Cryptanalysis of Tropical Encryption Scheme Based on Double Key Exchange

Xin Jiang, Huawei Huang* and Geyang Pan

School of Mathematical Sciences, Guizhou Normal University, Guiyang 550025, China
E-mail: 1719084872@qq.com; hwhuang7809@163.com; 1085167081@qq.com
**Corresponding Author*

Received 01 December 2022; Accepted 13 February 2023;
Publication 28 April 2023

Abstract

A tropical encryption scheme is analyzed in this paper, which uses double key exchange protocol (KEP). The key exchange protocol is divided into two stages: The first stage of the key exchange uses matrix power function in a tropical semiring; the obtained shared key at the first phase of the key exchange serves as an input for the second phase. This paper proves that the common secret key of the first key exchange phase can be obtained by solving linear equations, and when the order of the matrix is 50, the time to solve the shared key is less than 1 second. Finally, the common secret key of the second phase can be obtained through KU attack and common secret key of the first key exchange. So the protocol isn't secure.

Keywords: Tropical semiring, key-exchange protocol, tropical linear equations, KU attack.

Journal of Cyber Security and Mobility, Vol. 12_2, 205–220.
doi: 10.13052/jcsm2245-1439.1224

1 Introduction

Modern public key cryptosystems mainly rely on factorization problem [1] and discrete logarithm problem [2, 3]. Shor [4] proposed a quantum algorithm that can solve the above two problems in multiple times on a quantum computer. Therefore, new cryptosystem in the future need to resist quantum attacks. Many cryptologists have designed many different cryptosystems based on different algebraic structures, such as matrix groups [5–8], braid groups [9, 10], inner automorphism groups [11], and ring structures [12], but these schemes have been cracked [13–16]. In 2007, Maze, Monico and Rosenthal proposed the first kind of cryptosystem based on semigroups and semirings [17], which was cracked by Steinwant et al. Atani [18] and Durcheva [19] constructed cryptographic protocols based on semimodules over semirings and idempotent semirings respectively.

Imre Simon discovered the well-known Tropical semiring [20]. The operations $+$ and $\bullet$ in this structure are defined as min(or max) and addition. In recent years, because of the multiplication of tropical semiring is common addition, which greatly improves the computational efficiency, so it is extensively used in various cryptographic schemes. Grigoriev and Shpilrain proved that the problem of solving the systems of min-plus polynomial equations in tropical algebra is NP-hard. And they suggested using tropical semiring to design various key-exchange schemes [21, 22]. The higher powers of tropical matrix shows some patterns, thus Kotov and Ushakov [23] proposed a fairly successful attack on the protocols presented in [21]. In reference [22], the first part of the key has partial order relationship, thus Rudy and Monico [24] exploited simple binary search to break the protocol. (Other successful attacks include [25, 26].) Any Muanalifah, Sergei Sergeev [27] proposed three types of key exchange protocols by using Jones matrix and Line de la Puentela Puente matrix. In addition, Huang, Li published a cryptosystem using multiple exponentiation problem of tropical matrices [28]. Huang, Li and Deng applied tropical circular matrices to construct cryptographic protocols [29].

In this paper, we analyze a tropical encryption scheme based on double key exchange proposed in [30]. Attackers can get the shared key in the first stage of key exchange protocol by solving the tropical linear equations, instead of solving difficult problems in [30]. Then, with the shared key obtained in the first stage as input, the shared key in the second stage can be obtained by KU attack [23].

2 Preliminaries

In this section, we recall some fundamental concepts that are required for understanding the paper.

Definition 2.1 [31] (Semiring) A semiring is a nonempty set R on which operations of addition and multiplication have been defined to satisfy the following conditions.

(1) $(R, +)$ is a commutative monoid with identity element 0;
(2) $(R, \cdot)$ is a monoid with identity element 1_R;
(3) Multiplication distributes over addition from either side;
(4) $0r = 0 = r0$ for all $r \in R$;
(5) $1_R \neq 0$.

If $(R, \cdot)$ is commutative, then the semiring is called a commutative semiring.

