Noname manuscript No.
(will be inserted by the editor)

Modifying The Tropical Version of Stickel's Key Exchange Protocol

Any Muanalifah · Sergeĭ Sergeev

Received: date / Accepted: date

Abstract A tropical version of Stickel's key exchange protocol was suggested by Grigoriev and Sphilrain [2] and successfully attacked by Kotov and Ushakov [5]. 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 Stickel's protocol and discuss the application of that generalised attack to all our new protocols.

Keywords Stickel's protocol · Tropical Algebra · Cryptography · Commuting matrices

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

Any Muanalifah
School of Mathematics, University Of Birmingham
E-mail: any.math13@gmail.com

Sergeĭ Sergeev
School of Mathematics, University of Birmingham
E-mail: s.sergeev@bham.ac.uk

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 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 efficient and simple heuristic attacks on the protocol. We also show that the ideas of 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 tropical algebra, based on [4] and [6]. In Section 4 we introduce new protocols using commuting matrices. Finally, in Sections **??** and 5 we construct some attacks on our modified protocols.

2 Elements of tropical algebra

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

Definition 1 (Tropical matrix addition and multiplication) For $c \in \mathbb{R}_{\max}$ and $A \in \mathbb{R}_{\max}^{m\times n}$ one defines $c \otimes A$ by

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

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

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

For matrix $A = (a_{ij}) \in \mathbb{R}_{\max}^{m\times p}$ and 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

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

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

Definition 2 (Identity matrix) 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 words, all diagonal entries of a tropical identity matrix are equal to 0 and all off-diagonal entries are equal to $-\infty$.

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.

Definition 3 (Tropical diagonal matrices) 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 $D^- = \operatorname{diag}(d_1^-, \ldots, d_n^-)$, so 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

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

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 sum of tropical elementary matrices.

Definition 4 (Elementary matrices) Let $E^{ij} \in \mathbb{R}_{\max}^{n\times n}$ be a matrix with entries

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

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 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:

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

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

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

Furthermore, we can also consider tropical polynomials.

Definition 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 $k = 0, 1, ..., d$.

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 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 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 Generalized Kleene stars

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 8 (Generalized Kleene Stars) Let $A = (a_{ij})$ be an $n \times n$ tropical matrix which satisfies the following property:

$$a_{ij} \otimes a_{jk} \leq a_{ik} \otimes a_{jj} \quad \forall i, j, k \in [n]. \tag{1}$$

We call A a generalized Kleene star.

Notice that any Kleene star $A \in \mathbb{R}_{\max}^{n\times n}$ is a generalized Kleene star where $a_{jj} = 0$ for all $j \in [n]$ and (1) reduces to $a_{ij} \otimes a_{jk} \leq a_{ik}$ for all $i, j, k \in [n]$.

We will consider the following operation:

Definition 9 (Deformation) Let $A = (a_{ij})$ be a generalized $n \times n$ Kleene star and $\alpha \in \mathbb{R}$. Matrix $A^{(\alpha)} = (a_{ij}^{(\alpha)})$ defined by

$$a_{ij}^{(\alpha)} = a_{ij} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)} \quad \forall i, j \in [n]. \tag{2}$$

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 generalized Kleene stars is stable under deformations for $\alpha \leq 1$.

Theorem 1 *$A^{(\alpha)}$ satisfies* (1) *for any $\alpha \leq 1$.*

Proof We have for all i, j, k that

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

Hence the inequality which we want to prove is

$$\begin{aligned} &a_{ij} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)} \otimes a_{jk} \otimes (a_{jj} \oplus a_{kk})^{\otimes(\alpha-1)} \\ &\leq a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\alpha-1)} \otimes a_{jj}^{\otimes\alpha}. \end{aligned} \tag{3}$$

