Research Article

Tropical Cryptography Based on Multiple Exponentiation Problem of Matrices

Huawei Huang and Chunhua Li

1School of Mathematical Sciences, Guizhou Normal University, Guiyang 550001, China
2School of Science, East China Jiaotong University, Nanchang 330013, China

Correspondence should be addressed to Huawei Huang; hwhuang7809@163.com

Received 1 September 2021; Revised 19 April 2022; Accepted 28 June 2022; Published 9 September 2022

Copyright © 2022 Huawei Huang and Chunhua Li. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Because there is no multiplication of numbers in tropical algebra and the problem of solving the systems of polynomial equations in tropical algebra is NP-hard, in recent years some public key cryptography based on tropical semiring has been proposed. But most of them have some defects. This paper proposes new public key cryptosystems based on tropical matrices. The security of the cryptosystem relies on the difficulty of the problem of finding multiple exponentiations of tropical matrices given the product of the matrices powers when the subsemiring is hidden. This problem is a generalization of the discrete logarithm problem. But the problem generally cannot be reduced to discrete logarithm problem or hidden subgroup problem in polynomial time. Since the generating matrix of the used commutative subsemirings is hidden and the public key matrices are the product of more than two unknown matrices, the cryptosystems can resist KU attack and other known attacks. The cryptosystems based on multiple exponentiation problem can be considered as a potential postquantum cryptosystem.

1. Introduction

Contemporary public key cryptography relies mainly on two computational problems, integer factorization problem, and discrete logarithm problem. For example, Diffie–Hellman key exchange protocol and ElGamal encryption scheme are based on discrete logarithm problem [1, 2]. Shor proposed a quantum algorithm which can solve integer factorization problem and discrete logarithm problem in polynomial time on a quantum computer [3]. So, it is a research focus of cryptography to develop other new cryptosystems. The traditional cryptosystems are based on various commutative rings, such as finite field, residue class ring, and integer ring [4–8]. Many cryptologists hope to find other algebraic structures to build new public key cryptosystems.

In 2007, Maze, Monico, and Rosenthal proposed one of the first cryptosystems based on semigroups and semirings [9], using some ideas from [10], as well as from their previous article [11]. However, then it was broken by Steinwandt et al. [12]. Atani published a cryptosystem using semimodules over factor semirings [13]. Durcheva applied some idempotent semirings to construct cryptographic protocols [14]. A survey on semigroup action problem and its cryptographic applications was given by Goel, Gupta, and Dass [15].

Grigoriev and Shpilrain proved that the problem of solving the systems of min-plus polynomial equations in tropical algebra is NP-hard and suggested using a min-plus (tropical) semiring to design public key cryptosystem [16]. An obvious advantage of using tropical algebras as platforms is unparalleled efficiency because in tropical schemes, one does not have to perform any multiplications of numbers since tropical multiplication is the usual addition. But “tropical powers” of an element exhibit some patterns, even if such an element is a matrix over a tropical algebra. This weakness was exploited by Kotov and Ushakov to arrange a fairly successful attack on one of Grigoriev and Shpilrain’s schemes [17]. In 2019, Grigoriev and Shpilrain improved the original scheme and proposed the public key cryptosystems based on semi-direct product of tropical matrix semiring...
Our contribution: This paper provides a new public key cryptosystem based on tropical matrices. The security of the cryptosystem relies on the difficulty of the problem of finding multiple exponentiation of tropical matrices, which is a class of semigroup action problem proposed by Maze in [11]. The multiple exponentiation problem is also a generalization of the discrete logarithm problem. However, the problem generally cannot be reduced to discrete logarithm problem or hidden subgroup problem in polynomial time. Since the generating matrix of the used commutative sub-semirings is hidden and the public key matrices are the product of more than two unknown matrices, the cryptosystems can resist KU attack and other known attacks. It is seemed that our cryptosystems based on multiple exponentiation problem can be considered as a potential post-quantum cryptosystem.

The remainder of this paper is organized as follows. In Section 2, some preliminaries on tropical semiring are given. In Section 3, we define the multiple exponentiation problem of tropical matrices. In section 4, a key exchange protocol and a public key encryption scheme based on multiple exponentiation problem are presented. Finally, in Section 5 the possible attacks, parameter selection, and efficiency of the cryptosystems are discussed.

2. Preliminaries

Notation. In this paper, matrices are generally denoted by the capital letters. In order to facilitate future references, frequently used notations are listed below with their meanings.

\[ \mathcal{I}[x] = \{(a_n \otimes x^n) \oplus (a_{n-1} \otimes x^{n-1}) \oplus \ldots \oplus (a_1 \otimes x) \oplus a_0 | a_i \in \mathcal{I} \text{ and } n \geq 0 \}. \] (3)

The tropical polynomial operation and \( \oplus \) operation in \( \mathcal{I}[x] \) are similar to the classical polynomial addition and multiplication; however, every \( ^\oplus + \) calculation has to be substituted by a \( \oplus \) operation of \( \mathcal{I} \), and every \( ^\otimes \cdot \) calculation by a \( \otimes \) operation of \( \mathcal{I} \). It is easy to verify that \( \mathcal{I}[x] \)

\( Z^+ \) is set of all non-negative integers; \( Z^+[x] \) is polynomial semiring over \( Z^+ \); \( M_n(Z^+) \) is set of all \( n \times n \) matrices over \( Z^+ \); \( Z^+[C] \) is set of all polynomials of matrix \( C \in M_n(Z^+) \); \( \mathcal{I} \) is tropical semiring of integers \( Z \cup \{\infty\} \); \( \mathcal{I}[x] \) is tropical polynomial semiring over \( \mathcal{I} \); \( M_k(\mathcal{I}) \) is set of all \( k \times k \) tropical matrices over \( \mathcal{I} \); \( \mathcal{I}[N] \) is set of all tropical polynomials of tropical matrix \( N \in M_k(\mathcal{I}) \); \( \mathcal{H} \) is the vector \((H_1, H_2, \ldots, H_n)\), where \( H_i \in \mathcal{I}[N] \).

