


Article

Cryptosystems Based on Tropical Congruent Transformation of Symmetric Matrices

Huawei Huang 

School of Mathematical Sciences, Guizhou Normal University, Guiyang 550001, China; hwhuang7809@163.com

Abstract: Recently, public-key cryptography based on tropical semi-rings have been proposed. However, the majority of them are damaged. The main reason is that they use a public matrix to construct commutative matrix semi-rings. New public-key cryptosystems are proposed in this paper. They are based on tropical congruent transformation of symmetric matrix by circular matrix. The NP-hard problem of solving a tropical system of nonlinear equations underlies the cryptosystem's security. Since a known matrix cannot express the used commutative subsemi-rings of circular matrices and there is no tropical matrix addition operation and power of matrix, the cryptosystems can withstand known attacks, including the KU attack, RM attack, and IK attack. The length of the public key and private key of the new cryptosystems is half that of those described in the literature.

Keywords: public-key cryptography; key exchange protocol; tropical symmetric matrices; congruent transformation

1. Introduction

The integer factorization problem and the discrete logarithm problem are the two primary computing problems used in modern public-key encryption. For instance, the discrete logarithm problem provides the basis for the Diffie–Hellman key exchange protocol and ElGamal encryption [1,2]. On a quantum computer, Shor devised a quantum algorithm that can solve the discrete logarithm problem and the integer factorization problem in polynomial time [3]. Therefore, creating additional novel cryptosystems is a current study area for cryptography [4]. Traditional cryptosystems rely on a variety of commutative rings, including integer ring, residue class ring, and finite field. Numerous cryptologists seek out additional algebraic structures in an effort to create fresh public key cryptosystems [5]. More specifically, we generally hope to design some cryptosystems based on NP-hard problems of new algebraic structures (a problem is NP-hard if there exists some NP-complete problem that reduces to it in polynomial time).

One of the first cryptosystems based on semi-groups and semi-rings was proposed by Maze, Monico, and Rosenthal [6,7]. However, Steinwandt et al. eventually managed to crack it [8]. A cryptosystem based on semi-module over factor semi-ring was proposed by Atani [9]. Durcheva built cryptographic protocols using some idempotent semi-rings [10]. Ahmed et al. [11] cryptanalyzed these schemes in detail. By demonstrating that it is NP-hard to solve the tropical system of nonlinear equations, Grigoriev and Shpilrain [12] proposed employing tropical semi-rings to create public-key cryptosystems. Because tropical schemes do not require any number multiplications because addition is the norm in tropical multiplication, employing tropical algebras as platforms offers unequalled efficiency. However, even if an element is a matrix over a tropical algebra, its tropical powers still show some patterns. Kotov and Ushakov [13] set up a reasonably successful attack on one of Grigoriev and Shpilrain's schemes by taking advantage of this weakness.

The initial approach was enhanced by Grigoriev and Shpilrain, who also suggested public key cryptosystems using the semi-direct product of tropical semi-rings [14]. However, Rudy and Monico [15] and Isaac and Kahrobei [16] have recently proposed some attacks on the upgraded schemes.



Citation: Huang, H. Cryptosystems Based on Tropical Congruent Transformation of Symmetric Matrices. *Symmetry* **2022**, *14*, 2378. <https://doi.org/10.3390/sym14112378>

Academic Editor: Christos Volos

Received: 14 October 2022

Accepted: 8 November 2022

Published: 10 November 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the author. 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/>).

Symmetric matrices and congruent transformations of matrices have many important conclusions and applications in classical algebra [17–19]. But in tropical algebra, there are no similar results. For example, a tropical symmetric matrix is generally not congruent with a diagonal matrix. This paper suggests a public-key encryption and key exchange protocol based on the congruent transformation of a symmetric tropical matrix by a tropical circular matrix. These cryptosystems can withstand all known attacks, including the KU attack, RM attack, and IK attack, because the employed commutative semiring cannot be embodied by known matrices, and the addition operation of the matrix and the power of the matrix are not used in our cryptosystems. If the computational congruent transformation problem and decisional congruent transformation problem are hard, our cryptosystems are secure. By using symmetric matrices and congruent transformation, the length of the public key and private key of our cryptosystem is half that reported in [12,14].

The remainder of the paper is structured as follows. In Section 2, we concentrate on a few definitions that are fundamental concepts in tropical matrix algebra. In Section 3, we present the new public-key cryptosystems based on congruent transformation of symmetric tropical matrix by tropical circular matrix. Then, in Section 4, we examine the protocol's security and parameter choice. Section 5 provides the conclusion and recommendations for additional research.

