



Asymmetric Cryptography Based on the Tropical Jones Matrix

Huawei Huang ^{*}, Weisha Kong  and Ting Xu 

School of Mathematical Sciences, Guizhou Normal University, Guiyang 550025, China; 222100060199@gznu.edu.cn (W.K.); 222100060215@gznu.edu.cn (T.X.)

^{*} Correspondence: 201307045@gznu.edu.cn

Abstract: In recent years, the tropical polynomial factorization problem, the tropical matrix decomposition problem, and the tropical multivariate quadratic equation solving problem have been proved to be NP-hard. Some asymmetric cryptographic systems based on tropical semirings have been proposed, but most of them are insecure and have been successfully attacked. In this paper, a new key exchange protocol and a new encryption protocol are proposed based on the difficulty of finding the multiple exponentiation problem of the tropical Jones matrices. The analysis results indicate that our protocol can resist various existing attacks. The complexity of attacking an MEP by adversaries is raised due to the larger number of combinations in the tropical Jones matrices compared to regular matrix polynomials. Furthermore, the index semiring is the non-negative integer cyclic matrix semiring, leading to a higher efficiency in key generation.

Keywords: tropical algebra; Jones matrix; cryptography; key exchange protocol

1. Introduction

Asymmetric cryptography plays a crucial role in the modern fields of communication and information security, offering reliable solutions for safeguarding the confidentiality, integrity, and authentication of data. Widely applied in areas such as internet transmission, digital signatures, and virtual private networks (VPNs), it provides users with a secure and dependable means of communication.

Asymmetric cryptography was first presented by Diffie and Hellman in 1976. Cryptographers have designed several representative public key cryptosystems. The security of these cryptographic systems relies on the difficulty associated with solving certain conventional mathematical challenges, including the integer factorization problem (IFP) [1], the knapsack problem (KP) [2], the discrete logarithm problem (DLP) [3,4], and the shortest vector problem in lattice [5]. The IFP and DLP are also two computational problems that public key cryptography mainly relies on. However, it is possible to solve the two problems in polynomial time using the quantum algorithm [6] that Shor proposed. Therefore, future cryptographic systems need to resist quantum attack, and developing new cryptographic systems is currently a hot topic in cryptography research.

Tropical algebra is derived from the tropical set theory proposed by the scientist Imre Simon [7,8]. In tropical algebra, tropical addition involves taking the minimum or maximum value of two numbers, and tropical multiplication is the common addition. Later, some cryptography researchers combined tropical algebra with the concept of semirings and defined the algebraic structure of tropical semirings. In 2005, Kim and Roush [9] proved that if the coefficients are finite, or all the coefficients are 0 or infinity (the Boolean case), then the univariate polynomial factorization problem of tropical semirings is usually NP-complete. In 2014, Shitov [10] studied the tropical matrix factorization (MF) problem and proved that the k-MF problem is NP-hard when $k \geq 7$. (The k-MF problem is as follows: given a $m \times n$ matrix A on \mathbb{R}_{\min} , find a $m \times k$ matrix B and a $k \times n$ matrix C , such that $BC = A$).



Citation: Huang, H.; Kong, W.; Xu, T. Asymmetric Cryptography Based on the Tropical Jones Matrix. *Symmetry* **2024**, *16*, 456. <https://doi.org/10.3390/sym16040456>

Academic Editor: Jiale Zhang

Received: 13 March 2024

Revised: 3 April 2024

Accepted: 6 April 2024

Published: 9 April 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Since tropical addition involves taking the minimum or maximum value of two numbers, tropical multiplication is the common addition and the calculations in the tropical semiring are more efficient than the classical ring. Recently, many people have attempted to propose some key exchange protocols based on tropical matrix algebra that are not only efficient but also secure, but they have been successfully attacked. By imitating some famous “classical” schemes previously proposed, Grigoriev and Shpilrain initially proposed a key exchange protocol based on tropical semirings [11] in 2014. In this article, Grigoriev and Shpilrain reduced the 3-SAT problem to a system of multivariate quadratic polynomial equations (MQPs) of tropical semirings and proved that the MQP of tropical semirings is NP-hard. However, when the range of tropical matrix elements contains negative numbers, it is found that each term of the tropical matrix will soon become negative and will become smaller as the number of powers increases. According to this rule, Kotov and Ushakov [12] developed corresponding effective attack schemes. In response to this heuristic attack proposed by Kotov and Ushakov, Grigoriev and Shpilrain proposed a new improvement to the key exchange protocol. In 2019, they proposed a key exchange protocol [13] based on the semidirect product of tropical matrices. However, this scheme was successfully broken by Rudy and Monico [14] using a simple binary search. In addition, Isaac and Kahrobaei [15] and Muanalifah and Sergeev [16] have also successfully attacked the schemes. To remedy the Grigoriev–Shpilrain’s protocol, Muanalifah and Sergeev proposed the use of two classes of exchange matrices (the Jones matrix and the LP matrix) from tropical algebra [17] and utilized the bilateral action of the matrices to propose three key exchange protocols [18]. However, in this article, the user’s secret matrix may still be represented in the linear form of the powers of the fundamental elementary matrix. Hence, its modifications are not resistant to the generalized KU attack. In 2022, Huang and Li proposed a new key exchange protocol [19] based on the multiple exponentiation problem of matrices, using tropical algebra as a platform and the adjoint matrix of the first polynomial. The analysis results showed that the protocol can resist all known attacks. Durcheva [20] proposed a public key encryption scheme based on the circulant matrix product problem and the two-sided action problem of matrix polynomials in 2022. Jiang et al. [21] cracked the scheme through tropical linear equations. Ahmed et al. [22] summarizes and analyzes the previous tropical cryptography schemes. Other cryptographic schemes based on tropical algebra can be found in the references [23–25].