Definition 2.2 [20] (Tropical semiring) The nonnegative integer tropical commutative semiring is the set $W = N \cup \{\infty\}$ with two binary compositions $\oplus$ and $\otimes$ as follows:

$$x \oplus y = \min(x, y), \quad x \otimes y = x + y$$

∞ and 0 satisfied the following equations:

$$x \oplus \infty = x, \quad x \otimes \infty = \infty, \quad \forall x \in W,$$
$$x \oplus 0 = 0, \quad x \otimes 0 = x, \quad \forall x \in W$$

It can be easily seen that $(W, \oplus, \otimes)$ is a commutative semiring with addition identity ∞ and multiplication identity 0.

Let $M_n(W)$ be the set of all $n \times n$ matrices over *W*. We can define $\oplus$ and $\otimes$ as follows:

$$(A \oplus B)_{ij} = a_{ij} \oplus b_{ij}, \quad (A \otimes B)_{ij} = \bigoplus_{l=1}^{n} (a_{il} \otimes b_{lj}),$$
$$\forall\, A = (a_{ij}), \quad B = (b_{ij}) \in M_n(W)$$

Definition 2.3 [30] (Tropical polynomial) An expression is called tropical (min) polynomial as follows:

$$p(x) = \bigoplus_{i=1}^{n} a_i \otimes x^{\otimes i}$$

If $p(x) = \bigoplus_{i=1}^{n} a_i \otimes x^{\otimes i}$ is a polynomial and $A \in M_n(W)$, then we can also define $p(A)$ in the following method:

$$p(A) = \bigoplus_{i=1}^{n} a_i \otimes A^{\otimes i}.$$

It is clear that if $p(x)$, $q(x)$ are tropical polynomials, and $A \in M_n(W)$, then

$$p(A) \otimes q(A) = q(A) \otimes p(A)$$

Definition 2.4 [30] (Tropical matrix power function) Let the entries of the base matrix Q be chosen from a (semi)group *G* and the entries of the matrices *X* and *Y* be chosen from the tropical semiring *W*. Then tropical matrix power function is a mapping

$$F_Q(X)\colon Mat(W) \times Mat(G) \to Mat(G)$$

(denoted:$S = {}^{X}Q$) or a mapping

$$F_Q(Y)\colon Mat(G) \times Mat(W) \to Mat(G)$$

(denoted: $P = Q^Y$).

The elements of matrix *S* are computed according to the formula:

$$S_{ij} = \bigotimes_{k=1}^{n} q_{kj}^{\otimes x_{ik}} = \sum_{k=1}^{n} q_{kj} \cdot x_{ik}, \tag{1}$$

and elements of matrix *P* are computed according to the formula:

$$P_{ij} = \bigotimes_{k=1}^{n} q_{ik}^{\otimes y_{kj}} = \sum_{k=1}^{n} q_{ik} \cdot y_{kj} \tag{2}$$

It is worth noting that the operations after the second equal sign in (1) and (2) are the operations on classicial algebra.

Definition 2.5 [29] (circulant matrix) If a matrix *A* has the following form,

$$\begin{pmatrix} a_0 & a_{n-1} & a_{n-2} & \cdots & a_1 \\ a_1 & a_0 & a_{n-1} & \cdots & a_2 \\ a_2 & a_1 & a_0 & \cdots & a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_0 \end{pmatrix},$$

then it is called a circulant matrix.

Lemma 2.1 [30] If matrice X, Y and Z are circulant matrices, then matrices $S = {}^{X}Q$ and $P = Q^{Y}$ are also circulant matrices.

Lemma 2.2 Let X, Y are circulant matrices, then $X \otimes Y = Y \otimes X$.

3 Tropical Encryption Scheme

In this section, we describe the tropical encryption scheme based on double key exchange proposed in [30]. Let *W* be a tropical semiring as above, *S* is the set of circulant matrices over the *W* and *N* is the set of the natural numbers. Alice and Bob publicly agree on circulant matrices Q_1, Q_2, where $Q_1, Q_2 \in S$, and randomly choose matrix *M* whose entries form *N* (Q_1, Q_2, *M* has the same order).

First key exchange protocol phase:

(1) Alice chooses two circulant matrices $A_1, A_2 \in S$ (of the same order as the matrices Q_1, Q_2, *M*) as her private keys. She computes her public key $K_A = {}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes M$ and sends it to Bob;
(2) Bob chooses two circulant matrices $B_1, B_2 \in S$ (of the same order as the matrices Q_1, Q_2, M) as his private keys. He computes his public key $K_B = {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes M$ and sends it to Alice;
(3) Alice computes the common secret key: $K_{AB} = {}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes K_B$;
(4) Bob computes the common secret key: $K_{BA} = {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes K_A$.

