ANALYSIS OF FOUR PROTOCOLS BASED ON TROPICAL CIRCULANT MATRICES

I. M. BUCHINSKIY, M. V. KOTOV, AND A. V. TREIER

Abstract. Several key exchange protocols based on tropical circulant matrices were proposed in the last two years. In this paper, we show that protocols offered by M. Durcheva [11], by B. Amutha and R. Perumal [2], and by H. Huang, C. Li, and L. Deng [15] are insecure.

1. Introduction

The Diffie–Hellman key exchange algorithm [8] was the first widely used method of exchanging keys safely over an insecure channel. The original implementation of the protocol uses the multiplicative group of integers modulo p. Sidelnikov, Cherepnev, and Yaschenko [31] proposed the following key exchange method based on non-commutative semigroups. Let G be a non-commutative semigroup, H and R be commutative subsemigroups of G, and $W \in G$. These objects are public.

(1) Alice chooses two elements $P_A \in H$ and $Q_A \in R$ as her secret key. She computes $K_A = P_A \cdot W \cdot Q_A$ and sends it to Bob.
(2) Bob chooses two elements $P_B \in H$ and $Q_B \in R$ as his secret key. He computes $K_B = P_B \cdot W \cdot Q_B$ and sends it to Alice.
(3) Alice computes the common secret key $K_{AB} = P_A \cdot K_B \cdot Q_A$.
(4) Bob computes the common secret key $K_{BA} = P_B \cdot K_A \cdot Q_B$.

They share the same key because $P_A \cdot (P_B \cdot W \cdot Q_B) \cdot Q_A = P_B \cdot (P_A \cdot W \cdot Q_A) \cdot Q_B$. Also, a similar idea of using non-abelian groups was offered by Stickel [32].

The success of this method is determined by the choice of G, H, and R. Some examples of groups were analyzed by Sidelnikov, Cherepnev, and Yaschenko [31]. Also, a general analysis in the case of groups was done by Miasnikov and Roman'kov [25, 29].

Grigoriev and Shpilrain [13] suggested using tropical semigroups. There are two reasons for this choice. First, it helps avoid linear algebra attacks. Second, operations can be performed quickly and efficiently. The following G, H, and R were offered in their paper. G is the tropical semiring of square matrices of order n over the min-plus semiring $\mathbb{Z}_{\min,+}$, $W = I_n$, $H = \{p(A) \mid p(x) \in \mathbb{Z}_{\min,+}[x]\}$, and $R = \{q(B) \mid q(x) \in \mathbb{Z}_{\min,+}[x]\}$, where A and B are two non-commuting matrices over $\mathbb{Z}_{\min,+}$. Kotov and Ushakov [20] analyzed this protocol and suggested an attack on it. The key point of their method is the fact that sequences of powers of tropical matrices over the min-plus algebra often display some patterns.

Muanalifah and Sergeev [22] considered protocols with other G, H, and R and analyzed some attacks on them. In one of the protocols, they used the semiring of square matrices of order n over $\mathbb{R}_{\max,+}$ as G, and sets of quasi-polynomials of

Date: October 26, 2023.

Jones matrices [19] as H and R. In the other protocol, they used the same G and sets of Linde–De la Puente matrices [21] as H and R.

Durcheva [10] proposed a protocol where G is a matrix semiring over the max-plus semiring, $H = \{p(A)^m \mid p(x) \in \mathbb{R}_{\max,+}[x]\}$, and $R = \{p(A)^k \mid p(x) \in \mathbb{R}_{\max,+}[x]\}$. The matrix A and the integers m and k are public. Also, Durheva and Trendafilov [12] used the same G, $H = \{A^n \mid n \in \mathbb{N}\}$, and $R = \{B^m \mid m \in \mathbb{N}\}$. Ahmed, Pal, and Mohan [1] showed that these protocols are insecure.

Another interesting class of commuting matrices is circulant matrices. Recently, a few protocols based on these matrices were offered. Huang, Li, and Deng [15] offered a key exchange protocol based on tropical upper-t-circulant matrices. Amutha and Perumal [2] proposed protocols based on tropical lower-t-circulant matrices and tropical anti-t-p-circulant matrices. In this paper, we modify the attack from [20] and [22] and show that these protocols are insecure.

Durcheva [11] offered a new key exchange protocol employing circulant matrices. Jiang, Huang, and Pan [18] demonstrated that this protocol is not secure. This paper shows that it is also insecure when degrees of polynomials are not fixed.