2. Preliminaries

Let S be a non-empty set with operations “+” and “·”. Then S is called a semi-ring if the following conditions hold:

- (1) $(S, +)$ is a commutative semi-group with zero element 0;
- (2) (S, \cdot) is a semi-group with an identity element $1 \neq 0$ and $x \cdot 1 = 1 \cdot x = x$ for all $x \in S$;
- (3) the left and right distribution laws for addition are satisfied by multiplication;
- (4) for all $x \in S$, $x \cdot 0 = 0 \cdot x = 0$.

If the multiplication operation is commutative, then S is called a commutative semi-ring. Integer tropical commutative semi-ring is the set $\mathcal{Z} = \mathbb{Z} \cup \{\infty\}$ with addition operation and multiplication operation as follows:

$$\text{for all } a, b \in \mathbb{Z}, a \oplus b = \min(a, b), a \otimes b = a + b.$$

∞ is a element satisfying the equations : $\infty \oplus a = a$, $\infty \otimes a = \infty$. for all $a \in S$.

Then $(\mathcal{Z}, \oplus, \otimes)$ is a commutative semi-ring. Its zero element and identity element are ∞ and 0, respectively [12]. Let $M_k(\mathcal{Z})$ be the set of all $k \times k$ matrices over \mathcal{Z} . We can also define the tropical matrix addition operation and multiplication operation.

$$\text{for all } P = (p_{ij})_{k \times k'}, Q = (q_{ij})_{k \times k} \in M_k(\mathcal{Z}), \\ P \oplus Q = (p_{ij} \oplus q_{ij})_{k \times k'}, P \otimes Q = \left(\sum_{l=1}^n p_{il} \otimes q_{lj} \right)_{k \times k}$$

A matrix A is called a t -circular matrix if it has the following form,

$$A = \begin{pmatrix} a_0 & a_{k-1} + t & a_{k-2} + t & \cdots & a_1 + t \\ a_1 & a_0 & a_{k-1} + t & \cdots & a_2 + t \\ a_2 & a_1 & a_0 & \cdots & a_3 + t \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{k-1} & a_{k-2} & a_{k-3} & \cdots & a_0 \end{pmatrix}.$$

We denote A by $[a_0, a_1, \dots, a_{k-1}]_{k,t}$ (or $[a_0, a_1, \dots, a_{k-1}]_t$). Let

$$C_{k,t} = \{P \in M_k(\mathcal{Z}) | P \text{ is a circular matrix}\}.$$

It is easy to verify that $C_{k,t}$ is a commutative sub-semiring of $M_k(\mathcal{Z})$.

For a matrix A , the transpose of A is denoted by A^T . If $A^T = A$, then A is called a symmetric matrix. For matrices $A, B \in M_k(\mathcal{Z})$, if there exists a matrix $P \in M_k(\mathcal{Z})$ such that $P^T \otimes A \otimes P = B$, then A, B are congruent. Let

$$S_k = \{Y \in M_k(\mathcal{Z}) \mid Y \text{ is symmetric}\}.$$

If Y is a symmetric matrix and $P \in M_k(\mathcal{Z})$, then $P^T \otimes Y \otimes P$ is also symmetric.

Let P_1 and P_2 be two computational problems. P_1 is said to polytime reduce to P_2 , written $P_1 \leq_p P_2$, if there is an algorithm that solves P_1 which uses, as a subroutine, an algorithm for solving P_2 , and which runs in polynomial time if the algorithm for P_2 does. If $P_1 \leq_p P_2$ and $P_2 \leq_p P_1$, then P_1 and P_2 are said to be computationally equivalent.

Let $\mathcal{Z}[x_1, x_2, \dots, x_n]$ be the n -ary polynomial semiring over \mathcal{Z} . Let

$$p_1(x_1, x_2, \dots, x_n), p_2(x_1, x_2, \dots, x_n), \dots, p_m(x_1, x_2, \dots, x_n) \in \mathcal{Z}[x_1, x_2, \dots, x_n].$$

If $\deg p_i \geq 2$, ($i = 1, 2, \dots, m$), then the following tropical system is called a tropical system of nonlinear equations,

$$\begin{cases} p_1(x_1, x_2, \dots, x_n) = 0 \\ p_2(x_1, x_2, \dots, x_n) = 0 \\ \dots\dots\dots \\ p_m(x_1, x_2, \dots, x_n) = 0. \end{cases}$$

As we know, the problem of solving a tropical system of nonlinear equations is NP-hard [12].

In what follows, we sometimes denote $A \otimes B$ as AB for simplicity, and k, t is two positive integers.