It is easy to prove that

$$K_{AB} = {}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes K_B = {}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes M$$
$$= {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes {}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes M = K_{BA},$$

then Alice and Bob finally obtain shared key K_{AB} (or K_{BA}).

Second key exchange protocol phase:

At this stage, the shared secret key K_{AB} obtained is used as the input of the second key exchange phase.

(1) Alice generates random tropical polynomials $p_1(x), p_2(x)$, and computes her public key
$U = p_1(M) \otimes K_{AB} \otimes p_2(M)$ and sends it to Bob.
(2) Bob generates random tropical polynomials $q_1(x), q_2(x)$, and computes his public key
$V = q_1(M) \otimes K_{AB} \otimes q_2(M)$ and sends it to Alice.

(3) Alice computes common secret key: $A = p_1(M) \otimes V \otimes p_2(M)$;
(4) Bob computes common secret key: $B = q_1(M) \otimes U \otimes q_2(M)$;

It is easy to examine that Alice and Bob get common secret key, that is, $A = B$.

$$\begin{aligned} A &= p_1(M) \otimes V \otimes p_2(M) = p_1(M) \otimes q_1(M) \otimes K_{AB} \otimes q_2(M) \otimes p_2(M) \\ &= q_1(M) \otimes p_1(M) \otimes K_{AB} \otimes p_2(M) \otimes q_2(M) \\ &= q_1(M) \otimes U \otimes q_2(M) = B. \end{aligned}$$

Encryption phase:

(1) Bob computes the ciphertext $C = B \oplus T$, where $\oplus$ is bitwise sum modulo 2 of all entries of matrices *B* and *T*, *T* is plaintext encoded in binary form and has the same order of previously selected matrices Q_1, Q_2, *M*, and sends *C* to Alice.

Decryption phase:

(1) Alice decrypts *C* using her decryption key *A* as follows:

$$A \oplus C = A \oplus B \oplus T = A \oplus A \oplus T = T$$
$$(A = B, A \oplus A = 0)$$

4 An Attack on Tropical Encryption Scheme

We can clearly see that the security of the encryption scheme completely depends on key matrices in the key exchange protocol. Firstly, we discuss the first key exchange protocol.

Theorem 4.1 Let Q_1, Q_2, M, K_A, K_B be as above. Suppose circulant matrix *X* satisfying condition: $X \otimes M = K_A$, then shared key K_{AB} can be calculated.

Proof: Now suppose circulant matrix *X* satisfying $X \otimes M = K_A$, then

$$X \otimes K_B = X \otimes {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes M.$$

It is also known from Lemma 2.1 and Lemma 2.2 that

$${}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes X = X \otimes {}^{B_1}Q_1 \otimes {}^{B_2}Q_2, \text{ so}$$

$$X \otimes K_B = X \otimes {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes M = {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes X \otimes M$$
$$= {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes K_A = K_{AB} \qquad \square$$

From Theorem 4.1, an attacker can break the first stage of key exchange protocol, which only needs to solve tropical linear equations. However, it is easy to solve the tropical linear equations, so the attacker can obtain the shared key in the short time. It is easily seen that when select $n \times n$ of matrices, solutions can be found in $O(n^3)$ time,refer to monograph [32, 33] for more details. Next, we use this method to attack the example in the references [30, section 4].

Example 4.1 Suppose

$$Q_1 = \begin{pmatrix} 7 & 13 & 22 \\ 22 & 7 & 13 \\ 13 & 22 & 7 \end{pmatrix}, \quad Q_2 = \begin{pmatrix} 5 & 16 & 25 \\ 25 & 5 & 16 \\ 16 & 25 & 5 \end{pmatrix}, \quad M = \begin{pmatrix} 8 & 2 & 15 \\ 28 & 14 & 13 \\ 3 & 7 & 19 \end{pmatrix}.$$

(1) Alice selects two circulant matrices A_1, A_2 as her private keys:

$$A_1 = \begin{pmatrix} 6 & 30 & 20 \\ 20 & 6 & 30 \\ 30 & 20 & 6 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 10 & 12 & 27 \\ 27 & 10 & 12 \\ 12 & 27 & 10 \end{pmatrix}$$