For the sake of completeness, it is worthy of note that another key exchange protocol based on tropical matrix algebras was proposed by Grigoriev and Shpilrain [14]. They suggested using semidirect products to destroy patterns of sequences of powers of matrices which were exploited in the attacks on their first protocol. This protocol was thoroughly analyzed by Isaac and Kahrobaei [17], Muanalifah and Sergeev[23], and Rudy and Monico [30]. Also, Durcheva [9] proposed a key exchange protocol that uses pairs of dual tropical structures. It was shown that this protocol is also insecure by Ahmed, Pal, and Mohan [1] and by Kotov, Treier, and Buchinskiy [4].

For more information on using non-commutative algebraic structures in cryptography, see [24, 26, 28, 29].

The remainder of this paper is structured into four parts. In Section 2, tropical algebras, matrices, and other constructions over tropical algebras are discussed. In Section 3, the description of the protocols that we analyze is given. In Section 4, an attack on the protocols is introduced, and the results of our experiments are presented. The final section offers a conclusion of the work.

2. Tropical algebras

In this section, the tropical algebras, tropical matrices, tropical polynomials, and some other tropical constructions are defined.

The *max-plus algebra* $\mathbb{R}_{\max,+}$ is the set $\mathbb{R} \cup \{-\infty\}$ equipped with the operations $x \oplus y = \max(x, y)$ and $x \otimes y = x + y$. The *min-plus algebra* $\mathbb{R}_{\min,+}$ is the set $\mathbb{R} \cup \{\infty\}$ equipped with the operations $x \oplus y = \min(x, y)$ and $x \otimes y = x + y$. These two algebras are known as tropical algebras. These algebras are semirings, which means they are similar to rings but without the requirement that each element must have an additive inverse. Moreover, they are idempotent and commutative. We denote the unit for $\oplus$ as o, and the unit for $\otimes$ as e: $o = \infty$ and $e = 0$ for the min-plus semiring and $o = -\infty$ and $e = 0$ for the max-plus semiring.

Sometimes $\mathbb{Z}$ instead of $\mathbb{R}$ is used. We denote the corresponding algebras as $\mathbb{Z}_{\max,+}$ and $\mathbb{Z}_{\min,+}$. The tropical algebras have been widely studied and have many applications. For more information, we refer the reader to [5].

Let S be a semiring. The set of all $n \times n$ matrices $Mat_n(S)$ with entries in S can be equipped with addition $\oplus$ and multiplication $\otimes$ as well:

$$(a_{ij}) \oplus (b_{ij}) = (a_{ij} \oplus b_{ij}),$$

$$(a_{ij}) \otimes (b_{ij}) = (a_{i1} \otimes b_{1j} \oplus \cdots \oplus a_{in} \otimes b_{nj}).$$

The obtained set of matrices is also an idempotent semiring.

The identity matrix I has e on the diagonal and o elsewhere, whereas a scalar matrix is a matrix that has $c \in S$ on the diagonal and o elsewhere. Multiplying a matrix by a scalar is just multiplying by the corresponding scalar matrix.

A *circulant* matrix is a matrix of the form

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

It is easy to show that all the circulant matrices of order n form a commutative algebra because the sum and the product of two circulant matrices are circulant, and $A \otimes B = B \otimes A$.

Let t be an integer. A matrix of the form

$$\begin{pmatrix} a_0 & a_{n-1} \otimes t & a_{n-2} \otimes t & \cdots & a_1 \otimes t \\ a_1 & a_0 & a_{n-1} \otimes t & \cdots & a_2 \otimes t \\ a_2 & a_1 & a_0 & \cdots & a_3 \otimes t \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_0 \end{pmatrix} \qquad (2)$$

is called an *upper-t-circulant* matrix of order n [15]. Lower-t-circulant matrices are defined similarly. Let t be an integer. A matrix of the form

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

is called a *lower-t-circulant* matrix of order n [2].

Let p and t be integers. A matrix of the form

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

is called an *anti-t-p-circulant* matrix if $a_k - a_{k+1} = p$ for each k [2].

It is possible to show that all the upper-t-circulant matrices of order n form a commutative semiring. The same is true for lower-t-circulant matrices and for anti-t-p-circulant matrices.

We use the following notation: $Mat_n(S)$ is the set of all square matrices of order n over S, $C_n(S)$ is the set of all circulant matrices of order n, $UC_n(S, t)$ is the set of all upper-t-circulant matrices of order n, $LC_n(S,t)$ is the set of all lower-t-circulant matrces of order n, and $AC_n(S,p,t)$ is the set of all anti-t-p-circulant matrices of order n.