3. Cryptosystems Based on Congruent Transformation of Symmetric Matrix

3.1. Key Establishment Protocol Based on Congruent Transformation Problem

Definition 1. Let $Y \in S_k$ and $P \in C_{k,t}$. Suppose that $X = P^T Y P$. The congruent transformation problem (CTP) is to find a matrix $P \in C_{k,t}$ such that $X = P^T Y P$, given the matrices X and Y .

Protocol 1. Let $Y \in S_k$. k and Y are public.

- (1) Alice selects randomly a matrix $P \in C_{k,t}$ and computes $U = P^T Y P$. She sends the matrix U to Bob.
- (2) Bob selects randomly a matrix $Q \in C_{k,t}$ and computes $V = Q^T Y Q$. He sends the matrix V to Alice.
- (3) Alice and Bob compute $K_a = P^T V P$ and $K_b = Q^T U Q$, respectively. The shared secret key $K = K_a = K_b$.

Since the $C_{k,t}$ is the commutative subsemi-ring of $M_k(\mathcal{Z})$, we have $PQ = QP$ and $P^T Q^T = Q^T P^T$. Then

$$K_a = P^T V P = P^T (Q^T Y Q) P = (P^T Q^T) Y (Q P) = (Q^T P^T) Y (P Q) = Q^T (P^T Y P) Q = Q^T U Q = K_b.$$

Definition 2. Let $P, Q \in C_{k,t}$ and $Y \in S_k$. Suppose that $U = P^T Y P$ and $V = Q^T Y Q$. The computational congruent transformation problem (CCTP) is to find a matrix $K \in M_k(\mathcal{Z})$ satisfying $K = P^T Q^T Y Q P$, given U, V and Y .

Proposition 1. CCTP \leq_p CTP.

Theorem 1. Finding the shared secret key from the public information of Protocol 1 is equivalent to solving CCTP.

The conclusions of Proposition 1 and Theorem 1 are obvious, so we omit the proofs of them. In Appendix A, we provide a toy example of Protocol 1.

3.2. Public-Key Encryption Cryptosystem Based on Congruent Transformation Problem

Cryptosystem 1.

(1) Key generation.

Let $Y \in S_k$. k , t and Y are public. Suppose that $P \in C_{k,t}$ and $U = P^T Y P$. User's public key is U . User's private key is P .

(2) Encryption.

Alice wants to send a message $M \in M_k(\mathbb{Z})$ to the user.

- (i) Alice chooses randomly $Q \in C_{k,t}$ and computes $V = Q^T Y Q$.
- (ii) Alice computes $W = M + Q^T U Q$, where "+" is the addition of the standard integer matrix.
- (iii) Alice sends the ciphertext (V, W) to the user.

(3) Decryption.

After receiving the ciphertext (V, W) , the user attempts to decrypt it.

- (i) Using the secret key P , the user computes $T = P^T V P$.
- (ii) The user computes $W - T$, where "-" is the subtraction of the standard integer matrix.

Note that

$$\begin{aligned} W - T &= M + Q^T U Q - P^T V P \\ &= M + Q^T (P^T Y P) Q - P^T (Q^T Y Q) P \\ &= M + Q^T P^T Y P Q - P^T Q^T Y Q P \\ &= M + P^T Q^T Y Q P - P^T Q^T Y Q P \\ &= M. \end{aligned}$$

So the user gets the plaintext M .

Definition 3. Let $P, Q \in C_{k,t}$ and $Y, E \in S_k$. Suppose that $U = P^T Y P$ and $V = Q^T Y Q$. The decisional congruent transformation problem (DCTP) is to decide whether $E = P^T Q^T Y Q P$, given the matrices U, V, E and Y .

Proposition 2. $DCTP \leq_p CCTP$.

Proposition 2 is obvious, so we omit its proof.

Theorem 2. DCTP is computationally equivalent to the problem of deciding the validity of the ciphertexts of Cryptosystem 1.

Proof of Theorem 2. Suppose that there is an algorithm \mathcal{A}_1 that can decide whether the decryption of Cryptosystem 1 is correct.

$$\mathcal{A}_1(Y, U, (V, W), M) = \begin{cases} 1, & \text{if } M \text{ is the decryption of } (V, W); \\ 0, & \text{otherwise.} \end{cases}$$

Then, we use \mathcal{A}_1 to solve the decisional congruent transformation problem. Suppose we are given $Y, U (= P^T Y P), V (= Q^T Y Q), E$ and we want to determine if $E = P^T Q^T Y Q P$ or not. Take U as the public key and V as the first part of the ciphertext. Moreover, take $W = E$ as the second part of the ciphertext and $M = 0_k$ which is zero matrix in $M_k(\mathcal{Z})$. Input all of these into \mathcal{A}_1 . (Note that P is the secret key.) We have

$$\mathcal{A}_1(Y, U, (V, E), 0_k) = \begin{cases} 1, & \text{if } 0_k \text{ is the decryption of } (V, E); \\ 0, & \text{otherwise.} \end{cases}$$

0_k is the decryption of (V, E) if and only if $E - P^T Q^T Y Q P = 0_k$. So \mathcal{A}_1 outputs 1 exactly when $E = P^T Q^T Y Q P$. The decisional congruent transformation problem is resolved in this way.