(2) Alice's public key:

$$\begin{aligned} K_A &= {}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes M \\ &= {}^{\begin{pmatrix} 6 & 30 & 20 \\ 20 & 6 & 30 \\ 30 & 20 & 6 \end{pmatrix}}\begin{pmatrix} 7 & 13 & 22 \\ 22 & 7 & 13 \\ 13 & 22 & 7 \end{pmatrix} \otimes {}^{\begin{pmatrix} 10 & 12 & 27 \\ 27 & 10 & 12 \\ 12 & 27 & 10 \end{pmatrix}} \\ &\quad \begin{pmatrix} 5 & 16 & 25 \\ 25 & 5 & 16 \\ 16 & 25 & 5 \end{pmatrix} \otimes \begin{pmatrix} 8 & 2 & 15 \\ 28 & 14 & 13 \\ 3 & 7 & 19 \end{pmatrix} \\ &= \begin{pmatrix} 1305 & 1239 & 1444 \\ 1444 & 1305 & 1239 \\ 1239 & 1444 & 1305 \end{pmatrix} \otimes \begin{pmatrix} 8 & 2 & 15 \\ 28 & 14 & 13 \\ 3 & 7 & 19 \end{pmatrix} \\ &= \begin{pmatrix} 1267 & 1253 & 1252 \\ 1242 & 1246 & 1258 \\ 1247 & 1241 & 1254 \end{pmatrix} \end{aligned}$$

(3) Bob selects two circulant matrices B_1, B_2 as her private keys:

$$B_1 = \begin{pmatrix} 2 & 10 & 21 \\ 21 & 2 & 10 \\ 10 & 21 & 2 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 15 & 24 & 17 \\ 17 & 10 & 24 \\ 24 & 17 & 10 \end{pmatrix}$$

(4) Bob's public key:

$$\begin{aligned} K_B &= {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes M \\ &= \begin{pmatrix} 1106 & 1165 & 1268 \\ 1268 & 1106 & 1165 \\ 1165 & 1268 & 1106 \end{pmatrix} \otimes \begin{pmatrix} 8 & 2 & 15 \\ 28 & 14 & 13 \\ 3 & 7 & 19 \end{pmatrix} \\ &= \begin{pmatrix} 1114 & 1108 & 1121 \\ 1134 & 1120 & 1119 \\ 1109 & 1113 & 1125 \end{pmatrix}; \end{aligned}$$

(5) Shared key:

$$\begin{aligned} K_{AB} &= {}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes K_B \\ &= \begin{pmatrix} 1305 & 1239 & 1444 \\ 1444 & 1305 & 1239 \\ 1239 & 1444 & 1305 \end{pmatrix} \otimes \begin{pmatrix} 1114 & 1108 & 1121 \\ 1134 & 1120 & 1119 \\ 1109 & 1113 & 1125 \end{pmatrix} \\ &= \begin{pmatrix} 2373 & 2359 & 2358 \\ 2348 & 2352 & 2364 \\ 2353 & 2347 & 2360 \end{pmatrix}; \end{aligned}$$

$$\begin{aligned} K_{BA} &= {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes K_A \\ &= \begin{pmatrix} 1106 & 1165 & 1268 \\ 1268 & 1106 & 1165 \\ 1165 & 1268 & 1106 \end{pmatrix} \otimes \begin{pmatrix} 1267 & 1253 & 1252 \\ 1242 & 1246 & 1258 \\ 1247 & 1241 & 1254 \end{pmatrix} \\ &= \begin{pmatrix} 2373 & 2359 & 2358 \\ 2348 & 2352 & 2364 \\ 2353 & 2347 & 2360 \end{pmatrix} \end{aligned}$$

Attack: Suppose

$$X = \begin{pmatrix} a & c & b \\ b & a & c \\ c & b & a \end{pmatrix},$$

then

$$X \otimes M = \begin{pmatrix} a & c & b \\ b & a & c \\ c & b & a \end{pmatrix} \otimes \begin{pmatrix} 8 & 2 & 15 \\ 28 & 14 & 13 \\ 3 & 7 & 19 \end{pmatrix}$$

$$= \begin{pmatrix} \min(a+8, c+28, b+3) & \min(a+2, c+14, b+7) \\ \min(b+8, a+28, c+3) & \min(b+2, a+14, c+7) \\ \min(c+8, b+28, a+3) & \min(c+2, b+14, a+7) \end{pmatrix.$$

$$\begin{matrix} \min(a+15, c+13, b+19) \\ \min(b+15, a+13, c+19) \\ \min(c+15, b+13, a+19) \end{pmatrix}$$