2.1. Tropical Semiring over Integer. A semiring is an algebraic structure similar to a ring, but without the requirement that each element must have an additive inverse.

Definition 1 (see [23]) A nonempty set \( \mathcal{R} \) with two binary operations \( + \) and \( \cdot \) is called a semiring if

1. \((\mathcal{R}, +)\) is a commutative monoid with identity element \( 0 \);
2. \((\mathcal{R}, \cdot)\) is a monoid with identity element \( 1 \neq 0 \);
3. Both distributive laws hold in \( \mathcal{R} \);
4. \( a \cdot 0 = 0 \cdot a = 0 \) for all \( a \in \mathcal{R} \).

If a semiring's multiplication is commutative, then it is called a commutative semiring.

Definition 2 (see [16]) The tropical commutative semiring of integer is the set \( \mathcal{I} = \mathbb{Z} \cup \{\infty\} \) with two operations as follows:

\[ x \oplus y = \min(x, y), \]
\[ x \otimes y = x + y. \] (1)

The special \( \infty \) satisfies the equations:

\[ \infty \oplus x = x, \]
\[ \infty \otimes x = \infty. \] (2)

It is straightforward to see that \((\mathcal{I}, \oplus, \otimes)\) is a commutative semiring. In fact, \( \infty \) is the identity element of \((\mathcal{I}, \oplus)\) and \( 0 \) is the identity element of \((\mathcal{I}, \otimes)\).

Just as in the classical case, we define the set of all tropical polynomials over \( \mathcal{I} \) in the indeterminate \( x \). Let

2.2. Tropical Matrix Semiring over Integer. \( M_k(\mathcal{I}) \) denotes the set of all \( k \times k \) matrices over \( \mathcal{I} \). We can also define the tropical matrix \( \oplus \) and \( \otimes \) operations. To perform the \( A \oplus B \)
operation, the elements $m_{ij}$ of the resulting matrix $M$ are set to be equal to $a_{ij} \otimes b_{ij}$. The tropical matrix $\otimes$ operation is similar to the usual matrix multiplication; however, every “+” calculation has to be substituted by a $\oplus$ operation of $\mathcal{Z}$, and every “•” calculation by a $\odot$ operation of $\mathcal{Z}$. $M_k(\mathcal{Z})$ is a noncommutative semiring with respect to the tropical matrix $\oplus$ and $\odot$ operations.

Example 1.
\[
\begin{pmatrix}
4 & -5 \\
27 & 0
\end{pmatrix} \oplus 
\begin{pmatrix}
10 & 3 \\
1 & 9
\end{pmatrix} = 
\begin{pmatrix}
4 & -5 \\
1 & 0
\end{pmatrix}, \\
\begin{pmatrix}
4 & -5 \\
27 & 0
\end{pmatrix} \odot 
\begin{pmatrix}
10 & 3 \\
1 & 9
\end{pmatrix} = 
\begin{pmatrix}
-4 & 4 \\
1 & 9
\end{pmatrix}, \\
\begin{pmatrix}
10 & 3 \\
1 & 9
\end{pmatrix} \odot 
\begin{pmatrix}
4 & -5 \\
27 & 0
\end{pmatrix} = 
\begin{pmatrix}
14 & 3 \\
5 & -4
\end{pmatrix}.
\]

The role of the identity matrix $I$ is played by the matrix that has "0"s on the diagonal and $\infty$ elsewhere. Similarly, a scalar matrix would be a matrix with an element $\lambda \in S$ on the diagonal and $\infty$ elsewhere. Such a matrix commutes with any other square matrix (of the same size). Multiplying a matrix by a scalar amounts to multiplying it by the corresponding scalar matrix.

Example 2.
\[
3 \odot \begin{pmatrix}
4 & -5 \\
27 & 0
\end{pmatrix} = \begin{pmatrix}
3 \infty & \infty \\
\infty & \infty
\end{pmatrix} \odot 
\begin{pmatrix}
4 & -5 \\
27 & 0
\end{pmatrix} = 
\begin{pmatrix}
7 & -2 \\
30 & 3
\end{pmatrix}.
\]

Then, tropical diagonal matrices have something on the diagonal and $\infty$ elsewhere. Note that, in contrast to the "classical" situation, it is rather rare that a "tropical" matrix is invertible. More specifically, the only invertible tropical matrices are those that are obtained from a diagonal matrix by permuting rows and/or columns.

For a matrix $N \in M_k(\mathcal{Z})$, denote
\[
\mathcal{Z}[N] = \{(a_0 \odot N^n) \oplus (a_{n-1} \odot N^{n-1}) \oplus \cdots \oplus (a_0 \odot N) \oplus (a_0 \odot I) | a_i \in \mathcal{Z} \text{ and } n \geq 0\},
\]
where $N^n$ means $N \odot \cdots \odot N$ ($m$ times). It is clear that $\mathcal{Z}[N]$ is a commutative subsemiring of $M_k(\mathcal{Z})$ with respect to the tropical matrix addition and multiplication.

3. Multiple Exponentiation Problem of Tropical Matrices

3.1. Companion Matrix of Polynomial over Integer Ring $\mathcal{Z}$. Let $f_0, f_1, \ldots, f_{n-1}$ be non-negative integers and $f_0 > 0$. The companion matrix of a monic polynomial $f(x) = -f_0 - f_1 x - \cdots - f_{n-1} x^{n-1} + x^n$ is given by the $n \times n$ matrix
\[
C = \begin{pmatrix}
0 & 0 & \cdots & 0 & f_0 \\
1 & 0 & \cdots & 0 & f_1 \\
0 & 1 & \cdots & 0 & f_2 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 1 & f_{n-1}
\end{pmatrix}.
\]

Note that the entries of $C$ are all non-negative. Denote $\mathcal{Z}^+[C] = \{p(C)p(x) \in \mathcal{Z}^+[x]\}$.

It is easy to verify that $\mathcal{Z}^+[C]$ is a commutative subsemiring of $M_k(\mathcal{Z})$.