Conversely, suppose that there is an algorithm \mathcal{A}_2 that can solve the decisional congruent transformation problem. That is,

$$\mathcal{A}_2(Y, U, V, E) = \begin{cases} 1, & \text{if } E = P^T Q^T Y Q P; \\ 0, & \text{otherwise,} \end{cases}$$

where $U = P^T Y P$, $V = Q^T Y Q$. Then we use \mathcal{A}_2 to decide whether M is the decryption of the ciphertext (V, W) . After inputting $Y, U, V, W - M$, we have

$$\mathcal{A}_2(Y, U, V, W - M) = \begin{cases} 1, & \text{if } W - M = P^T Q^T Y Q P; \\ 0, & \text{otherwise,} \end{cases}$$

where $U = P^T Y P$, $V = Q^T Y Q$ and Y, U is the public key. Since $W - M = P^T Q^T Y Q P$ if and only if $M = W - P^T Q^T Y Q P$, \mathcal{A}_2 outputs 1 if and only if M is the correct plaintext. \square

Theorem 3. *CCTP is computationally equivalent to the problem of decrypting the ciphertexts of Cryptosystem 1.*

Proof of Theorem 3. Suppose that there is an algorithm \mathcal{A}_3 that can decrypt the ciphertexts of Cryptosystem 1. Input $U = P^T Y P$ and $V = Q^T Y Q$. Take any matrix in $M_k(\mathcal{Z})$ as W . Then, \mathcal{A}_3 outputs $M = W - P^T V P = W - P^T Q^T Y Q P$. Therefore, $W - M$ yields the solution $P^T Q^T Y Q P$ to the computational congruent transformation problem.

Conversely, suppose that there is an algorithm \mathcal{A}_4 that can solve the computational congruent transformation problem. If the ciphertext is (V, W) , then we input $U = P^T Y P$ and $V = Q^T Y Q$. Then, \mathcal{A}_4 outputs $P^T Q^T Y Q P$. Since

$$M = W - P^T V P = W - P^T Q^T Y Q P$$

we get the plaintext M . \square

4. Security Analysis and Parameter Selection

According to Theorems 1–3, Protocol 1 and Cryptosystem 1 can be attacked using a successful algorithm for resolving the congruent transformation problem.

Proposition 3. *CTP can be reduced to the problem of solving tropical system of nonlinear equations in polynomial time.*

Proof of Proposition 3. Let $Y \in S_k$ and $P \in C_{k,t}$. Suppose $X = P^T Y P$. Now, we want to find a matrix $P \in C_{k,t}$ such that $X = P^T Y P$, given the matrices X and Y .

Let $P = [x_0, x_1, \dots, x_{k-1}]_t$. Then

$$[x_0, x_1, \dots, x_{k-1}]_t^T \cdot Y \cdot [x_0, x_1, \dots, x_{k-1}]_t = X.$$

Since X and Y are known, we get a tropical system of nonlinear equations about x_0, x_1, \dots, x_{k-1} with k unknowns and $k(k+1)/2$ equations. Note that N is also symmetric. \square

As is well known, it is typically NP-hard to solve tropical systems of nonlinear equations [12]. We provide an exponentially complex problem-solving approach for congruent transformations.

Proposition 4. *There is an algorithm of solving CTP with computational complexity $O(k^3k!)$.*

Proof of Proposition 4. Through Proposition 3, we can get a tropical system of nonlinear equations about x_0, x_1, \dots, x_{k-1} with k unknowns and $k(k + 1)/2$ equations. Every term of the equations is in the form of $x_i x_j$ ($i, j = 0, 1, \dots, k - 1$). Denote

$$z_1 = x_0^2, z_2 = x_0 x_1, \dots, z_{k(k+1)/2} = x_{k-1}^2$$

Subsequently, a tropical system of linear equations is obtained with $k(k + 1)/2$ unknowns z_i and $k(k + 1)/2$ equations. We can obtain a tropical system of nonlinear equations by solving the tropical system of linear equations of z_i as follows,

$$x_0^2 = z_1, x_0 x_1 = z_2, \dots, x_{k-1}^2 = z_{k(k+1)/2}.$$

Since the multiplication in tropical algebra is the ordinary addition, it is actually a system of linear equations over an integer ring. However, we have k unknowns and $k(k + 1)/2$ equations. The linear equation system typically has no solution. However, if k equations of these $k(k + 1)/2$ equations have a solution, it may be possible to find x_0, x_1, \dots, x_{k-1} such that

$$[x_0, x_1, \dots, x_{k-1}]_t^T \cdot Y \cdot [x_0, x_1, \dots, x_{k-1}]_t = X.$$