The following tropical linear equations can be obtained from $X \otimes M = K_A$;

$$\begin{cases} \min(a+8, c+28, b+3) = 1267 \\ \min(a+2, c+14, b+7) = 1253 \\ \min(a+15, c+13, b+19) = 1252 \\ \min(b+8, a+28, c+3) = 1242 \\ \min(b+2, a+14, c+7) = 1246 \\ \min(b+15, a+13, c+19) = 1258 \\ \min(c+8, b+28, a+3) = 1247 \\ \min(c+2, b+14, a+7) = 1241 \\ \min(c+15, b+13, a+19) = 1254 \end{cases}$$

$$\Rightarrow \begin{cases} \min(a-1259, c-1239, b-1264) = 0 \\ \min(a-1251, c-1239, b-1246) = 0 \\ \min(a-1237, c-1239, b-1233) = 0 \\ \min(b-1234, a-1214, c-1239) = 0 \\ \min(b-1244, a-1232, c-1239) = 0 \\ \min(b-1243, a-1245, c-1239) = 0 \\ \min(c-1239, b-1219, a-1244) = 0 \\ \min(c-1239, b-1227, a-1234) = 0 \\ \min(c-1239, b-1241, a-1235) = 0 \end{cases}$$

$$\Rightarrow \begin{cases} a = -\min(-1259, -1251, -1237, -1214, -1232, \\ \qquad -1245, -1244, -1234, -1235) = 1259 \\ b = -\min(-1264, -1246, -1233, -1234, -1244, \\ \qquad -1243, -1219, -1227, -1241) = 1264 \\ \qquad c = 1239 \end{cases}$$

Compute shared key:

$$X \otimes K_B = \begin{pmatrix} 1259 & 1239 & 1264 \\ 1264 & 1259 & 1239 \\ 1239 & 1264 & 1259 \end{pmatrix} \otimes \begin{pmatrix} 1114 & 1108 & 1121 \\ 1134 & 1120 & 1119 \\ 1109 & 1113 & 1125 \end{pmatrix}$$

$$= \begin{pmatrix} 2373 & 2359 & 2358 \\ 2348 & 2325 & 2364 \\ 2325 & 2347 & 2360 \end{pmatrix}$$

The attacker in the second phase of the key exchange protocol can use attack method in [23]. Now, let's describe this attack.

Let matrices *X* and *Y* satisfy the following conditions:

$$X = \bigoplus_{i=0}^{D} x_i \otimes M^{\otimes i}, \quad Y = \bigoplus_{j=0}^{D} y_j \otimes M^{\otimes j}, \quad X \otimes K_{AB} \otimes Y = U$$

with unknown coefficients x_i, y_j. Therefore, to break the protocol, we need to find $x_0, \ldots, x_D, y_0, \ldots, y_D$ such that $\oplus_{i,j=0}^{D} x_i \otimes y_j \otimes V^{ij} = U$, where $V^{ij} = M^{\otimes i} \otimes K_{AB} \otimes M^{\otimes j}$. Then, $\min_{i,j}(x_i + y_j + T_{kl}^{ij}) = 0$ for each $k, l \in [1, n]$. Where $T^{ij} = V^{ij} - U$. Next, compute

$$m_{ij} = \min_{k,l} T_{kl}^{ij}, \quad P_{ij} = \{(k, l) : T_{kl}^{ij} = m_{ij}\}.$$

In the end, attackers find a cover $C \subseteq \{P_{00}, \ldots, P_{DD}\}$ of the set $\{1, 2, \ldots, \mathrm{n}\} \times \{1, 2, \ldots, \mathrm{n}\}$, and satisfy

$$\begin{cases} x_i + y_j = -m_{ij}, & P_{ij} \in C \\ x_i + y_j \geq -m_{ij}, & otherwise \end{cases}$$

is solvable. Refer to the literature [23] for more details about this attack.