3.2. Matrix Semigroup $\mathcal{Z}^+[C]$ Action on $(\mathcal{Z}[N])^n$. Let $f_0, f_1, \ldots, f_{n-1}$ be non-negative integers and $f_0 > 0$. Let $C$ be the companion matrix of the polynomial $f(x) = -f_0 - f_1 x - \cdots - f_{n-1} x^{n-1} + x^n$. Let $A = (a_{ij})_{n \times n} \in \mathcal{Z}^+[C]$, $N \in M_k(\mathcal{Z})$, and $H = (H_1, H_2, \ldots, H_n) \in (\mathcal{Z}[N])^n$. Consider an action $*$ of
\[
A \ast H = A \ast (H_1, H_2, \ldots, H_n) = \left(\prod_{i=1}^{n} H_i^{a_{i1}}, \prod_{i=1}^{n} H_i^{a_{i2}}, \ldots, \prod_{i=1}^{n} H_i^{a_{in}}\right),
\]
where $H_i^{a_{ii}}$ means $H_1 \odot \cdots \odot H_i (a_{ii} \text{ times})$. By the commutativity of $\mathcal{Z}[N]$, it is easy to prove that "$\ast$" is a semigroup action of $\mathcal{Z}^+[C]$ on $(\mathcal{Z}[N])^n$. In fact, a similar semigroup action was first defined by Maze in [11], where the action of $\mathcal{Z}[C]$ on the group direct product $G^n$ was considered.

Example 3. Let $f(x) = x^2 - 2$. The companion matrix of $f(x)$ is $C = \begin{pmatrix}
0 & 2 \\
1 & 0
\end{pmatrix}$. Let $N \in M_k(\mathcal{Z})$ as follows.
\[
N = \begin{pmatrix}
62 & 30 \\
1 & 86
\end{pmatrix}.
\]

Let $\overline{H} = (H_1, H_2) \in (\mathcal{Z}[N])^2$ as follows.
\[
H_1 = \begin{pmatrix}
38 & 43 \\
67 & 20
\end{pmatrix},
\]
\[
H_2 = \begin{pmatrix}
14 & 42 \\
25 & 38
\end{pmatrix},
\]
\[
H_3 = \begin{pmatrix}
25 & 15 \\
16 & 32
\end{pmatrix}.
\]
Let \( A = 3E + 5C = \left( \begin{array}{cc} 3 & 10 \\ 5 & 3 \end{array} \right) \). Then,
\[
A \ast \vec{H} = A \ast (H_1, H_2) = (H^3 \otimes H^{10}, H^5 \otimes H_2^2)
\]
\[
= \left( \begin{array}{ccc}
275 & 233 & 281 \\
252 & 210 & 258 \\
269 & 227 & 275
\end{array} \right),
\]
(12)

3.3. Multiple Exponentiation Problem of Tropical Matrices

**Definition 3.** Let \( f_0, f_1, \ldots, f_{n-1} \) be non-negative integers and \( f_0 > 0 \). Let \( C \) be the companion matrix of the polynomial \( f(x) = -f_0 - f_1 x - \cdots - f_{n-1} x^{n-1} + x^n \). Let \( N \in M_k(\mathbb{Z}) \) and \( \vec{H} = (H_1, H_2, \ldots, H_n) \in (\mathbb{Z}[N])^n \). Suppose that \( \vec{U} = A \ast \vec{H} \), where \( A \in \mathbb{Z}^+ [C] \). The multiple exponentiation problem of tropical matrices is to find \( A \in \mathbb{Z}^+ [C] \), given \( f(x), \vec{H} \), and \( \vec{U} \). (Note that \( N \) is unknown.) For simplicity, we abbreviate the problem to "ME problem."

As we know, most results in ordinary algebra do not hold in tropical algebra. Therefore, the certain properties of ordinary matrices like determinant, eigenvalues, and Cayley–Hamilton theorem cannot be used. But if \( H_1 \in \langle H_2 \rangle \) or \( H_2 \in \langle H_1 \rangle \), we can reduce the problem to discrete logarithm problem.

**Proposition 1.** Suppose \( H_1 \in \langle H_2 \rangle \) or \( H_2 \in \langle H_1 \rangle \), then the ME problem in Example 4 can be reduced to discrete logarithm problem in polynomial time.

**Proof.** Let \( \vec{U} = (U_1, U_2) \). Then,
\[
\begin{cases}
H_1^{a_0} H_2^{a_1} = U_1 \\
H_1^{a_0} H_2^{a_1} = U_2
\end{cases}
\]
(15)

Suppose \( H_2 \in \langle H_1 \rangle \). By solving a discrete logarithm problem in \( \langle H_1 \rangle \), we can get a positive integer \( m \) such that \( H_2 = H_1^m \). So, the equations (15) are equivalent to the following equations.
\[
\begin{cases}
H_1^{a_0 + 2ma_1} = U_1 \\
H_1^{a_0 + ma_1} = U_2
\end{cases}
\]
(16)

Example 4. Given \( f(x) = x^2 - 2 \), \( \vec{H} = (H_1, H_2) \), and \( \vec{U} \) as follows, we try to find \( A \in \mathbb{Z}^+ [C] \) such that \( \vec{U} = A \ast \vec{H} \).
\[
\vec{H} = \left( \begin{array}{ccc}
38 & 43 & 36 \\
67 & 20 & 68 \\
14 & 42 & 38
\end{array} \right), \quad \vec{U} = \left( \begin{array}{ccc}
275 & 233 & 281 \\
252 & 210 & 258 \\
269 & 227 & 275
\end{array} \right)
\]
(13)

In this case, \( U_1, U_2 \in \langle H_j \rangle \). By solving two discrete logarithm problems in \( \langle H_j \rangle \), we can get two positive integers \( t_1, t_2 \) such that \( U_1 = H_1^{t_1} \) and \( U_2 = H_2^{t_2} \). Therefore,
\[
\begin{cases}
a_0 + 2ma_1 = t_1 \\
a_1 + ma_0 = t_2
\end{cases}
\]
(17)

It is clear that we can obtain \( a_0, a_1 \) by solving a system of linear equations. \( \square \)

**Proposition 2.** If there exists a component \( H_i \) of \( \vec{H} \) such that \( (\forall j \neq i) H_j \notin \langle H_i \rangle \), then the ME problem can be reduced to discrete logarithm problem in polynomial time.

