EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
2025, Vol. 18, Issue 3, Article Number 5888
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

A Key Exchange Protocol Based on the Twin Conjugacy Search Problem Over Tropical Algebra

Kashifa Begum A.[1], V. Muthukumaran[1], V. Govindan[2], Haewon Byeon[3,*]

[1] *Department of Mathematics, College of Engineering and Technology, Faculty of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur - 603203, Chengalpattu, Tamil Nadu, India*
[2] *Department of Mathematics, Hindustan Institute of Technology and Science, Chennai - 603103, Tamil Nadu, India*
[3] *Convergence Department, Korea University of Technology and Education, Cheonan, South Korea*

Abstract. In public key cryptography, the security of the data leans on the hardness of solving some mathematical problems over algebraic structures, such as groups, rings, etc. The first published key exchange protocol is by Diffie and Hellman in 1976, whose security hinges on the challenges in solving the Discrete Logarithm Problem (DLP) over any finite field. In this research article, we present a key exchange protocol based on the Twin Conjugacy Search Problem (TCSP), a variant of the well-known Conjugacy Search Problem (CSP), and Tropical Algebra as a platform for the TCSP. We have provided two variants of the key exchange protocol and also provided a toy example. The chosen platform, Tropical Algebra, is a new approach and is easy to implement and not computationally hard as with other non-abelian groups as a platform, since one doesn't have to perform any complex multiplication or addition. The security and complexity analysis of the protocol have also been explored.

2020 Mathematics Subject Classifications: 14G50, 14T10, 15A80, 15B33

Key Words and Phrases: Conjugacy Search Problem, Twin Conjugacy Search Problem, Tropical Algebra, Public Key Exchange

1. Introduction

In the zone of modern cryptography, the security of information, its transmission and storage is predominant. The ability to shield sensitive data in an age of immanent digital communication and interconnected systems is a primitive concern. Cryptographic algorithms serve as the cutting edge in this venture, with one of the main stay being the

*Corresponding author.
DOI: https://doi.org/10.29020/nybg.ejpam.v18i3.5888

Email addresses: kb5928@srmist.edu.in (Kashifa Begum A.), muthu.v2404@gmail.com (V. Muthukumaran), govindoviya@gmail.com (V. Govindan), bhwpuma@naver.com (Haewon Byeon)

Discrete Logarithm Problem (DLP). The DLP has portrayed a core role in the development of secure communication protocol, digital signatures, and public key cryptosystems. Its resilience to attacks, at that time, formed the basis for the security of widely used schemes, such as the Diffie–Hellman key exchange, ElGamal encryption, and the Digital Signature Algorithm (DSA) [1–4].

The **Discrete Logarithm Problem (DLP)** for a group G is to find at least one $k \in G \ni$, for given any two elements $a, b \in G, b = a^k$.

One of the popular choices of G for the DLP are cyclic groups $\mathbb{Z}_p^*$, where p is any prime.

The recent advancements and evolution towards quantum computing made it easy to solve the DLP. Hence the search for a new hard problem for key exchange protocols led us to the Conjugacy Search Problem (CSP), one of the flair generalizations of the DLP. The combination of the DLP and CSP is given in [5].

The **Conjugacy Decision Problem (CDP)** for a group G is a decision making problem of determining, given any two elements $a, b \in G$, whether or not they are conjugate in G, i.e., if $\exists$ an element $g \in G \ni g^{-1}ag = b$.

The **Conjugacy Search Problem (CSP)** for a group G requires us to search, for any two given conjugate elements $a, b \in G$, a conjugating element $g \in G \ni g^{-1}ag = b$.

The (presumed) computational difficulty of this problem in some groups (namely in braid groups, garside groups, non-commutative semi groups) has been used in several group based public key protocols [6–8].

Though CSP on some particular platforms (the solutions to the CSP in polycyclic groups, p-groups, and matrix groups are given in [9]) are vulnerable to security, they still have the value of reference and the search for a suitable platform is an active area of research. Despite that the CSP and its variant versions (namely, the Twin Conjugacy Search Problem (TCSP) and the Double Conjugacy Search Problem (DCSP) [10, 11]) have a sufficient security level and play a significant role on non-abelian group based public key cryptography.

Nevertheless, the efficiency and security of cryptographic systems does not depend only on the type of algorithm, but also on the choice of the platform. One such unprobed platform is *Tropical Algebra*, a relatively recent branch of Mathematics which has emerged as a cogent tool with applications extending over diverse fields, from Optimization, Computer Science to Biology and Economics. The phrase *Tropical* was originated by French Mathematicians in admiration of the Hungarian–born Brazilian Computer Scientist Imre Simon. For introductory enlightenment on *Tropical Geometry* one can refer [12, 13].

The substance of Tropical Algebra lies in its competence to simplify complex problems by rebuilding them into a more viable algebraic structure, by replacing the traditional addition with the maximum (or minimum) operation and the traditional multiplication with the traditional addition operation. For contemporary evolution in tropical algebra one can refer [14–18].

Thus we have chosen Tropical Algebra as a platform for the TCSP based key exchange protocol, and also elaborated on the resilience of the protocol to various attacks including Brute Force attack and KU attack. The article is arranged as follows: In section 2, the preliminaries required are given. The TCSP over tropical algebra is given in section 3. The two versions of the protocol proposed is given in section 4. A toy example of the first protocol is given in section 5. In section 6, the security and complexity analysis of the protocol is given and the article is concluded in section 7.

2. Preliminaries

2.1. The Twin Conjugacy Search Problem

The TCSP is defined in [10] as follows:

The **Twin Conjugacy Search Problem (TCSP)** for a braid group B_n is to find $x_1, x_2 \in B_n$, for given $g, X_1, X_2 \in B_n, \ni X_1 = x_1 g x_1^{-1},\ X_2 = x_2 g x_2^{-1}$.