Our contribution: In this paper, we design a new class of key exchange protocol and asymmetric encryption protocol based on the tropical Jones matrix. The security of the designed key exchange protocol can be reduced to a specific type of semigroup action problem introduced by Maze in [17], which involves the difficulty of finding the multiple exponentiation of tropical matrices. The multiple exponentiation problem can be transformed into a constructive membership problem of a semigroup in polynomial time, and this problem is a provable hard problem in the quantum computing model [26]. In addition, this problem cannot be reduced to the DLP or the HSP (hidden subgroup problem) efficiently in most cases. So, our protocol has the property of anti-quantum computing. The greater amount of combinations of the tropical Jones matrices as opposed to standard matrix polynomials increases the difficulty of adversaries attacking the MEP. Through an analysis of the key exchange protocol, it is found that our protocol can also resist KU attack and other known attacks. Additionally, the index semiring is the non-negative integer cyclic matrix semiring, which increases key generation efficiency.

The remaining portions of this article are organized as follows. Section 2 contains some preliminary information on tropical semirings. Section 3 presents our protocols based on the tropical Jones matrix. In Section 4, we provide a straightforward example to illustrate this key exchange protocol. The efficiency of the proposed cryptographic protocol, possible attacks, and parameter selection are finally covered in Section 5. Finally, Section 6 summarizes this article.

2. Preliminaries

Note: We represent the set $\{1, 2, \dots, n\}$ and $\{1, 2, \dots, m\}$ as $[n]$ and $[m]$.

We first provide some essential information about tropical algebra. For more details, please refer to the monograph [27].

Definition 1 ([28] (Semiring)). *Let R be a nonempty set in which two binary operations are defined, where one is an addition operation and the other is a multiplication operation, if the operation meets the following criteria:*

- (1) *The set R forms a commutative monoid for “ $+$ ” and has an identity element denoted as 0 ;*
- (2) *The set R forms a monoid for “ \cdot ” and has an identity element denoted as 1 ;*
- (3) *$a \cdot (b + c) = a \cdot b + a \cdot c$; $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a \in R, b \in R, c \in R$;*
- (4) *$0 \cdot r = r \cdot 0 = 0$ for all $r \in R$;*
- (5) *$1 \neq 0$, then R is a semiring. If for any $a, b \in R$, satisfies $a \cdot b = b \cdot a$, then R is called a commutative semiring.*

Definition 2 ([29] (Tropical Semiring)). *The non-negative integer tropical commutative semiring is the set $\mathbb{T}_{\mathbb{Z}} = \mathbb{Z} \cup \{-\infty\}$ with two binary compositions \oplus and \otimes as follows:*

$$x \oplus y = \max(x, y), x \otimes y = x + y.$$

$-\infty$ and 0 satisfied the following equations:

$$x \oplus (-\infty) = x, x \otimes 0 = 0, \forall x \in \mathbb{Z}$$

The commutative semiring properties of with addition identity $-\infty$ and multiplication identity 0 are easily demonstrated.

This is an example:

$$9 \oplus 3 = 9, 7 \otimes 9 = 7 + 9 = 16$$

The set of all tropical polynomials over $\mathbb{T}_{\mathbb{Z}}$ can be defined where the unknown term is x , just like in the classical case. Let

$$\mathbb{T}_{\mathbb{Z}}[x] = \left\{ (a_n \otimes x^n) \oplus (a_{n-1} \otimes x^{n-1}) \oplus \dots \oplus (a_1 \otimes x) \oplus a_0 \mid a_i \in \mathbb{T}_{\mathbb{Z}}, n \geq 0 \right\}.$$

The \oplus and \otimes operations of tropical polynomials in $\mathbb{T}_{\mathbb{Z}}[x]$ are like the classical addition and multiplication, with each $+$ being replaced by \oplus and each \cdot being replaced by \otimes . Proving that $\mathbb{T}_{\mathbb{Z}}[x]$ is a commutative semiring under \oplus and \otimes is straightforward.

Definition 3 (Tropical Matrix). *Let $\mathbb{M}_k(\mathbb{T}_{\mathbb{Z}})$ be the set of all $k \times k$ matrices over $\mathbb{T}_{\mathbb{Z}}$. We define binary operations \oplus and \otimes on $\mathbb{M}_k(\mathbb{T}_{\mathbb{Z}})$:*

Record $A = [a_{ij}], B = [b_{ij}]$, then

$$A \oplus B = [a_{ij}] \oplus [b_{ij}] = [a_{ij} + b_{ij}],$$

$$A \otimes B = [a_{ij}] \otimes [b_{ij}] = [a_{i1} \otimes b_{1j} \oplus a_{i2} \otimes b_{2j} \oplus \dots \oplus a_{ik} \otimes b_{kj}].$$

So is a semiring and

$$O = \begin{bmatrix} -\infty & -\infty & \dots & -\infty \\ -\infty & -\infty & \dots & -\infty \\ \vdots & \vdots & \ddots & \vdots \\ -\infty & -\infty & \dots & -\infty \end{bmatrix}, I = \begin{bmatrix} 0 & -\infty & \dots & -\infty \\ -\infty & 0 & \dots & -\infty \\ \vdots & \vdots & \ddots & \vdots \\ -\infty & -\infty & \dots & 0 \end{bmatrix}$$

are the identity elements of $\mathbb{M}_k(\mathbb{T}_{\mathbb{Z}})$ under \oplus and \otimes respectively.

It is rare for tropical matrices to be reversible, unlike the classical situation. Only tropical matrices obtained by elementary row or column transformations of diagonal matrices can be reversed.

