2 + s, \cdots, b_1 + a_{n-1} + 2s, b_n + a_n + s\} \\
&= (B \otimes A)_{(n-1)1} \\
(A \otimes B)_{(n-1)2} &= \min\{a_{n-1} + b_n + 2s, a_{n-2} + b_1 + s, \cdots, a_1 + b_{n-2} + s, a_n + b_{n-1} + 2s\} \\
&= \min\{b_{n-1} + a_n + 2s, b_{n-2} + a_1 + s, \cdots, b_1 + a_{n-2} + k, b_n + a_{n-1} + 2s\} \\
&= (B \otimes A)_{(n-1)2} \\
&\ \ \vdots \\
(A \otimes B)_{(n-1)n} &= \min\{a_{n-1} + b_2 + 2, a_{n-2} + b_3 + s, \cdots, a_1 + b_n + 2s, a_n + b_1 + 2s\} \\
&= \min\{b_{n-1} + a_2 + 2, b_{n-2} + a_3 + s, \cdots, b_1 + a_n + 2s, b_n + a_1 + 2s\} \\
&= (B \otimes A)_{(n-1)n}
\end{aligned}$$

Similarly, the entries of $(n)^{th}$ row of the matrix $A \otimes B$ is,

$$
\begin{aligned}
(A \otimes B)_{n1} &= \min\{a_n + b_1 + s, a_{n-1} + b_2 + 2s, \cdots, a_2 + b_{n-1} + 2s, a_1 + b_n + s\} \\
&= \min\{b_n + a_1 + s, b_{n-1} + a_2 + 2s, \cdots, b_2 + a_{n-1} + 2s, b_1 + a_n + s\} \\
&= (B \otimes A)_{n1} \\
(A \otimes B)_{n2} &= \min\{a_n + b_n + s, a_{n-1} + b_1 + 2s, \cdots, a_2 + b_{n-2} + s, a_1 + b_{n-1} + 2s\} \\
&= \min\{b_n + a_n + s, b_{n-1} + a_1 + 2s, \cdots, b_2 + a_{n-2} + s, b_1 + a_{n-1} + 2s\} \\
&= (B \otimes A)_{n2} \\
&\ \ \vdots \\
(A \otimes B)_{nn} &= \min\{a_n + b_2, a_{n-1} + b_3 + 2s, \cdots, a_2 + b_n + 2s, a_1 + b_1 + 2s\} \\
&= \min\{a_n + b_2, a_{n-1} + b_3 + 2s, \cdots, a_2 + b_n + 2s, a_1 + b_1 + 2s\} \\
&= (B \otimes A)_{nn} \\
&\implies (A \otimes B)_{ij} = (B \otimes A)_{ij} \ \forall\ 1 \le i, j \le n.
\end{aligned}
$$

Thus,

$$A \otimes B = B \otimes A.$$

□

3. Public key exchange protocol 1

In this section, we discuss the protocol introduced in [21] with the help of lower-s-circulant matrices. Further we study the protocol which use upper or lower-s-circulant matrices to compare it with our proposed protocol that uses anti-s-p-circulant matrices $((\mathfrak{A}(D_p[\mathfrak{C}])_l^u)(s))_n$.

3.1. Description of the protocol 1

Step 1: Let Y, s, t be the public parameters.
Step 2: Alice selects two matrices C_1 and C_2 and finds the two matrices $\mathfrak{A}_1, \mathfrak{B}_1$.
Step 3: Bob selects two matrices C_3 and C_4 and finds the two matrices $\mathfrak{A}_2, \mathfrak{B}_2$.
Step 4: Alice finds $K_a = \mathfrak{A}_1 \otimes (Y) \otimes \mathfrak{B}_1$ and sends it to Bob.
Step 5: Bob finds $K_b = \mathfrak{A}_2 \otimes (Y) \otimes \mathfrak{B}_2$ and sends it to Alice.
Step 6: Alice computes $G_1 = \mathfrak{A}_1 \otimes K_b \otimes \mathfrak{B}_1$.
Step 7: Bob computes $G_2 = \mathfrak{A}_2 \otimes K_a \otimes \mathfrak{B}_2$.
Step 8: By the properties of tropical algebra, the shared keys are the same. $K = G_1 = G_2$.

Algorithm 1: Key exchange algorithm for protocol 1.

```
Input  : Matrices $Y, C_1, C_2, C_3, C_4$ and integers $s, t, n$
Output: Shared secret key
$\otimes$ := Tropical multiplication
$L(s)$ := Lower triangular matrix with entries ‘s’
$\mathfrak{A}_1 := C_1 + L(s)$
$\mathfrak{B}_1 := C_2 + L(t)$
$\mathfrak{A}_2 := C_3 + L(s)$
$\mathfrak{B}_2 := C_4 + L(t)$
$K_a := \mathfrak{A}_1 \otimes Y \otimes \mathfrak{B}_1$
$K_b := \mathfrak{A}_2 \otimes Y \otimes \mathfrak{B}_2$
$G_1 := \mathfrak{A}_1 \otimes K_b \otimes \mathfrak{B}_1$
$G_2 := \mathfrak{A}_2 \otimes K_a \otimes \mathfrak{B}_2$
return Shared secret key $G_1 = G_2$
```

3.2. *Key generation and parameters of protocol 1*

- Let Y, s, t be the public parameters, where the entries of Y are the elements from the tropical semiring $(\mathbb{Z} \cup \{\infty\}, \oplus, \otimes)$. Similarly s, t are integers.
- Alice selects two circulant matrices C_1 and C_2 from the tropical semiring $(M_n(\mathfrak{Z}), \oplus, \otimes)$ and finds the matrices $\mathfrak{A}_1, \mathfrak{B}_1$ with the use of s, t where $\mathfrak{C}_n$ is set of all circulant matrices of order n.
- $(c_1)^1, (c_2)^1, (c_3)^1, \cdots (c_n)^1$ and $(c_1)^2, (c_2)^2, (c_3)^2, \cdots (c_n)^2$ are the elements of circulant matrices C_1 and C_2 respectively.

$$\mathfrak{A}_1 = \begin{bmatrix} (c_1)^1 & (c_n)^1 & (c_{n-1})^1 & \cdots & (c_2)^1 \\ s \otimes (c_2)^1 & (c_1)^1 & (c_n)^1 & \cdots & (c_3)^1 \\ s \otimes (c_3)^1 & s \otimes (c_2)^1 & (c_1)^1 & \cdots & (c_4)^1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s \otimes (c_n)^1 & s \otimes (c_{n-1})^1 & s \otimes (c_{n-2})^1 & \cdots & (c_1)^1 \end{bmatrix}$$

$$\mathfrak{B}_1 = \begin{bmatrix} (c_1)^2 & (c_n)^2 & (c_{n-1})^2 & \cdots & (c_2)^2 \\ t \otimes (c_2)^2 & (c_1)^2 & (c_n)^2 & \cdots & (c_3)^2 \\ t \otimes (c_3)^2 & t \otimes (c_2)^2 & (c_1)^2 & \cdots & (c_4)^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ t \otimes (c_n)^2 & t \otimes (c_{n-1})^2 & t \otimes (c_{n-2})^2 & \cdots & (c_1)^2 \end{bmatrix}$$

