Any Muanalifah; Sergei Sergeev

Modifying the tropical version of Stickel's key exchange protocol

Applications of Mathematics, Vol. 65 (2020), No. 6, 727–753

Persistent URL: `http://dml.cz/dmlcz/148394`

65 (2020) APPLICATIONS OF MATHEMATICS No. 6, 727–753

MODIFYING THE TROPICAL VERSION OF STICKEL'S KEY EXCHANGE PROTOCOL

Any Muanalifah, Sergeĭ Sergeev, Birmingham

Received November 29, 2019. Published online October 27, 2020.

Abstract. A tropical version of Stickel's key exchange protocol was suggested by Grigoriev and Shpilrain (2014) and successfully attacked by Kotov and Ushakov (2018). We suggest some modifications of this scheme that use commuting matrices in tropical algebra and discuss some possibilities of attacks on these new modifications. We suggest some simple heuristic attacks on one of our new protocols, and then we generalize the Kotov and Ushakov attack on tropical Stickel's protocol and discuss the application of that generalized attack to all our new protocols.

Keywords: Stickel's protocol; tropical algebra; cryptography; commuting matrices

MSC 2020: 15A80, 94A60

1. Introduction

Tropical (or max-plus) semiring is the set $\mathbb{R}_{\max} = \mathbb{R} \cup \{-\infty\}$ equipped with the operations of tropical addition $a \oplus b = \max\{a, b\}$ and multiplication $a \otimes b = a + b$. Note that the tropical addition is not invertible, but the multiplication is a group operation. The multiplicative inverse of $a \in \mathbb{R}$ equals $-a$, and will be commonly denoted by a^-. The operations of tropical addition and multiplication are extended to matrices and vectors in the usual way.

Tropical algebra is a semiring, which means in particular that the addition operation does not admit inverses. Furthermore, the class of invertible matrices in this algebra is very scarce and the matrix inversion cannot be used by the attacker. For this reason, Grigoriev and Shpilrain [2] suggested the tropical algebra as a platform to modify Stickel's protocol. One of their ideas is that using the tropical algebra instead of the classical algebra is promising since matrices in the tropical algebra

The research has been supported by EPSRC Grant EP/P019676/1.

DOI: 10.21136/AM.2020.0325-19

are usually not invertible and the decomposition problem cannot be simplified in general. Kotov and Ushakov demonstrated the weakness of Stickel's key exchange in the tropical scheme by showing that they can attack it successfully without having to solve any "tough" problem [5].

The main idea of this paper is to consider some modifications of Stickel's protocol using classes of commuting matrices other than matrix powers or matrix polynomials. In one of the cases that we consider, the use of a different class of commuting matrices allows us to share less information with the attacker. This seems to be quite promising, however in this case we can also construct a simple and rather successful heuristic attack on the protocol. We also show that the ideas of the Kotov-Ushakov attack apply to all protocols that we construct, thus leading to an appropriate generalized version of this attack that can be specialized to a variety of protocols.

The paper is organized as follows. In Section 2, we start with some basic definitions and key notions of tropical matrix algebra. In Section 3, we introduce two new classes of commuting matrices in the tropical algebra. One of them, based on the work of Jones [4] on the roots of some special tropical matrices, extends the notions of matrix powers and polynomials for such matrices, and the other extends a class of commuting matrices found by Linde and de la Puente [6]. In Section 4, we introduce new protocols using these new classes of commuting matrices. Then, in Section 5, we recall the Kotov-Ushakov attack [5] on the tropical Stickel protocol, prove that it actually works, extend it to one of our new protocols and analyze its performance in practice. In Section 6, we construct some heuristic attacks on another protocol which we introduced before, and construct a generalized version of the Kotov-Ushakov attack which applies to all our new protocols.

2. Elements of tropical algebra

Let us start by introducing some basic definitions. By $[m]$ and $[n]$ we denote $\{1, \ldots, m\}$ and $\{1, \ldots, n\}$.

Definition 2.1 (Tropical matrix addition and multiplication). For $c \in \mathbb{R}_{\max}$ and $A \in \mathbb{R}_{\max}^{m \times n}$ we define $c \otimes A$ by

$$(c \otimes A)_{ij} = c \otimes a_{ij} \quad \forall\, i \in [m],\ \forall\, j \in [n].$$

For two matrices $A = (a_{ij}) \in \mathbb{R}_{\max}^{m \times n}$ and $B = (b_{ij}) \in \mathbb{R}_{\max}^{m \times n}$, we define $A \oplus B$ by

$$(A \oplus B)_{ij} = a_{ij} \oplus b_{ij} \quad \forall\, i \in [m],\ \forall\, j \in [n].$$

For a matrix $A = (a_{ij}) \in \mathbb{R}_{\max}^{m\times p}$ and a matrix $B = (b_{ij}) \in \mathbb{R}_{\max}^{p\times n}$, we define $A \otimes B \in \mathbb{R}_{\max}^{m\times n}$ as the matrix with entries

$$(A \otimes B)_{ij} = \bigoplus_{k=1}^{p} a_{ik} \otimes b_{kj} \quad \forall\, i \in [m],\ \forall\, j \in [n].$$

The neutral element with respect to matrix multiplication can be characterized as follows.

Definition 2.2 (Identity matrix)**.** The matrix $I \in \mathbb{R}_{\max}^{n\times n}$ is called a *tropical identity matrix* if its entries are

$$I_{ij} = \begin{cases} 0, & \text{if } i = j, \\ -\infty, & \text{if } i \neq j, \end{cases}$$

for $i, j \in [n]$.

In other words, all diagonal entries of a tropical identity matrix are equal to 0 and all off-diagonal entries are equal to $-\infty$.

The tropical identity matrix $I \in \mathbb{R}_{\max}^{n\times n}$ satisfies $A \otimes I = I \otimes A = A$ for all $A \in \mathbb{R}_{\max}^{n\times n}$, and it is a special case of the following concept.

Definition 2.3 (Tropical diagonal matrices)**.** A matrix $D \in \mathbb{R}_{\max}^{n\times n}$ is called a *tropical diagonal matrix*, if

$$D_{ij} = \begin{cases} d_i, & \text{if } i = j, \\ -\infty, & \text{if } i \neq j, \end{cases}$$

for some $d_i \in \mathbb{R}_{\max}$ and $i, j \in [n]$. We also denote $D = \operatorname{diag}(d_1, \ldots, d_n)$.

Diagonal matrices with finite diagonal entries are invertible: for any $D = \operatorname{diag}(d_1, \ldots, d_n)$ with $d_i \in \mathbb{R}$ for $i \in [n]$, the inverse is $D^- = \operatorname{diag}(d_1^-, \ldots, d_n^-)$, such that $D^- \otimes D = D \otimes D^- = I$. Diagonal matrices with finite entries form an abelian group. Another important group of invertible matrices consists of tropical permutation matrices. For a permutation σ of $\{1, \ldots, n\}$, the corresponding tropical permutation matrix P^σ is defined by

$$P_{ij}^\sigma = \begin{cases} 0, & j = \sigma(i), \\ -\infty, & \text{otherwise.} \end{cases}$$

Products of tropical diagonal and tropical permutation matrices are called tropical monomial matrices. The group of tropical monomial matrices is precisely the group of all invertible matrices in tropical matrix algebra (e.g., [1] Theorem 1.1.3).

Any matrix over $\mathbb{R}_{\max}$ can be written as a tropical linear combination of tropical elementary matrices.

Definition 2.4 (Elementary matrices). Let $E^{ij} \in \mathbb{R}_{\max}^{n\times n}$ be a matrix with entries

$$(E^{ij})_{kl} = \begin{cases} 0, & \text{if } k = i,\ l = j, \\ -\infty, & \text{otherwise,} \end{cases}$$

for $i, j \in \{1, \ldots, n\}$ and $k, l \in \{1, \ldots, n\}$.

Any matrix of this form is called a *tropical elementary matrix.*

Let us now consider the tropical matrix powers.

Definition 2.5 (Matrix powers).

$$A^{\otimes k} = \underbrace{A \otimes A \otimes \ldots \otimes A}_{k}.$$

Tropical matrix powers are a natural extension of scalar tropical powers:

$$a^{\otimes k} = \underbrace{a \otimes a \ldots \otimes a}_{k} = \underbrace{a + \ldots + a}_{k} = k \times a \quad \forall\, a \in \mathbb{R}_{\max},\ k \in \mathbb{N}.$$

Also note that scalar tropical matrix powers can be easily defined for arbitrary real exponents:

$$a^{\otimes r} = r \times a, \quad r \in \mathbb{R}.$$

Furthermore, we can also consider tropical polynomials.

Definition 2.6 (Polynomials). Tropical polynomial is a function of the form

$$x \mapsto p(x) = \bigoplus_{k=0}^{d} a_k \otimes x^{\otimes k},$$

where $a_k \in \mathbb{R}_{\max}$ for $k = 0, 1, \ldots, d$.

Here x can be a scalar or a square matrix of any dimension. As in the usual algebra, any two tropical matrix powers or polynomials of the same matrix commute, and therefore they can be used to build a tropical version of Stickel's protocol.

Using the tropical matrix powers we can define a tropical analogue of $(I - A)^{-1}$.

Definition 2.7 (Kleene stars). Suppose $A \in \mathbb{R}_{\max}^{n\times n}$. Then denote

$$A^* = I \oplus A \oplus A^{\otimes 2} \oplus \ldots$$

If this series converges, then it is called the Kleene star of A.

The Kleene stars can be characterized, by the following well-known result, as idempotents with all diagonal entries equal to 0.

Proposition 2.1 (e.g., [1]). *Let $A \in \mathbb{R}_{\max}^{n\times n}$. Then $A = B^*$ if and only if $A = A^{\otimes 2}$ and $a_{ii} = 0$ for all i.*

3. Two classes of commuting matrices

3.1. Jones matrices. Tropical polynomials are used in the tropical version of Stickel's protocol suggested by Grigoriev and Shpilrain. We now describe a special kind of matrices considered by Jones [4], for which the notion of polynomial can be extended.

Definition 3.1 (Jones matrices). Let $A = (a_{ij})$ be an $n \times n$ tropical matrix which satisfies the following property:

$$a_{ij} \otimes a_{jk} \leqslant a_{ik} \otimes a_{jj} \quad \forall\, i, j, k \in [n]. \tag{3.1}$$

We call A a Jones matrix.