Similarly, we can define a tropical matrix polynomial as follows:

$$\mathbb{T}_{\mathbb{Z}}[N] = \left\{ (a_n \otimes N^n) \oplus (a_{n-1} \otimes N^{n-1}) \oplus \cdots \oplus (a_1 \otimes N) \oplus (a_0 \otimes I^0) \mid a_i \in \mathbb{T}_{\mathbb{Z}}, n \geq 0 \right\}$$

where $N \in \mathbb{M}_k(\mathbb{T}_{\mathbb{Z}})$, $N^n = N \otimes N \otimes \cdots \otimes N$ (n times). $\mathbb{T}_{\mathbb{Z}}[N]$ is a commutative subsemiring of $\mathbb{M}_k(\mathbb{T}_{\mathbb{Z}})$ with respect to tropical matrix addition and multiplication.

Definition 4 ([23] (Circulant Matrix)). *If matrix C is in the following form:*

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

it is called a circulant matrix, where the terms are c_1, c_2, \dots, c_n . The set of all non-negative integer circulant matrices is denoted as $C_n(\mathbb{Z}^+)$.

2.1. Jones Matrix

In this section, we describe a specific type of matrices that were considered by Jones [30], and, by extending the polynomial concept, we can derive the concept of quasi-polynomials for Jones matrices, which will be applied to the protocol in Section 3.

Definition 5 ([18] (Jones Matrix)). *Let $A = [a_{ij}]$ be an $n \times n$ tropical matrix that satisfies the following property:*

$$a_{ij} \otimes a_{jk} \leq a_{ik} \otimes a_{jj}, \forall i, j, k \in [n],$$

we call A a Jones matrix.

Definition 6 ([18] (Deformation)). *Let $A = [a_{ij}]$ be a Jones matrix and $\alpha \in \mathbb{R}$. The matrix $A^{(\alpha)} = (a_{ij}^{(\alpha)})$ defined by*

$$a_{ij}^{(\alpha)} = a_{ij} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)}, \forall i, j \in [n]$$

is called a deformation of A .

Next, we will describe two theorems for a Jones matrix.

Theorem 1 ([18]). *If A is a Jones matrix, then $A^{(\alpha)}$ is also a Jones matrix for any $\alpha \leq 1$.*

Theorem 2 ([18]). *Let $A \in \mathbb{M}_k(\mathbb{T}_{\mathbb{Z}})$ be a Jones matrix, then*

$$A^{(\alpha)} \otimes A^{(\beta)} = A^{(\beta)} \otimes A^{(\alpha)}$$

for any α and β , such that $0 \leq \alpha \leq 1$ and $0 \leq \beta \leq 1$.

According to the above theorems, we define a quasi-polynomial and replace a monomial with a deformation.

Definition 7 ([18] (Quasi-polynomial)). Let $A \in \mathbb{M}_k(\mathbb{T}_{\mathbb{Z}})$ be a Jones matrix. Matrix B is termed a quasi-polynomial of A if

$$B = \bigoplus_{\alpha \in \mathcal{R}} a_{\alpha} \otimes N^{(\alpha)}$$

for some finite subset \mathcal{R} of rational numbers in $[0, 1]$ and $a_{\alpha} \in \mathbb{T}_{\mathbb{Z}}$ for $\alpha \in \mathcal{R}$. The set composed of all quasi-polynomials of N is denoted as $\mathbb{T}_{\mathbb{Z}}[N^{(\alpha)}]$.

2.2. A New Semigroup Action

Let A be a non-negative integer circulant matrix, $N \in \mathbb{M}_k(\mathbb{T}_{\mathbb{Z}})$ be a Jones matrix, and $\vec{H} = (H_1, H_2, \dots, H_n) \in \left(\mathbb{T}_{\mathbb{Z}}[N^{(\alpha)}]\right)^n$. Now consider the action of the multiplicative semigroup $C_n(\mathbb{Z}^+)$ on the Cartesian product $\left(\mathbb{T}_{\mathbb{Z}}[N^{(\alpha)}]\right)^n$, as shown below:

$$\vec{H}^A = (H_1^A, H_2^A, \dots, H_n^A) = \left(\bigotimes_{i=1}^n H_i^{a_{1i}}, \bigotimes_{i=1}^n H_i^{a_{2i}}, \dots, \bigotimes_{i=1}^n H_i^{a_{ni}} \right),$$

where $H_i^{a_{ji}} = H_i \otimes H_i \otimes \dots \otimes H_i$ (a_{ji} times). It can be easily proven that \vec{H}^A is a semigroup action of $C_n(\mathbb{Z}^+)$ on $\left(\mathbb{T}_{\mathbb{Z}}[N^{(\alpha)}]\right)^n$.

2.3. Multiple Exponentiation Problem of Tropical Matrices

According to Reference [19], we can give the definition of the ME problem of the tropical Jones matrix.

Definition 8 (ME problem). Let $C \in C_n(\mathbb{Z}^+)$, $N \in \mathbb{M}_k(\mathbb{T}_{\mathbb{Z}})$ be a Jones matrix, and $\vec{H} = (H_1, H_2, \dots, H_n) \in \left(\mathbb{T}_{\mathbb{Z}}[N^{(\alpha)}]\right)^n$, and assuming $\vec{U} = \vec{H}^A$, where $A \in C_n(\mathbb{Z}^+)$. The multiple exponentiation problem of tropical matrices is to find a matrix $A \in C_n(\mathbb{Z}^+)$ satisfying the above equation for given C, \vec{H} and \vec{U} . (Remember that N is unknown.) We refer to the issue as the “ME problem” for simplicity’s sake.

Many results in traditional algebra are known to be invalid in tropical algebra. Consequently, certain properties of ordinary matrices, such as Cayley–Hamilton theorem, eigenvalues, and determinant, do not apply. But if H_i ($i \in [n]$) satisfies certain conditions, we can simplify the problem to the DLP.