2.2. Chen and You's Key Exchange Protocol

There are two versions of the key exchange protocol based on the TCSP over braid group in [10] and we reiterate both the versions here.

Suppose that the two people who need to communicate are Alice and Bob.

Consider $H : B_{l+r} \to \{0,1\}^{l(k)}$, where H is a hash function, B_{l+r} is a braid group, and $l(k)$ is a security parameter. Let $g \in B_{l+r}$ be a public element.

2.2.1. Protocol I

(i) **Key Generation:** Alice chooses two secret parameters $x_1, x_2 \in LB_l$, and computes $X_i = x_i g x_i^{-1},\ i = 1, 2$. (X_1, X_2, g) is the public key and the private key is (x_1, x_2).

(ii) **Encryption:** Consider the cipher message $m \in B_{l+r}$, Bob selects a secret element $y \in RB_r$, and calculates $Y = ygy^{-1},\ Z_i = yX_i y^{-1},\ i = 1, 2,\ c = Enc_k(m),\ k = H(Y, Z)$. The ciphertext is (Y, c).

(iii) **Decryption:** To Decrypt the ciphertext (Y, c), Alice compute $Z_i = x_i Y x_i^{-1},\ i = 1, 2,\ m = Dec_k(c),\ k = H(Y, Z)$.

2.2.2. Protocol II

(i) **Key Generation:** Alice chooses two secret parameters $x_1, x_2 \in LB_l$, and computes $X_i = x_i g x_i^{-1},\ i = 1, 2$. The public key is (X_1, X_2, g) and the private key is (x_1, x_2).

(ii) **Encryption:** Bob selects two random parameters $y_1, y_2 \in RB_r$, and calculates $Y_i = y_i g y_i^{-1},\ i = 1, 2$. Bob also computes the secret keys $Z_{ij} = y_j X_i y_j^{-1},\ i = 1, 2,\ j = 1, 2$. The public key is (Y_1, Y_2, g) and the private key is (y_1, y_2).

(iii) **Decryption:** Alice computes the secret keys $Z_{ij} = x_i Y_j x_i^{-1},\ i = 1, 2,\ j = 1, 2$.

Because of $ccs(X_i, Y_j) = Z_{ij} = x_i Y_j x_i^{-1} = y_j X_i y_j^{-1},\ i = 1, 2,\ j = 1, 2$, Alice and Bob can calculate the same value through the hash function H:

$$k = H(ccs(X_1, Y_1),\ ccs(X_1, Y_2),\ ccs(X_2, Y_1),\ ccs(X_2, Y_2)).$$

2.3. Semiring

A **semiring** is a set R together with two binary operations '+' and '$\cdot$' $\ni$

- $(R, +)$ is a commutative monoid,
- $(R, \cdot)$ is a monoid,
- Multiplication by 0 annihilates R, i.e., $r \cdot 0 = 0 \cdot r = 0,\ \forall\ r \in R$, and
- Multiplication is both left and right distributive over addition, i.e.,

  $r \cdot (s + t) = (r \cdot s) + (r \cdot t)$

  $(s + t) \cdot r = (s \cdot r) + (t \cdot r),\ \forall\ r, s, t \in R.$

2.4. Tropical Algebra

A **tropical algebra** is the semiring $R_{min} = (R \cup \{+\infty\}, \oplus, \otimes)$, where the operations $\oplus$ and $\otimes$, referred to as tropical addition and tropical multiplication, respectively, are defined as ($\forall\ s, t \in R \cup \{+\infty\}$)

$$s \oplus t = \min\{s, t\},$$
$$s \otimes t = s + t.$$

2.5. Tropical Monomial

Let $x = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n_{min}, a \in \mathbb{R}$, and $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}^n$. Then a **tropical monomial** is the function

$$p(x) = a \otimes x_1^{\otimes \alpha_1} \otimes x_2^{\otimes \alpha_2} \otimes \cdots \otimes x_n^{\otimes \alpha_n},$$

where exponentiation is defined tropically as repeated tropical multiplication, i.e., $x_i^{\otimes \alpha_i} = \alpha_i x_i$.

Ex. $x_1 \otimes x_2 \otimes x_2 = x_1 \otimes x_2^{\otimes 2} = x_1 + 2x_2$.

2.6. Inverse of a Tropical Monomial

Let $p(x)$ be a tropical monomial over $\mathbb{R}_{min}$. We define the inverse of $p(x)$ to be a monomial $p'(x)$ over $\mathbb{R}_{min} \ni$

$$p(x) \otimes p'(x) = 0.$$

Ex. If $p(x) = a \otimes x^{\otimes n}$, then $p'(x) = -a \otimes (-x)^{\otimes n}$, where $a, x \in \mathbb{R}$ and $n \in \mathbb{N}$.

2.7. Tropical Matrix Algebra

2.7.1. Tropical Matrix

A matrix of order $n \times n$ with entries from tropical algebra R_{min} equipped with tropical addition $\oplus$ and multiplication $\otimes$ is called a **tropical matrix**.

The set of all $n \times n$ tropical matrices over R_{min} is denoted by $M_n(R_{min})$.