Notice that any Kleene star $A \in \mathbb{R}_{\max}^{n\times n}$ is a Jones matrix where $a_{jj} = 0$ for all $j \in [n]$ and (3.1) reduces to $a_{ij} \otimes a_{jk} \leqslant a_{ik}$ for all $i, j, k \in [n]$.

We will consider the following operation:

Definition 3.2 (Deformation). Let $A = (a_{ij})$ be a Jones matrix and $\alpha \in \mathbb{R}$. The matrix $A^{(\alpha)} = (a_{ij}^{(\alpha)})$ defined by

$$a_{ij}^{(\alpha)} = a_{ij} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)} \quad \forall\, i, j \in [n], \tag{3.2}$$

is called a *deformation* of A.

The proof techniques of the following two theorems are very close to those in Jones [4]. However, the statements were not explicitly stated and proved in that work.

The next theorem shows that the class of Jones matrices is stable under deformations for $\alpha \leqslant 1$.

Theorem 3.1. *If A is a Jones matrix, then $A^{(\alpha)}$ is also a Jones matrix for any $\alpha \leqslant 1$.*

P r o o f. We have for all i, j, k that

$$a_{ij}^{(\alpha)} \otimes a_{jk}^{(\alpha)} = a_{ij} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)} \otimes a_{jk} \otimes (a_{jj} \oplus a_{kk})^{\otimes(\alpha-1)},$$
$$a_{ik}^{(\alpha)} \otimes a_{jj}^{(\alpha)} = a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\alpha-1)} \otimes a_{jj}^{\otimes\alpha}.$$

Hence, the inequality which we want to prove is

$$a_{ij} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)} \otimes a_{jk} \otimes (a_{jj} \oplus a_{kk})^{\otimes(\alpha-1)} \leqslant a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\alpha-1)} \otimes a_{jj}^{\otimes\alpha}. \tag{3.3}$$

Multiplying both sides by $(a_{ii} \oplus a_{jj})^{\otimes(1-\alpha)} \otimes (a_{jj} \oplus a_{kk})^{\otimes(1-\alpha)} \otimes (a_{ii} \oplus a_{kk})^{\otimes(1-\alpha)}$, we obtain that (3.3) is equivalent to

$$a_{ij} \otimes a_{jk} \otimes (a_{ii} \oplus a_{kk})^{\otimes(1-\alpha)} \leqslant a_{ik} \otimes a_{jj}^{\otimes\alpha} \otimes (a_{ii} \oplus a_{jj})^{\otimes(1-\alpha)} \otimes (a_{jj} \oplus a_{kk})^{\otimes(1-\alpha)}. \tag{3.4}$$

To prove (3.4) we observe that

$$\begin{aligned} a_{ij} \otimes a_{jk} \otimes (a_{ii} \oplus a_{kk})^{\otimes(1-\alpha)} &= a_{ij} \otimes a_{jk} \otimes (a_{ii}^{\otimes(1-\alpha)} \oplus a_{kk}^{\otimes(1-\alpha)}) \\ &\leqslant a_{ik} \otimes a_{jj} \otimes (a_{ii}^{\otimes(1-\alpha)} \oplus a_{kk}^{\otimes(1-\alpha)}) \\ &= a_{ik} \otimes a_{jj} \otimes a_{ii}^{\otimes(1-\alpha)} \oplus a_{ik} \otimes a_{jj} \otimes a_{kk}^{\otimes(1-\alpha)} \end{aligned} \tag{3.5}$$

and that

$$(a_{ii} \oplus a_{jj})^{\otimes(1-\alpha)} \otimes (a_{jj} \oplus a_{kk})^{\otimes(1-\alpha)} \geqslant a_{ii}^{\otimes(1-\alpha)} a_{jj}^{\otimes(1-\alpha)},$$
$$(a_{ii} \oplus a_{jj})^{\otimes(1-\alpha)} \otimes (a_{jj} \oplus a_{kk})^{\otimes(1-\alpha)} \geqslant a_{jj}^{\otimes(1-\alpha)} a_{kk}^{\otimes(1-\alpha)},$$

which implies

$$\begin{aligned} &a_{ik} \otimes a_{jj}^{\otimes\alpha} (a_{ii} \oplus a_{jj})^{\otimes(1-\alpha)} \otimes (a_{jj} \oplus a_{kk})^{\otimes(1-\alpha)} \\ &\geqslant a_{ik} \otimes a_{jj}^{\otimes\alpha} (a_{ii}^{\otimes(1-\alpha)} a_{jj}^{\otimes(1-\alpha)} \oplus a_{jj}^{\otimes(1-\alpha)} a_{kk}^{\otimes(1-\alpha)}) \\ &= a_{ik} \otimes a_{jj} \otimes a_{ii}^{\otimes(1-\alpha)} \oplus a_{ik} \otimes a_{jj} \otimes a_{kk}^{\otimes(1-\alpha)}. \end{aligned} \tag{3.6}$$

Combining (3.5) and (3.6) yields (3.4). □

Note that in Theorem 3.1 α can be negative.

Matrix deformations do not always commute, as the following counterexample shows.

E x a m p l e 3.1. Let us consider the matrix $A = \begin{bmatrix} 0 & 1 & -1 \\ -1 & 0 & -2 \\ -1 & 0 & -2 \end{bmatrix}$. Then we have:

$$A^{(-2/3)} = \begin{bmatrix} 0 & 1 & -1 \\ -1 & 0 & -2 \\ -1 & 0 & \frac{4}{3} \end{bmatrix} \quad \text{and} \quad A^{(-4/5)} = \begin{bmatrix} 0 & 1 & -1 \\ -1 & 0 & -2 \\ -1 & 0 & \frac{8}{5} \end{bmatrix},$$

$$A^{(-2/3)} \otimes A^{(-4/5)} = \begin{bmatrix} 0 & 1 & \frac{3}{5} \\ -1 & 0 & -\frac{2}{5} \\ \frac{1}{3} & \frac{4}{3} & \frac{44}{15} \end{bmatrix}, \quad \text{and} \quad A^{(-4/5)} \otimes A^{(-2/3)} = \begin{bmatrix} 0 & 1 & \frac{1}{3} \\ -1 & 0 & -\frac{2}{3} \\ \frac{3}{5} & \frac{8}{5} & \frac{44}{15} \end{bmatrix}.$$

We can see that $A^{(-2/3)} \otimes A^{(-4/5)} \neq A^{(-4/5)} \otimes A^{(-2/3)}$.

Thus for $\alpha, \beta < 0$ we have $A^{(\alpha)} \otimes A^{(\beta)} \neq A^{(\beta)} \otimes A^{(\alpha)}$ in general. However, we can obtain the following result.

Theorem 3.2. *For any $\alpha, \beta \in \mathbb{R}$ such that $0 \leqslant \alpha \leqslant 1$, $0 \leqslant \beta \leqslant 1$ and $0 \leqslant \alpha + \beta \leqslant 1$, let A be a Jones matrix. Then we have $A^{(\alpha)} \otimes A^{(\beta)} = A^{(\beta)} \otimes A^{(\alpha)} = A^{(\alpha+\beta)}$.*

P r o o f. It suffices to prove that $A^{(\alpha)} \otimes A^{(\beta)} = A^{(\alpha+\beta)}$, i.e., that

$$\bigoplus_{j=1}^{n} a_{ij} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)} \otimes a_{jk} \otimes (a_{jj} \oplus a_{kk})^{\otimes(\beta-1)} = a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\alpha+\beta-1)}. \tag{3.7}$$

We have

$$\begin{aligned} &\bigoplus_{j=1}^{n} a_{ij} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)} \otimes a_{jk} \otimes (a_{jj} \oplus a_{kk})^{\otimes(\beta-1)} \\ &\quad = a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\alpha-1)} a_{kk}^{\otimes\beta} \oplus a_{ii}^{\otimes\alpha} \otimes a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\beta-1)} \\ &\quad\quad \oplus \bigoplus_{j \notin \{i,k\}} a_{ij} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)} \otimes a_{jk} \otimes (a_{jj} \oplus a_{kk})^{\otimes(\beta-1)}. \end{aligned} \tag{3.8}$$

Let us analyze the first two terms. For $a_{ii} \geqslant a_{kk}$ we obtain

$$\begin{aligned} &a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\alpha-1)} \otimes a_{kk}^{\otimes\beta} \oplus a_{ii}^{\otimes\alpha} \otimes a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\beta-1)} \\ &\quad = a_{ik} \otimes a_{kk}^{\otimes\beta} \otimes a_{ii}^{\otimes(\alpha-1)} \oplus a_{ik} \otimes a_{ii}^{\otimes(\alpha+\beta-1)} = a_{ik} \otimes a_{ii}^{\otimes(\alpha+\beta-1)} \\ &\quad = a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\alpha+\beta-1)}. \end{aligned} \tag{3.9}$$

The remaining case $a_{ii} \leqslant a_{kk}$ is treated similarly. As these two terms already yield the required expression $a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\alpha+\beta-1)}$, it remains to prove that the remaining terms do not exceed it. Since

$$\begin{aligned} &a_{ij} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)} \otimes a_{jk} \otimes (a_{jj} \oplus a_{kk})^{\otimes(\beta-1)} \\ &\quad \leqslant a_{ik} \otimes a_{jj} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)} \otimes (a_{jj} \oplus a_{kk})^{\otimes(\beta-1)}, \end{aligned}$$

it remains to show that

$$a_{jj} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)} (a_{jj} \oplus a_{kk})^{\otimes(\beta-1)} \leqslant (a_{ii} \oplus a_{kk})^{\otimes(\alpha+\beta-1)}, \tag{3.10}$$

which is equivalent to

$$a_{jj} \leqslant (a_{ii} \oplus a_{kk})^{\otimes(\alpha+\beta-1)}(a_{ii} \oplus a_{jj})^{\otimes(1-\alpha)}(a_{jj} \oplus a_{kk})^{\otimes(1-\beta)}. \tag{3.11}$$

If $a_{ii} \geqslant a_{kk}$, then we have

$$\begin{aligned}
&(a_{ii} \oplus a_{kk})^{\otimes(\alpha+\beta-1)} \otimes (a_{ii} \oplus a_{jj})^{\otimes(1-\alpha)} \otimes (a_{jj} \oplus a_{kk})^{\otimes(1-\beta)} \\
&\quad = a_{ii}^{\otimes(\alpha+\beta-1)} \otimes (a_{ii} \oplus a_{jj})^{\otimes(1-\alpha-\beta)} \otimes (a_{ii} \oplus a_{jj})^{\otimes\beta} \otimes (a_{jj} \oplus a_{kk})^{\otimes(1-\beta)} \\
&\quad \geqslant a_{ii}^{\otimes(\alpha+\beta-1)} \otimes (a_{ii} \oplus a_{jj})^{\otimes(1-\alpha-\beta)} \otimes a_{jj} \geqslant a_{jj}.
\end{aligned}$$

For the remaining case $a_{kk} \geqslant a_{ii}$ the same holds by symmetry. $\square$

In particular, $A^{(0)}$ is an idempotent and plays the role of unity for $A^{(\alpha)}$ for $0 \leqslant \alpha \leqslant 1$.