We denote an element of the semiring a raised to the n-th power by $a^{\otimes n}$. It is possible to define the set of polynomials over S. Also, let $A \in Mat_n(S)$ and $p(x) = \bigoplus_{i=0}^{d} p_i \otimes x^{\otimes i}$, then we can define $p(A)$ in the usual way $\bigoplus_{i=0}^{d} p_i \otimes A^{\otimes i}$.

Remark 1. Any circulant matrix (1) can be presented as

$$a_0 \otimes I \oplus a_1 \otimes P \oplus \cdots \oplus a_{n-1} \otimes P^{\otimes n-1}, \tag{3}$$

where

$$P = \begin{pmatrix} o & o & o & \cdots & o & e \\ e & o & o & \cdots & o & o \\ o & e & o & \cdots & o & o \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ o & o & o & \cdots & e & o \end{pmatrix}.$$

Remark 2. Any upper-t-circulant matrix (2) can be presented as (3), where

$$P = \begin{pmatrix} o & o & o & \cdots & o & t \\ e & o & o & \cdots & o & o \\ o & e & o & \cdots & o & o \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ o & o & o & \cdots & e & o \end{pmatrix}.$$

Remark 3. And any lower-t-circulant matrix (2) can be presented as (3), where

$$P = \begin{pmatrix} o & e & o & \cdots & o & o \\ o & o & e & \cdots & o & o \\ o & o & o & \cdots & o & o \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ t & o & o & \cdots & o & o \end{pmatrix}.$$

Remark 4. Now consider an anti-t-p-circlulant matrix (2). From the definition, we have $a_k = a_0 \otimes p^{\otimes k}$ for every k. Thus, we have

$$\begin{pmatrix} t \otimes a_0 & t \otimes a_0 \otimes p^{\otimes n-1} & \cdots & t \otimes a_0 \otimes p^{\otimes 2} & a_0 \otimes p \\ t \otimes a_0 \otimes p & t \otimes a_0 & \cdots & a_0 \otimes p^{\otimes 3} & t \otimes a_0 \otimes p^{\otimes 2} \\ t \otimes a_0 \otimes p^{\otimes 2} & t \otimes a_0 \otimes p & \cdots & t \otimes a_0 \otimes p^{\otimes 4} & t \otimes a_0 \otimes p^{\otimes 3} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ t \otimes a_0 \otimes p^{\otimes n-2} & a_0 \otimes p^{\otimes n-3} & \cdots & t \otimes a_0 & t \otimes a_0 \otimes p^{\otimes n-1} \\ a_0 \otimes p^{\otimes n-1} & t \otimes a_0 \otimes p^{\otimes n-2} & \cdots & t \otimes a_0 \otimes p & t \otimes a_0 \end{pmatrix}.$$

Therefore, every matrix $M \in AC_n(R,p,t)$ can be presented as $a_0 \otimes P$, where

$$P = \begin{pmatrix} t & t \otimes p^{\otimes n-1} & \cdots & t \otimes p^{\otimes 2} & p \\ t \otimes p & t & \cdots & p^{\otimes 3} & t \otimes p^{\otimes 2} \\ t \otimes p^{\otimes 2} & t \otimes p & \cdots & t \otimes p^{\otimes 4} & t \otimes p^{\otimes 3} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ t \otimes p^{\otimes n-2} & p^{\otimes n-3} & \cdots & t & t \otimes p^{\otimes n-1} \\ p^{\otimes n-1} & t \otimes p^{\otimes n-2} & \cdots & t \otimes p & t \end{pmatrix}.$$

Let $A = (a_{ij})$ and $B = (b_{ij})$ be two matrices. The *matrix power function* is defined in the following way [11]:

$$^{A}B = \left(\sum_{k=1}^{n} a_{ik} b_{kj} \right)_{ij} .$$

It is easy to show that if A and B are circulant matrices, then ^{A}B is a circulant matrix as well [11].

3. Protocols

In this section, we give descriptions of the protocols proposed in [11], [2] and [15].

3.1. **Huang, Li, and Deng's protocol.**

Huang, Li, and Deng [15] offered the following key exchange protocol based on tropical upper-t-circulant matrices.

Let R be the min-plus semiring, $n, s, t \in \mathbb{Z}_{>0}$, and $Y \in Mat_n(R) \backslash (UC_n(R, s) \cup UC_n(R, t))$. These numbers, semiring, and matrix are public.