2.7.2. Tropical Diagonal Matrix

A **tropical diagonal matrix** is an $n \times n$ tropical matrix with entries $a_i \in R,\ i = 1, ..., n$, on the diagonal and ∞ elsewhere, that is,

$$D = \begin{pmatrix} a_1 & \infty & \dots & \infty \\ \infty & a_2 & \dots & \infty \\ \vdots & \vdots & \ddots & \vdots \\ \infty & \infty & \dots & a_n \end{pmatrix}.$$

2.7.3. Tropical Matrix Multiplication

Let P, Q $\in M_n(R_{min})$. Then $T = P \otimes Q$ is given by

$$t_{ij} = \bigoplus_{k=1}^{n} (p_{ik} \otimes q_{kj}).$$

Ex. $\begin{pmatrix} 1 & 2 & -1 \\ 3 & 1 & 3 \\ 2 & -2 & 3 \end{pmatrix} \otimes \begin{pmatrix} 3 & 1 & 2 \\ 4 & -1 & 3 \\ 2 & 1 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & -3 \\ 5 & 0 & 1 \\ 2 & -3 & 1 \end{pmatrix}.$

2.7.4. Tropical Matrix Scalar Multiplication

Let P $\in M_n(\mathbb{R}_{min})$ and $s \in \mathbb{R}_{min}$. Then the tropical matrix scalar multiplication $s \otimes P$ is given by

$$s \otimes P = (s \otimes E) \otimes P = s \otimes p_{ij} = s + p_{ij},$$

where E is the multiplicative identity matrix.

Ex. $5 \otimes \begin{pmatrix} 1 & 2 & -1 \\ 3 & 1 & 3 \\ 2 & -2 & 3 \end{pmatrix} = \begin{pmatrix} 5 & \infty & \infty \\ \infty & 5 & \infty \\ \infty & \infty & 5 \end{pmatrix} \otimes \begin{pmatrix} 1 & 2 & -1 \\ 3 & 1 & 3 \\ 2 & -2 & 3 \end{pmatrix} = \begin{pmatrix} 6 & 7 & 4 \\ 8 & 6 & 8 \\ 7 & 3 & 8 \end{pmatrix}.$

2.7.5. Properties

The following are properties with respect to tropical matrix multiplication and scalar multiplication. For all $P, Q, S \in M_n(\mathbb{R}_{min}),\ m, n \in \mathbb{Z}$ and $s, t \in \mathbb{R}_{min}$,

- $P \otimes (Q \otimes S) = (P \otimes Q) \otimes S$ **(Associativity)**
- $P^{\otimes m} \otimes P^{\otimes n} = P^{\otimes n} \otimes P^{\otimes m} = P^{\otimes(m+n)}$ **(Commutativity)**
- **Multiplicative Identity Matrix:**

  $\exists$ an unique $n \times n$ matrix $E \in M_n(\mathbb{R}_{min}), \ni P \otimes E = E \otimes P = P$, where $E = \begin{pmatrix} 0 & \infty & \dots & \infty \\ \infty & 0 & \dots & \infty \\ \vdots & \vdots & \ddots & \vdots \\ \infty & \infty & \dots & 0 \end{pmatrix}$.
- **Multiplicative Inverse Matrix:**

  Multiplicative inverse of a matrix P is a matrix $P' \in M_n(\mathbb{R}_{min}) \ni P \otimes P' = E$. In general, tropical matrices are non-invertible.
- **Miscellaneous:**

  $s \otimes P = P \otimes s$

  $(s \otimes P) \otimes (t \otimes P) = (s \otimes t) \oplus (P \otimes P) = (s + t) \otimes P^{\otimes 2}$

3. The Twin Conjugacy Search Problem over Tropical Algebra

In this section, the TCSP over tropical algebra is defined. The security and complexity of the problem is also explored.

3.1. The Twin Conjugacy Search Problem over Tropical Algebra

The **Twin Conjugacy Search Problem (TCSP)** for the tropical algebra $R = M_n(\mathbb{R}_{min})$ is to find two matrices $A_1, A_2 \in R$ and two tropical monomials $p_1(x), p_2(x)$ over $\mathbb{R}_{min}$, for given $(g(A), X_1, X_2) \in R \times R \times R$, where $g(x)$ is a tropical monomial and $A \in R, \ni$

$$X_1 = p_1(A_1) \otimes g(A) \otimes p_1^{'}(A_1),$$
$$X_2 = p_2(A_2) \otimes g(A) \otimes p_2^{'}(A_2).$$

3.2. Security of the Twin Conjugacy Search Problem

(i) **Determinant Attack:** The determinant attack is not valid because of the non commutative property of determinants in tropical algebra. Even if an adversary knows $det(X_i)$ and $det(g(A))$, since $p_i(A_i), i = 1, 2$ are unknowns, this attack is invalid.

(ii) **Eigenvalue Attack:** This attack may work in some classical group or ring, but we have considered tropical algebra where finding the eigenvalues of a matrix is feeble. Even if an adversary finds the eigenvalues of X_i and $g(A)$, using it to find the secret elements $p_i(A_i)$ is not effectual.

(iii) **Cayley-Hamilton Attack:** In [19], it is said that finding the value of a matrix substituted in a polynomial is manageable if the matrix is known. Along with that to use the Cayley-Hamilton attack, an adversary must know two polynomials r_i over $\mathbb{R}_{min} \ni r_i(A_i) = \bigoplus_{k=1}^{n-1}(a_k \otimes A_i^k)$, since A_i are unknown this attack is invalid.

3.3. Brute - Force Complexity

To find the secret keys $p_i(A_i),\ i = 1, 2$, by Brute - Force Attack, is to find both p_i and $A_i,\ i = 1, 2$ or two $n \times n$ matrices $P_i \in R \ni P_i = p_i(A_i), i = 1, 2$. The time complexity of finding an $n \times n$ matrix is $O(n^2)$.

Suppose that R is finite, i.e., we take $R = M_n(\mathbb{Z}_{\eta_{min}})$, then the exhaustive search algorithm is given in Algorithm 1.