Corollary 3.1. *Let A be a Jones matrix. Then $A^{(0)}$ satisfies $A^{(\alpha)} \otimes A^{(0)} = A^{(0)} \otimes A^{(\alpha)} = A^{(\alpha)}$ for all $0 \leqslant \alpha \leqslant 1$.*

We also obtain the following result of Jones [4].

Corollary 3.2. *Let A be a Jones matrix. Then $A^{(k/l)} = (A^{(1/l)})^{\otimes k}$ holds for any integer $l > 0$ and integer k, $1 \leqslant k \leqslant l$.*

Proof. We use a simple induction: if $A^{(k/l)} = (A^{(1/l)})^{\otimes k}$, then $A^{(k+1/l)} = A^{(k/l)} \otimes A^{(1/l)} = (A^{(1/l)})^{\otimes k} \otimes A^{(1/l)} = (A^{(1/l)})^{\otimes(k+1)}$. $\square$

Now we are able to extend the commutativity to all α and β from the unit interval $[0,1]$.

Theorem 3.3. *If A is a Jones matrix, then $A^{(\alpha)} \otimes A^{(\beta)} = A^{(\beta)} \otimes A^{(\alpha)}$ for any α and β such that $0 \leqslant \alpha \leqslant 1$ and $0 \leqslant \beta \leqslant 1$.*

Proof. First consider the case of rational $\alpha = k_1/l_1$ and $\beta = k_2/l_2$. Then $\alpha = k_1 l_2/(l_1 l_2)$ and $\beta = k_2 l_1/(l_1 l_2)$. Then $A^{(\alpha)} = A^{(k_1 l_2/(l_1 l_2))} = (A^{(1/(l_1 l_2))})^{\otimes k_1 l_2}$ and $A^{(\beta)} = (A^{(1/(l_1 l_2))})^{\otimes k_2 l_1}$, so $A^{(\alpha)} \otimes A^{(\beta)} = A^{(\beta)} \otimes A^{(\alpha)}$ since both $A^{(\alpha)}$ and $A^{(\beta)}$ are powers of $A^{(1/(l_1 l_2))}$. The claim follows for any real α and β in $[0,1]$, since rational numbers are dense on the real line and since the tropical arithmetic operations are continuous. $\square$

We now discuss a connection between Kleene stars and Jones matrices. It helps us to construct Jones matrices in practice. The key observations are that 1) the set of Jones matrices is stable under scaling by diagonal matrices, 2) any Kleene star is a Jones matrix.

Proposition 3.1. *Let A be a Jones matrix and D and F be arbitrary diagonal matrices. Then $D \otimes A \otimes F$ is also a Jones matrix.*

P r o o f. Let $A \in \mathbb{R}^{n\times n}_{\max}$, $D = \operatorname{diag}(d_1, \ldots, d_n)$ and $F = \operatorname{diag}(f_1 \ldots, f_n)$. The inequality $a_{ij} \otimes a_{jk} \leqslant a_{ik} \otimes a_{jj}$ is equivalent to

$$d_i \otimes a_{ij} \otimes f_j \otimes d_j \otimes a_{jk} \otimes f_k \leqslant d_i \otimes a_{ik} \otimes f_k \otimes d_j \otimes a_{jj} \otimes f_j. \tag{3.12}$$

Observing that the entries of $B = D \otimes A \otimes F$ are equal to $b_{ij} = d_i \otimes a_{ij} \otimes f_j$ for all i and j, we obtain that (3.12) is the same as $b_{ij} \otimes b_{jk} \leqslant b_{ik} \otimes b_{jj}$. □

As any Kleene star is a Jones matrix, we have the following immediate corollary. It shows how Kleene stars can be used to construct Jones matrices.

Corollary 3.3. *Let A be a Kleene star and D and F be arbitrary diagonal matrices. Then $D \otimes A$, $A \otimes F$, and $D \otimes A \otimes F$ are Jones matrices.*

The other way around, if we have a Jones matrix with finite diagonal entries, then by means of an appropriate scaling it can be transformed to a Kleene star.

Proposition 3.2. *Let $B \in \mathbb{R}^{n\times n}_{\max}$ be a Jones matrix with finite diagonal entries. Then*

(i) *for $D = \operatorname{diag}(b_{11}^{-}, \ldots, b_{nn}^{-})$, $A_1 = B \otimes D$ and $A_2 = D \otimes B$ are Kleene stars;*
(ii) *for $D = \operatorname{diag}(b_{11}^{\otimes -1/2}, \ldots, b_{nn}^{\otimes -1/2})$, $A = D \otimes B \otimes D$ is a Kleene star.*

P r o o f. The Kleene star inequality $a_{ij} \otimes a_{jk} \leqslant a_{ik}$ is a special case of (3.1) for $a_{ii} = 0$. By Proposition 3.1, matrices A_1, A_2 and A satisfy (3.1). Then it suffices to observe that all diagonal entries of these matrices are equal to 0. □

3.2. Linde-de la Puente matrices. Let us consider the following set of matrices, which extends the set of matrices considered by Linde and de la Puente [6].

Definition 3.3 (Linde-de la Puente matrices). For arbitrary real numbers $r \leqslant 0$ and $k \geqslant 0$, we denote by $[2r, r]_n^k$ the set of matrices $A \in \mathbb{R}^{n\times n}_{\max}$ such that $a_{ii} = k$ for all $i \in [n]$ and $a_{ij} \in [2r, r]$ for $i, j \in [n]$ and $i \neq j$. Matrices of this form will be called *Linde-de la Puente matrices.*

We now show that any two matrices of this kind commute.

Theorem 3.4. *Let $A \in [2r, r]_n^{k_1}$, $B \in [2s, s]_n^{k_2}$ for any $r, s \leqslant 0$ and $a_{ii} = k_1 \geqslant 0$, $b_{ii} = k_2 \geqslant 0$. Then*

$$A \otimes B = B \otimes A = k_2 \otimes A \oplus k_1 \otimes B.$$

P r o o f. For all i, j we have

$$(3.13) \qquad (A \otimes B)_{ij} = a_{ii} \otimes b_{ij} \oplus a_{ij} \otimes b_{jj} \oplus \bigoplus_{p \notin \{i,j\}} a_{ip} \otimes b_{pj}$$
$$= k_1 \otimes b_{ij} \oplus k_2 \otimes a_{ij} \oplus \bigoplus_{p \notin \{i,j\}} a_{ip} \otimes b_{pj}.$$

We now argue that $a_{ip} \otimes b_{pj} \leqslant k_1 \otimes b_{ij} \oplus k_2 \otimes a_{ij}$. Indeed,

$$a_{ip} + b_{pj} \leqslant r + s \leqslant \max(2r, 2s) \leqslant \max(a_{ij}, b_{ij}) \leqslant \max(k_1 + b_{ij}, k_2 + a_{ij}).$$

Note that we used the well-known inequality $(r+s)/2 \leqslant \max(r, s)$. Then we obtain:

$$(3.14) \qquad (A \otimes B)_{ij} = k_1 \otimes b_{ij} \oplus a_{ij} \otimes k_2 \oplus \bigoplus_{p \notin \{i,j\}} a_{ip} \otimes b_{pj}$$
$$= k_1 \otimes b_{ij} \oplus a_{ij} \otimes k_2 = (k_2 \otimes A \oplus k_1 \otimes B)_{ij} = (B \otimes A)_{ij},$$

which shows the claim. □

Note that Linde and de la Puente obtained a special case of this result, for $s = r$ and $k_1 = k_2 = 0$.

We also observe the following commutativity property.

Theorem 3.5. *Let $A \in [2a, a]_n^k$ with $a \leqslant 0$ and $B = (b_{ij}) \in \mathbb{R}_{\max}^{n \times n}$. If $0 \leqslant b_{ij} \leqslant k$ for all $i, j \in [n]$, then $A \otimes B = B \otimes A$.*

P r o o f. For all i, j we have

$$(3.15) \qquad (A \otimes B)_{ij} = a_{ii} \otimes b_{ij} \oplus a_{ij} \otimes b_{jj} \oplus \bigoplus_{p \notin \{i,j\}} a_{ip} \otimes b_{pj} = k \otimes b_{ij},$$

since $a \leqslant 0 \leqslant b_{ij} \leqslant k$. Similarly, for all i and j

$$(3.16) \qquad (B \otimes A)_{ij} = b_{ii} \otimes a_{ij} \oplus b_{ij} \otimes a_{jj} \oplus \bigoplus_{p \notin \{i,j\}} b_{ip} \otimes a_{pj} = b_{ij} \otimes k.$$

Hence, $A \otimes B = B \otimes A$. □

4. Protocols based on commuting matrices in tropical algebra

In this section, we discuss several implementations of public key exchange protocols that use the new classes of commuting matrices in tropical algebra described in Section 3. These implementations follow the idea of the tropical version of Stickel's protocol suggested by Grigoriev and Shpilrain [2], which we recall next.

4.1. Tropical Stickel's protocol of [2].

Protocol 4.1 (Tropical Stickel's protocol of [2]). *Alice and Bob agree on public matrices $A, B, W \in \mathbb{R}_{\max}^{n\times n}$. Then they exchange messages as follows:*

(1) *Alice chooses two random tropical polynomials $p_1(x), p_2(x)$ and sends $U = p_1(A) \otimes W \otimes p_2(B)$ to Bob.*
(2) *Bob chooses two random tropical polynomials $q_1(x), q_2(x)$ and sends $V = q_1(A) \otimes W \otimes q_2(B)$ to Alice.*
(3) *Alice computes her secret key using the public key V which she obtained from Bob and she has $K_a = p_1(A) \otimes V \otimes p_2(A)$.*
(4) *Bob also computes his secret key using Alice's public key U and he obtains $K_b = q_1(A) \otimes U \otimes q_2(B)$.*

Note that Alice and Bob use different public keys, i.e., public matrices V and U, respectively, but since $p_1(A) \otimes q_1(A) = q_1(A) \otimes p_1(A)$ and $p_2(B) \otimes q_2(B) = q_2(B) \otimes p_2(B)$, in the end they have the same secret keys $K_a = K_b = p_1(A) \otimes q_1(A) \otimes W \otimes q_2(B) \otimes p_2(B)$.