(1) Alice chooses two matrices $P_1 \in UC_n(R, s)$ and $Q_1 \in UC_n(R, t)$. She computes her public key $K_A = P_1 \otimes Y \otimes Q_1$ and sends it to Bob.
(2) Bob chooses two matrices $P_2 \in UC_n(R, s)$ and $Q_2 \in UC_n(R, t)$. He computes his public key $K_B = P_2 \otimes Y \otimes Q_2$ and sends it to Alice.
(3) Alice computes her secret key $K_{AB} = P_1 \otimes K_B \otimes Q_1$.
(4) Bob computes his secret key $K_{BA} = P_2 \otimes K_A \otimes Q_2$.

Alice and Bob end up with the same key $K_{AB} = K_{BA} = K$, which can serve as the secret key.

3.2. **Amutha and Perumal's protocol 1.**

B. Amutha and R. Perumal [2] suggested a similar protocol based on lower-t-circulant matrices.

Let R be the min-plus semiring, $n \in \mathbb{Z}_{>0}$, $s, t \in \mathbb{Z}$, and $Y \in M_n(R)$.

(1) Alice chooses two matrices $P_1 \in LC_n(R, s)$ and $Q_1 \in LC_n(R, t)$. She computes her public key $K_A = P_1 \otimes Y \otimes Q_1$ and sends it to Bob.
(2) Bob chooses two matrices $P_2 \in LC_n(R, s)$ and $Q_2 \in LC_n(R, t)$. He computes his public key $K_B = P_2 \otimes Y \otimes Q_2$ and sends it to Alice.
(3) Alice computes her secret key $K_{AB} = P_1 \otimes K_B \otimes Q_1$.
(4) Bob computes his secret key $K_{BA} = P_2 \otimes K_A \otimes Q_2$.

Then, Alice and Bob share the same key $K_{AB} = K_{BA} = K$.

3.3. **Amutha and Perumal's protocol 2.**

Also, B. Amutha and R. Perumal [2] suggested another protocol based on anti-p-t-circulant matrices.

Let R be the min-plus semiring, $n \in \mathbb{Z}_{>0}$, $s, t, p \in \mathbb{Z}$, and $Y \in M_n(R)$.

(1) Alice chooses two matrices $P_1 \in AC_n(R, p, s)$ and $Q_1 \in AC_n(R, p, t)$. She computes her public key $K_A = P_1 \otimes Y \otimes Q_1$ and sends it to Bob.
(2) Bob chooses two matrices $P_2 \in AC_n(R, p, s)$ and $Q_2 \in AC_n(R, p, t)$. He computes his public key $K_B = P_2 \otimes Y \otimes Q_2$ and sends it to Alice.
(3) Alice computes her secret key $K_{AB} = P_1 \otimes K_B \otimes Q_1$.
(4) Bob computes his secret key $K_{BA} = P_2 \otimes K_A \otimes Q_2$.

It is possible to show that Alice and Bob share the same key $K_{AB} = K_{BA} = K$.

3.4. **Durcheva's protocol.** In [11] M. Durcheva suggested the following key exchange protocol. Let R be the max-plus or min-plus semiring, $Q_1, Q_2 \in C_n(R)$ and $M \in Mat_n(R)$ be public matrices.

The key exchange protocol is as follows.

(1) The first key-exchange phase:
   (a) Alice chooses two matrices $A_1, A_2 \in C_n(R)$ as her secret key. She calculates her public key $K_A = {}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes M$ and sends it to Bob.
   (b) Bob chooses two circulant matrices B_1 and B_2 as his secret key. He calculates his public key $K_B = {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes M$ and sends it to Alice.
   (c) Alice computes the common secret key $K_{AB} = {}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes K_B = {}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes M$.
   (d) Bob computes the common secret key $K_{BA} = {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes K_A = {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes {}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes M$.

(2) The second key-exchange phase:
   (a) Alice chooses two polynomials $p(x), t(x) \in R[x]$. She computes her public matrix $L_A = p(M) \otimes K_{AB} \otimes t(M)$ and sends it to Bob.
   (b) Bob chooses two polynomials $d(x), e(x) \in R[x]$. He computes his public matrix $L_B = d(M) \otimes K_{BA} \otimes e(M)$ and sends it to Alice.
   (c) Alice computes her secret key $L_{AB} = p(M) \otimes L_B \otimes t(M) = p(M) \otimes d(M) \otimes K_{BA} \otimes e(M) \otimes t(M)$.
   (d) Bob computes his secret key $L_{BA} = d(M) \otimes L_A \otimes e(M) = d(M) \otimes p(M) \otimes K_{AB} \otimes t(M) \otimes e(M)$.