If \( H_1 \notin \langle H_2 \rangle \) and \( H_2 \notin \langle H_1 \rangle \), the problem of finding \( a_0, a_1 \) from equation (14) cannot be reduced to discrete logarithm problem. In fact, in Example 4, the conditions are indeed satisfied.

In order to resist some other potential method of solving ME problem, we stress the condition that \( N \) is unknown. Since the matrix \( N \) is unknown, we cannot express \( H_1 \) and \( H_2 \) as the polynomials of \( N \). (Even if \( N \) is known, we have not found any effective method to find \( a_0 \) and \( a_1 \).)

**Remark 1.** Assume that \( a_0, a_1 \in [0, s - 1] \). Hence, in the example the total number of steps to solve ME problem by brute-force attack is \( s^2 \).
4. Public Key Cryptosystems Based on Tropical Matrix

In this section, we give a key exchange protocol similar to Diffie–Hellman protocol and a public key encryption scheme similar to ElGamal encryption scheme.

4.1. Key Exchange Protocol Based on Tropical Matrix. Let \( f_0, f_1, \ldots, f_{n-1} \) be non-negative integers and \( f_0 > 0 \). Let \( C \) be the companion matrix of the polynomial \( f(x) = -f_0 - f_1 x - \cdots - f_{n-1} x^{n-1} + x^n \), and \( H \in (\mathbb{Z}[N])^n \) such that there exists not a component \( H_i \) of \( H \) such that \( (\forall j \neq i) H_j \in \langle H \rangle \) \(\langle H \rangle \) \((i, j = 0, 1, \ldots, n-1)\). The public parameters of the protocol are \( f(x), H \). Key change protocol based on tropical matrix is the following.

4.1.1. Protocol 4.1.1

(1) Alice selects at random \( n \) private integers \( a_0, a_1, \ldots, a_{n-1} \) in \([0, s-1]\) and computes
\[ A = a_0 C^{n-1} + \cdots + a_{n-1} C + a_0 E = (a_{ij})_{n \times n} \] Bob selects at random \( n \) private integers \( b_0, b_1, \ldots, b_{n-1} \) in 
\([0, s-1]\) and computes
\[ B = b_0 C^{n-1} + \cdots + b_{n-1} C + b_0 E = (b_{ij})_{n \times n} \]
(2) Alice computes \( \overline{U} = A \ast H \) and sends to Bob the matrix \( \overline{U} \). And Bob computes \( \overline{V} = B \ast H \) and sends to Alice the matrix \( \overline{V} \).
(3) Alice computes
\[ K_{Alice} = A \ast \overline{V} = A \ast (B \ast H) = (A \ast B) \ast \overline{H} \] and Bob computes
\[ K_{Bob} = B \ast \overline{U} = B \ast (A \ast H) = (B \ast A) \ast \overline{H} \]
where “\( \ast \)” is the matrix multiplication in \( \mathbb{Z}^+ [C] \).

Since \( \mathbb{Z}^+ [C] \) is commutative, we have \( A \ast B = B \ast A \) and \( K_{Alice} = K_{Bob} \). So, Alice and Bob share a common secret key.

Definition 4. Let \( f_0, f_1, \ldots, f_{n-1} \) be non-negative integers and \( f_0 > 0 \). Let \( C \) be the companion matrix of the polynomial \( f(x) = -f_0 - f_1 x - \cdots - f_{n-1} x^{n-1} + x^n \), and \( H \in (\mathbb{Z}[N])^n \) such that \( \langle H \rangle \) \(\langle H \rangle \) \((i, j = 0, 1, \ldots, n-1)\). Suppose that \( \overline{U} = A \ast \overline{H} \) and \( \overline{V} = B \ast \overline{H} \), where \( A, B \in \mathbb{Z}^+ [C] \). The computational ME problem is to find the matrix vector \( \overline{K} \) such that \( \overline{K} = (AB) \ast \overline{H} \), given \( f(x), \overline{H}, \overline{U}, \) and \( \overline{V} \). For simplicity, we abbreviate the problem to “CME problem.”

Proposition 3. An algorithm that solves ME problem can be used to solve CME problem.

Proposition 4. Finding the common secret key from the public information of Protocol 4.1.1 is equivalent to solving the CME problem.

4.2. Public Key Encryption Scheme Based on Tropical Matrix

4.2.1. Scheme 4.2.1. Key generation.

Let \( f_0, f_1, \ldots, f_{n-1} \) be non-negative integers and \( f_0 > 0 \). Let \( C \) be the companion matrix of the polynomial \( f(x) = -f_0 - f_1 x - \cdots - f_{n-1} x^{n-1} + x^n \), and \( H \in (\mathbb{Z}[N])^n \). There exists not a component \( H_i \) of \( H \) such that \( \langle (\forall j \neq i) H_j \in \langle H \rangle \rangle \) \(\langle H \rangle \) \((i, j = 0, 1, \ldots, n-1)\). The public parameters are \( f(x), H \). The key generation center chooses at random integers \( a_0, a_1, \ldots, a_{n-1} \) in \([0, s-1]\) and computes
\[ A = a_0 C^{n-1} + \cdots + a_{n-1} C + a_0 E = (a_{ij})_{n \times n} \]
\[ \overline{U} = A \ast H \]
The public key of Alice is \( \overline{U} \). The private key of Alice is \( A \)
(\( (a_0, a_1, \ldots, a_{n-1}) \)).

Encryption.

Bob wants to send a plaintext messages \( \overline{M} \in (\mathbb{M}_k (\mathbb{Z})]^n \) to Alice.