The range for entries of matrices is $[0, 10^{10}]$. Table 1 provides the time required to solve *X* under different orders of the matrix. When the order of the

Table 1 Average time to solve X

Order of Matrices	Range for Entries of Matrices	Time to Solve X (sec)
20	$[0, 10^{10}]$	0.001111388
30	$[0, 10^{10}]$	0.003949738
40	$[0, 10^{10}]$	0.010951591
50	$[0, 10^{10}]$	0.021650982

matrix is 50, solving the linear equations needs $O(50^3)$ times, but the attacker only need one solution. It can be clearly seen from Table 1 that obtaining a solution does not exceed 1 second, so the attacker can obtain the shared key in the first phase in a relatively short time. (Experimental platform: Intel(R) Core (TM) i3-1115G4@ 3.00GHz).

5 Conclusion

This paper analyzes the security of tropical encryption scheme based on double key exchange [30] and describes an attack, and the method mainly obtains the shared key of communication parties by solving the linear equations on the tropical semiring. This paper proves that attacker only needs to solve the linear equations to obtain the shared key in the first phase of key exchange protocol, and does not need to solve the difficult problem described in [30]. Table 1 shows that when the order of the matrix is 50, the attacker can obtain the shared key in the second phase in less than 1 second. Then, the shared key in the second stage can be obtained by adopting the KU attack [23]. Thus, the encryption scheme proposed in [30] is cracked.

Future works worth studying include the following:

(1) Try to select other types of matrices to design key exchange protocols based on the difficult problems in literature [30].
(2) Try to study the double-key cryptosystem more deeply.
(3) Combine existing attack methods to analyze other cryptographic systems.

Acknowledgement

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).

References

[1] Rivest R L, Shamir A and Adleman L M. A method for obtaining digital signatures and public-key cryptosystems. Commun, ACM, 21, 120–126, 1978.

[2] Diffie W, Hellman M E, "New directions in cryptography". IEEE Transactions on Information Teory, 22(6), 644–654, 1976.

[3] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inf. Theory, 31, 469–472, 1985.

[4] Shor P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput, 26, 1484–1509, 1997.

[5] Baumslag G, Fine B and Xu X. Cryptosystems using linear groups. Appl. Algebra Eng. Commun. Comput, 17, 205–217, 2006.

[6] Kahrobaei D, Koupparis C and Shpilrain V. Public key exchange using matrices over group rings. Groups-Complex. Cryptol, 5, 97–115, 2013.

[7] Rososhek S K. New practical algebraic public-key cryptosystem and some related algebraic and computational aspects. Appl. Math, 4, 1043–1049, 2013.

[8] Rososhek S K. Modified matrix modular cryptosystems. Br. J. Math. Comput. Sci, 5, 613–636, 2015.

[9] Anshel I, Anshel M and Goldfeld D. An algebraic method for public-key cryptography. Math. Res. Lett, 6, 287–291, 1999.

[10] Garber D. Braid group cryptography. In Braids: Introductory Lectures on Braids, Configurations and Their Applications; World Scientific: Singapore, 329–403, 2010.

[11] Paeng S H, Ha K C, Kim J H, Chee S and Park C. New public key cryptosystem using finite non Abelian groups. In Proceedings of the 21st Annual International Cryptology Conference, Santa Barbara, CA, USA, 19–23 August 2001, Springer: Berlin/Heidelberg, Germany, 470–485, 2001.

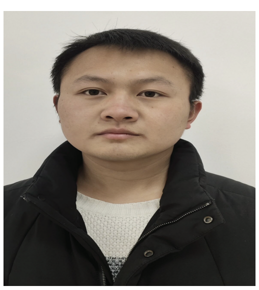
[12] Hoffstein J, Pipher J, Silverman J H. NTRU: A ring-based public key cryptosystem. In Proceedings of the International Algorithmic Number Theory Symposium, Portland, OR, USA, 21–25 June 1998; Springer: Berlin/Heidelberg, Germany, 267–288, 1998.

[13] Eftekhari M. Cryptanalysis of some protocols using matrices over group rings. In Proceedings of the 9th International Conference on Cryptology in Africa, Dakar, Senegal, 24–26 May 2017; Springer: Cham, Switzerland, 223–229, 2017.