Multiplying both parts 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) is equivalent to

$$\begin{aligned} &a_{ij} \otimes a_{jk} \otimes (a_{ii} \oplus a_{kk})^{\otimes(1-\alpha)} \\ &\leq a_{ik} \otimes a_{jj}^{\otimes\alpha} \otimes (a_{ii} \oplus a_{jj})^{\otimes(1-\alpha)} \otimes (a_{jj} \oplus a_{kk})^{\otimes(1-\alpha)}. \end{aligned} \tag{4}$$

To prove (4) we observe that

$$\begin{aligned} &a_{ij} \otimes a_{jk} \otimes (a_{ii} \oplus a_{kk})^{\otimes(1-\alpha)} = a_{ij} \otimes a_{jk} \otimes (a_{ii}^{\otimes(1-\alpha)} \oplus a_{kk}^{\otimes(1-\alpha)}) \\ &\leq a_{ik} \otimes a_{jj} \otimes (a_{ii}^{\otimes(1-\alpha)} \oplus a_{kk}^{\otimes(1-\alpha)}) = a_{ik} \otimes a_{jj} \otimes a_{ii}^{\otimes(1-\alpha)} \oplus a_{ik} \otimes a_{jj} \otimes a_{kk}^{\otimes(1-\alpha)} \end{aligned} \tag{5}$$

and that

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

which implies

$$\begin{aligned} & a_{ik} \otimes a_{jj}^{\otimes\alpha} (a_{ii} \oplus a_{jj})^{\otimes(1-\alpha)} \otimes (a_{jj} \oplus a_{kk})^{\otimes(1-\alpha)} \\ & \geq a_{ik} \otimes a_{jj}^{\otimes\alpha} (a_{ii}^{\otimes(1-\alpha)} a_{jj}^{\otimes(1-\alpha)} \oplus a_{jj}^{\otimes(1-\alpha)} a_{kk}^{\otimes(1-\alpha)}) \\ & = a_{ik} \otimes a_{jj} \otimes a_{ii}^{\otimes(1-\alpha)} \oplus a_{ik} \otimes a_{jj} \otimes a_{kk}^{\otimes(1-\alpha)}. \end{aligned} \tag{6}$$

Combining (5) and (6) yields (4).

Note that in Theorem 1 α can be negative.

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

Example 1 Let us consider matrix $A = \begin{bmatrix} 0 & 1 & -1 \\ -1 & 0 & -2 \\ -1 & 0 & -2 \end{bmatrix}$, then we have:

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

$$A^{(-\frac{2}{3})} \otimes A^{(-\frac{4}{5})} = \begin{bmatrix} 0 & 1 & \frac{3}{5} \\ -1 & 0 & -\frac{2}{5} \\ \frac{1}{3} & \frac{4}{3} & \frac{44}{15} \end{bmatrix}$$

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

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

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 2 *For any $\alpha, \beta \in \mathbb{R}$ such that $0 \leq \alpha \leq 1$, $0 \leq \beta \leq 1$ and $0 \leq \alpha + \beta \leq 1$, we have $A^{(\alpha)} \otimes A^{(\beta)} = A^{(\beta)} \otimes A^{(\alpha)} = A^{(\alpha+\beta)}$.*

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

$$\bigoplus_{j=1}^{n} a_{ij} (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)} \otimes a_{jk} \otimes (a_{jj} \oplus a_{kk})^{\otimes(\beta-1)} = a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\alpha+\beta-1)}. \tag{7}$$

We have

$$\begin{aligned} & \bigoplus_{j=1}^{n} a_{ij} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)} \otimes a_{jk} \otimes (a_{jj} \oplus a_{kk})^{\otimes(\beta-1)} \\ & = a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\alpha-1)} a_{kk}^{\otimes\beta} \oplus a_{ii}^{\otimes\alpha} \otimes a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\beta-1)} \\ & \oplus \bigoplus_{j \notin \{i,k\}} a_{ij} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)} \otimes a_{jk} \otimes (a_{jj} \oplus a_{kk})^{\otimes(\beta-1)}. \end{aligned} \tag{8}$$