(1) Bob chooses at random integers \( b_0, b_1, \ldots, b_{n-1} \) in \([0, s-1]\) and computes
\[ B = b_0 C^{n-1} + \cdots + b_{n-1} C + b_0 E = (b_{ij})_{n \times n} \]
(2) Bob computes \( \overline{V} = B \ast H \) as a part of ciphertext.
(3) Bob sends the ciphertext \( \overline{Q} = \overline{M} + B \ast \overline{U} \) as the rest of the ciphertext, where “\( + \)” is the ordinary integer matrix vector addition.
(4) Bob sends the ciphertext \( \overline{Q}, \overline{Q} \) to Alice.

Decryption.

Alice receives the ciphertext \( \overline{Q}, \overline{Q} \) and tries to decrypt it.

(1) Using her private key \( A \), Alice computes \( \overline{W} = A \ast \overline{V} \).
(2) Alice computes \( \overline{Q} - \overline{W} \), where “\( - \)” is the ordinary integer matrix vector subtraction.

Since
\[ \overline{Q} - \overline{W} = \overline{M} + B \ast \overline{U} - A \ast \overline{V} \]
\[ = \overline{M} + B \ast (A \ast H) - A \ast (B \ast H) \]
\[ = \overline{M} + (BA) \ast H - (AB) \ast H \]
\[ = \overline{M} \]
Alice gets the plaintext messages \( \overline{M} \).

Definition 5. Let \( f_0, f_1, \ldots, f_{n-1} \) be non-negative integers and \( f_0 > 0 \). Let \( C \) be the companion matrix of the polynomial \( f(x) = -f_0 - f_1 x - \cdots - f_{n-1} x^{n-1} + x^n \), and \( H \in (\mathbb{Z}[N])^n \). Suppose \( \overline{U} = A \ast H \) and \( \overline{V} = B \ast H \),

where \( A, B \in \mathbb{Z}^+ [C] \). Let \( R \in (\mathcal{X}[N])^n \). The decisional ME problem is to decide whether \( R = (AB) \ast \overline{H} \), given \( f(x), \overline{H}, U, V, \) and \( \overline{R} \). For simplicity, we abbreviate it to “DME problem.”

**Proposition 5.** An algorithm that solves CME problem can be used to solve DME problem.

**Theorem 1.** An algorithm that solves DME problem can be used to decide the validity of the ciphertexts of Scheme 4.2.1, and an algorithm that decides the validity of the ciphertexts of Scheme 4.2.1 can be used to solve DME problem.

**Proof.** Suppose first that the algorithm \( \mathcal{A}_1 \) can decide whether a decryption of Scheme 4.2.1 is correct. In other words, when given a decryption \( f(x), \overline{H}, U, (V, Q), M \), the algorithm \( \mathcal{A}_1 \) outputs “yes” if \( M \) is the decryption of \((V, Q)\) and outputs “no” otherwise. Let us use \( \mathcal{A}_2 \) to solve the DME problem. Suppose you are given \( f, f(x), \overline{H}, U = (A \ast \overline{H}), V = (B \ast \overline{H}) \), and \( \overline{R} \), and you want to decide whether or not \( \overline{R} = (AB) \ast \overline{H} \). Let \( Q = \overline{R} = M \) be the claimed decryption of \((V, Q)\). Input \( Q \) into \( \mathcal{A}_1 \) and decide whether \( \mathcal{A}_1 \) outputs “yes” exactly when \( \overline{M} = (0, 0, \ldots, 0) \) is the same as \( \overline{R} = (AB) \ast \overline{H} \), namely, when \( \overline{R} = (AB) \ast \overline{H} \). This solves the decisional DME problem.

Conversely, suppose an algorithm \( \mathcal{A}_2 \) can solve the DME problem. This means that if you give \( \mathcal{A}_2 \) inputs \( f(x), \overline{H}, U = (A \ast \overline{H}), V = (B \ast \overline{H}) \), and \( \overline{R} \), then \( \mathcal{A}_2 \) outputs “yes” if \( \overline{R} = (AB) \ast \overline{H} \) and outputs “no” if not. Let \( M \) be the claimed decryption of \((V, Q)\). Input \( Q \) into \( \mathcal{A}_2 \) and decide whether \( \mathcal{A}_2 \) outputs “yes” exactly when \( \overline{M} = (0, 0, \ldots, 0) \) is the correct plaintext for the ciphertext \((V, Q)\). If and only if \( \overline{M} = (0, 0, \ldots, 0) \) is the correct plaintext for the ciphertext \((V, Q)\). Therefore, \( \overline{M} = (0, 0, \ldots, 0) \) is the correct plaintext for the ciphertext \((V, Q)\). Therefore, with these inputs, \( \mathcal{A}_2 \) outputs “yes” exactly when \( \overline{M} = (0, 0, \ldots, 0) \) is the correct plaintext.

**Theorem 2.** An algorithm that solves CME problem can be used to decrypt the ciphertexts of Scheme 4.2.1, and an algorithm that decrypts the ciphertexts of Scheme 4.2.1 can be used to solve CME problem.

**Proof.** If we have an algorithm \( \mathcal{A}_3 \) that can decrypt all ciphertexts of Scheme 4.2.1, then input \( \overline{U} = A \ast \overline{H} \) and \( \overline{V} = B \ast \overline{H} \). Take any vector for \( Q \). Then, \( \mathcal{A}_3 \) outputs \( \overline{M} = \overline{Q} - A \ast \overline{V} = \overline{Q} - (AB) \ast \overline{H} \). Therefore, \( \overline{Q} - \overline{M} \) yields the solution \((AB) \ast \overline{H}\) to the CME problem.

Conversely, suppose we have an algorithm \( \mathcal{A}_4 \) that can solve CME problem. If we have an ciphertext \((V, Q)\), then we input \( \overline{U} = A \ast \overline{H} \) and \( \overline{V} = B \ast \overline{H} \). Then, \( \mathcal{A}_4 \) outputs \((AB) \ast \overline{H}\). Since \( \overline{M} = \overline{Q} - A \ast \overline{V} = \overline{Q} - (AB) \ast \overline{H} \), we obtain the plaintext \( M \). □

5. Possible Attacks, Parameter Selection, and Efficiency

5.1. Possible Attacks

1. **Brute-force attack.** Suppose that \( A = a_{n-1}C^{n-1} + \cdots + a_1C + a_0 \in [0, s - 1] \). It is clear that attacker has \( s^2 \) choices to choose \( A \). So, the parameters \( s \) and \( n \) must satisfy \( s^2 \geq 2^{60} \).