It is easy to verify that they share the same keys $L_{AB} = L_{BA} = L$.

4. Attacks

In this section, we recall the attack from [20] and improvements to this attack made by Muanalifah and Sergeev [22]. After that, we show how it can be used to break the protocols described above. In the final subsection, we will present the results of our experiments.

4.1. **The general attack.** To break Grigoriev and Shpilrain's protocol described in the introduction, for an eavesdropper, it is sufficient to find a solution to the following system of equations:

$$X \otimes A = A \otimes X,\ Y \otimes B = B \otimes Y,\ X \otimes Y = K_A. \tag{4}$$

Let $X = \bigoplus_{i=0}^{D} x_i \otimes A^{\otimes i}$ and $Y = \bigotimes_{j=0}^{D} y_j \otimes B^{\otimes j}$. For such matrices, the first and the second equation in (4) are satisfied. Therefore, we need to solve

$$\bigoplus_{i=0,j=0}^{D} x_i \otimes y_j \otimes A^{\otimes i} \otimes B^{\otimes j} = K_A.$$

Denoting $T^{ij} = A^{\otimes i} \otimes B^{\otimes j} - K_A$, we can rewrite this equation as

$$\bigotimes_{i=0,j=0}^{D} x_i \otimes y_j \otimes T^{ij} = E,$$

where E is the matrix of the corresponding size with all entries equal to 0.

Therefore, we have the following system of equations:

$$\min_{ij}(x_i + x_j + T^{ij}_{kl}) = 0 \text{ for each } k, l \in \{1, \ldots, n\}. \tag{5}$$

Solving this system is the main goal of the attack. Compute $m_{ij} = \min_{k,l} T^{ij}_{kl}$ and $P_{ij} = \operatorname{argmin}_{k,l} T^{ij}_{kl}$.

It is possible to show [22] that, to solve (5), we need to find a subset C of $\{0, \ldots, D\} \times \{0, \ldots, D\}$ such that $\bigcup_{(i,j)\in C} P_{ij} = \{1, \ldots, n\} \times \{1, \ldots, n\}$ and values $x_i, y_i, i, j \in \{0, \ldots, D\}$, satisfying

$$\begin{cases} x_i + y_j = -m_{ij} & \text{if } (i,j) \in C, \\ x_i + y_j \geqslant -m_{ij} & \text{otherwise.} \end{cases} \tag{6}$$

Hence, in order to solve the system (5), we can enumerate the minimal covers and then choose that cover that defines the consistent system of equations and inequalities (6).

It is known that finding a minimal set cover problem is one of Karp's 21 problems shown to be NP-complete in 1972. Nevertheless, using some heuristics is sufficient to check a small portion of the covers.

The heuristics are to sort covers using their sizes and to sort covers of the same size using the value of $|\{i \mid \exists j\,(i,j) \in C\}| \cdot |\{j \mid \exists i\,(i,j) \in C\}|$. It helps to reduce the number of tested covers significantly.

Also, note that many P_{ij} often coincide or have no intersections. This fact helps to enumerate all minimal covers by a simple recursive procedure.

Muanalifah and Sergeev [22] noticed that this attack can be applied in the following general situation when the equation is

$$X \otimes W \otimes Y = K_A,$$

$X \in H$ can be presented as a finite sum $X = \bigoplus_i x_i \otimes B_i$, and $Y \in R$ can be presented as a finite sum $Y = \bigoplus_j y_j \otimes C_j$.

Then we have

$$\left(\bigoplus_{i=1}^{D_1} x_i \otimes B_i\right) \otimes W \otimes \left(\bigoplus_{j=1}^{D_1} y_j \otimes C_j\right) = K_A$$

.

Denoting $T^{ij} = B_i \otimes W \otimes C_j - K_A$, we obtain

$$\bigoplus_{i,j} (x_i \otimes y_j) \otimes T^{ij} = E.$$

Therefore, this system of equations has a similar structure and can be solved similarly.

As we can see, the most challenging part is to enumerate covers because the number of covers is usually enormous. We need to enumerate them in order to find a solution at the beginning of our process. We found that the following heuristics and tricks help.

First, as we noticed earlier, many P_{ij} coincide or have no intersections. Thus, we can use a simple recursive procedure to enumerate all the minimal covers $C \subseteq \{P_{ij}\}_{i,j}$.

Second, we sort the covers by size and start from the smallest.