- Alice computes $K_a = \mathfrak{A}_1 \otimes (Y) \otimes \mathfrak{B}_1$.
- Bob selects two circulant matrices C_3 and C_4 from the tropical semiring $(M_n(\mathfrak{Z}), \oplus, \otimes)$ and finds the matrices $\mathfrak{A}_2$ and $\mathfrak{B}_2$ with the help of s, t.
- $(c_1)^3, (c_2)^3, (c_3)^3, \cdots (c_n)^3$ and $(c_1)^4, (c_2)^4, (c_3)^4, \cdots (c_n)^4$ were the elements of circulant matrices C_3

and C_4 respectively.

$$\mathfrak{A}_2=\begin{bmatrix}(c_1)^3 & (c_n)^3 & (c_{n-1})^3 & \cdots & (c_2)^3\\ s\otimes(c_2)^3 & (c_1)^3 & (c_n)^3 & \cdots & (c_3)^3\\ s\otimes(c_3)^3 & s\otimes(c_2)^3 & (c_1)^3 & \cdots & (c_4)^3\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ s\otimes(c_n)^3 & s\otimes(c_{n-1})^3 & s\otimes(c_{n-2})^3 & \cdots & (c_1)^3\end{bmatrix}$$

$$\mathfrak{B}_2=\begin{bmatrix}(c_1)^4 & (c_n)^4 & (c_{n-1})^4 & \cdots & (c_2)^4\\ t\otimes(c_2)^4 & (c_1)^4 & (c_n)^4 & \cdots & (c_3)^4\\ t\otimes(c_3)^4 & t\otimes(c_2)^4 & (c_1)^4 & \cdots & (c_4)^4\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ t\otimes(c_n)^4 & t\otimes(c_{n-1})^4 & t\otimes(c_{n-2})^4 & \cdots & (c_1)^4\end{bmatrix}$$

- Bob computes $K_b=\mathfrak{A}_2\otimes(Y)\otimes\mathfrak{B}_2$.
- Alice finds the matrix
$$G_1=\mathfrak{A}_1\otimes K_b\otimes\mathfrak{B}_1.$$
- Bob finds the matrix
$$G_2=\mathfrak{A}_2\otimes K_a\otimes\mathfrak{B}_2.$$
- Finally, the shared keys are same $K=G_1=G_2$.
The proof is given in the following Proposition 3.2.

3.3. A toy example

Example 3.1. Consider

$$Y=\begin{bmatrix}-601 & -615 & 54332\\ -554 & 98 & 45\\ 4325 & 65 & 3232\end{bmatrix}, s=-154, t=1797, n=3$$

Alice choose

$$C_1=\begin{bmatrix}-8 & 126 & 335\\ 335 & -8 & 126\\ 126 & 335 & -8\end{bmatrix}, C_2=\begin{bmatrix}-423 & -827 & 232\\ 232 & -423 & -827\\ -827 & 232 & -423\end{bmatrix}$$

and she finds

$$\mathfrak{A}_1=\begin{bmatrix}-8 & 126 & 335\\ 181 & -8 & 126\\ -28 & 181 & -8\end{bmatrix}, \mathfrak{B}_1=\begin{bmatrix}-423 & -827 & 232\\ 2029 & -423 & -827\\ 970 & 2029 & -423\end{bmatrix}$$

Bob choose

$$C_3=\begin{bmatrix}959 & -7 & 131\\ 131 & 959 & -7\\ -7 & 131 & 959\end{bmatrix}, C_4=\begin{bmatrix}-712 & 18822 & 573\\ 573 & -712 & 18822\\ 18822 & 573 & -712\end{bmatrix}$$

and he finds

$$\mathfrak{A}_y=\begin{bmatrix}959 & -7 & 131\\ -23 & 959 & -7\\ -161 & -23 & 959\end{bmatrix}, \mathfrak{B}_y=\begin{bmatrix}-712 & 18822 & 573\\ 2370 & -712 & 18822\\ 20619 & 2370 & -712\end{bmatrix}$$

Alice finds

$$K_a = \begin{bmatrix} -1032 & -1436 & -1450 \\ -985 & -1389 & -1261 \\ -1052 & -1456 & -1470 \end{bmatrix} \text{and sends to Bob.}$$

Bob finds

$$K_b = \begin{bmatrix} -1273 & -621 & -674 \\ -1336 & -1350 & -51 \\ -1474 & -1488 & -690 \end{bmatrix} \text{and sends to Alice.}$$

Alice finds

$$G_1 = \begin{bmatrix} -1704 & -2108 & -2051 \\ -1771 & -2175 & -2189 \\ -1905 & -2309 & -2323 \end{bmatrix}$$

Bob finds

$$G_2 = \begin{bmatrix} -1704 & -2108 & -2051 \\ -1771 & -2175 & -2189 \\ -1905 & -2309 & -2323 \end{bmatrix}$$

Thus, the shared keys are equal $G_1 = G_2$.

Suppose an attacker tries to find $\mathfrak{A}_1, \mathfrak{B}_1$ from the known matrices K_a, Y, s, t

$$\begin{bmatrix} a_0 & a_2 & a_1 \\ a_1 - 154 & a_0 & a_2 \\ a_2 - 154 & a_1 - 154 & a_0 \end{bmatrix} \otimes \begin{bmatrix} -601 & -615 & 54332 \\ -554 & 98 & 45 \\ 4325 & 65 & 3232 \end{bmatrix} \otimes \begin{bmatrix} b_0 & b_2 & b_1 \\ b_1 + 1797 & b_0 & b_2 \\ b_2 + 1797 & b_1 + 1797 & b_0 \end{bmatrix} = \begin{bmatrix} -1032 & -1436 & -1450 \\ -985 & -1389 & -1261 \\ -1052 & -1456 & -1470 \end{bmatrix}$$