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

$$\begin{aligned} & a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\alpha-1)} \otimes a_{kk}^{\otimes\beta} \oplus a_{ii}^{\otimes\alpha} \otimes a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\beta-1)} \\ & = a_{ik} \otimes a_{kk}^{\otimes\beta} \otimes a_{ii}^{\otimes(\alpha-1)} \oplus a_{ik} \otimes a_{ii}^{\otimes(\alpha+\beta-1)} = a_{ik} \otimes a_{ii}^{\otimes(\alpha+\beta-1)} \\ & = a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\alpha+\beta-1)}. \end{aligned} \tag{9}$$

The remaining case $a_{ii} \leq a_{kk}$ 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

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

it remains to show that

$$a_{jj} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)}(a_{jj} \oplus a_{kk})^{\otimes(\beta-1)} \leq (a_{ii} \oplus a_{kk})^{\otimes(\alpha+\beta-1)}. \tag{10}$$

which is equivalent to

$$a_{jj} \leq (a_{ii} \oplus a_{kk})^{\otimes(\alpha+\beta-1)}(a_{ii} \oplus a_{jj})^{\otimes(1-\alpha)}(a_{jj} \oplus a_{kk})^{\otimes(1-\beta)}. \tag{11}$$

If $a_{ii} \geq a_{kk}$ then we have

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

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

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

Corollary 1 *Matrix $A^{(0)}$ satisfies $A^{(\alpha)} \otimes A^{(0)} = A^{(0)} \otimes A^{(\alpha)} = A^{(\alpha)}$ for all $0 \leq \alpha \leq 1$.*

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

Corollary 2 *$A^{(k/l)} = (A^{(1/l)})^{\otimes k}$ holds for any integer $l > 0$ and integer k: $1 \leq k \leq l$.*

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

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

Theorem 3 *$A^{(\alpha)} \otimes A^{(\beta)} = A^{(\beta)} \otimes A^{(\alpha)}$ for any α and β such that $0 \leq \alpha \leq 1$ and $0 \leq \beta \leq 1$.*

Proof First consider the case of rational $\alpha = \frac{k_1}{l_1}$ and $\beta = \frac{k_2}{l_2}$. Then $\alpha = \frac{k_1 l_2}{l_1 l_2}$ and $\beta = \frac{k_2 l_1}{l_1 l_2}$. Then $A^{(\alpha)} = A^{\left(\frac{k_1 l_2}{l_1 l_2}\right)} = \left(A^{\left(\frac{1}{l_1 l_2}\right)}\right)^{\otimes k_1 l_2}$ and $A^{(\beta)} = \left(A^{\left(\frac{1}{l_1 l_2}\right)}\right)^{\otimes k_2 l_1}$, so $A^{(\alpha)} \otimes A^{(\beta)} = A^{(\beta)} \otimes A^{(\alpha)}$ since both $A^{(\alpha)}$ and $A^{(\beta)}$ are powers of $A^{\left(\frac{1}{l_1 l_2}\right)}$. 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.

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

Proposition 2 *Let A be a generalized Kleene star and D and F be arbitrary diagonal matrices. Then $D \otimes A \otimes F$ is also a generalized Kleene star.*

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

$$d_i \otimes a_{ij} \otimes f_j \otimes d_j \otimes a_{jk} \otimes f_k \leq d_i \otimes a_{ik} \otimes f_k \otimes d_j \otimes a_{jj} \otimes f_j. \qquad (12)$$

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 (12) is the same as $b_{ij} \otimes b_{jk} \leq b_{ik} \otimes b_{jj}$.

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

Corollary 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 generalized Kleeme stars.*

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

Proposition 3 *Let $B \in \mathbb{R}_{\max}^{n\times n}$ be a generalized Kleene star 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.

Proof The Kleene star inequality $a_{ij} \otimes a_{jk} \leq a_{ik}$ is a special case of (1) when $a_{ii} = 0$. By Proposition 2, matrices A_1, A_2 and A satisfy (1). Then it suffices to observe that all diagonal entries of these matrices are equal to 0.