Third, for each cover $(P_{i_1j_1}, P_{i_2j_2}, \ldots, P_{i_kj_k})$, we build the tuple of sets of pairs $(T_1, T_2, \ldots, T_k)$, where $T_l = \{(i,j) \mid P_{ij} = P_{i_lj_l}\}$.

Fourth, if $|T_l| = 1$, then the only pair of this set must be chosen. We form the set of such mandatory pairs M. For the rest, we test each pair (i,j) if $M \cup \{(i,j)\}$ defines a consistent system of equations and inequalities and throw away unsuitable pairs. If we have T_l such that $|T_l| > 1$, then we sort this set using the following weight function

$$w((i,j)) = -\left(\sum_{m\neq l} \frac{\sum_{(p,q)\in T_m}[p=i]}{|T_m|} + 1\right)\cdot\left(\sum_{m\neq l} \frac{\sum_{(p,q)\in T_m}[q=j]}{|T_m|} + 1\right),$$

where $[\cdot]$ is the Iverson bracket.

Fifth, we lazily enumerate elements of the Cartesian product of the sorted and filtered T_l, $l \in 1,\dots,k$. For this, we use a procedure that attempts to yield lighter tuples sooner. We generate chunks of covers and add them to a priority queue Q using the following weight function:

$$w(S) = -\sum_{(i,j)\in S}\left(\Big(\sum_{(p,q)\in S}[i=p]\Big)\cdot\Big(\sum_{(p,q)\in S}[j=q]\Big)\right)^2.$$

Sixth, we take the top element of the priority queue Q and build the corresponding system (6). Finally, the simplex method can be used to determine if this system is consistent. We use the function `optimize.linprog` from the SciPy library. This function is a wrapper of the C++ implementation of the dual revised simplex method [16].

4.2. **Analysis of Huang, Li, and Deng's protocol and Amutha and Perumal's protocols.** Using Remarks 2, 3, and 4, we find that the attack described above is applicable to Huang, Li, and Deng's protocol and Amutha and Perumal's protocols.

4.3. **Analysis of Durcheva's protocol.** An analysis of this protocol was done by Jiang, Huang, and Pan [18]. Here, we want to present some improvements to their attack. Recall the main steps of their attack. For an eavesdropper to break the protocol means to compute L based on Q_1, Q_2, M, K_A, K_B, L_A, and L_B. It can be found in two steps. In the first step, K will be computed. In the second step, L will be computed using K.

An eavesdropper does not have to find A_1 and A_2 in order to compute K, it is sufficient to find a matrix A' satisfying the following conditions

$$K_A = A' \otimes M,$$
$$A' \otimes ({}^{B_1}Q_1 \otimes {}^{B_2}Q_2) = ({}^{B_1}Q_1 \otimes {}^{B_2}Q_2) \otimes A',$$

or to solve a similar system for Bob's public key. If A' satisfies the conditions above, then the product $A' \otimes K_B$ equals A.

The second condition is true automatically if A' is a circulant matrix. The first one is a linear system, and a solution to this system can be easily found [5].

The second key exchange phase can be analyzed as follows. Any polynomial of a matrix A is a finite sum of the powers of the matrix A, but we do not have any upper bound for these powers. So, the attack from [20] cannot be applied here directly. Let us recall the following definition. A sequence of matrices $\{A_i\}_{i=0}^{\infty}$ is called *almost linear periodic* if there exist a period ρ, a factor c, and a defect δ such that for all $i > \delta$ the following equation holds:

$$A_{i+\rho} = (c) + A_i.$$

For sequences of powers of a matrix over tropical algebras, this property has been well studied [3, 6, 7, 27]. Therefore, if A has this property, then we can consider only powers of the matrix A from 0 to $\rho + \delta$ to present all the matrices in $\{p(A) \mid p(x) \in \mathbb{Z}_{\min,+}[x]\}$. Thus, first, we try to compute the defect and period of the matrix M. Second, if it was done, we use the attack described in 4.1.

4.4. **Experiments.** The described attack was implemented in Python [1]. We used the following parameters for our experiments. We ran our experiments for matrices of sizes $5, 10, 25$, and 50. The number of tests for each size is 100. For Durcheva's and Grigoriev and Shpilrain's protocols, elements of randomly generated matrices are in $[0, 10^5]$. For the other protocols, elements of circulant matrices and parameters are in $[-10^5, 10^5]$. The degrees of the generated polynomials are in $[5, 15]$, and the coefficients are in $[-10^5, 10^5]$. The upper bound used in the attack on Durcheva's protocol is 20.