Then, he will end up with the following tropical non-linear system,
$\min\{(-601) \otimes a_0 \otimes b_0, 1182 \otimes a_0 \otimes b_1, 56129 \otimes a_0 \otimes b_2, 4325 \otimes a_1 \otimes b_0, 1862 \otimes a_1 \otimes b_1, 5029 \otimes a_1 \otimes b_2, (-554) \otimes a_2 \otimes b_0, 1895 \otimes a_2 \otimes b_1, 1842 \otimes a_2 \otimes b_2\} = -1031$
$\min\{(-615) \otimes a_0 \otimes b_0, 56129 \otimes a_0 \otimes b_1, (-601) \otimes a_0 \otimes b_2, 65 \otimes a_1 \otimes b_0, 5029 \otimes a_1 \otimes b_1, 4325 \otimes a_1 \otimes b_2, 98 \otimes a_2 \otimes b_0, 1842 \otimes a_2 \otimes b_1, (-554) \otimes a_2 \otimes b_2\} = -1436$
$\min\{54332 \otimes a_0 \otimes b_0, (-601) \otimes a_0 \otimes b_1, (-615) \otimes a_0 \otimes b_2, 3232 \otimes a_1 \otimes b_0, 4325 \otimes a_1 \otimes b_1, 65 \otimes a_1 \otimes b_2, 45 \otimes a_2 \otimes b_0, (-554) \otimes a_2 \otimes b_1, 98 \otimes a_2 \otimes b_2\} = -1450$
$\min\{(-554) \otimes a_0 \otimes b_0, 98 \otimes a_0 \otimes b_1 + 1842 \otimes a_0 \otimes b_2, (-755) \otimes a_1 \otimes b_0, 1028 \otimes a_1 \otimes b_1, 55975 \otimes a_1 \otimes b_2, 4325 \otimes a_2 \otimes b_0, 1862 \otimes a_2 \otimes b_1, 5029 \otimes a_2 \otimes b_2\} = -985$
$\min\{98 \otimes a_0 \otimes b_0, 1842 \otimes a_0 \otimes b_1, (-554) \otimes a_0 \otimes b_2, (-769) \otimes a_1 \otimes b_0, 55975 \otimes a_1 \otimes b_1, 1042 \otimes a_1 \otimes b_2, (-89) \otimes a_2 \otimes b_0, 55975 \otimes a_2 \otimes b_1, 4325 \otimes a_2 \otimes b_2\} = -1389$
$\min\{45 \otimes a_0 \otimes b_0, (-554) \otimes a_0 \otimes b_1, 98 \otimes a_0 \otimes b_2, 54178 \otimes a_1 \otimes b_0, (-755) \otimes a_1 \otimes b_1, (-769) \otimes a_1 \otimes b_2 + 3232 \otimes a_2 \otimes b_0 + 4325 \otimes a_2 \otimes b_1 + 65 \otimes a_2 \otimes b_2\} = -1261$
$\min\{4325 \otimes a_0 \otimes b_0 + 1895 \otimes a_0 \otimes b_1 + 5029 \otimes a_0 \otimes b_2 + (-708) \otimes a_1 \otimes b_0 + 1741 \otimes a_1 \otimes b_1, 1688 \otimes a_1 \otimes b_2, (-755) \otimes a_2 b_0, 1028 \otimes a_2 \otimes b_1, 55975 a_2 b_2\} = -1052$
$\min\{65 \otimes a_0 \otimes b_0, 5029 \otimes a_0 \otimes b_1, 4325 \otimes a_0 \otimes b_2, (-56) \otimes a_1 \otimes b_0, 1688 \otimes a_1 \otimes b_1, (-708) \otimes a_1 \otimes b_2, (-769) \otimes a_2 \otimes b_0, 55975 \otimes a_2 \otimes b_1, (-755) \otimes a_2 \otimes b_2\} = -1456$
$\min\{3232 \otimes a_0 \otimes b_0, 4325 \otimes a_0 \otimes b_1, 65 \otimes a_0 \otimes b_2, (-109) \otimes a_1 \otimes b_0, (-708) \otimes a_1 \otimes b_1, (-56) \otimes a_1 \otimes b_2, 54486 \otimes a_2 \otimes b_0, (-755) \otimes a_2 \otimes b_1, (-769) \otimes a_2 \otimes b_2\} = -1470$

To attack the protocol, this system of non-linear equations has to be solved. But we already know that solving non-linear tropical equations is NP-Hard [13].

3.4. Security analysis

The security of this protocol relies on the non-commutativity the lower-s-circulant matrix and the lower-t-circulant matrix.

Proposition 3.2. *If $P_1 \in (\mathfrak{C}_l(s))_n, Q_1 \in (\mathfrak{C}_l(t))_n, P_2 \in (\mathfrak{C}_l(s))_n, Q_2 \in (\mathfrak{C}_l(t))_n$ and $s \neq t$, then*

1) $P_2 \otimes K_a \otimes Q_2 = P_1 \otimes K_b \otimes Q_1$
2) $K_a \otimes K_b$ *and* $K_b \otimes K_a \neq P_2 \otimes K_a \otimes Q_2$ *and* $P_1 \otimes K_b \otimes Q_1$

where $K_a = (P_1 \otimes Y \otimes Q_1)$, $K_b = (P_2 \otimes Y \otimes Q_2)$.

Proof. 1) In this part of the proposition we prove that the shared secret keys are equal.
We know that by Proposition 2.7, $P_1 \otimes P_2 = P_2 \otimes P_1$ and $P_1 \otimes Q_1 \neq Q_1 \otimes P_1$.
Now, we consider,

$$\begin{aligned} R.H.S &= P_1 \otimes K_b \otimes Q_1 \\ &= P_1 \otimes (P_2 \otimes Y \otimes Q_2) \otimes Q_1 \\ &= (P_1 \otimes P_2) \otimes Y \otimes (Q_2 \otimes Q_1) \\ &= (P_2 \otimes P_1) \otimes Y \otimes (Q_1 \otimes Q_2) \\ &= P_2 \otimes (P_1 \otimes Y \otimes Q_1) \otimes Q_2 \\ &= P_2 \otimes K_a \otimes Q_2 \\ &= L.H.S \end{aligned}$$

Hence, we proved that the shared keys are equal.

2) In this part of the proposition, we show that an attacker cannot find the secret key with the known matrices K_a, K_b . Now, to prove the security of the protocol 1,

$$\begin{aligned} K_a \otimes K_b &= (P_1 \otimes Y \otimes Q_1) \otimes (P_2 \otimes Y \otimes Q_2) \\ &= P_1 \otimes Y \otimes (Q_1 \otimes P_2) \otimes Y \otimes Q_2 \end{aligned}$$

By Proposition 2.4

$$\begin{aligned} P_1 \otimes Y \otimes (Q_1 \otimes P_2) \otimes Y \otimes Q_2 &\neq P_1 \otimes Y \otimes (P_2 \otimes Q_1) \otimes Y \otimes Q_2 \\ &\neq P_2 \otimes K_a \otimes Q_2, P_1 \otimes K_b \otimes Q_1 \end{aligned}$$

Hence, $K_a \otimes K_b$ and $K_b \otimes K_a \neq P_2 \otimes K_a \otimes Q_2$ and $P_1 \otimes K_b \otimes Q_1$

□

The time complexity of solving a tropical Grobner basis [23] for a tropical non-linear system of equations with $n \times n$ matrices is known to be $O(2^{(2^n)})$ which is extremely larger than $O(n^3)$.

4. Public key exchange protocol 2

In this section, we propose a new key exchange protocol based on the anti-s-p-circulant matrices. We have given the algorithm, example and the security analysis of the proposed protocol.

4.1. Description of the protocol 2

Step 1: Let Y, s, t, p be the public parameters.
Step 2: Alice selects two p-circulant matrices C_1 and C_2 and finds the two matrices P_1, Q_1.
Step 3: Bob selects two p-circulant matrices C_3 and C_4 and finds the two matrices P_2, Q_2.

Step 4: Alice finds $K_a = P_1 \otimes (Y) \otimes Q_1$ and sends it to Bob.
Step 5: Bob finds $K_b = P_2 \otimes (Y) \otimes P_2$ and sends it to Alice.
Step 6: Alice computes $G_1 = (P_1 \otimes (K_b) \otimes Q_1)$.
Step 7: Bob computes $G_2 = (P_2 \otimes (K_a) \otimes Q_2)$.
Step 8: Computed values of both keys are same $K = G_1 = G_2$.