The complexity of solving a tropical system of linear equations with $k(k + 1)/2$ unknowns z_i and $k(k + 1)/2$ equations is $O((k(k + 1)/2)^2)$. Since there are k equations with x_i ($i = 0, 1, 2, \dots, k - 1$) in the system

$$x_0^2 = z_0, x_0 x_1 = z_1, \dots, x_{k-1}^2 = z_{k(k+1)/2}.$$

There are more than $k!$ options available when choosing k equations from $k(k + 1)/2$ equations. When there are k equations and k unknowns, the complexity of solving integer linear equations is $O(k^3)$. As a result, $O(k^3k!)$ is the computational complexity of the aforementioned algorithm. \square

In Appendix B, an example of CTP with small parameters is demonstrated.

The commutative subsemiring in our cryptosystems is that of t -circular matrices. This is different from [12,14]. They used a known matrix M and then adopted the commutative subsemi-ring $\mathcal{Z}[M] = \{p(M) | p(x) \in \mathcal{Z}[x]\}$. Kotov and Ushakov [13] created an effective technique (KU Attack Algorithm) to attack the key exchange protocol in [12] because the secret matrix may be represented as a polynomial of M . Let

$$T_1 = \sum_{i=0}^d x_i P_1^i, T_2 = \sum_{i=0}^d y_i P_2^i$$

where $x_i, y_j \in \mathcal{Z}$, and d is the upper bound for the degrees of polynomials. $T_1 Y T_2 = X$ gives $\sum_{i=0}^d x_i y_j P_1^i Y P_2^j = X$. This gives

$$\min(x_i + y_j + A_{rs}^{ij}) = 0, \text{ for all } 1 \leq r, s \leq k$$

where $A^{ij} = P_1^i Y P_2^j - X$. Algorithm 1 is a precise description of a KU attack.

Algorithm 1: (KU Attack)

Input: $P_1, P_2, X(= p_1(P_1)Yp_2(P_2))$.

Output: $x_1, \dots, x_d, y_1, \dots, y_d$, such that $T_1YT_2 = X$, where $T_1 = \sum_{i=0}^d x_i P_1^i, T_2 = \sum_{i=0}^d y_i P_2^i$.

- (1) Compute $m_{ij} = \min_{i,j} (A_{rs}^{ij})$ and $B_{ij} = \{(r, s) \mid A_{rs}^{ij} = m_{ij}\}$;
- (2) Among minimal covers of $\{1, 2, 3, \dots, k\} \times \{1, 2, 3, \dots, k\}$ by B_{ij} , which are all minimal subsets $D \subseteq \{0, 1, 2, \dots, d\} \times \{0, 1, 2, \dots, d\}$ such that $\cup_{(i,j) \in C} B_{ij} = \{1, 2, 3, \dots, k\} \times \{1, 2, 3, \dots, k\}$
find the cover satisfying the following conditions

$$\begin{cases} -m_{ij} = x_i + y_j, & \text{if } (i, j) \in D; \\ -m_{ij} > x_i + y_j, & \text{if } (i, j) \in D. \end{cases}$$

Our cryptosystems can withstand KU attack because the employed commutative subsemi-rings of circular matrices cannot be represented by a known matrix.

The initial approach was enhanced by Grigoreiv and Shpilrain [14], who also suggested public key cryptosystems based on the semidirect product of tropical matrices. However, the addition of the tropical matrix is included in the first part of the semidirect product multiplication. As a result, the powers of semidirect product multiplication have partial order preservation. By this characteristic, Rudy and Monico [15] created a straightforward binary search algorithm (RM Attack), which they used to break the cryptosystem of [14]. The RM attack is described in pseudocode in Algorithm 2.

Algorithm 2: (RM Attack)

Input: $M, H, A \in M_k(\mathcal{Z})$, where $(M, H)^n = (A, H^n)$, for an integer $n (1 \leq n \leq r)$.

Output: n .

- (1) Let $p = 1$ and $q = r$;
- (2) Run the subsequent loop when $p \leq q$.
 - (i) $m = p + (q - p) / 2$
 - (ii) Compute $(M, H)^m = (S, T)$.
If $S < A, q = m - 1$;
If $S > A, p = m + 1$;
If $S = A$, output $n = m$.

In our cryptosystems, there is no tropical matrix addition operation and the partial order cannot be used. Thus, our cryptosystems can resist RM attack.