2. **Tropical matrix decomposition attack.**

   Suppose that \( \overline{U} = (U_1, U_2, \ldots, U_n) \). If attacker can find \( A = (a_{ij})_{mn} \) such that

   \[
   \begin{align*}
   H_1^{\ast ij} & \ast H_2^{\ast ij} \ast \cdots \ast H_n^{\ast ij} = U_1 \\
   H_1^{\ast ij} & \ast H_2^{\ast ij} \ast \cdots \ast H_n^{\ast ij} = U_2 \\
   \vdots & \cdots \\
   H_1^{\ast ij} & \ast H_2^{\ast ij} \ast \cdots \ast H_n^{\ast ij} = U_n \\
   A' & = CA'
   \end{align*}
   \]

   Then he can get the shared key \((A \ast B) \ast \overline{H}\) by \( A' \) and the public information. He can perform the following steps to find \( A' \).

   (i) Factor \( U_j = G_1 \ast G_2 \ast \cdots \ast G_n \), where \( G_i \in \langle H_j \rangle \).

   (ii) Find \( a_{ij} \) such that \( H_i \ast a_{ij} = G_i \), \( i, j = 1, 2, \ldots, n \), by solving discrete logarithm problem in \( \langle H_j \rangle \).

   (iii) Verify whether or not \( A' \ast C = CA' \). If not, go to (i).

   However, it is hard to factor \( U_j = G_1 \ast G_2 \ast \cdots \ast G_n \), where \( G_i \in \langle H_j \rangle \) and \( n > 2 \). Generally, it is NP-hard by Shitov [24].

3. **KU attack.** In our cryptosystems, the used commutative subsemiring in our cryptosystems is the subsemiring \( \mathcal{X}[N] \) and \( N \) is unknown. This is different from that in literature [16]. They used two public tropical matrices \( M_1, M_2 \neq M_1 \ast M_2 \) and then adopted the commutative subsemiring \( \mathcal{X}[M_1], \mathcal{X}[M_2] \). Let \( p_1(M_1) \in \mathcal{X}[M_1] \), \( p_2(M_2) \in \mathcal{X}[M_2] \), and \( p_1(M_1) \ast p_2(M_2) = U \). The security of the cryptosystem relies on the difficulty of the problem of finding \( S_i \in \mathcal{X}[M_1] \) and \( S_j \in \mathcal{X}[M_2] \) such that \( S_i \ast S_j = U \). Because the secret matrix can be expressed as a polynomial of \( M \). Kotov and Ushakov designed an efficient algorithm to attack the tropical key exchange protocol [17]. In our cryptosystems, since attacker does not know \( N \), the KU attack will not work. To find \( N \) from public information, attacker is faced with the following problem. Given \( H_1, H_2, \ldots, H_n \in M_k(\mathcal{X}) \), find \( N \in M_k(\mathcal{X}) \) such that
where \( d_{i_0}, d_{i_1}, \ldots, d_{i_n} \) (\( i = 1, 2, \ldots, n \)) and \( N \) are all unknown. It is clear that this is a problem of solving systems of min-plus polynomial equations which is NP-hard [16].

Even if \( N \) is obtained by attacker. It seems also hard to find the private key matrix \( A \) from the public key \( \overline{U} = A * H \). As we know, KU attack can only decompose a tropical matrix into the product of two matrices such as \( \overline{U} = S_1 S_2 \). If \( n > 2 \), each component matrix of \( \overline{U} \) is the product of matrices more than two. In this case, KU attack will also not work.

(4) Generalized KU attack. In order to remedy Grigorev–Shpilrain’s protocols, Muanalifah and Sergeev suggested some modifications that use two types of matrices that are Jones matrices and Linde–de la Puente matrices [22]. But the authors also pointed out that their modifications cannot resist the generalized KU attack which can also decompose the public matrix into the product of two Jones matrices (Linde–de la Puente matrices) expressed as the linear form of the tropical basic elementary matrix. In our cryptosystems, if \( n > 2 \), then each component matrix of \( \overline{U} \) is the product of matrices more than two. In this case, the generalized KU attack will also not work for our cryptosystems.

(5) RM attack. Grigorev and Shpilrain [18] improved the original scheme and proposed the public key cryptosystems based on semi-direct product of tropical matrix semiring. But the first component of semi-direct product multiplication contains the addition of tropical matrix. Because the addition operation of tropical matrix is idempotent, the powers of semi-direct product multiplication have partial order preservation. Using this property, Rudy and Monaco designed a simple binary search algorithm and cracked the cryptosystem in [18]. In our cryptosystems, \( A * H \) has not the addition operation of tropical matrix. So, our cryptosystems can resist this attack.

(6) Quantum attack. ME problem is the generalization of the discrete logarithm problem. As we know, the discrete logarithm problem can be reduced in polynomial time to hidden subgroup problem which can be solved in polynomial time by the generalized Shor quantum algorithm [25]. If the semigroup action is derived from a module over ring, there exist the similar reduction algorithms for the corresponding semigroup action problem. When the semigroup action is induced by a semimodule over semiring that cannot be embedded in a module, no effective reduction algorithm has been found for the corresponding semigroup action problem. It is easy to verify that “\(*\)” is a semigroup action derived from the semimodule \( (\mathbb{Z}[N])[a] \) over the semiring \( \mathbb{Z}^+ [C] \) and ME problem is indeed the corresponding semigroup action problem induced by the semimodule. Since the semimodule \( (\mathbb{Z}[N])[a] \) cannot be embedded in a module, ME problem cannot be reduced in polynomial time to hidden subgroup problem generally.

Table 1 provides the comparison among relevant tropical cryptographic schemes.