Proposition 1 ([18]). If a component H_i of \vec{H} exists such that

$$(\forall j \neq i) H_j \in \langle H_i \rangle (i, j \in [n]),$$

then the ME problem can be simplified to the DLP in polynomial time.

3. Key Exchange Protocol and Encryption Protocol Based on the Jones Matrix

This section presents a key exchange protocol that is similar to the Diffie–Hellman protocol. It is based on the multiple exponentiation problem of tropical matrices and a public key encryption protocol such as the ElGamal encryption protocol.

3.1. A New Key Exchange Protocol

Let $\vec{H} = (H_1, H_2, \dots, H_n) \in \left(\mathbb{T}_{\mathbb{Z}}[N^{(\alpha)}]\right)^n$ be such that no component H_i of \vec{H} exists such that $(\forall j \neq i) H_j \in \langle H_i \rangle$ ($i, j = 0, 1, 2, \dots, n - 1$). The protocol’s public parameters are \vec{H} . Protocol A

- (1) Alice randomly selects a circulant matrix $A \in C_n(\mathbb{Z}^+)$, calculates $\vec{U} = \vec{H}^A$, and sends \vec{U} to Bob;
- (2) Bob randomly selects a circulant matrix $B \in C_n(\mathbb{Z}^+)$, calculates $\vec{V} = \vec{H}^B$, and sends \vec{V} to Alice;
- (3) Alice calculates

$$K_{Alice} = \vec{V}^{\vec{A}} = \left(\vec{H}^B \right)^A = \vec{H}^{B \cdot A};$$

- (4) Bob calculates

$$K_{Bob} = \vec{U}^{\vec{B}} = \left(\vec{H}^A \right)^B = \vec{H}^{A \cdot B}.$$

Note that “ \cdot ” is the matrix multiplication in $C_n(\mathbb{Z}^+)$.

Given that $C_n(\mathbb{Z}^+)$ is commutative, we obtain $A \cdot B = B \cdot A$ and $K_{Alice} = K_{Bob}$. Thus, Bob and Alice have a shared secret key.

3.2. A Common Key Encryption Protocol Based on the Jones Matrix

Protocol B

- (1) Key Generation

Let $\vec{H} = (H_1, H_2, \dots, H_n) \in \left(\mathbb{T}_{\mathbb{Z}}[N^{(\alpha)}] \right)^n$. No component H_i of \vec{H} exists such that $(\forall j \neq i) H_j \in \langle H_i \rangle (i, j = 0, 1, 2, \dots, n-1)$. The protocol's public parameters are \vec{H} . The key generation center randomly chooses a circulant matrix A in $C_n(\mathbb{Z}^+)$, and computes

$$\vec{U} = \vec{H}^A.$$

Alice's public key is shown as \vec{U} . Alice's secret key is A .

- (2) Encryption

Bob needs to do the following calculation to send the plaintext message $\vec{M} \in (\mathbb{M}_k[\mathbb{T}_{\mathbb{Z}}])^n$ to Alice.

- ① Bob randomly selects a circulant matrix $B \in C_n(\mathbb{Z}^+)$, then computes $\vec{V} = \vec{H}^B$, and takes it as the first part of the ciphertext.
- ② Bob calculates $\vec{Q} = \vec{M} + \vec{U}^{\vec{B}}$ as the final component of the ciphertext. Note that the “+” here is an ordinary matrix addition operation.
- ③ Bob sends ciphertext (\vec{V}, \vec{Q}) just calculated to Alice.

- (3) Decryption

After receiving the ciphertext (\vec{V}, \vec{Q}) sent by Bob, Alice decrypts it with her private key.

- ① Alice first computes $\vec{W} = \vec{V}^{\vec{A}}$.
- ② Alice then computes $\vec{Q} - \vec{W}$ to get the original plaintext message. Note that “−” here is an ordinary matrix subtraction operation.

Verification:

$$\begin{aligned}\vec{Q} - \vec{W} &= \vec{M} + \vec{U} - \vec{V} \\ &= \vec{M} + \left(\vec{H}^{\rightarrow A}\right)^B - \left(\vec{H}^{\rightarrow B}\right)^A \\ &= \vec{M} + \vec{H}^{\rightarrow A \cdot B} - \vec{H}^{\rightarrow B \cdot A} \\ &= \vec{M}\end{aligned}$$

4. A Toy Example

To help readers comprehend the above key exchange protocol, we have included a basic example in this section.

Alice and Bob both choose a Jones matrix $N = \begin{bmatrix} 6 & 5 & 6 \\ 6 & 16 & 12 \\ 5 & 9 & 12 \end{bmatrix}$ and $\vec{H} = \left(N^{\left(\frac{1}{2}\right)}, N^{\left(\frac{1}{3}\right)}, N^{\left(\frac{1}{4}\right)}\right)$,

i.e.,

$$\vec{H} = \left(\begin{bmatrix} 3 & -3 & 0 \\ -2 & 8 & 4 \\ -1 & 1 & 6 \end{bmatrix}, \begin{bmatrix} 2 & -\frac{17}{3} & -2 \\ -\frac{14}{3} & \frac{16}{3} & \frac{4}{3} \\ -3 & -\frac{5}{3} & 4 \end{bmatrix}, \begin{bmatrix} \frac{3}{2} & -7 & -3 \\ -6 & 4 & 0 \\ -4 & -3 & 3 \end{bmatrix} \right).$$

Alice's private key is $A = \begin{bmatrix} 2 & 3 & 4 \\ 4 & 2 & 3 \\ 3 & 4 & 2 \end{bmatrix} \in C_n(\mathbb{Z}^+)$, she computes

$$\vec{U} = \vec{H}^{\rightarrow A} = \left(\begin{bmatrix} 27 & 37 & 33 \\ 38 & 48 & 44 \\ 31 & 41 & 37 \end{bmatrix}, \begin{bmatrix} \frac{101}{3} & \frac{131}{3} & \frac{119}{3} \\ \frac{134}{3} & \frac{164}{3} & \frac{152}{3} \\ \frac{113}{3} & \frac{143}{3} & \frac{131}{3} \end{bmatrix}, \begin{bmatrix} \frac{97}{3} & \frac{127}{3} & \frac{115}{3} \\ \frac{130}{3} & \frac{160}{3} & \frac{148}{3} \\ \frac{109}{3} & \frac{139}{3} & \frac{127}{3} \end{bmatrix} \right),$$

then sends \vec{U} to Bob.