Algorithm 1 Exhaustive Search Algorithm

Input: $X, g(A) \in R \ni X = p(A_1) \otimes g(A) \otimes\ p'(A_1)$
Output: Secret parameter $p(A_1) \in R$
for $i \leftarrow 1$ to $\eta - 1$ **do**
  $\tilde{p}(A_i) \leftarrow p_i(A_i)$
  for $j \leftarrow 1$ to $\eta - 1$ **do**
    $X_j = \tilde{p}(A_i) \otimes g(A) \otimes \tilde{p}'(A_i)$
    if $X = X_j$ **then**
      return X_j and $p_i(A_i)$
    end if
  end for
end for

4. The Key Exchange Protocol based on the Twin Conjugacy Search Problem over Tropical Algebra

We propose two key exchange protocols based on the TCSP over tropical algebra.

Assume Alice and Bob are the two parties who need to exchange information.

Consider the tropical algebra $R = M_n(\mathbb{R}_{min})$. Let $H \subset R$ be the subset containing all the tropical diagonal matrices. Let $g(x)$ be a public tropical monomial over $\mathbb{R}_{min}$ and $A \in R \setminus H$ be public tropical matrix.

4.1. The Key Exchange Protocol I

(i) **Key Generation:** Alice chooses two random secret tropical monomials $p_1(x), p_2(x)$ over $\mathbb{R}_{min}$, two secret matrices $D_i \in H,\ i = 1, 2$ and sends (X_1, X_2) to Bob, where $X_1 = p_1(D_1) \otimes g(A) \otimes p_1'(D_1)$ and $X_2 = p_2(D_2) \otimes g(A) \otimes p_2'(D_2)$. Thus the public key is (X_1, X_2, g, A), and the private key is (p_1, p_2, D_1, D_2).

(ii) **Encryption:** Bob chooses a random secret tropical monomial $q(x)$ over $\mathbb{R}_{min}$, a secret matrix $B \in H$ and sends Y to Alice, where $Y = q(B) \otimes g(A) \otimes q'(B)$. Thus the public key is (Y, g, A), and the private key is (q, B).

(iii) **Decryption:** Alice receives Y and computes $Z_1 = p_1(D_1) \otimes Y \otimes p_1'(D_1),\ Z_2 = p_2(D_2) \otimes Y \otimes\ p_2'(D_2)$. Bob receives (X_1, X_2) and computes $\tilde{Z}_1 = q(B) \otimes X_1 \otimes q'(B),\ \tilde{Z}_2 = q(B) \otimes X_2 \otimes q'(B)$.

(iv) **Correctness:** Since $p_i(D_i) \otimes q(B) = q(B) \otimes p_i(D_i)$, and $p_i'(D_i) \otimes q(B) = q(B) \otimes p_i'(D_i),\ i = 1, 2$, Alice and Bob have same secret key, that is, $Z_i = \tilde{Z}_i,\ i = 1, 2$.

Table 1: The Key Exchange Protocol I

Alice		**Bob**
$p_1(x), p_2(x) \leftarrow \mathbb{R}_{min},\ D_1, D_2 \leftarrow H$		
$X_1 = p_1(D_1) \otimes g(A) \otimes p_1'(D_1)$		
$X_2 = p_2(D_2) \otimes g(A) \otimes p_2'(D_2)$		
	$\xrightarrow{X_1, X_2}$	
		$q(x) \leftarrow \mathbb{R}_{min},\ B \leftarrow H$
		$Y = q(B) \otimes g(A) \otimes q'(B)$
	$\xleftarrow{Y}$	
$Z_1 = p_1(D_1) \otimes Y \otimes p_1'(D_1)$		$\tilde{Z}_1 = q(B) \otimes X_1 \otimes q'(B)$
$Z_2 = p_2(D_2) \otimes Y \otimes\ p_2'(D_2)$		$\tilde{Z}_2 = q(B) \otimes X_2 \otimes q'(B)$
	$Z_1 = \tilde{Z}_1$	
	$Z_2 = \tilde{Z}_2$	

4.2. The Key Exchange Protocol II

(i) **Key Generation:** Alice chooses two random secret tropical monomials $p_1(x), p_2(x)$ over $\mathbb{R}_{min}$, two secret matrices $D_1, D_2 \in H$ and sends (X_1, X_2) to Bob, where $X_1 = p_1(D_1) \otimes g(A) \otimes\ p_1'(D_1)$ and $X_2 = p_2(D_2) \otimes g(A) \otimes\ p_2'(D_2)$. Then the public key is (X_1, X_2, g, A), while the private key is (p_1, p_2, D_1, D_2).

(ii) **Encryption:** Bob chooses two random secret tropical monomials $q_1(x)$, $q_2(x)$ over $\mathbb{R}_{min}$, two secret matrices $B_1, B_2 \in H$ and sends (Y_1, Y_2) to Alice, where $Y_1 = q_1(B_1) \otimes g(A) \otimes\ q_1'(B_1)$ and $Y_2 = q_2(B_2) \otimes g(A) \otimes q_2'(B_2)$. Then the public key is (Y_1, Y_2, g, A), while the private key is (q_1, q_2, B_1, B_2).

(iii) **Decryption:** Alice receives (Y_1, Y_2) and computes $Z_{ij} = p_i(D_i) \otimes Y_j \otimes p'_i(D_i),\ i, j = 1, 2$. Bob receives (X_1, X_2) and computes $\tilde{Z_{ij}} = q_j(B_j) \otimes X_i \otimes q'_j(B_j),\ i = 1, 2,\ j = 1, 2$.

(iv) **Correctness:** Since $p_i(D_i) \otimes q_j(B_j) = q_j(B_j) \otimes p_i(D_i)$, and $p'_i(D_i) \otimes q_j(B_j) = q_j(B_j) \otimes p'_i(A_i),\ i, j = 1, 2$, Alice and Bob have same secret key, that is, $Z_{ij} = \tilde{Z_{ij}},\ i = 1, 2,\ j = 1, 2$.