Algorithm 2: Key exchange algorithm for protocol 2.

```
Input  : Matrices $Y, C_1, C_2, C_3, C_4$ and integers $s, t, p$
Output: Shared secret key
$\otimes$ := Tropical multiplication
$AL(a)$ := Anti-lower triangular matrix with entries ‘a’
$AU(a)$ := Anti-upper triangular matrix with entries ‘a’
$ALU(a) := AL(a) + AU(a)$
$P_1 := C_1 + ALU(s)$
$Q_1 := C_2 + ALU(t)$
$P_2 := C_3 + ALU(s)$
$Q_2 := C_4 + ALU(t)$
$K_a := P_1 \otimes Y \otimes Q_1$
$K_b := P_2 \otimes Y \otimes Q_2$
$G_1 := P_1 \otimes K_b \otimes Q_1$
$G_2 := P_2 \otimes K_a \otimes Q_2$
return Shared secret key $G_1 = G_2$
```

4.2. Key generation and parameters of protocol 2

- Let Y, s, t, p be the public parameters, where the entries of Y are the elements from the tropical semiring $(\mathfrak{Z}, \oplus, \otimes)$. Similarly $s, t \in \mathbb{Z}$.
- Alice selects two p-circulant matrices C_1 and C_2 from the tropical semiring $(M_n(\mathfrak{Z}), \oplus, \otimes)$ and finds P_1, Q_1 are the anti-s-p-circulant and anti-t-p-circulant matrices with the use of p-circulant matrices C_1 and C_2 respectively.
- $(c_1)^1, (c_2)^1, (c_3)^1, \cdots (c_n)^1$ and $(c_1)^2, (c_2)^2, (c_3)^2, \cdots (c_n)^2$ are the elements of p-circulant matrices C_1 and C_2 respectively.

$$P_1 = \begin{bmatrix} s \otimes (c_1)^1 & s \otimes (c_n)^1 & s \otimes (c_{n-1})^1 & \cdots & (c_2)^1 \\ s \otimes (c_2)^1 & s \otimes (c_1)^1 & s \otimes (c_n)^1 & \cdots & s \otimes (c_3)^1 \\ s \otimes (c_3)^1 & s \otimes (c_2)^1 & (c_1)^1 & \cdots & s \otimes (c_4)^1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (c_n)^1 & s \otimes (c_{n-1})^1 & s \otimes (c_{n-2})^1 & \cdots & s \otimes (c_1)^1 \end{bmatrix}$$

$$Q_1 = \begin{bmatrix} t \otimes (c_1)^2 & t \otimes (c_n)^2 & t \otimes (c_{n-1})^2 & \cdots & (c_2)^2 \\ t \otimes (c_2)^2 & t \otimes (c_1)^2 & t \otimes (c_n)^2 & \cdots & t \otimes (c_3)^2 \\ t \otimes (c_3)^2 & t \otimes (c_2)^2 & (c_1)^2 & \cdots & t \otimes (c_4)^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (c_n)^2 & t \otimes (c_{n-1})^2 & t \otimes (c_{n-2})^2 & \cdots & t \otimes (c_1)^2 \end{bmatrix}$$

- Alice computes $K_a = P_1 \otimes (Y) \otimes Q_1$.
- Bob selects two p-circulant matrices C_3 and C_4 from the tropical semiring $(M_n(\mathfrak{Z}), \oplus, \otimes)$. P_2, Q_2 are the anti-s-p-circulant and anti-t-p-circulant matrices with the use of C_3 and C_4 respectively.
- $(c_0)^3, (c_1)^3, (c_2)^3, \cdots (c_{n-1})^3$ and $(c_0)^4, (c_1)^4, (c_2)^4, \cdots (c_{n-1})^4$ are the elements of C_3 and C_4 respectively.

$$P_2 = \begin{bmatrix} s \otimes (c_1)^3 & s \otimes (c_n)^3 & s \otimes (c_{n-1})^3 & \cdots & (c_2)^3 \\ s \otimes (c_2)^3 & s \otimes (c_1)^3 & s \otimes (c_n)^3 & \cdots & s \otimes (c_3)^3 \\ s \otimes (c_3)^3 & s \otimes (c_2)^3 & (c_1)^3 & \cdots & s \otimes (c_4)^3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (c_n)^3 & s \otimes (c_{n-1})^3 & s \otimes (c_{n-2})^3 & \cdots & s \otimes (c_1)^3 \end{bmatrix}$$

$$Q_2 = \begin{bmatrix} t \otimes (c_1)^4 & t \otimes (c_n)^4 & t \otimes (c_{n-1})^4 & \cdots & (c_2)^4 \\ t \otimes (c_2)^4 & t \otimes (c_1)^4 & t \otimes (c_n)^4 & \cdots & t \otimes (c_3)^4 \\ t \otimes (c_3)^4 & t \otimes (c_2)^4 & (c_1)^4 & \cdots & t \otimes (c_4)^4 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (c_n)^4 & t \otimes (c_{n-1})^4 & t \otimes (c_{n-2})^4 & \cdots & t \otimes (c_1)^4 \end{bmatrix}$$

- Bob computes $K_b = P_2 \otimes (Y) \otimes Q_2$.
- Alice finds the matrix
$$G_1 = P_1 \otimes K_b \otimes Q_1.$$
- Bob finds the matrix
$$G_2 = P_2 \otimes K_a \otimes Q_2.$$
- Finally, shared keys were same $K = G_1 = G_2$.

The proof is given in the following Proposition 4.2.

4.3. A toy example

Example 4.1. Consider

$$Y = \begin{bmatrix} 1090000 & -33434 & 32434543 \\ 23 & -2251 & 955543 \\ -55432 & 32455 & 34442 \end{bmatrix}, s = -71, t = 98876, n = 3$$

Alice choose

$$C_1 = \begin{bmatrix} -12201 & -12205 & -12203 \\ -12203 & -12201 & -12205 \\ -12205 & -12203 & -12201 \end{bmatrix}, C_2 = \begin{bmatrix} -2082 & -2086 & -2084 \\ -2084 & -2082 & -2086 \\ -2086 & -2084 & -2082 \end{bmatrix}$$

and finds

$$P_1 = \begin{bmatrix} -12272 & -12276 & -12203 \\ -12274 & -12201 & -12276 \\ -12205 & -12274 & -12272 \end{bmatrix}, Q_1 = \begin{bmatrix} -100958 & -100962 & -2084 \\ -100960 & -2082 & -100962 \\ -2086 & -100960 & -100958 \end{bmatrix}$$

Bob choose

$$C_3 = \begin{bmatrix} -284 & -288 & -286 \\ -286 & -284 & -288 \\ -288 & -286 & -284 \end{bmatrix}, C_4 = \begin{bmatrix} -205 & -209 & -207 \\ -207 & -205 & -209 \\ -209 & -207 & -205 \end{bmatrix}$$

and finds

$$P_2 = \begin{bmatrix} -355 & -359 & -286 \\ -357 & -284 & -359 \\ -288 & -357 & -355 \end{bmatrix}, Q_2 = \begin{bmatrix} -99081 & -99085 & -207 \\ -99083 & -205 & -99085 \\ -209 & -99083 & -99081 \end{bmatrix}$$