The parameters of the system we used are Python 3.10, Windows 10 Pro 64-bit, 12th Gen Intel(R) Core(TM) i7-12700H 2.70 GHz, 16.0 GB RAM. The success rate is 100% for all the experiments. The running time can be found in Table 1.

Protocol	$n = 5$	$n = 10$	$n = 25$	$n = 50$
Amutha and Perumal's protocol 1	0.38	0.38	0.69	7.16
Amutha and Perumal's protocol 2	0.36	0.34	0.40	0.69
Durcheva's protocol, the second phase	0.37	0.53	2.37	20.75
Grigoriev and Shpilrain's protocol	0.32	0.41	1.71	13.87
Huang, Li, and Deng's protocol	0.29	0.30	0.63	6.63

Table 1. Experimental results of the attack (time in seconds)

5. Conclusion

This paper showed that the protocols described in [11, 2, 15] are insecure. We showed that the attacks from [20] and [22] with some changes can be applied here successfully. The success rate of our attack is 100%. Our analysis can further be used to analyze other protocols based on tropical matrix algebras.

Funding

The research was supported by the Russian Scientific Foundation, project No. 22-11-20019.

References

[1] K. Ahmed, S. Pal, and R. Mohan. "A review of the tropical approach in cryptography". In: *Cryptologia* 47.1 (2023), pp. 63–87. doi: 10.1080/01611194.2021.1994486.

[2] B. Amutha and R. Perumal. "Public key exchange protocols based on tropical lower circulant and anti-circulant matrices". In: *AIMS Math.* 8.7 (2023), pp. 17307–17334. doi: 10.3934/math.2023885.

[3] F. Baccelli et al. *Synchronization and linearity: an algebra for discrete event systems.* John Wiley & Sons Ltd, 1992.

[1] https://github.com/mkotov/tropical3

[4] I. Buchinskiy, M. Kotov, and A. Treier. “An attack on a key exchange protocol based on max-times and min-times algebras”. In: *Indian J. Pure Appl. Math.* (2023). DOI: 10.1007/s13226-023-00469-0.

[5] P. Butkovič. *Max-linear systems: theory and algorithms.* London: Springer, 2010. ISBN: 978-1-84996-298-8. DOI: 10.1007/978-1-84996-299-5.

[6] G. Cohen et al. “A linear-system-theoretic view of discrete-event processes and its use for performance evaluation in manufacturing”. In: *IEEE Trans. Automatic Control* 30.3 (1985), pp. 210–220. DOI: 10.1109/TAC.1985.1103925.

[7] R. Cuninghame-Green. “Lecture notes in economics and mathematical systems”. In: *Minimax algebra.* Vol. 166. Springer-Verlag New York, NY, USA, 1979. DOI: 10.1007/978-3-642-48708-8.

[8] W. Diffie and M. E. Hellman. “New Directions in Cryptography”. In: *IEEE Trans. Inf. Theory* 22.6 (1976), pp. 644–654. DOI: 10.1109/TIT.1976.1055638.

[9] M. I. Durcheva. “An application of different dioids in public key cryptography”. In: *AIP Conf. Proc.* Vol. 1631. AIP. 2014, pp. 336–343. DOI: 10.1063/1.4902495.

[10] M. I. Durcheva. “Public key cryptography with max-plus matrices and polynomials”. In: *AIP Conf. Proc.* Vol. 1570. AIP. 2013, pp. 491–498. DOI: 10.1063/1.4854794.

[11] M. I. Durcheva. “TrES: Tropical Encryption Scheme Based on Double Key Exchange”. In: *Eur. J. Inf. Tech. Comp. Sci.* 2.4 (2022), pp. 11–17. DOI: 10.24018/compute.2022.2.4.70.

[12] M. I. Durcheva and I. D. Trendafilov. “Public key cryptosystem based on max-semirings”. In: *AIP Conf. Proc.* Vol. 1497. AIP. 2012, pp. 357–364. DOI: 10.1063/1.4766805.

[13] D. Grigoriev and V. Shpilrain. “Tropical cryptography”. In: *Comm. Algebra* 42.6 (2014), pp. 2624–2632. DOI: 10.1080/00927872.2013.766827.

[14] D. Grigoriev and V. Shpilrain. “Tropical cryptography II: extensions by homomorphisms”. In: *Comm. Algebra* 47.10 (2019), pp. 4224–4229. DOI: 10.1080/00927872.2019.1581213.