3.2 Matrices of the form $[2r, r]^k_n$

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

Definition 10 For arbitrary real number $r \leq 0$ and real number $k \geq 0$, we denote by $[2r, r]^k_n$ 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 $i \neq j$.

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

Theorem 4 *Let $A \in [2r, r]^{k_1}_n, B \in [2s, s]^{k_2}_n$ for any $r, s \leq 0$ and $a_{ii} = k_1 \geq 0$, $b_{ii} = k_2 \geq 0$ then*

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

Proof For all i, j we have

$$\begin{aligned}(A \otimes B)_{ij} &= a_{ii} \otimes b_{ij} \oplus a_{ij} \otimes b_{jj} \oplus \bigoplus_{p\notin\{i,j\}} a_{ip} \otimes b_{pj} \\ &= k_1 \otimes b_{ij} \oplus k_2 \otimes a_{ij} \oplus \bigoplus_{p\notin\{i,j\}} a_{ip} \otimes b_{pj}.\end{aligned} \tag{13}$$

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

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

Note that we used the well-known inequality $\frac{r+s}{2} \leq \max(r, s)$. Then we obtain:

$$\begin{aligned}(A \otimes B)_{ij} &= k_1 \otimes b_{ij} \oplus a_{ij} \otimes k_2 \oplus \bigoplus_{p\notin\{i,j\}} a_{ip} \otimes b_{pj} \\ &= k_1 \otimes b_{ij} \oplus a_{ij} \otimes k_2 \\ &= (k_2 \otimes A \oplus k_1 \otimes B)_{ij} \\ &= (B \otimes A)_{ij},\end{aligned} \tag{14}$$

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

Proof

$$\begin{aligned}(A \otimes B)_{ij} &= a_{ii} \otimes b_{ij} \oplus a_{ij} \otimes b_{jj} \oplus \bigoplus_{p\notin\{i,j\}} a_{ip} \otimes b_{pj} \\ &= k \otimes b_{ij}.\end{aligned} \tag{15}$$

$$
\begin{aligned}
(B \otimes A)_{ij} &= b_{ii} \otimes a_{ij} \oplus b_{ij} \otimes a_{jj} \oplus \bigoplus_{p \notin \{i,j\}} b_{ip} \otimes a_{pj} \\
&= b_{ij} \otimes k.
\end{aligned} \tag{16}
$$

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 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 next recall.

4.1 Tropical Stickel's protocol of [2]

Protocol 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 a public key V which is obtained from Bob and she have $K_a = p_1(A) \otimes V \otimes p_2(A)$.*
4. *Bob also computes his secret key using Alice public key U and obtain $K_b = q_1(A) \otimes U \otimes q_2(B)$.*

Note that both Alice and Bob using 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, if $A \in \mathbb{R}_{\max}^{n\times n}$ is a generalized Kleene star then its deformations $A^{(\alpha)}$ and $A^{(\beta)}$ commute for any $\alpha, \beta \colon 0 \leq \alpha, \beta \leq 1$. Using this we can define a quasi-polynomial, where the role of monomials is played by deformations.

Definition 11 (Quasi-polynomial) Let $A \in \mathbb{R}_{\max}^{n\times n}$ be a generalized Kleene star. 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 2 (Stickel's protocol using tropical quasi-polynomial).
Alice and Bob agree on some generalized Kleene stars $A, B \in \mathbb{R}_{\max}^{n\times n}$ 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 next describe are based on Theorems 4 and 5.