Bob's private key is $B = \begin{bmatrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{bmatrix} \in C_n(\mathbb{Z}^+)$. He computes

$$\vec{V} = \vec{H}^{\rightarrow B} = \left(\begin{bmatrix} \frac{11}{2} & \frac{11}{3} & 5 \\ \frac{14}{3} & \frac{44}{3} & \frac{32}{3} \\ 4 & \frac{23}{3} & 11 \end{bmatrix}, \begin{bmatrix} 6 & 5 & 6 \\ 6 & 16 & 12 \\ 5 & 9 & 12 \end{bmatrix}, \begin{bmatrix} 8 & \frac{31}{3} & 10 \\ \frac{34}{3} & \frac{64}{3} & \frac{52}{3} \\ 9 & \frac{43}{3} & 16 \end{bmatrix} \right),$$

then sends \vec{V} to Alice.

Alice calculates

$$K_{Alice} = \left(\begin{bmatrix} \frac{425}{3} & \frac{455}{3} & \frac{443}{3} \\ \frac{458}{3} & \frac{488}{3} & \frac{476}{3} \\ \frac{437}{3} & \frac{467}{3} & \frac{455}{3} \end{bmatrix}, \begin{bmatrix} \frac{401}{3} & \frac{431}{3} & \frac{419}{3} \\ \frac{434}{3} & \frac{464}{3} & \frac{452}{3} \\ \frac{413}{3} & \frac{443}{3} & \frac{431}{3} \end{bmatrix}, \begin{bmatrix} \frac{389}{3} & \frac{419}{3} & \frac{407}{3} \\ \frac{422}{3} & \frac{452}{3} & \frac{440}{3} \\ \frac{401}{3} & \frac{431}{3} & \frac{419}{3} \end{bmatrix} \right).$$

And Bob calculates

$$K_{Bob} = \left(\begin{bmatrix} \frac{425}{3} & \frac{455}{3} & \frac{443}{3} \\ \frac{458}{3} & \frac{488}{3} & \frac{476}{3} \\ \frac{437}{3} & \frac{467}{3} & \frac{455}{3} \end{bmatrix}, \begin{bmatrix} \frac{401}{3} & \frac{431}{3} & \frac{419}{3} \\ \frac{434}{3} & \frac{464}{3} & \frac{452}{3} \\ \frac{413}{3} & \frac{443}{3} & \frac{431}{3} \end{bmatrix}, \begin{bmatrix} \frac{389}{3} & \frac{419}{3} & \frac{407}{3} \\ \frac{422}{3} & \frac{452}{3} & \frac{440}{3} \\ \frac{401}{3} & \frac{431}{3} & \frac{419}{3} \end{bmatrix} \right),$$

where $K_{Alice} = K_{Bob}$. Therefore, Alice and Bob share the key.

5. Security Analysis and Parameter Selection

In this section, we analyze the security of the proposed key exchange protocol. The analysis shows that our protocol can resist all known attacks and has the property of anti-quantum computing. First, we prove that Protocol B is semantically secure.

Definition 9 ([19]). Suppose $\vec{U} = A * \vec{H}$ and $\vec{V} = B * \vec{H}$, where $A, B \in C_n(\mathbb{Z}^+)$. Let $R \in (\mathbb{T}_{\mathbb{Z}}[N^{(\alpha)}])^n$. The decisional ME problem is to decide whether $\vec{R} = \vec{H}^{\vec{AB}}$, given $\vec{H}, \vec{U}, \vec{V}$, and \vec{R} . To simplify, we denote it as the “DME”.

Theorem 3. An algorithm capable of resolving the DME problem can effectively ascertain the legitimacy of ciphertexts within Protocol B. Conversely, an algorithm designed to determine the validity of ciphertexts within Protocol B can be harnessed to address the DME problem.

Proof. Let us initially assume that algorithm \mathcal{A}_1 possesses the capability to determine the correctness of a decryption within Protocol B. When given the inputs $\vec{H}, \vec{U}, (\vec{V}, \vec{Q})$, and \vec{M} , the algorithm \mathcal{A}_1 outputs “yes” if \vec{M} is the decryption of (\vec{V}, \vec{Q}) and outputs “no” otherwise. Given the input $\vec{H}, \vec{U}, (\vec{V}, \vec{Q})$, and \vec{M} , the algorithm \mathcal{A}_1 outputs “yes” if \vec{M} is the decryption of (\vec{V}, \vec{Q}) and “no” otherwise. Now, we use \mathcal{A}_1 to solve the DME problem. Suppose we are given $\vec{H}, \vec{U}(= \vec{H}^{\vec{A}}), \vec{V}(= \vec{H}^{\vec{B}})$, and \vec{R} , and our aim is to determine whether $\vec{R} = \vec{H}^{\vec{AB}}$. Let $\vec{Q} = \vec{R}$ and $\vec{M} = (0_k, \dots, 0_k)$, where 0_k is the $k \times k$ zero matrix of $M_k(\mathbb{Z})$. Input all of these parameters into \mathcal{A}_1 . Note that A is now the secret key. The decryption of (\vec{V}, \vec{Q}) is

$$\vec{Q} - \vec{V}^{\vec{A}} = \vec{R} - (\vec{H}^{\vec{B}})^{\vec{A}} = \vec{R} - \vec{H}^{\vec{AB}}.$$

Consequently, \mathcal{A}_1 outputs “yes” precisely when $\vec{M} = (0_k, \dots, 0_k)$ equals $\vec{R} - \vec{H}^{\vec{AB}}$, specifically when $\vec{R} = \vec{H}^{\vec{AB}}$. This resolution effectively addresses the decision DME problem.