[15] H. Huang, C. Li, and L. Deng. “Public-Key Cryptography Based on Tropical Circular Matrices”. In: *Appl. Sci.* 12.15 (2022), p. 7401. DOI: 10.3390/app12157401.

[16] Q. Huangfu and J. Hall. “Parallelizing the dual revised simplex method”. In: *Mathematical Programming Computation* 10.1 (2018), pp. 119–142. DOI: 10.1007/s12532-017-0130-5.

[17] S. Isaac and D. Kahrobaei. “A closer look at the tropical cryptography”. In: *Int. J. Comput. Math.: Comput. Syst. Theory* 6.2 (2021), pp. 137–142. DOI: 10.1080/23799927.2020.1862303.

[18] X. Jiang, H. Huang, and G. Pan. “Cryptanalysis of Tropical Encryption Scheme Based on Double Key Exchange”. In: *J. Cyber Secur. Mobil.* 12.02 (2023), pp. 205–220. DOI: 10.13052/jcsm2245-1439.1224.

[19] D. Jones. “Special and structured matrices in max-plus algebra”. PhD thesis. University of Birmingham, 2017.

[20] M. Kotov and A. Ushakov. "Analysis of a key exchange protocol based on tropical matrix algebra". In: *J. Math. Cryptol.* 12.3 (2018), pp. 137–141. DOI: 10.1515/jmc-2016-0064.

[21] J. Linde and M. de la Puente. "Matrices commuting with a given normal tropical matrix". In: *Linear Algebra Appl.* 482 (2015), pp. 101–121. DOI: 10.1016/j.laa.2015.04.032.

[22] A. Muanalifah and S. Sergeev. "Modifying the tropical version of Stickel's key exchange protocol". In: *Appl. Math.* 65.6 (2020), pp. 727–753. DOI: 10.21136/AM.2020.0325-19.

[23] A. Muanalifah and S. Sergeev. "On the tropical discrete logarithm problem and security of a protocol based on tropical semidirect product". In: *Comm. Algebra* 50.2 (2022), pp. 861–879. DOI: 10.1080/00927872.2021.1975125.

[24] A. Myasnikov, V. Shpilrain, and A. Ushakov. *Group-based cryptography.* Basel: Birkhäuser, 2008. ISBN: 978-3-7643-8826-3. DOI: 10.1007/978-3-7643-8827-0.

[25] A. G. Myasnikov and V. A. Roman'kov. "A linear decomposition attack". In: *Groups Complexity Cryptology* 7.1 (2015), pp. 81–94. DOI: 10.1515/gcc-2015-0007.

[26] A. G. Myasnikov, V. Shpilrain, and A. Ushakov. *Non-commutative cryptography and complexity of group-theoretic problems.* Vol. 177. Math. Surv. Monogr. Amer. Math. Soc., 2011. ISBN: 978-0-8218-5360-3. DOI: 10.1090/surv/177.

[27] K. Nachtigall and et al. "Powers of matrices over an extremal algebra with applications to periodic graphs". In: *Mathematical Methods of Operations Research* 46.1 (1997), pp. 87–102. DOI: 10.1007/BF01199464.

[28] V. A. Roman'kov. *Algebraic Cryptography.* Omsk: Omsk State University Press, 2013. ISBN: 978-5-7779-1600-6.

[29] V. A. Roman'kov. *Algebraic cryptology.* Omsk: Omsk State University Press, 2020. ISBN: 978-5-7779-2491-9.

[30] D. Rudy and C. Monico. "Remarks on a tropical key exchange system". In: *J. Math. Cryptol.* 15.1 (2021), pp. 280–283. DOI: 10.1515/jmc-2019-0061.

[31] V. M. Sidelnikov, M. A. Cherepnev, and V. V. Yashchenko. "Systems of open distribution of keys on the basis of noncommutative semigroups". In: *Dokl. Math.* 48.2 (1994), pp. 384–386.

[32] E. Stickel. "A new method for exchanging secret keys". In: *ICITA'05.* Vol. 2. IEEE. 2005, pp. 426–430. DOI: 10.1109/ICITA.2005.33.

I. M. Buchinskiy, Sobolev Institute of Mathematics of SB RAS, Omsk, Russia
Email address: buchvan@mail.ru

M. V. Kotov, Sobolev Institute of Mathematics of SB RAS, Omsk, Russia
Email address: matvej.kotov@gmail.com

A. V. Treier, Sobolev Institute of Mathematics of SB RAS, Omsk, Russia
Email address: alexander.treyer@gmail.com