Isaac and Kahrobaei [16] proposed another cryptanalysis of the cryptosystems in [13]. They use the public matrices to derive a user's private key by finding the almost linear period of tropical matrix. Let $\{H^n \mid n \in \mathbb{Z}^+\}$ is a sequence of matrices. If there exist positive integers p, d and a constant c such that for all $n > d$ indices i, j the equation $H_{ij}^{n+p} = c + H_{ij}^n$ holds, then d is called the defect of the sequence of matrices and p is called the almost linear period of the sequence of matrices. The IK attack is described in pseudocode in Algorithm 3.

Algorithm 3: (IK Attack)

Input: $M, H, A \in M_k(\mathcal{Z})$, where $(M, H)^n = (A, H^n)$, for an integer $n (1 \leq n \leq r)$.

Output: n .

- (1) Construct a sequence of matrices $\{M_n \mid n \in \mathbb{Z}^+\}$, where $M_1 = M, M_n = M_{n-1} \circ H \oplus M$;
- (2) Find the defect d and almost linear period p of $\{M_n \mid n \in \mathbb{Z}^+\}$ by the sequence of matrices $\{D_n \mid n \in \mathbb{Z}^+\}$, where $D_n = M_n - M_{n-1}$;
- (3) Enumerate r from 1 to $p-1$ such that $A - M_{d+1} - \sum_{i=1}^r D_{d+i}$ is x times $\sum_{i=d+1}^{d+p} D_i$;
- (4) Output $n = d + xp + r$.

In our cryptosystems, there is not any power of matrix. This class of attack does not work for our cryptosystems.

We evaluate the security of our proposed cryptosystem [12,14], and other pertinent cryptosystems. Table 1 presents the comparing findings.

Table 1. Comparison of several tropical cryptosystems.

Cryptosystems	Problems	KU Attack	IK Attack	RM Attack
Grigoriev et al. [12]	Two-side abelian action problem	×	✓	✓
Grigoriev et al. [14]	Semidirect product problem	✓	×	×
Our cryptosystem	Congruent transformation problem	✓	✓	✓

✓ means that the cryptosystem can withstand the corresponding attack, and × means it does not.

Note that the length of public key and private key of our cryptosystem is half that described in [12,14] by using symmetric matrices and congruent transformation. Let secret key $P = [a_0, a_1, \dots, a_{n-1}]_t$. It is clear that $(a_0, a_1, \dots, a_{n-1})$ can be taken as the secret key. If $a_i \in [0, 2^s)$, then the length of a secret key is less than $n \log s$ bits. Public key $U = P^T Y P$ is a symmetric matrix. We can take the upper triangular part of U as the public key. The length of a public key is less than $k(k+1) \log(3s)/2$ bits.

Let $t \in (0, 2^{10})$ and the entries of matrices are the integer in $[0, 2^{20})$. The highest limits of the size of the secret key and public key for various values are shown in Table 2. The experimental results show that the time of the operation $P^T Y P$ is about 1ms (Experimental platform: Intel(R) Core(TM) i7-5500U CPU @ 2.40GHz). We suggest $k \geq 50$ to avoid potential heuristic attacks similar to KU attacks. The larger k can ensure that the cryptosystem is more secure. However, in a resource-constrained environment, the public key and private key should not be too large. Therefore, the size of k depends on the occasion of use.

Table 2. Performance evaluation under various k .

k	Length of sk (kB)	Length of pk (kB)	Complexity of Solving CTP
20	0.049	1.538	$O(2^{74})$
30	0.073	3.406	$O(2^{122})$
40	0.098	6.006	$O(2^{175})$
50	0.122	9.338	$O(2^{231})$
60	0.146	13.403	$O(2^{290})$
70	0.171	18.201	$O(2^{351})$
80	0.195	23.730	$O(2^{414})$

sk denotes secret key, and pk denotes public key.

5. Conclusions and Further Research

This article suggests brand-new public-key cryptosystems based on tropical congruent transformation of a symmetric matrix by a circular matrix. The NP-hard problem of solving tropical systems of nonlinear equations underlies the security of cryptosystems. Since a known matrix cannot express the used commutative subsemi-rings of circular matrices and there is no tropical matrix addition operation and power of matrix, the cryptosystems can withstand known attacks, including the KU attack, RM attack, and IK attack.

If we regard $P^T Y P$ as Y^P , then CTP corresponds to discrete logarithm problem, CCTP correlates to CDH problem, and DCTP correlates to DDH problem. Theoretically, any public key cryptosystem based on CDH problem (or DDH problem) can be transformed into the scheme based on CCTP (or DCTP) of tropical matrix semi-ring. We can construct identity authentication and digital signature methods based on CCTP or DCTP.