4.2. Stickel's protocol with quasi-polynomials. By Theorem 3.3, if $A \in \mathbb{R}_{\max}^{n\times n}$ is a Jones matrix, then its deformations $A^{(\alpha)}$ and $A^{(\beta)}$ commute for any α, β: $0 \leqslant \alpha, \beta \leqslant 1$. Using this we can define a quasi-polynomial, where the role of monomials is played by deformations.

Definition 4.1 (Quasi-polynomial). Let $A \in \mathbb{R}_{\max}^{n\times n}$ be a Jones matrix. A matrix B is called a quasi-polynomial of A if

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

for some finite subset $\mathcal{R}$ of rational numbers in $[0, 1]$ and $a_\alpha \in \mathbb{R}_{\max}$ for $\alpha \in \mathcal{R}$.

The requirements that $\mathcal{R}$ consists of rational numbers and is finite are not necessary in theory, but we have to impose them for practical implementation.

We now suggest another tropical implementation of Stickel's protocol, where we use tropical quasi-polynomials instead of tropical polynomials.

Protocol 4.2 (Stickel's protocol using tropical quasi-polynomials). *Alice and Bob agree on some Jones matrices $A, B \in \mathbb{R}_{\max}^{n\times n}$ and an arbitrary matrix $W \in \mathbb{R}_{\max}^{n\times n}$.*

(1) *Alice chooses two random quasi-polynomials $p'_1(A)$, $p'_2(B)$ and computes $U = p'_1(A) \otimes W \otimes p'_2(B)$. Then Alice sends U to Bob.*

(2) *Bob chooses two random quasi-polynomials* $q_1'(A)$, $q_2'(B)$ *and computes* $V = q_1'(A) \otimes W \otimes q_2'(B)$. *Then Bob sends* V *to Alice.*
(3) *Alice and Bob compute their secret keys* $K_a = p_1'(A) \otimes V \otimes p_2'(B)$ *and* $K_b = q_1'(A) \otimes U \otimes q_2'(B)$, *respectively.*

Since $p_1'(A) \otimes q_1'(A) = q_1'(A) \otimes p_1'(A)$ and $p_2'(B) \otimes q_2'(B) = q_2'(B) \otimes p_2'(B)$, we have a common secret key $K_a = K_b$.

4.3. Protocols using $[2r, r]_n^k$. The protocols that we describe next are based on Theorems 3.4 and 3.5.

Protocol 4.3. *Alice and Bob agree on a public matrix* $W \in \mathbb{R}_{\max}^{n\times n}$.

(1) *Alice chooses matrices* $A_1 \in [2a, a]_n^{k_1}$ *and* $A_2 \in [2b, b]_n^{k_2}$ *for some random* $a, b < 0$ *and* $k_1, k_2 \geqslant 0$. *Then Alice sends* $U = A_1 \otimes W \otimes A_2$ *to Bob.*
(2) *Bob chooses matrices* $B_1 \in [2c, c]_n^{l_1}$ *and* $B_2 \in [2d, d]_n^{l_2}$ *for some random* $c, d < 0$ *and* $l_1, l_2 \geqslant 0$. *Then Bob sends* $V = B_1 \otimes W \otimes B_2$ *to Alice.*
(3) *Alice computes the secret key* $K_a = A_1 \otimes V \otimes A_2 = A_1 \otimes B_1 \otimes W \otimes B_2 \otimes A_2$ *and Bob computes the secret key* $K_b = B_1 \otimes U \otimes B_2 = B_1 \otimes A_1 \otimes W \otimes A_2 \otimes B_2$.

Protocol 4.4. *Alice and Bob agree on a public matrix* $W \in \mathbb{R}_{\max}^{n\times n}$.

(1) *Alice chooses a matrix* $A_1 \in [2a, a]_n^k$ *and sends* k *to Bob.*
(2) *Bob chooses a matrix* $B_2 \in [2b, b]_n^l$ *and sends* l *to Alice.*
(3) *Alice chooses a matrix* A_2 *with entries in* $[0, l]$, *computes* $U = A_1 \otimes W \otimes A_2$ *and sends it to Bob.*
(4) *Bob chooses a matrix* B_1 *with entries in* $[0, k]$, *computes* $V = B_1 \otimes W \otimes B_2$ *and sends it to Alice.*
(5) *Alice computes the secret key* $K_a = A_1 \otimes V \otimes A_2 = A_1 \otimes B_1 \otimes W \otimes B_2 \otimes A_2$ *and Bob computes the secret key* $K_b = B_1 \otimes U \otimes B_2 = B_1 \otimes A_1 \otimes W \otimes A_2 \otimes B_2$.

For both protocols, since $A_1 \otimes B_1 = B_1 \otimes A_1$ and $A_2 \otimes B_2 = B_2 \otimes A_2$, it is immediate that Alice and Bob have the same secret key $K_a = K_b$.

5. Security of Stickel's protocol with tropical quasi-polynomials

5.1. Attacking tropical Stickel's protocol. To break any implementation of Stickel's protocol, we can follow the idea of cryptanalysis of classical Stickel's protocol suggested in [7]. Applying this idea to Protocol 4.1, an attacker, commonly named Eve, needs to find matrices X and Y such that the following conditions hold:

$$A \otimes X = X \otimes A, \quad B \otimes Y = Y \otimes B, \tag{5.1}$$

and

$$X \otimes W \otimes Y = U. \tag{5.2}$$

If Eve finds such X and Y, then she can compute the key by multiplying V from the left by X and from the right by Y. Then she will obtain

$$X \otimes V \otimes Y = X \otimes q_1(A) \otimes W \otimes q_2(B) \otimes Y.$$

Since $q_1(A)$ commutes with X and $q_2(B)$ commutes with Y, we have

$$X \otimes V \otimes Y = q_1(A) \otimes X \otimes W \otimes Y \otimes q_2(B) = q_1(A) \otimes U \otimes q_2(B) = K_b.$$

Kotov and Ushakov [5] observed that when we seek X and Y in the form of tropical polynomials, solving this problem is reduced to solving a tropical one-sided system where the variables satisfy certain conditions.

Equation (5.2) can be equivalently written as

$$\bigoplus_{\alpha,\beta=0}^{D} x_\alpha \otimes y_\beta \otimes (A^{\otimes\alpha} \otimes W \otimes B^{\otimes\beta} - U) = E, \tag{5.3}$$

where E is a matrix of the same dimension as A or B with all entries equal to 0. As we denote $T^{\alpha\beta} = A^{\otimes\alpha} \otimes W \otimes B^{\otimes\beta} - U$, it is convenient to rewrite (5.3) as

$$\bigoplus_{\alpha,\beta=0}^{D} (x_\alpha \otimes y_\beta \otimes T^{\alpha\beta}_{\gamma\delta}) = 0 \quad \forall\, \gamma, \delta \in [n]. \tag{5.4}$$

If we denote $z_{\alpha\beta} = x_\alpha \otimes y_\beta$, then we find that this is a system of tropical linear one-sided equations (of the type "$A \otimes x = b$") with coefficients $T^{\alpha\beta}_{\gamma\delta}$ and unknowns $z_{\alpha\beta}$, where the pairs $\gamma\delta$ play the role of rows and the pairs $\alpha\beta$ play the role of columns. Such systems are considered, e.g., in [1], but here we have an additional requirement that unknowns have a special structure: $z_{\alpha\beta} = x_\alpha \otimes y_\beta = x_\alpha + y_\beta$.

These ideas motivate the following attack suggested by Kotov and Ushakov [5]. The goal of this attack is to solve (5.4). Following the usual optimization notation, we denote by $\arg\min\limits_{\gamma,\delta}(-T_{\gamma\delta}^{\alpha\beta})$ the set of pairs (γ,δ) at which the minimum of $T_{\gamma\delta}^{\alpha\beta}$ is attained.

Attack 5.1 (Kotov-Ushakov [5])**.**

(1) *Compute*

$$c_{\alpha\beta} = \min_{\gamma,\delta}(-T_{\gamma\delta}^{\alpha\beta}), \quad S_{\alpha\beta} = \arg\min_{\gamma,\delta}(-T_{\gamma\delta}^{\alpha\beta}). \tag{5.5}$$

(2) *Among all minimal covers of* $[n]\times[n]$ *by* $S_{\alpha\beta}$*, that is, all minimal subsets* $\mathcal{C}\subseteq\{0,\dots,D\}\times\{0,\dots,D\}$ *such that*

$$\bigcup_{(\alpha,\beta)\in\mathcal{C}} S_{\alpha\beta} = [n]\times[n], \tag{5.6}$$

find a cover for which the system

$$\begin{cases} x_\alpha + y_\beta = c_{\alpha\beta} & \text{if } (\alpha,\beta)\in\mathcal{C},\\ x_\alpha + y_\beta \leqslant c_{\alpha\beta} & \text{if } (\alpha,\beta)\notin\mathcal{C}, \end{cases} \tag{5.7}$$

is solvable.

We now prove that Attack 5.1 actually works.

Theorem 5.1. *Let* $A,B,W\in\mathbb{R}_{\max}^{n\times n}$ *and* U *be the message sent by Alice to Bob in Protocol* 4.1*. If* D *is bigger than the maximal degree of any tropical polynomial that can be used by Alice and Bob in that protocol, then the Kotov-Ushakov attack yields*

$$X = \bigoplus_{\alpha=0}^{D} x_\alpha \otimes A^{\otimes\alpha}, \quad Y = \bigoplus_{\beta=0}^{D} y_\beta \otimes B^{\otimes\beta}, \tag{5.8}$$

which satisfy $X\otimes W\otimes Y = U$*.*

Proof. Since D is bigger than the maximal degree of any tropical polynomial used by Alice and Bob, it is clear from Protocol 4.1 that $U = X\otimes W\otimes Y$, where X and Y satisfy (5.8) for some x_α and y_β, for $\alpha,\beta\in\{0,\dots,D\}$. Therefore, there exist x_α and y_β that satisfy (5.3) or, equivalently, (5.4). It is also clear that any x_α and y_β that solve (5.4) yield X and Y that satisfy (5.8) and $X\otimes W\otimes Y = U$. Thus the protocol can be broken by solving (5.4) and (with $T^{\alpha\beta}$ defined using U that is produced by the protocol) this system is solvable.