Alice finds

$$K_a = \begin{bmatrix} -168593 & -168597 & -146668 \\ -168666 & -168670 & -146670 \\ 168662 & -168666 & -146601 \end{bmatrix}$$

and sends to Bob.
Bob finds

$$K_b = \begin{bmatrix} -154799 & -154803 & -132874 \\ -154872 & -154876 & -132876 \\ -154868 & -154872 & -132807 \end{bmatrix}$$

and sends to Alice.
Alice finds

$$G_1 = \begin{bmatrix} -268112 & -268110 & -268114 \\ -268108 & -268106 & -268110 \\ -268110 & -268108 & -268112 \end{bmatrix}$$

Bob finds

$$G_2 = \begin{bmatrix} -268112 & -268110 & -268114 \\ -268108 & -268106 & -268110 \\ -268110 & -268108 & -268112 \end{bmatrix}$$

Shared keys $G_1 = G_2$

$$\begin{bmatrix} a_0 - 71 & a_2 - 71 & a_1 \\ a_1 - 71 & a_0 & a_2 - 71 \\ a_2 & a_1 - 71 & a_0 - 71 \end{bmatrix} \otimes \begin{bmatrix} 1090000 & -33434 & 32434543 \\ 23 & -2251 & 955543 \\ -55432 & 32455 & 34442 \end{bmatrix} \otimes \begin{bmatrix} b_0 + 98876 & b_2 + 98876 & b_1 \\ b_1 + 98876 & b_0 & b_2 + 98876 \\ b_2 & b_1 + 98876 & b_0 + 98876 \end{bmatrix}$$
$$= \begin{bmatrix} -168593 & -168597 & -146668 \\ -168666 & -168670 & -146670 \\ 168662 & -168666 & -146601 \end{bmatrix}$$

To attack the protocol the attacker has to solve the following tropical non-linear system of equations.
$\min\{1188805 \otimes a_0 \otimes b_0, 65371 \otimes a_0 \otimes b_1, 32434472 \otimes a_0 \otimes b_2, 43444 \otimes a_1 \otimes b_0, 1313310 \otimes a_1 \otimes b_1, 34442 \otimes a_1 \otimes b_2, 98828 \otimes a_2 \otimes b_0, 96554 \otimes a_2 \otimes b_1, 955472 \otimes a_2 \otimes b_2\} = -168593$
$\min\{-33505 \otimes a_0 \otimes b_0, 32533348 \otimes a_0 \otimes b_1, 1188805 \otimes a_0 \otimes b_2, 32455 \otimes a_1 \otimes b_0, 133318 \otimes a_1 \otimes b_1, 43444 \otimes a_1 \otimes b_2, (-2322) \otimes a_2 \otimes b_0, 1054348 \otimes a_2 \otimes b_1, 98828 \otimes a_2 \otimes b_2\} = -168597$
$\min\{32533348 \otimes a_0 \otimes b_0, 1089929 \otimes a_0 \otimes b_1, 65371 \otimes a_0 \otimes b_2, 133318 \otimes a_1 \otimes b_0, (-55432) \otimes a_1 \otimes b_1, 131331 \otimes a_1 \otimes b_2, 1054348 \otimes a_2 \otimes b_0, (-48) \otimes a_2 \otimes b_1, 96554 \otimes a_2 \otimes b_2\} = -146668$

$\min\{98899 \otimes a_0 \otimes b_0, 96625 \otimes a_0 \otimes b_1, 955543 \otimes a_0 \otimes b_2, 1188805 \otimes a_1 \otimes b_0, 65371 \otimes a_1 \otimes b_1, 32434472 \otimes a_1 \otimes b_2, 43373 \otimes a_2 \otimes b_0, 131260 \otimes a_2 \otimes b_1, 34371 \otimes a_2 \otimes b_2\} = -168666$

$\min\{(-2251) \otimes a_0 \otimes b_0, 1054419 \otimes a_0 \otimes b_1, 98899 \otimes a_0 \otimes b_2, (-33505) \otimes a_1 \otimes b_0, 32533348 \otimes a_1 \otimes b_1, 1188805 \otimes a_1 \otimes b_2, 32384 \otimes a_2 \otimes b_0, 133247 \otimes a_2 \otimes b_1, 43373 \otimes a_2 \otimes b_2\} = -168670$

$\min\{1054419 \otimes a_0 \otimes b_0, 23 \otimes a_0 \otimes b_1, 96625 \otimes a_0 \otimes b_2, 32533348 \otimes a_1 \otimes b_0, 1089929 \otimes a_1 \otimes b_1, 65371 \otimes a_1 \otimes b_2, 133247 \otimes a_2 \otimes b_0, (-55503) \otimes a_2 \otimes b_1, 131260 \otimes a_2 \otimes b_2\} = -146670$

$\min\{43373 \otimes a_0 \otimes b_0, 131260 \otimes a_0 \otimes b_1, 34371 \otimes a_0 \otimes b_2, 98828 \otimes a_1 \otimes b_0, 96554 \otimes a_1 \otimes b_1, 955472 \otimes a_1 \otimes b_2, 1188876 \otimes a_2 \otimes b_0, 33434 \otimes a_2 \otimes b_1, 32434543 \otimes a_2 \otimes b_2\} = 168662$

$\min\{32384 \otimes a_0 \otimes b_0, 133247 \otimes a_0 \otimes b_1, 43373 \otimes a_0 \otimes b_2, (-2322) \otimes a_1 \otimes b_0, 1054348 \otimes a_1 \otimes b_1, 98828 \otimes a_1 \otimes b_2, (-33434) \otimes a_2 \otimes b_0), 32533419 \otimes a_2 \otimes b_1, 1188876 \otimes a_2 \otimes b_2 = -168666$

$\min\{133247 \otimes a_0 \otimes b_0, (-55503) \otimes a_0 \otimes b_1, 131260 \otimes a_0 \otimes b_2, 1054348 \otimes a_1 \otimes b_0, (-48) \otimes a_1 \otimes b_1, 96554 \otimes a_1 \otimes b_2, 32533419 \otimes a_2 \otimes b_0, 1090000 \otimes a_2 \otimes b_1, 65442 \otimes a_2 \otimes b_2\} = -146601$

Solving this system of non-linear equation is NP-Hard. Thus, this makes our protocol secure [13].

4.4. Security analysis

The security of this protocol relies on the non-commutativity of anti-s-circulant matrix with anti-t-circulant matrix.

Theorem 4.2. *If* $P_1 \in ((\mathfrak{A}(D_p[C])_l^u)(s))_n, Q_1 \in ((\mathfrak{A}(D_p[C])_l^u)(t))_n, P_2 \in ((\mathfrak{A}(D_p[C])_l^u)(s))_n, Q_2 \in ((\mathfrak{A}(D_p[C])_l^u)(t))_n$ *then*

1) $P_2 \otimes K_a \otimes Q_2 = P_1 \otimes K_b \otimes Q_1$
2) $K_a \otimes K_b$ *and* $K_b \otimes K_a \neq P_2 \otimes K_a \otimes Q_2$ *and* $P_1 \otimes K_b \otimes Q_1$

where $K_a = (P_1 \otimes Y \otimes Q_1)$*,* $K_b = (P_2 \otimes Y \otimes Q_2)$

Proof. 1) We know that by Proposition 2.8, $P_1 \otimes P_2 = P_2 \otimes P_1$ and $P_1 \otimes Q_1 \neq Q_1 \otimes P_1$.