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: Not applicable.

Conflicts of Interest: The author states there are no competing interests.

Appendix A. A Toy Example of Protocol 1

Let $k = 5, t = 28$. The entries of matrices are in $[0, 2^{10})$. The public symmetric matrix Y is as follows,

$$Y = \begin{pmatrix} 455 & 554 & 271 & 892 & 794 \\ 554 & 676 & 463 & 340 & 580 \\ 271 & 463 & 250 & 784 & 365 \\ 892 & 340 & 784 & 310 & 407 \\ 794 & 580 & 365 & 407 & 883 \end{pmatrix}.$$

(1) Alice selects randomly a t -circular matrix P as follow.

$$P = [87, 90, 780, 219, 128]_{28}$$

Alice computes $U = P^T Y P$. She sends the matrix U to Bob.

$$U = \begin{pmatrix} 629 & 448 & 445 & 514 & 586 \\ 448 & 430 & 427 & 496 & 479 \\ 445 & 427 & 424 & 487 & 476 \\ 514 & 496 & 487 & 484 & 545 \\ 586 & 479 & 476 & 545 & 622 \end{pmatrix},$$

(2) Bob selects randomly a t -circular matrix Q as follow.

$$Q = [702, 452, 796, 363, 823]_{28}$$

Bob computes $V = Q^T Y Q$. He sends the matrix V to Alice.

$$V = \begin{pmatrix} 1036 & 1133 & 1125 & 1094 & 1306 \\ 1133 & 1154 & 1114 & 1269 & 1093 \\ 1125 & 1114 & 1214 & 1183 & 1053 \\ 1094 & 1269 & 1183 & 1423 & 1208 \\ 1306 & 1093 & 1053 & 1208 & 1032 \end{pmatrix},$$

(3) Alice computes $K = P^T V P$. Bob computes $K = Q^T U Q$.

$$K = \begin{pmatrix} 1210 & 1271 & 1268 & 1250 & 1241 \\ 1271 & 1291 & 1288 & 1233 & 1230 \\ 1268 & 1288 & 1357 & 1230 & 1227 \\ 1250 & 1233 & 1230 & 1212 & 1209 \\ 1241 & 1230 & 1227 & 1209 & 1206 \end{pmatrix}.$$

Appendix B. An Example of CTP with Small Parameters

Let $k = 3, t = 10$. The entries of matrices are in $[0, 100]$. The public matrix Y is as follow.

$$Y = \begin{pmatrix} 17 & 0 & 35 \\ 0 & 60 & 48 \\ 35 & 48 & 31 \end{pmatrix}.$$

Alice selects randomly a t -circular matrices $P = [38, 2, 18]_{10}$. Alice computes $U = P^T Y P$. She sends U to Bob.

$$U = \begin{pmatrix} 40 & 30 & 14 \\ 30 & 35 & 49 \\ 14 & 49 & 40 \end{pmatrix}.$$

Given k, t, Y and U , Bob tries to find Alice's secret matrix P .

Let $P = [x_0, x_1, x_2]_{10}$. Then

$$[x_0 \ x_1 \ x_2]_{10}^T \begin{pmatrix} 17 & 0 & 35 \\ 0 & 60 & 48 \\ 35 & 48 & 31 \end{pmatrix} [x_0 \ x_1 \ x_2]_{10} = \begin{pmatrix} 40 & 30 & 14 \\ 30 & 35 & 49 \\ 14 & 49 & 40 \end{pmatrix} (\#).$$

From it, he can get a multivariate quadratic equation system over a tropical semi-ring as follows,

$$\begin{cases} 17x_0^2 \oplus 0x_0x_1 \oplus 35x_0x_2 \oplus 60x_1^2 \oplus 48x_1x_2 \oplus 31x_2^2 & = & 40 \\ 0x_0^2 \oplus 35x_0x_1 \oplus 27x_0x_2 \oplus 48x_1^2 \oplus 10x_1x_2 \oplus 45x_2^2 & = & 30 \\ 35x_0^2 \oplus 27x_0x_1 \oplus 10x_0x_2 \oplus 10x_1^2 \oplus 45x_1x_2 \oplus 58x_2^2 & = & 14 \\ 60x_0^2 \oplus 48x_0x_1 \oplus 10x_0x_2 \oplus 31x_1^2 \oplus 45x_1x_2 \oplus 37x_2^2 & = & 35 \\ 48x_0^2 \oplus 10x_0x_1 \oplus 45x_0x_2 \oplus 45x_1^2 \oplus 37x_1x_2 \oplus 20x_2^2 & = & 49 \\ 31x_0^2 \oplus 45x_0x_1 \oplus 58x_0x_2 \oplus 37x_1^2 \oplus 20x_1x_2 \oplus 80x_2^2 & = & 40 \end{cases}.$$