It remains to show that the Kotov-Ushakov attack actually finds a solution to (5.4) (provided that a solution exists, which is the case).

Consider the system

$$\bigoplus_{\alpha,\beta=0}^{D} z_{\alpha\beta} \otimes T^{\alpha\beta}_{\gamma\delta} = 0 \quad \forall\, \gamma, \delta \in [n]. \tag{5.9}$$

According to the theory of $A \otimes x = b$, and namely [1] Theorem 3.1.1 and Corollary 3.1.2, we have:

(1) If the solution exists, then the vector $C = (c_{\alpha\beta})$, where $c_{\alpha\beta} = \min_{\gamma,\delta}(-T^{\alpha\beta}_{\gamma\delta})$ is the greatest solution.

(2) A vector $Z = (z_{\alpha\beta})$ is a solution if and only if there exists a set $\mathcal{C} \subseteq \{0, \ldots, D\} \times \{0, \ldots, D\}$ such that (5.6) holds and $z_{\alpha\beta} = c_{\alpha\beta}$ for all $(\alpha, \beta) \in \mathcal{C}$ and $z_{\alpha\beta} \leqslant c_{\alpha\beta}$ for all (α, β).

Since $z_{\alpha\beta} = x_\alpha \otimes y_\beta$ for all α and β, it follows that checking the solvability of (5.4) amounts to finding at least one system (5.7) that is solvable with $\mathcal{C}$ being a minimal cover (i.e., a set satisfying (5.6) that is minimal with respect to inclusion). This is what Attack 5.1 actually does. □

Note that Theorem 5.1 was not formally stated and proved in [5].

Although the complexity of Attack 5.1 in terms of the maximal degree of polynomials is non-polynomial, it is quite efficient when, for example, this maximal degree stays bounded and the dimension of matrices is allowed to grow, see [5].

We now describe a version of the Kotov and Ushakov attack that applies to Protocol 4.2, where we have tropical quasi-polynomials instead of polynomials. In this case, instead of (5.1) we need to require that X, or Y, commute with any quasi-polynomial of A, or of B respectively. Obviously, it is then reasonable to seek X and Y themselves in the form of quasi-polynomials.

5.2. Kotov and Ushakov attack on Protocol 4.2. We first select a big enough finite subset $\mathcal{T}$ of rational numbers in $[0, 1]$ such that, e.g., we have $\mathcal{R} \subseteq \mathcal{T}$ with certainty for any set $\mathcal{R}$ that can be used by Alice and Bob. Then we define

$$X = \bigoplus_{\alpha\in\mathcal{T}} x_\alpha \otimes A^{(\alpha)}, \quad Y = \bigoplus_{\beta\in\mathcal{T}} y_\beta \otimes B^{(\beta)}. \tag{5.10}$$

Then using (5.2) we impose

$$X \otimes W \otimes Y = \bigoplus_{\alpha,\beta\in\mathcal{T}} x_\alpha \otimes A^{(\alpha)} \otimes W \otimes y_\beta \otimes B^{(\beta)} = \bigoplus_{\alpha,\beta\in\mathcal{T}} x_\alpha \otimes y_\beta \otimes A^{(\alpha)} \otimes W \otimes B^{(\beta)} = U. \tag{5.11}$$

Equation (5.11) can be equivalently written as

$$\bigoplus_{\alpha,\beta\in\mathcal{T}} x_\alpha \otimes y_\beta \otimes (A^{(\alpha)} \otimes W \otimes B^{(\beta)} - U) = E, \tag{5.12}$$

where E is a matrix of the same dimension as A or B with all entries equal to 0. As we denote $T^{\alpha\beta} = A^{(\alpha)} \otimes W \otimes B^{(\beta)} - U$, we can rewrite (5.12) as follows:

$$\max_{\alpha,\beta\in\mathcal{T}} (x_\alpha \otimes y_\beta \otimes T^{\alpha\beta}_{\gamma\delta}) = 0 \quad \forall\, \gamma, \delta \in [n].$$

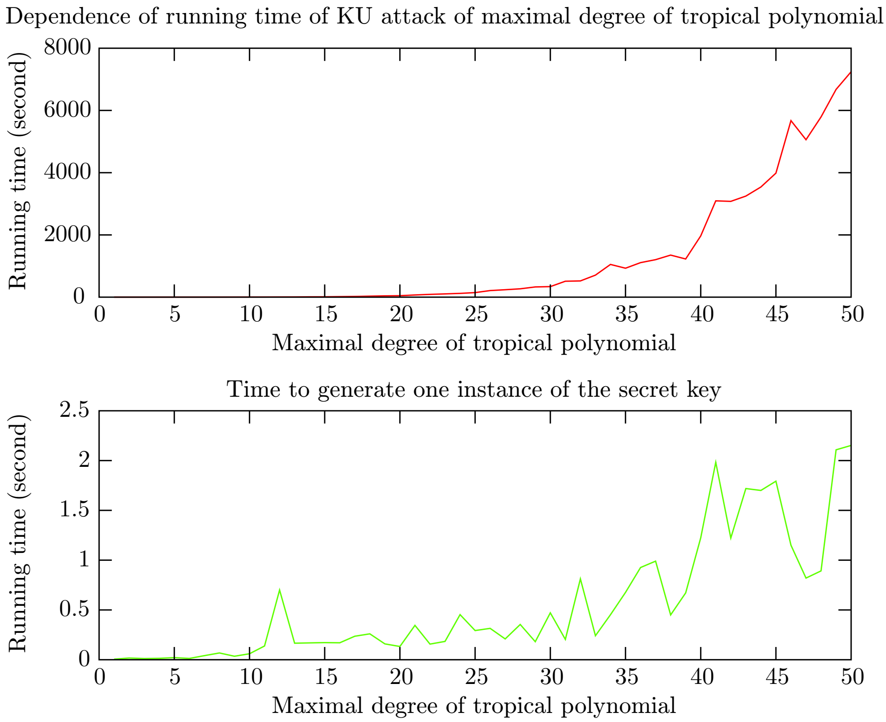

Figure 1. (a) Dependence of average computation of Attack 5.1 on the maximal degree of tropical polynomials and (b) running time for generating K_a or K_b in Protocol 4.1.

This system is very similar to (5.4): a system of the type "$A \otimes x = b$", where the role of unknowns is played by $z_{\alpha\beta} = x_\alpha + y_\beta$. This leads us to the following attack:

Attack 5.2.

(1) *Compute* $c_{\alpha\beta}$ *and* $S_{\alpha\beta}$ *by* (5.5), *where* $T^{\alpha\beta} = A^{(\alpha)} \otimes W \otimes B^{(\beta)} - U$ *and* $\alpha, \beta \in \mathcal{T}$.

(2) *Among the minimal sets* $\mathcal{C} \subseteq \mathcal{T} \times \mathcal{T}$ *that satisfy* (5.6) *we seek those which satisfy*

$$\begin{cases} x_\alpha + y_\beta = c_{\alpha\beta}, & \textit{if } (\alpha, \beta) \in \mathcal{C}, \\ x_\alpha + y_\beta \leqslant c_{\alpha\beta}, & \textit{if } (\alpha, \beta) \notin \mathcal{C}. \end{cases} \tag{5.13}$$

Thus the Kotov-Ushakov attack on the Protocol 2 is very similar to the original one. The proof of the following theorem is omitted, since it is also very similar to that of Theorem 5.1.

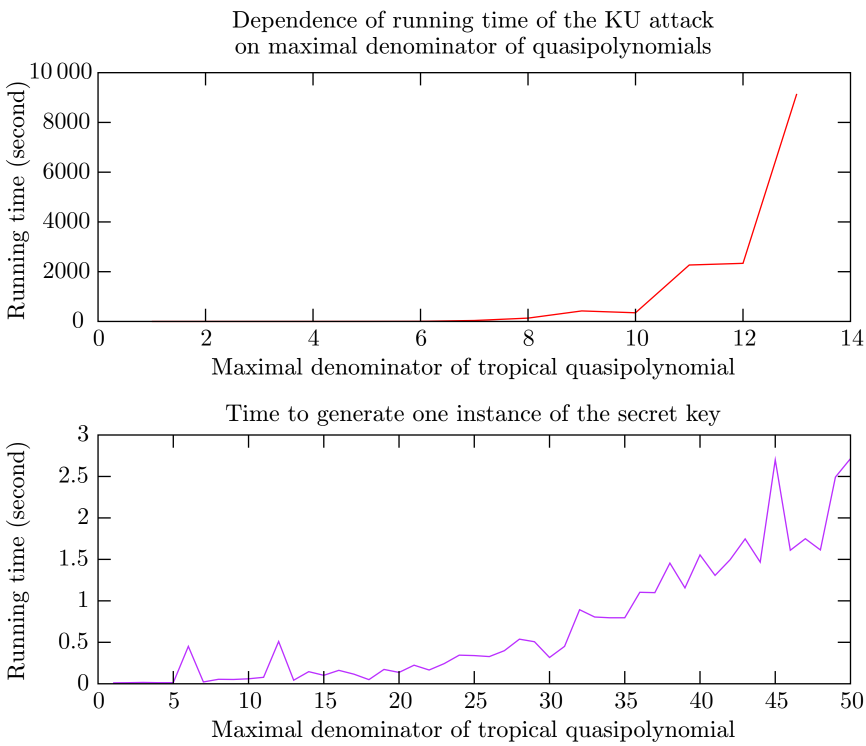

Figure 2. (a) Dependence of average computation of Attack 5.2 on the maximal denominator of tropical quasi-polynomials and (b) running time for generating K_a or K_b in Protocol 4.2.

Theorem 5.2. *Let $A, B, W \in \mathbb{R}_{\max}^{n\times n}$ and U be the message sent by Alice to Bob in Protocol 4.2. If $\mathcal{R} \subseteq \mathcal{T}$ for any set $\mathcal{R}$ that can be used by Alice and Bob in that protocol, then the Kotov-Ushakov attack yields*

$$X = \bigoplus_{\alpha\in\mathcal{T}} x_\alpha \otimes A^{(\alpha)}, \quad Y = \bigoplus_{\beta\in\mathcal{T}} y_\beta \otimes B^{(\beta)}, \tag{5.14}$$

which satisfy $X \otimes W \otimes Y = U$.