[14] Steinwandt R. Loopholes in two public key cryptosystems using the modular group. In Proceedings of the 4th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2001, Cheju Island, Korea, 13–15 February 2001; Springer: Berlin/Heidelberg, Germany, 180–189, 2001.
[15] Hofheinz D, Steinwandt R. A practical attack on some braid group based cryptographic primitives. In Proceedings of the 6th International Workshop on Theory and Practice in Public Key Cryptography, Miami, FL, USA, 6–8 January 2003; Springer: Berlin/Heidelberg, Germany, 187–198, 2003.
[16] Gentry C, Szydlo M. Cryptanalysis of the revised NTRU signature scheme. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, 28 April–2 May 2002; Springer: Berlin/Heidelberg, Germany, 299–320, 2002.
[17] Maze G, Monico C and Rosenthal J. Public Key Cryptography based on semigroup Actions. Adv. Math. Commun, 1, 489–507, 2007.
[18] Atani R E, Atani S E, and Mirzakuchaki S. "Public key cryptography based on semimodules over quotient semirings," International Mathematical Forum, 2(52), 2561–2570, 2007.
[19] Durcheva M. "Public key cryptosystem based on two sided action of different Exotic semirings," International Mathe-matical Forum, 2(52), 2561–2570, 2007.
[20] David S, Bernd S. Tropical Mathematics. Mathematics Magazine, 82(3), 163–173, 2004.
[21] Grigoriev D, Shpilrain V. Tropical cryptography, Communications in Algebra, 42(6): 2624–2632, 2014.
[22] Grigoriev D, Shpilrain V. Tropical cryptography II: Extensions by homomorphis-ms. Communications in Algebra, 47(10): 4224–4229, 2019.
[23] Kotov M, Ushakov A. Analysis of a key exchange protocol based on tropical matrix algebra. Journal of Mathematical Cryptology, 12(3): 137–141, 2018.
[24] Rudy D, Monico C. Remarks on a Tropical Key Exchange System. J. Math. Cryptol, 15, 280–283, 2021.
[25] Isaac S, Kahrobaei D. A closer look at the tropical cryptography. International Journal of Computer Mathematics: Computer Systems Theory, 6 (2):137–42, 2021.

[26] Muanalifah A, Sergeev S. On the tropical discrete logarithm problem and security of a protocol based on tropical semidirect product. Communications in Algebra 49:1–19, 2021.
[27] Muanalifah A, Sergeev S N. Modifying the Tropical Version of Stickel's Key Exchange Protocol. Applications of Mathematics, 65(6). 727–753, 2020.
[28] Huang H, Li C. Tropical Cryptography Based on Multiple Exponentiation Problem of Matrices. Security and Communication Networks, 1–9, 2022.
[29] Huang H, Li C and Deng L. Public-Key Cryptography Based on Tropical Circular Matrices. Applied Sciences, 12. 7401, 2022.
[30] Durcheva M. TrES: Tropical Encryption Scheme Based on Double Key Exchange. European Journal of Information Technologies and Computer Science, 10(24018), 2736–5492, 2022.
[31] Golan J S. Semirings and their Applications. Dordrecht: Kluwer Academic Publishers, Chapter 1–18, 1999.
[32] Butkovi¡ C P. Max-linear Systems: Theory and Algorithms. Springer, London, Springer Monographs in Mathematics, Chapter 3, 2010.
[33] Litvinov G L, Rodionov A Y and Sergeev S N. et al. Universal algorithms for solving the matrix Bellman equations over semirings. Soft Comput 17, 1767–1785, 2013.

Biographies



Xin Jiang received his BS from the Anshun University, Anshun, China in 2020. He is currently a graduate student in the School of Mathematical Sciences of Guizhou Normal University in Guiyang, China. His recent research interests include algebra and cryptography.

Huawei Huang received his BS from the Jiangxi Normal University, Nanchang, China in 2001, MS from the Jiangxi Normal University, Nanchang, China in 2004 and PhD from the Xidian University, Xi'an, China in 2008. He is currently an Associate Professor in the School of Mathematical Sciences, Guizhou Normal University, Guiyang, China. His recent research interests include algebra and cryptography.

Geyang Pan received his BS from the Lingnan Normal University, Zhanjiang, China in 2021. He is currently a graduate student in the School of Mathematical Sciences of Guizhou Normal University in Guiyang, China. His recent research interests include algebra and cryptography.