Table 2: The Key Exchange Protocol II

Alice		**Bob**
$p_1(x), p_2(x) \leftarrow \mathbb{R}_{min},\ D_1, D_2 \leftarrow H$		
$X_1 = p_1(D_1) \otimes g(A) \otimes p'_1(D_1)$		
$X_2 = p_2(D_2) \otimes g(A) \otimes p'_2(D_2)$		
	$\xrightarrow{X_1, X_2}$	
		$q_1(x), q_2(x) \leftarrow \mathbb{R}_{min},\ B_1, B_2 \leftarrow H$
		$Y_1 = q_1(B_1) \otimes g(A) \otimes q'_1(B_1)$
		$Y_2 = q_2(B_2) \otimes g(A) \otimes q'_2(B_2)$
	$\xleftarrow{Y_1, Y_2}$	
$Z_{ij} = p_i(D_i) \otimes Y_j \otimes p'_i(D_i)$		$\tilde{Z_{ij}} = q_j(B_j) \otimes X_i \otimes q'_j(B_j)$
	$Z_{ij} = \tilde{Z_{ij}},$ $i = 1, 2,\ j = 1, 2$	

5. A Toy Example of the Protocol

In this section, a toy example of the first protocol is given.

Let $p_1(x) = 2 \otimes x^{\otimes 2},\ p_2(x) = 5 \otimes x^{\otimes 3},\ q(x) = 2 \otimes x,\ D_1 = \begin{pmatrix} 2 & \infty & \infty \\ \infty & 3 & \infty \\ \infty & \infty & 6 \end{pmatrix},\ D_2 = \begin{pmatrix} 1 & \infty & \infty \\ \infty & -5 & \infty \\ \infty & \infty & 4 \end{pmatrix},\ B = \begin{pmatrix} 6 & \infty & \infty \\ \infty & 5 & \infty \\ \infty & \infty & -3 \end{pmatrix}$ be private.

Let $g(x) = 3 \otimes x^{\otimes 2}$ and $A = \begin{pmatrix} 1 & 2 & -1 \\ 3 & 5 & -2 \\ -1 & 2 & 3 \end{pmatrix}$ be public.

Then $p'_1(x) = -2 \otimes (-x)^{\otimes 2},\ p_2(x) = -5 \otimes (-x)^{\otimes 3},\ q(x) = -2 \otimes (-x)$.

Alice calculates

$$p_1(D_1) = 2 \otimes \begin{pmatrix} 2 & \infty & \infty \\ \infty & 3 & \infty \\ \infty & \infty & 6 \end{pmatrix}^{\otimes 2} = 2 \otimes \begin{pmatrix} 4 & \infty & \infty \\ \infty & 6 & \infty \\ \infty & \infty & 12 \end{pmatrix} = \begin{pmatrix} 6 & \infty & \infty \\ \infty & 8 & \infty \\ \infty & \infty & 14 \end{pmatrix},$$

$$p_1'(D_1) = -2 \otimes \begin{pmatrix} -2 & \infty & \infty \\ \infty & -3 & \infty \\ \infty & \infty & -6 \end{pmatrix}^{\otimes 2} = -2 \otimes \begin{pmatrix} -4 & \infty & \infty \\ \infty & -6 & \infty \\ \infty & \infty & -12 \end{pmatrix} = \begin{pmatrix} -6 & \infty & \infty \\ \infty & -8 & \infty \\ \infty & \infty & -14 \end{pmatrix},$$

$$p_2(D_2) = 5 \otimes \begin{pmatrix} 1 & \infty & \infty \\ \infty & -5 & \infty \\ \infty & \infty & 4 \end{pmatrix}^{\otimes 3} = 5 \otimes \begin{pmatrix} 3 & \infty & \infty \\ \infty & -15 & \infty \\ \infty & \infty & 12 \end{pmatrix} = \begin{pmatrix} 8 & \infty & \infty \\ \infty & -10 & \infty \\ \infty & \infty & 17 \end{pmatrix},$$

$$p_2'(D_2) = -5 \otimes \begin{pmatrix} -1 & \infty & \infty \\ \infty & 5 & \infty \\ \infty & \infty & -4 \end{pmatrix}^{\otimes 3} = -5 \otimes \begin{pmatrix} -3 & \infty & \infty \\ \infty & 15 & \infty \\ \infty & \infty & -12 \end{pmatrix} = \begin{pmatrix} -8 & \infty & \infty \\ \infty & 10 & \infty \\ \infty & \infty & -17 \end{pmatrix},$$

$$g(A) = 3 \otimes \begin{pmatrix} 1 & 2 & -1 \\ 3 & 5 & -2 \\ -1 & 2 & 3 \end{pmatrix}^{\otimes 2} = 3 \otimes \begin{pmatrix} -2 & 1 & 0 \\ -3 & 0 & 1 \\ 0 & 1 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 4 & 3 \\ 0 & 3 & 4 \\ 3 & 4 & 1 \end{pmatrix}.$$

$$\text{Also } X_1 = \begin{pmatrix} 6 & \infty & \infty \\ \infty & 8 & \infty \\ \infty & \infty & 14 \end{pmatrix} \otimes \begin{pmatrix} 1 & 4 & 3 \\ 0 & 3 & 4 \\ 3 & 4 & 1 \end{pmatrix} \otimes \begin{pmatrix} -6 & \infty & \infty \\ \infty & -8 & \infty \\ \infty & \infty & -14 \end{pmatrix} = \begin{pmatrix} 1 & 2 & -5 \\ 2 & 3 & -2 \\ 11 & 10 & 1 \end{pmatrix},$$

$$X_2 = \begin{pmatrix} 8 & \infty & \infty \\ \infty & -10 & \infty \\ \infty & \infty & 17 \end{pmatrix} \otimes \begin{pmatrix} 1 & 4 & 3 \\ 0 & 3 & 4 \\ 3 & 4 & 1 \end{pmatrix} \otimes \begin{pmatrix} -8 & \infty & \infty \\ \infty & 10 & \infty \\ \infty & \infty & -17 \end{pmatrix} = \begin{pmatrix} 1 & 22 & -6 \\ -18 & 3 & -23 \\ 12 & 31 & 1 \end{pmatrix}.$$