Protocol 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 $k_1, k_2 \geq 0$. 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 $l_1, l_2 \geq 0$. 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. *Alice and Bob agree on a public matrix $W \in \mathbb{R}_{\max}^{n\times n}$.*

1. *Alice chooses matrix $A_1 \in [2a, a]_n^k$ and sends k to Bob.*
2. *Bob chooses matrix $B_2 \in [2b, b]_n^l$ and sends l to Alice.*
3. *Alice chooses 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 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 1, an attacker commonly named Eve, needs to find matrix X and Y such that the following conditions hold:

$$A \otimes X = X \otimes A, \quad B \otimes Y = Y \otimes B, \tag{17}$$

and

$$X \otimes W \otimes Y = U. \tag{18}$$

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

$$\begin{aligned} X \otimes V \otimes Y &= q_1(A) \otimes X \otimes W \otimes Y \otimes q_2(B) \\ &= q_1(A) \otimes U \otimes q_2(A) = K_b. \end{aligned}$$

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. Although the complexity of their attack in terms of the maximal degree of polynomial is non-polynomial, it is quite efficient when, for example, this maximal degree stays bounded and the dimension of matrices is allowed to grow.

We now describe a version of Kotov and Ushakov attack that applies to Protocol 2 where we have tropical quasi-polynomials instead of polynomials. In this case, instead of (17) we need to require that X, respectively Y, commute with any quasi-polynomial of A, respectively of B. 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 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

$$\begin{aligned} X &= \bigoplus_{\alpha \in \mathcal{T}} x_\alpha \otimes A^{(\alpha)}. \\ Y &= \bigoplus_{\beta \in \mathcal{T}} y_\beta \otimes B^{(\beta)}. \end{aligned} \tag{19}$$

then using (18) we impose

$$\begin{aligned} X \otimes W \otimes Y &= \bigoplus_{\alpha,\beta\in\mathcal{T}} x_\alpha \otimes A^{(\alpha)} \otimes W \otimes y_\beta \otimes B^{(\beta)} \\ &= \bigoplus_{\alpha,\beta\in\mathcal{T}} x_\alpha \otimes y_\beta \otimes A^{(\alpha)} \otimes W \otimes B^{(\beta)} = U. \end{aligned} \tag{20}$$

Equation (20) can be equivalently written as

$$\bigoplus_{\alpha,\beta\in\mathcal{T}} x_\alpha \otimes y_\beta \otimes (A^{(\alpha)} \otimes W \otimes B^{(\beta)} - U) = E, \tag{21}$$

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 (21) as follows:

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

If we denote $z_{\alpha\beta} = x_\alpha \otimes y_\beta = x_\alpha + y_\beta$ 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 pairs kl play the role of rows and pairs $\alpha\beta$ play the role of columns. Such systems are considered, e.g., in Butkovič[1], but here we have an additional requirement that unknowns have a special structure: $z_{\alpha\beta} = x_\alpha \otimes y_\beta = x_\alpha + y_\beta$. Following Kotov and Ushakov [5], to solve this system let us denote $c_{\alpha\beta} = \min_{\gamma,\delta}(-T^{\alpha\beta}_{\gamma\delta})$ and the set of entries where the minimum is achieved by $S_{\alpha\beta} = \arg\min_{\gamma,\delta}(-T^{\gamma\delta}_{kl})$. Then we need to find a minimal cover, i.e., a minimal subset $\mathcal{C} \subseteq \mathcal{T} \times \mathcal{T}$ such that

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

and unknowns x_α, y_β with $\alpha, \beta \in \mathcal{T}$ such that:

$$\begin{cases} x_\alpha + y_\beta = c_{\alpha\beta} & \text{if}(\alpha,\beta) \in C \\ x_\alpha + y_\beta \ \le c_{\alpha\beta} & \text{otherwise.} \end{cases} \tag{22}$$

Thus the Kotov-Ushakov attack on the protocol with tropical quasi-polynomials is very similar to the original one. We implemented it in GAP by modifying the existing code from [5]. Table 1 shows how the the average computation time grows in practice as we increase the maximal degree of monomials in tropical polynomial (Protocol 1) or the maximal denominator of the degree of monomials in tropical quasi-polynomial (Protocol 2).

On 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 minimnal covers, as reported in [5].