where $ax_i x_j$ means $a \otimes x_i \otimes x_j$. By solving the tropical linear equations, the attacker can obtain a solution,

$$\begin{cases} x_0 \otimes x_0 & = & 30 & \text{(A1)} \\ x_0 \otimes x_1 & = & 40 & \text{(A2)} \\ x_0 \otimes x_2 & = & 25 & \text{(A3)} \\ x_1 \otimes x_1 & = & 4 & \text{(A4)} \\ x_1 \otimes x_2 & = & 20 & \text{(A5)} \\ x_2 \otimes x_2 & = & 29 & \text{(A6)} \end{cases}.$$

Obviously, the number of possible situations that has a solution is greater than 3!. It is easy to verify that only the Equations (A2), (A4) and (A5) have a solution satisfying (#).

References

- Diffie, W.D.; Hellman, E. New directions in cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654. [\[CrossRef\]](#)
- ElGamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory* **1985**, *31*, 469–472. [\[CrossRef\]](#)
- Shor, P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **1997**, *26*, 1484–1509. [\[CrossRef\]](#)
- Bernstein, D.J.; Lange, T. Post-quantum cryptography. *Nature* **2017**, *549*, 188–194. [\[CrossRef\]](#) [\[PubMed\]](#)
- Affum, E.; Zhang, X.; Wang, X.; Ansuura, J.B. Efficient Lattice CP-ABE AC Scheme Supporting Reduced-OBDD Structure for CCN/NDN. *Symmetry* **2020**, *12*, 166. [\[CrossRef\]](#)
- Maze, G.; Monico, C.; Rosenthal, J. A Public key cryptosystem based on actions by semi-groups. In Proceedings of the IEEE International Symposium on Information Theory, Lausanne, Switzerland, 30 June–5 July 2002; pp. 266–289.
- Maze, G.; Monico, C.; Rosenthal, J. Public key cryptography based on semi-group actions. *Adv. Math. Commun.* **2007**, *1*, 489–507. [\[CrossRef\]](#)
- Steinwandt, R.; Corona, A. Cryptanalysis of a 2-party key establishment based on a semi-group action problem. *Adv. Math. Commun.* **2011**, *5*, 87–92. [\[CrossRef\]](#)
- Atani, R.E. Public key cryptography based on semimodules over quotient semi-rings. *Int. Math. Forum* **2007**, *2*, 2561–2570. [\[CrossRef\]](#)
- Durcheva, M. Public Key Cryptosystem Based on Two Sided Action of Different Exotic Semi-rings. *J. Math. Syst. Sci.* **2014**, *4*, 6–13.
- Ahmed, K.; Pal, S.; Mohan, R. A review of the tropical approach in cryptography. *Cryptologia* **2021**, *46*, 1–25. [\[CrossRef\]](#)
- Grigoriev, D.; Shpilrain, V. Tropical cryptography. *Commun. Algebra* **2014**, *42*, 2624–2632. [\[CrossRef\]](#)
- Kotov, M.; Ushakov, A. Analysis of a key exchange protocol based on tropical matrix algebra. *J. Math. Cryptol.* **2018**, *12*, 137–141. [\[CrossRef\]](#)
- Grigoriev, D.; Shpilrain, V. Tropical cryptography II-Extensions by homomorphisms. *Commun. Algebra* **2019**, *47*, 4224–4229. [\[CrossRef\]](#)
- Rudy, D.; Monico, C. Remarks on a Tropical Key Exchange System. *J. Math. Cryptol.* **2021**, *15*, 280–283. [\[CrossRef\]](#)
- Isaac, S.; Kahrobaei, D. A closer look at the tropical cryptography. *Int. J. Comput. Math. Comput. Syst. Theory* **2021**, *6*, 137–142. [\[CrossRef\]](#)
- Wang, G.; Liu, J. An improved diagonal transformation algorithm for the maximum eigenvalue of zero symmetric nonnegative matrices. *Symmetry* **2022**, *14*, 1707. [\[CrossRef\]](#)

18. Zahra, E.; Reza, S.; Donal, O.; Fehaid, S.A. Minimum superstability of stochastic ternary antiderivations in symmetric matrix-valued FB-Algebras and symmetric matrix-valued FC-Algebras. *Symmetry* **2022**, *14*, 2064. [[CrossRef](#)]
19. Alhevaz, A.; Baghipur, M.; Ganie, H.A.; Shang, Y. The generalized distance spectrum of the join of graphs. *Symmetry* **2020**, *12*, 169. [[CrossRef](#)]