Now we consider,

$$\begin{aligned} R.H.S &= P_1 \otimes K_b \otimes Q_1 \\ &= P_1 \otimes (P_2 \otimes Y \otimes Q_2) \otimes Q_1 \\ &= (P_1 \otimes P_2) \otimes Y \otimes (Q_2 \otimes Q_1) \\ &= (P_2 \otimes P_1) \otimes Y \otimes (Q_1 \otimes Q_2) \\ &= P_2 \otimes (P_1 \otimes Y \otimes Q_1) \otimes Q_2 \\ &= P_2 \otimes K_a \otimes Q_2 = L.H.S \end{aligned}$$

Hence the shared keys are equal.

2) Now to prove the security of the protocol 1

$$K_a \otimes K_b = (P_1 \otimes Y \otimes Q_1) \otimes (P_2 \otimes Y \otimes Q_2)$$

By Proposition 2.4, we have,

$$\begin{aligned} P_1 \otimes Y \otimes (Q_1 \otimes P_2) \otimes Y \otimes Q_2 &\neq P_1 \otimes Y \otimes (P_2 \otimes Q_1) \otimes Y \otimes Q_2 \\ &\neq P_2 \otimes K_a \otimes Q_2, P_1 \otimes K_b \otimes Q_1 \end{aligned}$$

Hence,

$$K_a \otimes K_b \neq P_2 \otimes K_a \otimes Q_2 \ \& \ P_1 \otimes K_b \otimes Q_1$$

$$\begin{aligned} K_b \otimes K_a &= (P_2 \otimes Y \otimes Q_2) \otimes (P_1 \otimes Y \otimes Q_1) \\ &= P_2 \otimes Y \otimes (Q_2 \otimes P_1) \otimes Y \otimes Q_1 \end{aligned}$$

By Proposition 2.4

$$\begin{aligned} P_2 \otimes Y \otimes (Q_2 \otimes P_1) \otimes Y \otimes Q_1 &\neq P_2 \otimes Y \otimes (P_1 \otimes Q_2) \otimes Y \otimes Q_1 \\ &\neq P_2 \otimes K_a \otimes Q_2, P_1 \otimes K_b \otimes Q_1 \end{aligned}$$

Hence, we have,

$$K_b \otimes K_a \neq P_2 \otimes K_a \otimes Q_2 \ \& \ P_1 \otimes K_b \otimes Q_1$$

□

The tropical Grobner basis algorithm which is one approach to solving tropical non-linear systems [23]. In the worst case, the time complexity of computing a tropical Grobner basis for a system of equations with n by n matrices is known to be $O(2^{(2^n)})$.

4.5. Possible attacks

The following are some of the attacks that an adversary may try to attack the proposed key exchange protocol and we have given how our key exchange scheme is secure against those attacks.

4.5.1. Brute force attack

The brute force attack is an attacking technique in which the man in the middle tries all possible values to find the key. Suppose the attacker tries to get the key $G = P_1 \otimes P_2 \otimes Y \otimes Q_1 \otimes Q_2$ from the public matrix Y and from the shared matrices $K_a = P_1 \otimes (Y) \otimes Q_1, K_b = P_2 \otimes (Y) \otimes Q_2$ guessing the secret parameters is very hard since there are infinite possibilities. Also, if he try to find the values of P_1, Q_1 and P_2, Q_2 from K_a and K_b respectively then the possibility of finding P_1, Q_1 and P_2, Q_2 are infinite since we have taken the entries from the tropical semiring $(\mathbb{Z} \cup \{\infty\}, \oplus, \otimes)$. Thus, we can conclude that protocol 2 is secure from brute force attack.

4.5.2. Linear algebra attack

The linear algebra attack is a key recovery technique by which an adversary may try to use the linear algebraic properties to attack the cryptosystem. The attack of Sphilrain on the classical Stickel's key exchange protocol is based on the fact that the keys were generated using invertible matrices.

In protocol 2, since we deal with tropical algebra, the matrices which we use $((\mathfrak{A}(D_p[C])_l^u)(s))_n$ are not generally invertible. Thus, it makes our protocol secure from linear algebra attacks.

4.5.3. Kotov and Ushakov attack

The KU attack is based on the fact that the tropical matrices displays pattern in higher tropical power. And also tropical multiplication of tropical coefficient is actually the usual addition of the coefficient with all the entries of the matrix. This fact helped Kotov and Ushakov to find the matrix

$$T^{ij} = U - [A^{\odot i} \odot B^{\odot j}]$$

which allowed them to find the private parameters.

In protocol 2, we have used commutative elements from the semiring and we have not taken tropical powers of any matrix that is the primary reason why Kotov and Ushakov attack [17] won't work on protocol 2. We know that any circulant matrix with entries $a_0, a_1, \cdots, a_{n-1}$ can be written as the form of $a_0 I + a_1 P + \cdots + a_{n-1} P^{n-1}$ in classical algebra, where $P = [0, 1, \cdots, 0; 0, 0, 1, \cdots, 0; \cdots; 1, 0, \cdots, 0]$. In protocol 2 public matrix Y cannot be written as the polynomial format unlike the one in [13]. The private parameters P_1, Q_1, P_2, Q_2 are not a circulant matrix they are from the lower/upper circulant matrices and they cannot be represented by the shared matrices $P_1 \otimes Y \otimes Q_1$ and $P_2 \otimes Y \otimes Q_2$.

4.5.4. Rudy and Monico attack

The public key exchange protocol based on semidirect product of max plus matrices discussed in Section 4 of article [18] is developed by Grigoriev and Shpilrain. Let $R = (M_{n\times n}(\mathbb{Z}), \oplus, \otimes)$ and Alice and Bob agree the public matrices $M, H \in R$. Final key of Alice is $(B \circ H^m) \oplus A = B \oplus H^m \oplus (B \otimes H^m) \oplus A$ equals to the key of Bob $(A \circ H^n) \oplus B = A \oplus H^n \oplus (A \otimes H^n) \oplus B$ [18]. Where H^m and H^n denoted the m^{th} and n^{th} tropical power of H matrix respectively. This protocol is attacked by Rudy and Monico by the simple binary search attack [19]. The main idea of the simple binary search attack is to find the tropical power m at which the tuple (M, H) becomes (A, H^m) with the known A. But in protocol 2 we never use any tropical powers. Hence, Rudy and Monico attack is not valid in protocol 2.

5. Comparative analysis

In this section, we have compared the experimental results of both protocol 1 and protocol 2 with some familiar tropical protocols. The following experiments were done in a computer with 11th Gen Intel(R) Core(TM) i5-11300H @ 3.10 GHz processor with 8 GB ram running on windows 11 with 64-bits operating system. The algorithms of the protocols are executed in maple 2018 software.

Table 1. Comparison with some tropical schemes.

Schemes	Kotov and Ushakov attack	Rudy and Monico attack
Grigoriev's protocol in [13]	✗	✗
Grigoriev's protocol in [18]	✓	✗
Protocol based on upper or lower-s-circulant matrices	✓	✓
Proposed protocol 2	✓	✓

Note: In the Table 1, ✗ denotes that the scheme is attacked by the corresponding attack and ✓ denotes that the scheme is safe against the attack.