Bob calculates

$$q(B) = 2 \otimes \begin{pmatrix} 6 & \infty & \infty \\ \infty & 5 & \infty \\ \infty & \infty & -3 \end{pmatrix} = \begin{pmatrix} 8 & \infty & \infty \\ \infty & 7 & \infty \\ \infty & \infty & -1 \end{pmatrix},$$

$$q'(B) = -2 \otimes \begin{pmatrix} -6 & \infty & \infty \\ \infty & -5 & \infty \\ \infty & \infty & 3 \end{pmatrix} = \begin{pmatrix} -8 & \infty & \infty \\ \infty & -7 & \infty \\ \infty & \infty & 1 \end{pmatrix},$$

$$g(A) = 3 \otimes \begin{pmatrix} 1 & 2 & -1 \\ 3 & 5 & -2 \\ -1 & 2 & 3 \end{pmatrix}^{\otimes 2} = 3 \otimes \begin{pmatrix} -2 & 1 & 0 \\ -3 & 0 & 1 \\ 0 & 1 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 4 & 3 \\ 0 & 3 & 4 \\ 3 & 4 & 1 \end{pmatrix}.$$

$$\text{Also } Y = \begin{pmatrix} 8 & \infty & \infty \\ \infty & 7 & \infty \\ \infty & \infty & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 4 & 3 \\ 0 & 3 & 4 \\ 3 & 4 & 1 \end{pmatrix} \otimes \begin{pmatrix} -8 & \infty & \infty \\ \infty & -7 & \infty \\ \infty & \infty & 1 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 12 \\ -1 & 3 & 12 \\ -6 & -4 & 1 \end{pmatrix}.$$

Alice's shared secret key

$$Z_1 = \begin{pmatrix} 6 & \infty & \infty \\ \infty & 8 & \infty \\ \infty & \infty & 14 \end{pmatrix} \otimes \begin{pmatrix} 1 & 5 & 12 \\ -1 & 3 & 12 \\ -6 & -4 & 1 \end{pmatrix} \otimes \begin{pmatrix} -6 & \infty & \infty \\ \infty & -8 & \infty \\ \infty & \infty & -14 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 4 \\ 1 & 3 & 6 \\ 2 & 2 & 1 \end{pmatrix},$$

$$Z_2 = \begin{pmatrix} 8 & \infty & \infty \\ \infty & -10 & \infty \\ \infty & \infty & 17 \end{pmatrix} \otimes \begin{pmatrix} 1 & 5 & 12 \\ -1 & 3 & 12 \\ -6 & -4 & 1 \end{pmatrix} \otimes \begin{pmatrix} -8 & \infty & \infty \\ \infty & 10 & \infty \\ \infty & \infty & -17 \end{pmatrix} = \begin{pmatrix} 1 & 23 & 3 \\ -19 & 3 & -15 \\ 3 & 23 & 1 \end{pmatrix}.$$

Bob's shared secret key

$$\tilde{Z_1} = \begin{pmatrix} 8 & \infty & \infty \\ \infty & 7 & \infty \\ \infty & \infty & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 2 & -5 \\ 2 & 3 & -2 \\ 11 & 10 & 1 \end{pmatrix} \otimes \begin{pmatrix} -8 & \infty & \infty \\ \infty & -7 & \infty \\ \infty & \infty & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 4 \\ 1 & 3 & 6 \\ 2 & 2 & 1 \end{pmatrix},$$

$$\tilde{Z_2} = \begin{pmatrix} 8 & \infty & \infty \\ \infty & 7 & \infty \\ \infty & \infty & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 22 & -6 \\ -18 & 3 & -23 \\ 12 & 31 & 1 \end{pmatrix} \otimes \begin{pmatrix} -8 & \infty & \infty \\ \infty & -7 & \infty \\ \infty & \infty & 1 \end{pmatrix} = \begin{pmatrix} 1 & 23 & 3 \\ -19 & 3 & -15 \\ 3 & 23 & 1 \end{pmatrix}.$$

Thus $Z_1 = \tilde{Z_1} = \begin{pmatrix} 1 & 3 & 4 \\ 1 & 3 & 6 \\ 2 & 2 & 1 \end{pmatrix}$ and $Z_2 = \tilde{Z_2} = \begin{pmatrix} 1 & 23 & 3 \\ -19 & 3 & -15 \\ 3 & 23 & 1 \end{pmatrix}$.

6. Security and Complexity Analysis of the Protocol

6.1. Completeness of the Protocol

In this subsection, we prove the completeness of the proposed key exchange protocols.