We implemented Attack 5.2 in GAP by modifying the existing code from [5]. Figures 1 and 2 show how the average computation time grows in practice as we increase the maximal degree of monomials in the tropical polynomial (Protocol 4.1) or the maximal denominator of the degree of monomials in the tropical quasi-polynomial (Protocol 4.2).

On the one hand, we see that the average computation time of the Kotov-Ushakov attack grows quite rapidly with the increase of the maximal degree of tropical polynomials or the maximal denominator of tropical quasi-polynomials. On the other hand, this increase is not so dramatic, and a possible reason for this is the slow growth of the average number of tested minimal covers, as reported in [5].

6. Security of protocols using Linde-de la Puente matrices

6.1. Attacks on Protocol 4.3 in some special cases. Recall that Alice's secret key is $K_a = A_1 \otimes V \otimes A_2 = A_1 \otimes B_1 \otimes W \otimes B_2 \otimes A_2$. Using Theorem 3.4, we obtain

$$\begin{aligned} K_a &= (l_1 \otimes A_1 \oplus k_1 \otimes B_1) \otimes W \otimes (k_2 \otimes B_2 \oplus l_2 \otimes A_2) \\ &= (l_1 \otimes k_2 \otimes A_1 \otimes W \otimes B_2) \oplus (l_1 \otimes l_2 \otimes A_1 \otimes W \otimes A_2) \\ &\quad \oplus (k_1 \otimes k_2 \otimes B_1 \otimes W \otimes B_2) \oplus (k_1 \otimes l_2 \otimes B_1 \otimes W \otimes A_2) \\ &= \underline{(l_1 \otimes l_2 \otimes U) \oplus (k_1 \otimes k_2 \otimes V)} \oplus (l_1 \otimes k_2 \otimes A_1 \otimes W \otimes B_2) \\ &\quad \oplus (k_1 \otimes l_2 \otimes B_1 \otimes W \otimes A_2). \end{aligned} \tag{6.1}$$

Let us discuss how Eve can find $l_1 \otimes l_2$ and $k_1 \otimes k_2$ and hence recover the first two terms of the above expression (underlined).

Lemma 6.1. *We have $k_1 \otimes k_2 = u_{st} \otimes w_{st}^-$ and $l_1 \otimes l_2 = v_{st} \otimes w_{st}^-$, where s, t is any pair of indices for which $\max\limits_{i,j} w_{ij} = w_{st}$.*

P r o o f. We have

$$\begin{aligned} u_{st} &= k_1 \otimes w_{st} \otimes k_2 \oplus \bigoplus_{(s',t')\neq(s,t)} (A_1)_{ss'} \otimes w_{s't'} \otimes (A_2)_{t't}, \\ v_{st} &= l_1 \otimes w_{st} \otimes l_2 \oplus \bigoplus_{(s',t')\neq(s,t)} (B_1)_{ss'} \otimes w_{s't'} \otimes (B_2)_{t't}. \end{aligned} \tag{6.2}$$

However, we also have $(A_1)_{ss'} \leqslant k_1$, $(A_2)_{t't} \leqslant k_2$, $(B_1)_{ss'} \leqslant l_1$, $(B_2)_{t't} \leqslant l_2$ and $w_{s't'} \leqslant w_{st}$, and therefore $u_{st} = k_1 \otimes w_{st} \otimes k_2$ and $v_{st} = l_1 \otimes w_{st} \otimes l_2$, and hence the claim follows. □

Using Lemma 6.1, the attacker can recover $l_1 \otimes l_2 \otimes U \oplus k_1 \otimes k_2 \otimes V$ which is the underlined part of $K_a = K_b$. Let us consider the following special case when this allows the attacker to recover the whole key.

Definition 6.1 (W is vanishing). W is called *vanishing in* $A_1 \otimes W \otimes A_2$ *and* $B_1 \otimes W \otimes B_2$ if $A_1 \otimes W \otimes A_2 = A_1 \otimes A_2$ and $B_1 \otimes W \otimes B_2 = B_1 \otimes B_2$.

Theorem 6.1 (Attack when W is vanishing). *If W is vanishing in $A_1 \otimes W \otimes A_2$ and $B_1 \otimes W \otimes B_2$, then*

$$K_a = K_b = l_1 \otimes l_2 \otimes U \oplus k_1 \otimes k_2 \otimes V, \tag{6.3}$$

where $k_1 \otimes k_2 = u_{st} \otimes w_{st}^-$, and $l_1 \otimes l_2 = v_{st} \otimes w_{st}^-$, and s, t is any pair of indices for which $\max_{i,j} w_{ij} = w_{st}$.

Proof. Let $U = A_1 \otimes W \otimes A_2 = A_1 \otimes A_2$ and $V = B_1 \otimes W \otimes B_2 = B_1 \otimes B_2$. In this case $K_b = B_1 \otimes A_1 \otimes A_2 \otimes B_2 = K_a = K$. Repeatedly applying Theorem 3.4 we find that

$$\begin{aligned} K &= k_2 \otimes l_1 \otimes l_2 \otimes A_1 \oplus k_1 \otimes l_1 \otimes l_2 \otimes A_2 \\ &\quad \oplus k_1 \otimes k_2 \otimes l_2 \otimes B_1 \oplus k_1 \otimes k_2 \otimes l_1 \otimes B_2 \\ &= l_1 \otimes l_2 \otimes U \oplus k_1 \otimes k_2 \otimes V. \end{aligned}$$

The expressions for $k_1 \otimes k_2$ and $l_1 \otimes l_2$ follow from Lemma 6.1. □

In our experiments, the case of vanishing W was not typical, occurring in no more than about 1% experiments. When the range of the entries of W is much bigger than that of other matrices ($A^{(1)}$, $A^{(2)}$, $B^{(1)}$ and $B^{(2)}$), it is more natural to assume that the following property holds.

Definition 6.2 (W is dominant). Let $A^{(1)} = (a_{ij}^{(1)})$, $A^{(2)} = (a_{ij}^{(2)})$, $B^{(1)} = (b_{ij}^{(1)})$ and $B^{(2)} = (b_{ij}^{(2)})$ be $n \times n$ matrices over $\mathbb{R}_{\max}$. Matrix $W = (w_{ij}) \in \mathbb{R}_{\max}^{n \times n}$ is called *dominant in* $A^{(1)} \otimes W \otimes A^{(2)}$, $B^{(1)} \otimes W \otimes B^{(2)}$, $A^{(1)} \otimes W \otimes B^{(2)}$, $A^{(1)} \otimes W \otimes B^{(2)}$, if the following property

$$\begin{aligned} (A^{(1)} \otimes W \otimes A^{(2)})_{il} &= a_{is}^{(1)} \otimes w_{st} \otimes a_{tl}^{(2)}, \\ (B^{(1)} \otimes W \otimes B^{(2)})_{il} &= b_{is}^{(1)} \otimes w_{st} \otimes b_{tl}^{(2)}, \\ (A^{(1)} \otimes W \otimes B^{(2)})_{il} &= a_{is}^{(1)} \otimes w_{st} \otimes b_{tl}^{(2)}, \\ (B^{(1)} \otimes W \otimes A^{(2)})_{il} &= b_{is}^{(1)} \otimes w_{st} \otimes a_{tl}^{(2)} \end{aligned} \tag{6.4}$$

holds for all i, l and some s and t such that $w_{st} = \max_{i,j} w_{ij}$.

It turns out that we also can reconstruct the whole key in this case.

Theorem 6.2 (Attack when W is dominant)**.** *Suppose that W is dominant in $A^{(1)} \otimes W \otimes A^{(2)}$, $B^{(1)} \otimes W \otimes B^{(2)}$, $A^{(1)} \otimes W \otimes B^{(2)}$ and $B^{(1)} \otimes W \otimes A^{(2)}$. Then the entries of the key $K = (k_{il})$ can be found as follows:*

$$k_{il} = w_{st}^{-} \otimes (v_{st} \otimes u_{il} \oplus u_{st} \otimes v_{il} \oplus u_{it} \otimes v_{sl} \oplus v_{it} \otimes u_{sl}). \tag{6.5}$$

P r o o f. Using (6.1) and (6.4), we obtain for the entries k_{il} that

$$\begin{aligned} k_{il} = {} & (l_1 \otimes l_2 \otimes u_{il}) \oplus (k_1 \otimes k_2 \otimes v_{il}) \oplus (l_1 \otimes k_2 \otimes a_{is}^{(1)} \otimes w_{st} \otimes b_{tl}^{(2)}) \\ & \oplus (k_1 \otimes l_2 \otimes b_{is}^{(1)} \otimes w_{st} \otimes a_{tl}^{(2)}). \end{aligned} \tag{6.6}$$

The attacker can compute $l_1 \otimes l_2$ and $k_1 \otimes k_2$ as in Lemma 6.1: $l_1 \otimes l_2 = v_{st} \otimes w_{st}^{-}$ and $k_1 \otimes k_2 = u_{st} \otimes w_{st}^{-}$. To compute the rest, we observe that by (6.4)

$$\begin{aligned} u_{it} &= a_{is}^{(1)} \otimes w_{st} \otimes a_{tt}^{(2)}, \quad & u_{sl} &= a_{ss}^{(1)} \otimes w_{st} \otimes a_{tl}^{(2)}, \\ v_{it} &= b_{is}^{(1)} \otimes w_{st} \otimes b_{tt}^{(2)}, \quad & v_{sl} &= b_{ss}^{(1)} \otimes w_{st} \otimes b_{tl}^{(2)}, \end{aligned}$$

and recall that $a_{tt}^{(2)} = k_2$, $a_{ss}^{(1)} = k_1$, $b_{tt}^{(2)} = l_2$ and $b_{ss}^{(1)} = l_1$. Using this we then obtain that

$$\begin{aligned} u_{it} \otimes w_{st}^{-} &= a_{is}^{(1)} \otimes k_2, \quad & u_{sl} \otimes w_{st}^{-} &= k_1 \otimes a_{tl}^{(2)}, \\ v_{it} \otimes w_{st}^{-} &= b_{is}^{(1)} \otimes l_2, \quad & v_{sl} \otimes w_{st}^{-} &= l_1 \otimes b_{tl}^{(2)}. \end{aligned}$$

Substituting this into (6.6), we obtain

$$k_{il} = v_{st} \otimes w_{st}^{-} \otimes u_{il} \oplus u_{st} \otimes w_{st}^{-} \otimes v_{il} \oplus u_{it} \otimes w_{st}^{-} \otimes v_{sl} \oplus v_{it} \otimes w_{st}^{-} \otimes u_{sl},$$

which can be simplified to (6.5). □

We also considered formulae (6.3) and (6.5) as heuristic attacks on Protocol 4.3. To analyze the success of these attacks we considered the following two parameters:

1) the *success rate*, i.e., the percentage of instances where the secret key $K_a = K_b$ is exactly equal to expression (6.3) or (6.5),

2) the *similarity rate*: the average percentage of entries of the matrix computed by (6.3) or (6.5) which are equal to those in the secret key $K_a = K_b$ in the case of "no success" when the matrix computed by (6.3) or (6.5) does not coincide with the key. We performed 10000 experiments for matrices of dimensions 5, 20, 30 and 40 and with entries of W randomly selected in various ranges using Matlab R2018a.