Most of the tropical protocols proposed in recent years involves the exponentiation of the tropical matrices. When we compare the time complexity of tropical power based algorithms with our proposed algorithm, we can see that the time complexity of those algorithms is higher than our algorithms. That is, $O(n^3) < O(n^{n+3})$ where, n is the dimension of matrices involved in tropical powers.

The idea of using commuting matrices in tropical linear algebra on the Stickel's protocol instead of tropical powers and polynomials have already been examined in [24–26]. In many protocols they have used circulant matrices but, the main idea of our paper is to generate secret keys efficiently with the commutative subset $((\mathfrak{A}(D_p[\mathfrak{C}])^u_l)(s))_n, \oplus, \otimes)$ of tropical semiring $(M_{n\times n}(\mathfrak{Z}), \oplus, \otimes)$.

5.1. *Comparison of protocol based on upper or lower-s-circulant matrices and proposed protocol 2*

The key exchange protocol 1 is based on upper or lower-s-circulant matrices which contains $2n$ elements in $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$ and the protocol 2 based on anti-s-p-circulant matrices P_1, P_2, Q_1, Q_2 which are performed with $2n$ elements. The time complexity of both protocols are same. From Figure 1 we can analyse the key generation time of protocol 1 and protocol 2.

Given data in Table 2 is plotted in Figure 1 above.

Table 2. Key generation time in seconds.

Key size (Bits)	Time taken (sec) (Protocol based on upper or lower circulant matrices)	Time taken (sec) (Proposed protocol 2)
32	0.017	0.016
50	0.068	0.042
64	0.087	0.075
128	0.13	0.1
256	0.22	0.19

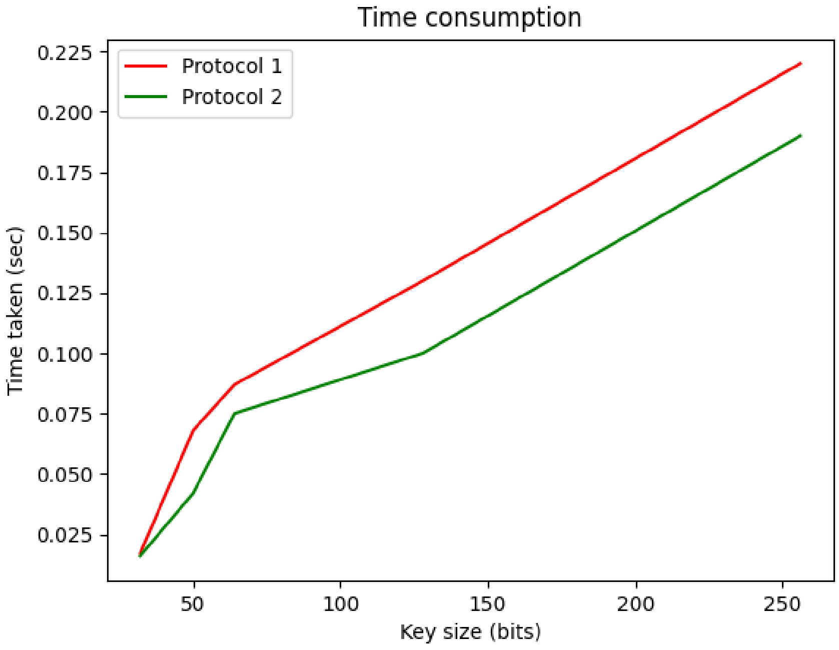

Figure 1. Time comparison graph in seconds.

Memory usage: We have analysed memory usage of protocol based on upper or lower-s-circulant matrices and our proposed protocol 2. This shows that the memory usage of our proposed protocol 2 is better than the memory usage of protocol 1.

Experimental datas of memory usage given in Table 3 is plotted in Figure 2.

Table 3. Comparison of memory usage in MiB.

Bits	Memory usage (Protocol based on upper or lower-s-circulant matrices)	Memory usage (Proposed protocol 2)
32	1.046	1.005
50	1.14	1.099
64	1.342	1.239
128	1.494	1.330
256	1.54	1.441

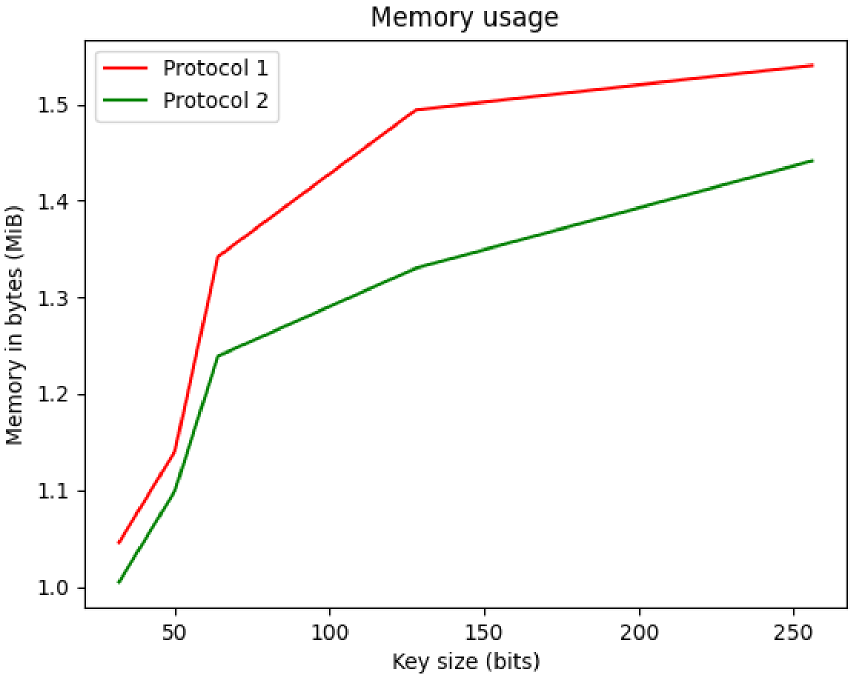

Figure 2. Comparison of memory usage (MiB).

Time complexity of protocol based on upper or lower-s-circulant matrices: In the key exchange protocol 1, we have four public parameters Y, s, t, n. Here Y, s, t are fixed and variable is n. Matrices $\mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{B}_1, \mathfrak{B}_2$ each with $2n$ elements and tropical multiplication is performing four times in the protocol. Therefore, the total time complexity of multiplying five matrices in the tropical semiring $(\mathfrak{C}_l(s))_n$ with order n is $O(n^3 \times 4) = O(n^3)$.

Time complexity of proposed protocol 2: In the key exchange protocol 2, we have four public parameters Y, s, t, n. Here Y, s, t are fixed and variable is n. Matrices P_1, P_2, Q_1, Q_2 each with $2n$

elements and tropical multiplication is performing four times in the protocol. Therefore, the total time complexity of multiplying five matrices in the tropical semiring $((\mathfrak{A}(D_p[\mathfrak{C}])_l^u)(s))_n, \oplus, \otimes)$ with order n is $O(n^3 \times 4) = O(n^3)$.