5.2. Parameter Selection and Efficiency. By Proposition 2, if there exists a component \( H_i \) of \( \overline{H} \) such that \( (\forall j \neq i) H_j \in \langle H_i \rangle (i, j = 0, 1, \ldots, n - 1) \), then the ME problem can be reduced to discrete logarithm problem in polynomial time. To avoid this case, \( \overline{H} \) needs to satisfy the condition that there exists not a component \( H_i \) of \( \overline{H} \) such that \( (\forall j \neq i) H_j \in \langle H_i \rangle (i, j = 0, 1, \ldots, n - 1) \). Note that \( N \) is unknown and \( H_1, H_2, \ldots, H_n \in \mathbb{Z}[N] \). We can choose \( H_i \) such that

\[
H_i = (d_{i_0} \otimes N^9) \oplus (d_{i_8} \otimes N^8) \oplus \cdots \oplus (d_{i_1} \otimes N) \oplus (d_{i_0} \otimes I_k).
\]

where \( d_{i_0}, d_{i_1}, \ldots, d_{i_9} \) are integers selected randomly in \( [0, 1024] \). Then, the number of possible \( H_i \) is \( 2^{100} \). Experiments show that it is easy to generate \( H_1, H_2, \ldots, H_n \) satisfying the above condition.

Generally, for \( N \in M_k (\mathbb{Z}) \), the monogenic subsemigroup \( \langle N \rangle \) is infinite. But for many tropical matrices \( N \in M_k (\mathbb{Z}) \), there are non-negative integers \( l, m \) and integer \( \epsilon \) such that \( \epsilon \otimes N^l = N^{l+m} \). If \( l, m \) are the smallest non-negative integers such that \( \epsilon \otimes N^l = N^{l+m} \), then \( l \) is called the pseudo-index of the matrix \( N \) and \( m \) is called the pseudo-period of the matrix \( N \). If the pseudo-indexes and the pseudo-periods of \( N \) and \( H_i (i = 1, 2, \ldots, n) \) are all small, then there may be some potential heuristic attacks. The pseudo-index of tropical matrix increases with the increase of \( k \). Our experiments show that it is feasible to generate \( N \) and \( H_i (i = 1, 2, \ldots, n) \) with pseudo-indexes more than \( k^2 \) \( (k < 30) \). In \( A * H \) and \( B * H \), the entries of \( A, B \) are the exponents of \( H_i \). Since \( A, B \in \mathbb{Z} [C] \), the entries of \( C \) and \( s \) should not be too large. We recommend \( f(x) = x^s - 1 \) and
numbers of bit operations required for multiplying two Intel(R) Core(TM) i7-4700MQ CPU @ 2.40GHz).

Table 2, we also compare the running time of the operation of bit operations required for calculating $k(s, n, k)$. Suppose the entries of the matrices $A, B$ are in $[0, s - 1]$ and the entries of $AB$ are less than $n(s - 1)^2$. To resist some potential heuristic attacks, we recommend the parameters $s, n, k$ satisfying $k^2 \geq n(s - 1)^2$.

If we use the "square-multiply" algorithm to compute the power of tropical matrix, then computing $A \cdot \bar{H}$ requires $n^2 \log s + n(n - 1)$ tropical matrix multiplications. The numbers of bit operations required for multiplying two tropical matrices of order $k$ are $O(k^3)$. So, the total number of bit operations required for computing $A \cdot \bar{H}$ is $O(k^3 n^2 \log s).

The size of secret key ($a_{00}, a_{10}, \ldots, a_{n-1}$) is less than $n \log s$ bits. Suppose the entries of the matrices $N$ are in the range $[0, T]$ and $H_i = \sum_{j=0}^{k^2} d_{ij} \in N^3$ where $d_{ij} \in [0, d]$. Then, the size of public key $U$ is less than $n^2 k^2 \log((s - 1)(d + 9T))$ bits.

Select $T = 100$ and $d = 1024$. Table 2 provides the upper bounds of the size of secret key and public key for different values of $k, n, s$ such that $s^2 \approx 2^{30}$ and $k^2 \approx n(s - 1)^2$. And in Table 2, we also compare the running time of the operation $A \cdot \bar{H}$ under different parameters (experimental platform: Intel(R) Core(TM) i7-4700MQ CPU @ 2.40 GHz).

### 6. Conclusion and Further Research

This paper proposes a new key exchange protocol and a new public key encryption scheme based on multiple exponentiation problem of tropical matrices which can resist all known attacks. Since the generating matrix $N$ of the used commutative subsemirings $\mathbb{Z}[N]$ is hidden and the public key matrices are the product of more than two unknown matrices, the cryptosystems can resist KU attack and generalized KU attack. There is no addition of tropical matrix in $A \cdot \bar{H}$. The attack method proposed by Rudy and Monico does not work for ME problem. As a semigroup action problem derived from semimodules on semirings, ME problem cannot be reduced to hidden subgroup problem in polynomial time. Our cryptosystem can be considered as a potential postquantum cryptosystem.

The algebraic properties of pseudo-index and pseudo-period of tropical matrix have not been clearly studied. We can only use enumeration method to find the pseudo-index and pseudo-period of tropical matrix and generate tropical matrices with pseudo-index less than 900. Therefore, in order to prevent potential heuristic attacks, the dimension $n$ of $\bar{H}$ needs to be large ($n \geq 90$). However, this makes the operation efficiency of $A \cdot \bar{H}$ low. If we can generate effectively tropical matrices with large pseudo-index or large pseudo-period, we can choose small $n$ to improve the operation efficiency.

Future works worth studying include the following

1. Study the properties of pseudo-index and pseudo-period of tropical matrix. If a fast algorithm of generating tropical matrix with large pseudo-index (or pseudo-period) and small order can be found, then the smaller $n$ and $k$ can be chosen. This will improve the computational efficiency of our cryptosystem.

2. Use other commutative tropical matrix semirings instead of $\mathbb{Z}[N]$. For example, we can design a public key cryptosystem based on ME problem of Jones matrix or Linde–de la Puente matrix. ME problem of commutative matrices over other semirings can also be considered.