On the contrary, let us assume an algorithm \mathcal{A}_2 can effectively tackle the DME problem. This implies that if provided with inputs $\vec{H}, \vec{U}(= \vec{H}^{\vec{A}}), \vec{V}(= \vec{H}^{\vec{B}})$, and \vec{R} , the algorithm \mathcal{A}_2 produces “yes” if $\vec{R} = \vec{H}^{\vec{AB}}$ and “no” otherwise. Let it be the claimed decryption of the ciphertext. Consider \vec{M} as the asserted decryption of the ciphertext (\vec{V}, \vec{Q}) . Input $\vec{Q} - \vec{M}$ as \vec{R} . It is worth noting that \vec{M} represents the accurate plaintext for the ciphertext (\vec{V}, \vec{Q}) only if $\vec{M} = \vec{Q} - \vec{V}^{\vec{A}} = \vec{Q} - \vec{H}^{\vec{AB}}$, which occurs if and only if $\vec{Q} - \vec{M} = \vec{H}^{\vec{AB}}$. Hence, \vec{M} is the accurate plaintext if and only if $\vec{R} = \vec{H}^{\vec{AB}}$. Therefore, given these inputs, \mathcal{A}_2 yields “yes” precisely when \vec{M} is the accurate plaintext.

The Theorem is proved. \square

5.1. Possible Attacks

- (1) Brute-force attack. Assuming $A \in C_n(\mathbb{Z}^+)$ is a circulant matrix with terms $a_0, a_1, \dots, a_{n-1} \in [0, s-1]$. The attacker clearly has s^n options from which to select A , so the parameters s and n must satisfy $s^n \geq 2^{80}$.
- (2) Tropical matrix decomposition attack. Tropical matrix decomposition attack involves a search for a circulant matrix A' such that $\vec{H}^{\vec{A}'} = \vec{U}$ and $A'C = CA'$, then the attacker can find the shared key. However, the attacker needs to factor \vec{U} into the form of $G_1 G_2 \dots G_n$, where $G_i \in \langle H_j \rangle, n \geq 2$ is NP-hard, so the tropical matrix decomposition attack is not effective.

- (3) KU attack. Since the Jones matrix is unknown, if we want to find N , the system of equations needs to be solved as follows:

$$\begin{cases} \bigoplus_{\alpha_1 \in \mathcal{R}} a_{\alpha_1} \otimes N^{(\alpha_1)} = H_1 \\ \bigoplus_{\alpha_2 \in \mathcal{R}} a_{\alpha_2} \otimes N^{(\alpha_2)} = H_2 \\ \dots\dots\dots \\ \bigoplus_{\alpha_n \in \mathcal{R}} a_{\alpha_n} \otimes N^{(\alpha_n)} = H_n \end{cases}$$

Solving the above system of equations is NP-hard. Therefore, the KU attack is ineffective.

Assuming the attacker knows the matrix N , finding the private key A from the public key \vec{U} is what they must accomplish. KU attacks are limited to breaking down tropical matrices into their product, like $U = X \otimes Y$. In this protocol, the KU attack will not function if the \vec{H} component value is more than two. Therefore, we require that the components of \vec{H} be greater than or equal to three.

- (4) Generalized KU attack. Additionally, a common matrix can be broken down by the generalized KU attack into the linear equivalent of the tropical basic elementary matrix: the product of two Jones matrices. However, in our cryptosystems, if $n > 2$, then each component matrix of \vec{U} is the result of multiplying by more than two matrices. In this instance, our cryptosystems are likewise unaffected by the generalized KU attack.
- (5) RM attack. Grigoriev and Shpilrain designed another key exchange protocol based on the action of the semidirect product. However, in this key exchange protocol, the addition operation of the tropical matrix is used, and the addition of the tropical matrix has the property of idempotent, so the power of this part of the semidirect product is partially order-preserving. Rudy and Monico used this feature to create a straightforward binary search algorithm that allowed them to break the cryptosystem in [14]. There is no tropical matrix addition operation in \vec{H}^A in our cryptosystems. Thus, our cryptosystems can also resist this attack.
- (6) Quantum attack. Andrew et al. [26] proved that the constructive membership problem of the semigroup is a provable hard quantum computation model, and the lower bound of its quantum computation complexity is exponential. Since the ME problem can be transformed into a semigroup constructive member problem, our cryptosystems have the property of anti-quantum computing.

Table 1 provides the comparison of our protocols with other relevant schemes in terms of resisting various known attacks.

Table 1. Comparison among relevant tropical schemes.

Schemes	Mathematical Problems	KU Attack	RM Attack	G-KU Attack
Grigoriev [11]	Two-sided matrix action problem	×	✓	×
Grigoriev [13]	Semidirect product problem	✓	×	✓
Muanalifah [16]	Two-sided matrix action problem	✓	✓	×
Huang [19]	Multiple exponentiation problem	✓	✓	✓
Our protocols	Multiple exponentiation problem	✓	✓	✓

5.2. Parameter Selection and Efficiency

Nachtigall et al. defined a sequence of matrices to be almost linear periodic in [31]. In the following definition, if the matrix $H = [h_{ij}]$, then h_{ij}^p denotes the ij^{th} element of H^p .