Both protocol 1 and protocol 2 have the same time complexity but the memory usage of protocol 2 is lesser than that of protocol 1. The reason is that the protocol 2 is generated by the use of commutative subset of $((\mathfrak{A}(D_p[\mathfrak{C}])_l^u)(s))_n, \oplus, \otimes)$ of tropical semiring $(M_{n\times n}(\mathfrak{Z}), \oplus, \otimes)$. Let protocol 1 is performed with the lower-s-circulant matrices of order n and protocol 2 is performed with anti-s-p-circulant matrices of order k, where $k > n$ then, protocol 2 would be more efficient than protocol 1.

6. Conclusions

In this paper, we have proposed the key exchange protocol by introducing the commutative set of anti-s-p-circulant matrices. Most of the protocols over tropical semirings were proposed based on the tropical powers of the matrices. Attacks on the tropical protocols are commonly based on the fact that they exhibit pattern in higher powers. Some of the popular attacks are linear periodicity attack, RM attack, KU attack, etc. To overcome these attacks, we have proposed our protocol which do not involve the exponentiation of tropical matrices. We have given further analysis of the protocol 1 and additionally we have proved some propositions. In the security analysis, we have proved that our proposed protocol is resistant against popular attacks of the existing tropical protocols. Comparative analysis of protocol 1 and our proposed protocol 2 is given. We can see that our proposed protocol performs better in terms of memory usage. In future, we may try to apply these protocols in the security of digital signature and identity authentication schemes. Also, our future work is to find the existence and uniqueness of the solution of tropical two sided matrix action problem.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

The authors would like to thank the editor and reviewers for their valuable comments and suggestions, which greatly help us improve the presentation of this article. We thank the referees for their thoughtful reading of this manuscript and their feedback.

Conflict of interest

The authors declare no conflict of interest.

References

1. F. Piper, S. Murphy, *Cryptography: a very short introduction*, New York: Oxford Academic, 2002. https://doi.org/10.1093/actrade/9780192803153.003.0001
2. G. Manikandan, R. Perumal, Symmetric cryptography for secure communication in IoT, *Materials Today: Proceedings*, **2020** (2020), 737. https://doi.org/10.1016/j.matpr.2020.09.737

3. S. Arshad, M. Khan, New extension of data encryption standard over 128-bit key for digital images, *Neural Comput. Applic.*, **33** (2021), 13845–13858. https://doi.org/10.1007/s00521-021-06023-5

4. E. Fernando, D. Agustin, M. Irsan, D. F. Murad, H. Rohayani, D. Sujana, Performance comparison of symmetries encryption algorithm AES and DES with raspberry Pi, *2019 International Conference on Sustainable Information Engineering and Technology (SIET)*, Lombok, Indonesia, 2019, 353–357. http://doi.org/10.1109/SIET48054.2019.8986122

5. A. J. Menezes, P. C. V. Oorschot, S. A. Vanstone, *Handbook of applied cryptography*, 1 Eds., Boca Raton: CRC Press, 1997. https://doi.org/10.1201/9780429466335

6. K. Ahmed, S. Pal, R. Mohan, A review of the tropical approach in cryptography, *Cryptologia*, **47** (2023), 63–87. https://doi.org/10.1080/01611194.2021.1994486

7. Y. W. Kao, K. Y. Huang, H. Z. Gu, S. M. Yuan, uCloud: a user-centric key management scheme for cloud data protection, *IET Inform. Secur.*, **7** (2013), 144–154. https://doi.org/10.1049/iet-ifs.2012.0198

8. M. Habeeb, D. Kahrobaei, C. Koupparis, V. Shpilrain, Public key exchange using semidirect product of (semi) groups, In: *Applied cryptography and network security*, Heidelberg: Springer, 2013, 475–486. https://doi.org/10.1007/978-3-642-38980-1_30

9. M. Kreuzer, A. D. Myasnikov, A. Ushakov, A linear algebra attack to group-ring-based key exchange protocols, In: *Applied cryptography and network security*, Cham: Springer, 2014, 37–43. https://doi.org/10.1007/978-3-319-07536-5_3

10. D. Kahrobaei, C. Koupparis, V. Shpilrain, A CCA secure cryptosystem using matrices over group rings, *Contemporary Mathematics*, **633** (2015), 73–81. http://doi.org/10.1090/conm/633/12652

11. W. Diffie, M. Hellman, New directions in cryptography, *IEEE T. Inform. Theory*, **22** (1976), 644–654. http://doi.org/10.1109/TIT.1976.1055638

12. V. Shpilrain, Cryptanalysis of Stickel's key exchange scheme, In: *Computer science–theory and applications*, Berlin: Springer, 2008, 283–288. http://doi.org/10.1007/978-3-540-79709-8_29

13. D. Grigoriev, V. Shpilrain, Tropical cryptography, *Commun. Algebra*, **42** (2014), 2624–2632. http://doi.org/10.1080/00927872.2013.766827

14. Z. Izhakian, Basics of linear algebra over the extended tropical semiring, *Contemporary Mathematics*, **495** (2009), 173–191.

15. Z. Izhakian, L. Rowen, The tropical rank of a tropical matrix, *Commun. Algebra*, **37** (2009), 3912–3927. https://doi.org/10.1080/00927870902828793

16. D. Jones, Matrix roots in the max-plus algebra, *Linear Algebra Appl.*, **631** (2021), 10–34. https://doi.org/10.1016/j.laa.2021.08.008

17. M. Kotov, A. Ushakov, Analysis of a key exchange protocol based on tropical matrix algebra, *J. Math. Cryptol.*, **12** (2018), 137–141. https://doi.org/10.1515/jmc-2016-0064

18. D. Grigoriev, V. Shpilrain, Tropical cryptography II: extensions by homomorphisms, *Commun. Algebra*, **47** (2019), 4224–4229. https://doi.org/10.1080/00927872.2019.1581213

19. D. Rudy, C. Monico, Remarks on a tropical key exchange system, *J. Math. Cryptol.*, **15** (2021), 280–283. https://doi.org/10.1515/jmc-2019-0061

20. S. Isaac, D. Kahrobaei, A closer look at the tropical cryptography, *Int. J. Comput. Math.*, **6** (2021), 137–142. https://doi.org/10.1080/23799927.2020.1862303

21. H. Huang, C. Li, L. Deng, Public-key cryptography based on tropical circular matrices, *Appl. Sci.*, **12** (2022), 7401. https://doi.org/10.3390/app12157401

22. F. Olia, S. Ghalandarzadeh, A. Amiraslani, S. Jamshidvand, Solving linear systems over tropical semirings through normalization method and its applications, *J. Algebra Appl.*, **20** (2021), 2150159. https://doi.org/10.1142/S0219498821501590

23. F. Mohammadi, M. Michałek, B. Sturmfels: "invitation to nonlinear algebra", *Jahresber. Dtsch. Math. Ver.*, **124** (2022), 197–204. https://doi.org/10.1365/s13291-022-00252-w

24. A. Muanalifah, S. Sergeev, Modifying the tropical version of stickel's key exchange protocol, *Appl. Math.*, **65** (2020), 727–753. https://doi.org/10.21136/AM.2020.0325-19

25. S. Mehmood, Key exchange protocol based on matrices using tropical algebra, Master Thesis, Capital University of Science and Science and Technology, 2019.

26. M. I. Durcheva, Public key cryptography with max-plus matrices and polynomials, *AIP Conference Proceedings*, **1570** (2013), 491–498. http://doi.org/10.1063/1.4854794

AIMS Press