3. ME problem of tropical matrices is a generalization of the discrete logarithm problem. If we regard $A \cdot \bar{H}$ as $\bar{H}$, then ME problem corresponds to discrete logarithm problem, CME problem corresponds to CDH problem, and DME problem corresponds to DDH problem. We believe that other cryptographic applications based on ME problem are also feasible. For example, we can consider the digital signature schemes and identity authentication schemes and other cryptographic applications based on CME assumption or DME assumption, such as [26–28]. However, as we point out previously, the cryptographic system based on ME problem over tropical matrix has no high computational efficiency, since the number of matrices $n$ and the order $k$ of the matrix are large in order to ensure security. It may limit some possible application scenarios.
Data Availability

The data underlying the results presented in the study are available within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (no. 61462016) and the Science and Technology Foundation of Guizhou Province Awardid: QIANKEHEJICHU-ZK [2021] Ordinary 313.

References

[1] W. Diffie and M. E. Hellman, “New directions in cryptography,” IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.
[2] T. E. Gamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469–472, 1985.
[3] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM Review, vol. 41, no. 2, pp. 303–332, 1999.
[4] F. Luo, F. Wang, K. Wang, J. Li, and K. Chen, “LWR-Based Fully Homomorphic Encryption, Revisited,” Security and Communication Networks, vol. 2018, Article ID 5967635, 2018.
[5] L. Wang, X. Shen, J. Li, J. Shao, and Y. Yang, “Cryptographic primitives in blockchains,” Journal of Network and Computer Applications, vol. 127, pp. 43–58, 2019.
[6] A. K. Jadoon, L. Wang, T. Li, and M. A. Zia, “Lightweight cryptographic techniques for automotive cybersecurity,” Wireless Communications and Mobile Computing, vol. 2018, Article ID 1640167, 2018.
[7] Z. Huang, J. Lai, and W. Chen, “Simulation-based selective opening security for receivers under chosen-ciphertext attacks,” Designs, Codes and Cryptography, vol. 87, no. 6, pp. 1345–1371, 2019.
[8] Z. Huang, J. Lai, W. Chen, M. Raees-ul-Haq, and L. Jiang, “Practical public key encryption with selective opening security for receivers,” Information Sciences, vol. 478, pp. 15–27, 2019.
[9] G. Maze, C. Monico, and J. Monico, “Public key cryptography based on semigroup actions,” Advances in Mathematics of Communications, vol. 1, no. 4, pp. 489–507, 2007.
[10] I. Anshel, M. Anshel, and D. Goldfeld, “An algebraic method for public-key cryptography,” Mathematical Research Letters, vol. 6, no. 3, pp. 287–291, 1999.
[11] G. Maze, C. Monico, and J. Rosenthal, “A public key cryptosystem based on actions by semigroups,” in Proceedings of the IEEE International Symposium on Information Theory (ISIT’02), Lausanne, Switzerland, July, 2002.
[12] R. Steinwandt and A. Suárez Corona, “Cryptanalysis of a 2-party key establishment based on a semigroup action problem,” Advances in Mathematics of Communications, vol. 5, no. 1, pp. 87–92, 2011.
[13] R. E. Atani, S. E. Atani, and S. Mirzakuchaki, “Public key cryptography based on semimodules over quotient semirings,” International Mathematical Forum, vol. 2, no. 52, pp. 2561–2570, 2007.
[14] M. Durechea, “Public key cryptosystem based on two sided action of different Exotic semirings,” International Mathematical Forum, vol. 2, no. 52, pp. 2561–2570, 2007.
[15] N. Goel, I. Gupta, and B. K. Dass, “Survey on SAP and its application in public-key cryptography,” Journal of Mathematical Cryptology, vol. 14, no. 1, pp. 144–152, 2020.
[16] D. Grigoriev and V. Shpilrain, “Tropical cryptography,” Communications in Algebra, vol. 42, no. 6, pp. 2624–2632, 2014.
[17] M. Kotov and A. Ushakov, “Analysis of a key exchange protocol based on tropical matrix algebra,” Journal of Mathematical Cryptology, vol. 12, no. 3, pp. 137–141, 2018.
[18] D. Grigoriev and V. Shpilrain, “Tropical cryptography II: e,” Communications in Algebra, vol. 47, no. 10, pp. 4224–4229, 2019.
[19] D. Rudy and C. Monico, “Remarks on a tropical key exchange system,” Journal of Mathematical Cryptology, vol. 15, no. 1, pp. 280–283, 2021.
[20] S. Issac and D. Kahrobaei, “A closer look at the tropical cryptography,” International Journal of Computer Mathematics: Computer Systems Theory, vol. 6, no. 2, pp. 137–142, 2021.
[21] A. Muanalilaf and S. Sergeev, “On the tropical discrete logarithm problem and security of a protocol based on tropical semidirect product,” Communications in Algebra, vol. 50, no. 2, pp. 861–879, 2022.
[22] A. Muanalilaf and S. Sergeev, “Modifying the tropical version of Stickel’s key exchange protocol,” Applications of Mathematics, vol. 65, no. 6, pp. 727–753, 2020.
[23] V. Gupta and J. N. Chaudhari, “Monic ideals in a group-semiring,” Asian-European Journal of Mathematics, vol. 4, no. 3, pp. 445–450, 2011.
[24] Y. Shitov, “The complexity of tropical matrix factorization,” Advances in Mathematics, vol. 254, no. 3, pp. 138–156, 2012.
[25] R. Joosza, “Quantum factoring, discrete logarithms, and the hidden subgroup problem,” Computing in Science & Engineering, vol. 3, no. 2, pp. 34–43, 2001.
[26] T. Li, Z. Liu, J. Li, C. Jia, and K. C. Li, “CDPS: a cryptographic system,” in Proceedings of Mathe- matical Cryptology, vol. 50, no. 2, pp. 861–879, 2022.
[27] T. Li, Z. Liu, P. Li, Z. Liu, and C. Jia, “Outsourced privacy-preserving classification service over encrypted data,” Journal of Network and Computer Applications, vol. 106, pp. 100–110, 2018.