For the attack based on (6.5), the results of our experiments are shown in Table 1. As we would expect, both the average success rate and the average similarity rate grow with the range of W. Also, the average success rate rapidly decreases with dimension, while the change of similarity rate is rather insignificant. For the entries of W randomly selected in $[0, 100000]$ and other parameters within $[-100, 100]$ and the given four dimensions, the average success rate for the attack based on (6.5) becomes overwhelming, indicating that in this case W is highly likely to be dominant.

Dimension of matrices	5	20	30	40
Success rate, entries of W in $[-5, 5]$	17.81%	0.03%	0%	0%
Similarity rate, entries of W in $[-5, 5]$	90.55%	86.17%	85.99%	85.18%
Success rate, entries of W in $[-50, 50]$	45.44%	4.2%	1.59%	1.17%
Similarity rate, entries of W in $[-50, 50]$	94.62%	94.18%	94.30%	94.47%
Success rate, entries of W in $[-100, 100]$	66.8%	13.51%	6.99 %	3.62%
Similarity rate, entries of W in $[-100, 100]$	97.41%	97.31%	97.53%	97.58%
Success rate, entries of W in $[-500, 500]$	92.5%	35.13%	26.61%	22.17%
Similarity rate, entries of W in $[-500, 500]$	98.38%	96.63%	97.23%	97.96%
Success rate, entries of W in $[-1000, 1000]$	96.57%	44.88%	33.97%	29.02%
Similarity rate, entries of W in $[-1000, 1000]$	99.70%	95.32%	94.40%	94.91%
Success rate, entries of W in $[-10000, 10000]$	99.72%	85.87%	72.20%	59.51%
Similarity rate, entries of W in $[-10000, 10000]$	99.97%	98.35%	96.50%	94.44%
Success rate, entries of W in $[-100000, 100000]$	99.99%	98.68%	96.35%	92.66%
Similarity rate, entries of W in $[-100000, 100000]$	99.99%	99.87%	99.56%	99.15%

Table 1. Dependency of the success and similarity rate on dimension and the range of entries of W for the attack based on (6.5). Parameters a, b are in the range $[-20, -1]$, parameters c, d are in the range $[-100, -60]$, and k_1, k_2, l_1, l_2 are random positive numbers in the range $[0, 100]$.

The performance of the attack based on (6.3) for W in all ranges shown in Table 1 was quite poor: in all series of 10000 experiments, the average success rate did not exceed 1.2% and the average similarity rate (among the unsuccessful cases) did not exceed 2.1%.

In view of the success of the simple heuristic attack based on (6.5), for which we observed at least 85% similarity rate between the key and the outcome of this attack in all our series of 10000 experiments, it is still challenging to suggest W that would be in some sense guaranteed to withstand this attack and the one based on (6.3) and for which no other obvious heuristic attacks would work. However, on the attacker's side we still would like to have an attack that can reconstruct $K_a = K_b$ with certainty. Such attack will be developed in the next subsections.

6.2. Generalized Kotov-Ushakov attack. The previous subsection yields a simple but efficient enough heuristic attack on Protocol 4.3 based on (6.5). We now discuss how the Kotov-Ushakov attack can be generalized to apply to both Protocols 4.3 and 4.4. The main idea is to use the tropical identity matrix and tropical elementary matrices to generate the matrices from the set $[2r, r]_n^k$, so that they will play the role of matrix powers in the Kotov-Ushakov attack.

We first describe a generalization of the Kotov-Ushakov attack, which can be then specialized to both protocols. In the generalized Kotov-Ushakov attack we seek matrices X and Y such that

$$\begin{gathered} X = \bigoplus_{\alpha \in \mathcal{A}} x_\alpha \otimes A_\alpha, \quad Y = \bigoplus_{\beta \in \mathcal{B}} y_\beta \otimes B_\beta, \\ X \otimes W \otimes Y = U, \quad x_\alpha \in \mathcal{X}_\alpha(s), \quad y_\beta \in \mathcal{Y}_\beta(t). \end{gathered} \tag{6.7}$$

Here $\{A_\alpha \colon \alpha \in \mathcal{A}\}$ and $\{B_\beta \colon \beta \in \mathcal{B}\}$ are finite sets of matrices such that any matrix that can be used by Alice and by Bob, respectively, can be represented as in the first line of (6.7), provided that the coefficients x_α and y_β satisfy the conditions written in the last line of (6.7). In these conditions, $\mathcal{X}_\alpha(s)$ and $\mathcal{Y}_\beta(t)$ are subsets of $\mathbb{R}$ whose specification depends on vectors s and t of unknown parameters.

The solution of (6.7) is based on the same ideas from [5] that were already used in Subsection 5.2. After we substitute the first line of (6.7) into the decomposition problem $X \otimes W \otimes Y = U$ and denote

$$T^{\alpha\beta} = A_\alpha \otimes W \otimes B_\beta - U, \tag{6.8}$$

the decomposition problem reduces to solving the system

$$\max_{\alpha \in \mathcal{A}, \beta \in \mathcal{B}} (x_\alpha \otimes y_\beta \otimes T^{\alpha\beta}_{\gamma\delta}) = 0 \quad \forall\, \gamma, \delta \in [n]. \tag{6.9}$$

Here, unlike in Subsection 5.2, x_α and y_β also satisfy the conditions in the last line of (6.7). Our attack then aims to solve equation (6.9) with these conditions.

Attack 6.1 (Generalized Kotov-Ushakov attack)**.**

(1) *For all* $\alpha \in \mathcal{A}$ *and* $\beta \in \mathcal{B}$, *compute*

$$c_{\alpha\beta} = \min_{\gamma, \delta \in [n]} (-T^{\alpha\beta}_{\gamma\delta}), \quad S_{\alpha\beta} = \arg \min_{\gamma, \delta \in [n]} (-T^{\alpha\beta}_{\gamma\delta}). \tag{6.10}$$

(2) *Among all minimal covers of* $[n] \times [n]$ *by* $S_{\alpha\beta}$*, that is, all minimal subsets* $\mathcal{C} \subseteq \mathcal{A} \times \mathcal{B}$ *such that*

$$\bigcup_{(\alpha,\beta)\in\mathcal{C}} S_{\alpha\beta} = [n] \times [n], \tag{6.11}$$

find a cover for which the system

$$\begin{cases} x_\alpha + y_\beta = c_{\alpha\beta}, & \text{if } (\alpha,\beta) \in \mathcal{C}, \\ x_\alpha + y_\beta \leqslant c_{\alpha\beta}, & \text{if } (\alpha,\beta) \notin \mathcal{C}, \\ x_\alpha \in \mathcal{X}_\alpha(s), & y_\beta \in \mathcal{Y}_\beta(t) \end{cases} \tag{6.12}$$

is solvable.

Note that we do not generally know the nature and the complexity of the conditions $x_\alpha \in \mathcal{X}_\alpha(s)$, $y_\beta \in \mathcal{Y}_\beta(t)$, and vectors s and t can themselves be constrained. However, in the specifications of Attack 6.1 that will follow in the next subsections, system (6.12) is always linear, so its solvability can be checked by the simplex method. The practical solvability of problem (6.12) depends on how $\mathcal{X}_\alpha(s)$ and $\mathcal{Y}_\beta(t)$ are specified. In both cases considered below these sets are intervals or points, so problem (6.12) is still a linear programming problem.

We now present a theorem about the validity of Attack 6.1.

Theorem 6.3. *If* (6.7) *is solvable, then Attack* 6.1 *yields a solution to that system.*

Proof. As in the proof of Theorem 5.1, we consider the system

$$\bigoplus_{\alpha\in\mathcal{A},\,\beta\in\mathcal{B}} z_{\alpha\beta} \otimes T^{\alpha\beta}_{\gamma\delta} = 0, \quad \gamma,\delta \in [n], \tag{6.13}$$

which is a slight generalization of (5.9). The validity of Attack 6.1 is then implied by the theory of $A \otimes x = b$ ([1] Theorem 3.1.1 and Corollary 3.1.2), taking into account that $z_{\alpha\beta} = x_\alpha \otimes y_\beta$, $x_\alpha \in \mathcal{X}_\alpha(s)$ and $y_\beta \in \mathcal{Y}_\beta(t)$. $\square$

6.3. Kotov-Ushakov attack on Protocol 4.3. In Protocol 4.3, we have $A_1 \in [2a, a]^{k_1}_n$ and $A_2 \in [2b, b]^{k_2}_n$ with unknown nonpositive a, b, and unknown nonnegative k_1 and k_2. Using tropical elementary matrices A_α and B_β with α and β being pairs of indices from $[n]$, we can represent any matrix in $[2a, a]^{k_1}_n$ and $[2b, b]^{k_2}_n$ as in the first line of (6.7). However, for this we also need to restrict the coefficients x_α to belong to $[2a, a]$ for some $a \leqslant 0$ if $\alpha = (i, j)$ with $i \neq j$ or to be equal to some

$k_1 \geqslant 0$ if $i = j$. Similarly, the coefficients y_β should belong to $[2b, b]$ for some $b \leqslant 0$ if $\beta = (i, j)$ with $i \neq j$ or to be equal to some $k_2 \geqslant 0$ if $i = j$.