Definition 10 ([31] (Almost linear periodic)). *If there is a period ρ , linear factor ξ , and some defect d such that the following equation applies for all indices i, j and all $p > d$, then a sequence of matrices $\{H^p, p \in \mathbb{N}\}$ is almost linearly periodic:*

$$h_{ij}^{p+\rho} = \xi + h_{ij}^p.$$

In [32], Beccelli et al. demonstrated that the higher powers sequence of tropical matrices is almost linear periodic. In our protocol, if the exponent p and period ρ of the Jones matrix N are small, there is a possibility of potential heuristic attacks. The exponent p of the tropical matrix increases with the increase of the order k of the matrix. We have shown through experiments that it is feasible to generate a Jones matrix N and H_i with an exponent exceeding k^2 and using this feature to attack does not work.

From Proposition 1, we know that if there exists a component H_i of \vec{H} such that $(\forall j \neq i)H_j \in \langle H_i \rangle (i, j \in [n])$, then the ME problem can be simplified to the DLP in polynomial time. To avoid this situation, \vec{H} must satisfy that there is no component H_i of \vec{H} such that $(\forall j \neq i)H_j \in \langle H_i \rangle (i, j \in [n])$.

In Protocol A and B, we recommend using the following parameters:

- (1) The order of the Jones matrix N is $k = 10$ and the element selection in $[0, 1000]$;
- (2) Because the deformation of the Jones matrix means that the terms of the matrix may contain fractions, we recommend $a_\alpha = 0$, where exponent α is selected rational numbers in $[0, 1]$;
- (3) Because the terms of the private key matrices A and B are exponents of $H_i (i \in [n])$, the terms of the circulant matrices A and B cannot be too large. Here, we recommend selecting their terms in $[0, 10]$.

Now, we analyze the computational efficiency of encryption Protocol B. The most time-consuming operations in the protocol are the matrix exponentiations $\vec{H}^{\rightarrow A}, \vec{H}^{\rightarrow B}, \vec{U}^{\rightarrow B}, \vec{V}^{\rightarrow B}$. (In the key generation process, \vec{H} is randomly generated, and the private key matrix A is randomly selected from cyclic matrices, compared to matrix exponentiation operations, so their time consumption can be neglected. In the encryption and decryption processes, the computation time for the ordinary matrix addition and subtraction is also typically very fast and can be neglected compared to matrix exponentiation.)

Table 2 compares the execution time of the operation $\vec{U} = \vec{H}^{\rightarrow A}$ with various parameters, and Table 3 compares the execution time of the key generation, encryption, and decryption processes under different parameters (research platform: AMD Ryzen 7 6800H with Radeon Graphics3.20 GHz).

Table 2. Performance comparison under some parameters.

k	n	s	Timing of $\vec{H}^{\rightarrow A}$ (s)
10	80	2	1.082
14	51	3	1.929
21	40	4	2.38
25	39	5	5.618
28	33	6	5.686

Table 3. Performance comparison of encryption under some parameters.

k	n	s	Timing of Key Generation (s)	Timing of Encryption (s)	Timing of Decryption (s)
10	80	2	1.085	2.052	1.506
14	51	3	1.933	3.38	2.804
21	40	4	2.383	4.787	4.256
25	39	5	5.623	9.33	8.775
28	33	6	5.692	9.546	9.089

Similar to the scheme in reference [19], our protocol is also built upon employing the tropical matrix multiple exponentiation problem. However, we employ the tropical Jones matrix MEP instead of the matrix polynomial MEP. Specifically, the base semiring we use is $\mathbb{T}_{\mathbb{Z}}[N^{(\alpha)}]$, not $\mathbb{T}_{\mathbb{Z}}[N]$. Under the same parameters, the quasi-polynomial set of Jones matrices is much larger than the general matrix polynomial set, greatly increasing the adversary's search space. Additionally, since our index semiring is $C_n(\mathbb{Z}^+)$ rather than $\mathbb{Z}^+(D)$ in the key generation process, we only need to randomly generate a cyclic matrix without calculating the matrix polynomials, which makes the key generation efficiency higher in our protocol. Table 4 compares our protocol with the protocol in reference [19].

Table 4. Comparison with the protocol in [19].

Protocol	Base Semiring	Index Semiring	Hard Problem
[19]	$\mathbb{T}_{\mathbb{Z}}[N]$	$\mathbb{Z}^+(D)$	Matrix polynomial MEP
This paper	$\mathbb{T}_{\mathbb{Z}}[N^{(\alpha)}]$	$C_n(\mathbb{Z}^+)$	Jones matrix MEP

6. Conclusions

In this paper, we propose a new key exchange protocol and a new public key encryption protocol by using the multiplication of the quasi-polynomial of the Jones matrix, which has the property of commutativity when $\alpha \in [0, 1]$. The security of the protocol is analyzed. Because the component of public key \vec{H} in our protocols is more than two, our protocols can resist a KU attack and a generalized KU attack. Furthermore, in our cryptosystem, the addition operation of the matrix is not involved, so our protocols can resist an RM attack. Since the ME problem can be transformed into a semigroup constructive member problem, our cryptosystems have the property of anti-quantum computing.

Author Contributions: Conceptualization, H.H. and W.K.; methodology, H.H.; software, W.K.; validation, H.H., W.K., and T.X.; writing—original draft preparation, W.K.; and writing—review and editing, W.K. and H.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the Science and Technology Foundation of Guizhou Province (QIANKEHEJICHU-ZK [2021] Ordinary313) and the National Natural Science Foundation of China (No. 61462016).