Lemma 1. *Tropical diagonal matrix multiplication is commutative.*

Proof. Let D and E be two $n \times n$ tropical diagonal matrices $\in H$. We wish to prove that $D \otimes E = E \otimes D$.

$$\begin{aligned}(D \otimes E)_{ij} &= \bigoplus_{j=1}^{n} (D_{ij} \otimes E_{ji}) \\ &= \min_{j} (D_{ij} + E_{ji})\end{aligned}$$

Since D and E are diagonal matrices, $D_{ij} = \infty$ for $i \neq j$ and $E_{ji} = \infty$ for $i \neq j$. Therefore, $(D \otimes E)_{ij} = \infty$ for $i \neq j$ and the only non-infinite term in the product occurs when $i = j$. Therefore,

$$(D \otimes E)_{ii} = \min_{i} (D_{ii} + E_{ii})$$

Similarly, for the product matrix $E \otimes D$, we have

$$(E \otimes D)_{ij} = \bigoplus_{j=1}^{n} (E_{ij} \otimes D_{ji}) = \min_{j} (E_{ij} + D_{ji})$$

$$(E \otimes D)_{ii} = \min_{i} (E_{ii} + D_{ii})$$

Thus,

$$D \otimes E = E \otimes D. \ \square$$

Theorem 1. *The protocols are complete, i.e.,* $Z_i = \tilde{Z}_i,\ i = 1, 2$ *and* $Z_{ij} = \tilde{Z}_{ij},\ i = 1, 2, j = 1, 2.$

Proof. To prove that Protocol I is complete, we need to prove that $Z_i = \tilde{Z}_i,\ i = 1, 2.$

$$\begin{aligned} Z_i &= p_i(D_i) \otimes Y \otimes p_i'(D_i),\ i = 1, 2 \\ &= p_i(D_i) \otimes (q(B) \otimes g(A) \otimes q'(B)) \otimes p_i'(D_i) \\ &= (p_i(D_i) \otimes q(B)) \otimes g(A) \otimes (q'(B) \otimes p_i'(D_i)) \\ &= (q(B) \otimes p_i(D_i)) \otimes g(A) \otimes (p_i'(D_i) \otimes q'(B)) \\ &= q(B) \otimes (p_i(D_i) \otimes g(A) \otimes p_i'(D_i)) \otimes q'(B) \\ &= q(B) \otimes X_i \otimes q'(B) \\ &= \tilde{Z}_i,\ i = 1, 2. \end{aligned}$$

To prove that Protocol II is complete, we need to prove that $Z_{ij} = \tilde{Z}_{ij},\ i = 1, 2, j = 1, 2.$

$$\begin{aligned} Z_{ij} &= p_i(D_i) \otimes Y_j \otimes p_i'(D_i),\ i = 1, 2, j = 1, 2 \\ &= p_i(D_i) \otimes (q_j(B_j) \otimes g(A) \otimes q_j'(B_j)) \otimes p_i'(D_i) \\ &= (p_i(D_i) \otimes q_j(B_j)) \otimes g(A) \otimes (q_j'(B_j) \otimes p_i'(D_i)) \\ &= q_j(B_j) \otimes p_i(D_i) \otimes g(A) \otimes p_i'(D_i) \otimes q_j'(B_j) \\ &= q_j(B_j) \otimes (p_i(D_i) \otimes g(A) \otimes p_i'(D_i)) \otimes q_j'(B_j) \\ &= q_j(B_j) \otimes X_i \otimes q_j'(B_j) \\ &= \tilde{Z_{ij}},\ i = 1, 2, j = 1, 2. \ \square \end{aligned}$$

6.2. Security Analysis

6.2.1. Linear Algebra Attack

In linear algebra attack, an adversary uses the algebraic properties to discover the secret key. Since we have considered tropical algebra as a platform for our protocol, to find exactly the secret matrices by this attack is not likely.

For the first protocol, to find the key Z_i from X_i, one needs to know $p_i(D_i),\ i = 1, 2,$ or to find the key from Y, one needs to know $q(B)$.

Similarly, for the protocol II, to find the key Z_{ij} from X_i, one needs to know $p_i(D_i),\ i = 1, 2$ or to find the key from Y_j, one needs to know $q_j(B_j),\ j = 1, 2.$

Since tropical addition and multiplication of matrices are not invertible, this attack is not possible.

6.2.2. Brute-Force Attack

In this attack, an adversary uses every possible matrix to obtain the secret matrices from $X_i, i = 1, 2$ and $g(A)$. As we have considered $R = M_n(\mathbb{R}_{min})$, an infinite number of possible matrices are at hand, it becomes hard to get the desired matrix by this attack for adequate size of the matrix. Also, the brute force complexity for finite R is discussed in section 3.3. Thus this attack is not feasible.

6.2.3. Kotov-Ushakov Attack

In [19], the authors expressed that tropical power of matrices exhibit a specific pattern. This attack is not possible, since in both the protocols powers of unknown matrices $D_i,\ i = 1, 2$ and $B, B_j,\ j = 1, 2$ are used to generate the keys Z_i and $Z_{ij},\ i = 1, 2, j = 1, 2$.

6.2.4. Rudy-Monico Attack

This attack lies on the strength of finding the power of a known tropical matrix [20]. Since we have used powers of unknown matrices $D_i,\ i = 1, 2$ and $B, B_j,\ j = 1, 2$ in our protocols, this attack is not achievable.

6.3. Complexity Analysis

We bestow the number of bit operations required for the generation of the secret keys:

For the first protocol,

- The number of bit operations required to tropical multiply two $n \times n$ matrices is $O(n^3)$.
- The number of bit operations required to tropical multiply a diagonal matrix and usual non-diagonal matrix is $O(n^2)$.
- To find $X_i,\ i = 1, 2$ the number of bit operations required is $n^2 + n^2$, which is proportional to $O(n^2)$.
- To find Y, the number of bit operations required is $n^2 + n^2$, which is proportional to $O(n^2)$.

Hence to find the secret keys $Z_i,\ i = 1, 2$, the number of bit operations required is $O(n^2)$.

Similarly, for the protocol II, the number of bit operations required to find the secret keys $Z_{ij},\ i = 1, 2, j = 1, 2$ is $O(n^2)$.