Formally, we set A_α and B_β for $\alpha = \beta = (i, j)$ to be:

$$A_\alpha = A^{ij} = B_\beta = B^{ij} = E^{ij}, \tag{6.14}$$

where $(i, j) \in [n]^2$.

Sets $\mathcal{X}$ and $\mathcal{Y}$ satisfy

$$\mathcal{X}_{(i,j)}(a, k) = \begin{cases} [2a, a], & i \neq j \\ \{k\}, & i = j, \end{cases} \tag{6.15}$$

$$\mathcal{Y}_{(i,j)}(b, l) = \begin{cases} [2b, b], & i \neq j \\ \{l\}, & i = j, \end{cases} \tag{6.16}$$

where $k, l \geqslant 0$ and $a, b \leqslant 0$.

We now write, essentially, a specialization of Attack 6.1 to Protocol 4.3 in the case where $\mathcal{A}$ and $\mathcal{B}$ both equal to the set of elementary matrices (which is in one-to-one correspondence with $[n]^2$).

Attack 6.2.

(1) *For all* $\alpha = (i, j) \in [n]^2$ *and* $\beta = (s, t) \in [n]^2$, *compute*

$$c_{ijst} = c_{\alpha\beta} = \min_{\gamma,\delta \in [n]} (-T^{\alpha\beta}_{\gamma\delta}), \quad S_{ijst} = S_{\alpha\beta} = \arg\min_{\gamma,\delta \in [n]} (-T^{\alpha\beta}_{\gamma\delta}), \tag{6.17}$$

where A_α, B_β *are defined by* (6.14) *and* $T^{\alpha\beta}$ *by* (6.8) *(where* $\alpha = (i, j)$, $\beta = (s, t)$ *with* $i, j, s, t \in [n]$*).*

(2) *Among the minimal subsets* $\mathcal{C} \subseteq [n]^2 \times [n]^2$ *such that*

$$\bigcup_{(\alpha,\beta) \in \mathcal{C}} S_{\alpha\beta} = [n] \times [n], \tag{6.18}$$

find a cover for which the system

$$\begin{aligned} & x_{ij} + y_{st} = c_{ijst}, \quad \text{for } (i, j, s, t) \in \mathcal{C} \\ & x_{ij} + y_{st} \leqslant c_{ijst}, \quad \text{otherwise}, \\ & 2a \leqslant x_{ij} \leqslant a, \quad 2b \leqslant y_{st} \leqslant b \quad \forall\, i \neq j,\ s \neq t, \\ & x_{ii} = k_1, \quad y_{ss} = k_2 \quad \forall\, i, s, \\ & a, b \leqslant 0, \quad k_1, k_2 \geqslant 0, \end{aligned} \tag{6.19}$$

is solvable.

Note that this is a linear system of equalities and inequalities whose solvability can be checked by the simplex method.

We now explain why the attack is valid.

Theorem 6.4. *Let $W \in \mathbb{R}_{\max}^{n\times n}$ and let U be the message sent by Alice to Bob in Protocol 4.3. Then Attack 6.2 yields matrices $X \in [2a,a]_n^{k_1}$ and $Y \in [2b,b]_n^{k_2}$ for some $a,b \leqslant 0$ and $k_1,k_2 \geqslant 0$ that satisfy $X \otimes W \otimes Y = U$.*

P r o o f. In this case we have to solve system (6.7) with A_α and B_β being tropical elementary matrices and with $\mathcal{A} = \mathcal{B}$ being the set of all such matrices, and with the sets that contain x_α and y_α taking the forms of (6.15) and (6.16), respectively, also with the conditions $a,b \leqslant 0$ and $k_1,k_2 \geqslant 0$ on the parameters of these sets. This system is the same as $X \otimes W \otimes Y = U$ where it is required that $X \in [2a,a]_n^{k_1}$ and $Y \in [2b,b]_n^{k_2}$ for some $a,b \leqslant 0$ and $k_1,k_2 \geqslant 0$. The latter system has a solution since U is the message sent by Alice to Bob in Protocol 4.3.

Since (6.12) in this case becomes (6.19), Attack 6.2 is indeed a specialization of Attack 6.1, and by Theorem 6.3 it finds a solution to the above-described specialization of system (6.7), and hence it finds Linde-de la Puente matrices X and Y which satisfy $X \otimes W \otimes Y = U$. $\square$

6.4. Kotov-Ushakov attack on Protocol 4.4. In Protocol 4.4, we have $A_1 \in [2a,a]_n^k$ and $A_2 \in [0,l]_n$ (where $[0,l]_n$ is the set of $n\times n$ matrices whose all entries belong to $[0,l]$) with unknown nonpositive a and unknown nonnegative k and l. Using tropical elementary matrices and I as A_α and only tropical elementary matrices as B_β with α and β being pairs of indices from $\{1,\dots,n\}$, we can represent any matrix in $[2a,a]_n^k$ and $[0,l]_n$ as in the first line of (6.7). However, for this we also need to restrict the coefficients x_α to belong to $[2a,a]$ for some $a \leqslant 0$ if $\alpha = (i,j)$ with $i \neq j$ or to be equal to k if $i = j$. The coefficients y_β should belong to $[0,l]$ for any $\beta = (i,j)$ with $i,j \in [n]$.

Formally, we set A_α and B_β for each $\alpha = \beta = (i,j)$ to be the tropical elementary matrix E^{ij}. Here again $(i,j) \in [n]^2$.

Sets $\mathcal{X}$ and $\mathcal{Y}$ satisfy

$$\mathcal{X}_{(i,j)}(a) = \begin{cases} [2a,a], & i \neq j \\ \{k\}, & i = j, \end{cases} \tag{6.20}$$

$$\mathcal{Y}_{(i,j)} = [0,l] \quad \forall\, i,j. \tag{6.21}$$

Observe that k and l are not parameters in this case, since Alice and Bob are sending them to one another, so we have to assume that they can be intercepted by Eve. However, a is an unknown parameter satisfying $a \leqslant 0$.

Hence, we suggest the following attack.

Attack 6.3.

(1) *Compute* $c_{\alpha\beta} = c_{ijst}$ *and* $S_{\alpha\beta} = S_{ijst}$ *by* (6.17), *where* A_α *and* B_β *are defined by* (6.14) *and* $T^{\alpha\beta}$ *by* (6.8) *for* $\alpha = (i, j)$ *and* $\beta = (s, t)$ *with* $i, j, s, t \in [n]$.

(2) *Among the minimal sets* $\mathcal{C} \subseteq [n]^2 \times [n]^2$ *that satisfy* (6.18) *we seek those which satisfy*

$$\begin{aligned} &x_{ij} + y_{st} = c_{ijst} && \text{for } (i, j, s, t) \in \mathcal{C}, \\ &x_{ij} + y_{st} \leqslant c_{ijst} && \textit{otherwise}, \\ &2a \leqslant x_{ij} \leqslant a && \forall\, i \neq j,\ x_{ii} = k,\ \forall\, i \\ &0 \leqslant y_{st} \leqslant l && \forall\, s, t,\ a \leqslant 0. \end{aligned} \tag{6.22}$$

Note that this is a linear system of equalities and inequalities whose solvability can be checked by the simplex method. The proof of the validity of this attack is similar to that of Theorem 6.4 and is omitted.

7. Conclusions and further research

Using the results previously obtained in [4] and [6] and extending them, we described two useful classes of commuting matrices in tropical algebra and suggested some new implementations of Stickel's protocol based on them. For one of these implementations we developed two simple attacks which, strictly speaking, work only in very special situations but one of them can be rather successfully used as a heuristic attack in a general situation. We also showed how the Kotov-Ushakov attack can be generalized to apply to all of our protocols. We analyzed the performance of this attack on the tropical Stickel protocol suggested by [2] and our new modification that uses quasi-polynomials. We conclude that the Kotov-Ushakov attack works well when the number of generators (A_α and B_β) is limited, but the complexity quickly grows as the number of these generators increases. This means that the Kotov-Ushakov attack is not really so successful for big D in the tropical Stickel protocol of [2] (Protocol 4.1) as well as when too large subsets of rational numbers in $[0, 1]$ are used in the protocol with quasi-polynomials (Protocol 4.2). We also do not expect it to be successful for large n in the protocols with $[2r, r]_n^k$ matrices (Protocols 4.3 and 4.4). Therefore, it still makes sense to search for alternative attacks on our new protocols. For Protocol 4.3, since at least one rather successful heuristic attack has been found, it is neccessary to look for a class of matrices W that will safeguard against such attacks.

Intuitively, matrix commutativity in tropical algebra should be more common than in the usual algebra and it is a promising topic of research of independent interest.

Besides that, some new protocols using tropical algebra have been recently suggested in [3]. Unlike the previous tropical implementations of Stickel protocol, these new protocols use more sophisticated algebraic tools such as semi-direct product, and therefore they are immune to the Kotov-Ushakov attack and present a new interesting object of study.

References

[1] *P. Butkovič*: Max-Linear Systems: Theory and Algorithms. Springer Monographs in Mathematics. Springer, London, 2010. zbl MR doi

[2] *D. Grigoriev, V. Shpilrain*: Tropical cryptography. Commun. Algebra *42* (2014), 2624–2632. zbl MR doi

[3] *D. Grigoriev, V. Shpilrain*: Tropical cryptography II. Extensions by homomorphisms. Commun. Algebra *47* (2019), 4224–4229. zbl MR doi

[4] *D. Jones*: Special and Structured Matrices in Max-Plus Algebra: PhD Thesis. University of Birmingham, Birmingham, 2018.

[5] *M. Kotov, A. Ushakov*: Analysis of a key exchange protocol based on tropical matrix algebra. J. Math. Cryptol. *12* (2018), 137–141. zbl MR doi

[6] *J. Linde, M. J. de la Puente*: Matrices commuting with a given normal tropical matrix. Linear Algebra Appl. *482* (2015), 101–121. zbl MR doi

[7] *V. Shpilrain*: Cryptanalysis of Stickel's key exchange scheme. Computer Science - Theory and Applications. Lecture Notes in Computer Science 5010. Springer, Berlin, 2008, pp. 283–288. zbl MR doi

Authors' address: *Any Muanalifah*, *Sergeĭ Sergeev* (corresponding author), University of Birmingham, School of Mathematics, Birmingham, Edgbaston B15 2TT, United Kingdom, e-mail: `any.math13@gmail.com`, `s.sergeev@bham.ac.uk`.