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

- Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [[CrossRef](#)]
- Rueppel, R.A. The knapsack as a nonlinear function. In *Analysis and Design of Stream Ciphers*; Springer: Berlin/Heidelberg, Germany, 1986; pp. 163–191.
- Diffie, W.; Hellman, M.E. New Directions in Cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654. [[CrossRef](#)]
- Gamal, T.E. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory* **1984**, *31*, 469–472.
- Cai, J.Y.; Cusick, T.W. A lattice-based public-key cryptosystem. In *Selected Areas in Cryptography, Proceedings of the 5th Annual International Workshop, SAC'98, Kingston, ON, Canada, 17–18 August 1998*; Springer: Berlin/Heidelberg, Germany, 1998.
- Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Rev.* **1999**, *41*, 303–332. [[CrossRef](#)]
- Simon, I. Recognizable sets with multiplicities in the tropical semiring. In *Mathematical Foundations of Computer Science 1988, Proceedings of the 13th Symposium Carlsbad, Czechoslovakia, 29 August–2 September 1988*; Springer: Berlin/Heidelberg, Germany, 1988; pp. 107–120.
- Simon, I. On semigroups of matrices over the tropical semiring. *RAIRO-Theor. Inform. Appl.* **1994**, *28*, 277–294. [[CrossRef](#)]
- Kim, K.H.; Roush, F.W. Factorization of polynomials in one variable over the tropical semiring. *arXiv* **2005**, arXiv:math/0501167.

10. Shitov, Y. The complexity of tropical matrix factorization. *Adv. Math.* **2014**, *254*, 138–156. [[CrossRef](#)]
11. Grigoriev, D.; Shpilrain, V. Tropical cryptography. *Commun. Algebra* **2014**, *42*, 2624–2632. [[CrossRef](#)]
12. Kotov, M.; Ushakov, A. Analysis of a key exchange protocol based on tropical matrix algebra. *J. Am. Coll. Surg.* **2018**, *207*, S56–S57. [[CrossRef](#)]
13. Grigoriev, D.; Shpilrain, V. Tropical cryptography II: Extensions by homomorphisms. *Commun. Algebra* **2019**, *47*, 4224–4229. [[CrossRef](#)]
14. Rudy, D.; Monico, C. Remarks on a Tropical Key Exchange System. *J. Math. Cryptol.* **2021**, *15*, 280–283. [[CrossRef](#)]
15. Isaac, S.; Kahrobaei, D. A Closer Look at the Tropical Cryptography. *Int. J. Comput. Math.: Comput. Syst. Theory* **2021**, *6*, 137–142. [[CrossRef](#)]
16. Muanalifah, A.; Sergeev, S. On the tropical discrete logarithm problem and security of a protocol based on tropical semidirect product. *arXiv* **2021**, arXiv:2101.02781. [[CrossRef](#)]
17. Maze, G.; Monico, C.; Rosenthal, J. A public key cryptosystem based on actions by semigroups. In Proceedings of the IEEE International Symposium on Information Theory, Lausanne, Switzerland, 30 June–5 July 2002.
18. Muanalifah, A.; Sergeev, S. Modifying the tropical version of Stickel’s key exchange protocol. *Appl. Math.* **2020**, *65*, 727–753. [[CrossRef](#)]
19. Huang, H.; Li, C. Tropical Cryptography Based on Multiple Exponentiation Problem of Matrices. *Secur. Commun. Netw.* **2022**, *2022*, 1–9. [[CrossRef](#)]
20. Durcheva, M.I. TrES: Tropical Encryption Scheme Based on Double Key Exchange. *Eur. J. Inf. Technol. Comput. Sci.* **2022**, *2*, 11–17. [[CrossRef](#)]
21. Jiang, X.; Huang, H.; Pan, G. Cryptanalysis of Tropical Encryption Scheme Based on Double Key Exchange. *J. Cyber Secur. Mobil.* **2023**, *12*, 205–220. [[CrossRef](#)]
22. Ahmed, K.; Pal, S.; Mohan, R. A review of the tropical approach in cryptography. *Cryptologia* **2023**, *47*, 63–87. [[CrossRef](#)]
23. Huang, H. Cryptosystems Based on Tropical Congruent Transformation of Symmetric Matrices. *Symmetry* **2022**, *14*, 2378. [[CrossRef](#)]
24. Amutha, B.; Perumal, R. Public key exchange protocols based on tropical lower circulant and anti-circulant matrices. *AIMS Math.* **2023**, *8*, 17307–17334. [[CrossRef](#)]
25. Mehmood, S. *Key Exchange Protocol Based on Matrices Using Tropical Algebra*; Capital University: Bexley, OH, USA, 2019.
26. Childs, A.M.; Ivanyos, G. Quantum computation of discrete logarithms in semigroups. *arXiv* **2013**, arXiv:1310.6238. [[CrossRef](#)]
27. Butkovic, P. *Max-Linear Systems: Theory and Algorithms*; Springer: London, UK, 2010.
28. Golan, J.S. *Semirings and Their Applications*; Springer Science & Business Media: Berlin, Germany, 1999; Chapter 21.
29. David, S.; Bernd, S. Tropical Mathematics. *Math. Mag.* **2009**, *82*, 163–173.
30. Jones, D. Special and Structured Matrices in Max-Plus Algebra. Ph.D. Thesis, University of Birmingham, Birmingham, UK, 2018.
31. Nachtigall, K. Powers of matrices over an extremal algebra with applications to periodic graphs. *Math. Methods Oper. Res.* **1997**, *40*, 87–102. [[CrossRef](#)]
32. Baccelli, F.; Cohen, G.; Olsder, G.J.; Quadrat, J.P. *Synchronization and Linearity: An Algebra for Discrete Event Systems*; John Wiley & Sons Ltd.: Hoboken, NJ, USA, 1994.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.