Table 3: Comparative Analysis I

Aspect	**Braid Group,** B_n	**Tropical Matrix Algebra**
Algebraic Structure	Group	Semiring
Commutativity	Non-commutative	Non-commutative
Generators	$\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$	$M_n(\mathbb{R}_{min})$ is not finitely generated
Operations	Composition of braids	Tropical addition (min/max), Tropical multiplication (addition)
Accessibility	It isn't widely accessible since braid groups require deeper understanding of group theory	It is widely accessible since tropical algebra relies on basic arithmetic.

Table 4: Comparative Analysis II

Aspect	**Chen et al. [10]**	**Our Protocol**
Algebraic Structure	Braid Group	Tropical Matrix Algebra
Base Problem	TCSP	TCSP
Time Complexity	For Braid Concatenation, $O(n)$, and for Braid Simplification, $O(n^2)$	$O(n^2)$

6.4. Comparative Analysis

In this section, we have compared our chosen platform, tropical algebra, with another algebraic structure, i.e., a Braid group.

While the braid group holds significant theoretical value and serves specialized applications, it remains conceptually and computationally complex, with relatively limited practical accessibility. Tropical algebra, on the other hand, are quite computationally and conceptually approachable, making them easily implementable and widely usable in everyday applications.

Therefore, in terms of practical utility and accessibility, tropical algebra offer a clear advantage, whereas braid groups are better suited to specialized, niche domains.

7. Conclusion

The permanent increase in computational power requires us to search for new platforms for existing protocols. Tropical algebra seems to be an ideal candidate. In this article, we have delved into the intriguing realm of the Twin Conjugacy Search Problem by employing the innovative framework of Tropical Algebra. The security and complexity of the TCSP over tropical algebra have been explored. We showed that our our key exchange protocols based on the TCSP over tropical algebra are secure against Linear Algebra, Kotov-Ushakov, Rudy-Monico and Brute - Force Attack. The complexity of the protocols along with a comparative analysis have also been described.

Acknowledgements

We sincerely appreciate the editors and anonymous reviewers for their insightful suggestions, which greatly enhanced the quality of this paper.

Funding

This research Supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF- RS-2023-00237287, NRF-2021S1A5A8062526) and local government-university cooperation-based regional innovation projects (2021RIS-003).

Declaration of competing interest: The author confirms the absence of any known financial conflicts of interest or personal relationships that might have influenced the work presented in this paper.

Author's Contribution: All authors made equal contributions to the manuscript, participated in its drafting and revision, and approved the final version.

References

[1] W Diffie and M Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, Nov 1976.

[2] T Elgamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, Jul 1985.

[3] Digital signature standard (dss). *National Institute of Standards and Technology (U.S.)*, 1994.

[4] Any Muanalifah and Sergeĭ Sergeev. On the tropical discrete logarithm problem and security of a protocol based on tropical semidirect product. *Communications in Algebra*, 50(2):861–879, 2022.

[5] Neha Goel, Indivar Gupta, M. K. Dubey, and B. K. Dass. Undeniable signature scheme based over group ring. *Applicable Algebra in Engineering, Communication and Computing*, 27(6):523–535, Dec 2016.

[6] Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju sung Kang, and Choonsik Park. New public-key cryptosystem using braid groups. *Lecture Notes in Computer Science*, pages 166–183, 2000.

[7] Volker Gebhardt and Juan González-Meneses. Solving the conjugacy problem in garside groups by cyclic sliding. *Journal of Symbolic Computation*, 45(6):629–656, Jun 2010.

[8] Dima Grigoriev and Vladimir Shpilrain. Authentication from matrix conjugation. *Groups – Complexity – Cryptology*, 1(2), Jan 2009.

[9] Simran Tinani, Carlo Matteotti, and Joachim Rosenthal. Solutions to the conjugacy search problem in various platform groups. *AWM Research Symposium*, 2022.

[10] Xiaoming Chen, Weiqing You, and Li Wenxi. The twin conjugacy search problem and applications, Jun 2018.

[11] V. Muthukumaran, M. Adhiyaman, and D. Ezhilmaran. A secure and enhanced public key cryptosystem using double conjugacy search problem near-ring. *Advances in Mathematics: Scientific Journal*, 9(3):1389–1395, Jul 2020.

[12] Illia Itenberg, Grigory Mikhalkin, and Eugenii Shustin. *Tropical Algebraic Geometry*. Birkhäuser Basel, 2009.

[13] Diane Maclagan and Bernd Sturmfels. Introduction to tropical geometry. *Graduate Studies in Mathematics*, Apr 2015.

[14] Sara Kališnik and Davorin Lešnik. Symmetric polynomials in tropical algebra semirings. *Journal of Symbolic Computation*, 93:100–119, Jul 2019.

[15] Dima Grigoriev and Vladimir Shpilrain. Tropical cryptography. *Communications in Algebra*, 42(6):2624–2632, Jun 2014.

[16] Huawei Huang and Chunhua Li. Tropical cryptography based on multiple exponentiation problem of matrices. *Security and Communication Networks*, 2022:1–9, Sep 2022.

[17] Mariana Ivanova Durcheva. Tres: Tropical encryption scheme based on double key exchange. *European Journal of Information Technologies and Computer Science*, 2(4):11–17, Aug 2022.

[18] Sulaiman Alhussaini, Craig Collett, and Sergeĭ Sergeev. On the tropical two-sided discrete logarithm and a key exchange protocol based on the tropical algebra of pairs. *Communications in Algebra*, 52(10):4115–4134, 2024.

[19] Matvei Kotov and Alexander Ushakov. Analysis of a key exchange protocol based on tropical matrix algebra. *Journal of Mathematical Cryptology*, 12(3):137–141, Sep 2018.

[20] Dylan Rudy and Chris Monico. Remarks on a tropical key exchange system. *Journal of Mathematical Cryptology*, 15(1):280–283, Dec 2020.