Table 1 Growth of average computation time of the Kotov-Ushakov attack on Protocol 1 and Protocol 2 vs. growth of maximal degree and maximal denominator in (19). Dimension of matrices: 10 × 10, entries of A and B are in the range $[-100, 100]$

Protocol using tropical polynomial					
Maximal degree	2	4	6	10	12
Average computation time (second)	0.01718	0.05695	0.15487	0.82611	1.68796

Protocol using tropical quasi-polynomial					
Maximal denominator	2	3	4	5	6
Average computation time (second)	0.03851	0.08804	0.18156	0.84635	1.87849

6 Security of protocols using $[2r, r]_n^k$ matrices

6.1 Attacks on Protocol 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 4, we obtain

$$\begin{aligned} K_a &= (l_1 \otimes A_1 \oplus k_1 \otimes B_1) \otimes W \otimes (k_2 \otimes B_2 \oplus l_2 \otimes A_2) \\ &= (l_1 \otimes k_2 \otimes A_1 \otimes W \otimes B_2) \oplus (l_1 \otimes l_2 \otimes A_1 \otimes W \otimes A_2) \\ &\quad \oplus (k_1 \otimes k_2 \otimes B_1 \otimes W \otimes B_2) \oplus (k_1 \otimes l_2 \otimes B_1 \otimes W \otimes A_2) \\ &= \underline{(l_1 \otimes l_2 \otimes U) \oplus (k_1 \otimes k_2 \otimes V)} \oplus (l_1 \otimes k_2 \otimes A_1 \otimes W \otimes B_2) \\ &\quad \oplus (k_1 \otimes l_2 \otimes B_1 \otimes W \otimes A_2). \end{aligned} \tag{23}$$

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 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* $\max_{i,j} w_{ij} = w_{st}$.

Proof We have

$$\begin{aligned} u_{st} &= k_1 \otimes w_{st} \otimes k_2 \oplus \bigoplus_{(s',t') \neq (s,t)} (A_1)_{ss'} \otimes w_{s't'} \otimes (A_2)_{t't}, \\ v_{st} &= l_1 \otimes w_{st} \otimes l_2 \oplus \bigoplus_{(s',t') \neq (s,t)} (B_1)_{ss'} \otimes w_{s't'} \otimes (B_2)_{t't}. \end{aligned} \tag{24}$$

However, we also have $(A_1)_{ss'} \leq k_1$, $(A_2)_{t't} \leq k_2$, $(B_1)_{ss'} \leq l_1$, $(B_2)_{t't} \leq l_2$ and $w_{s't'} \leq w_{st}$, 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 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 12 **(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 (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*

$$K_a = K_b = l_1 \otimes l_2 \otimes U \oplus k_1 \otimes k_2 \otimes V, \tag{25}$$

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 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 1.

Trying to escape from the case of vanishing W, we tried to consider the case when the range of the entries of W is much bigger than that of other matrices ($A^{(1)}$, $A^{(2)}$, $B^{(1)}$ and $B^{(2)}$). However, then we can assume that the following property holds.

Definition 13 (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 $W = (w_{st}) \in \mathbb{R}_{\max}^{n \times n}$ is called *dominant in $A^{(1)} \otimes W \otimes A^{(2)}$ and $B^{(1)} \otimes W \otimes B^{(2)}$*, if the following properties hold:

$$\begin{aligned} (A^{(1)} \otimes W \otimes A^{(2)})_{il} &= a_{is}^{(1)} \otimes w_{st} \otimes a_{tl}^{(2)}, \quad \forall i, l, \\ (B^{(1)} \otimes W \otimes B^{(2)})_{il} &= b_{is}^{(1)} \otimes w_{st} \otimes b_{tl}^{(2)}, \quad \forall i, l, \end{aligned} \tag{26}$$

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

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

Theorem 7 (Attack when W is dominant) *Suppose that W is dominant in $A^{(1)} \otimes W \otimes A^{(2)}$ and $B^{(1)} \otimes W \otimes B^{(2)}$. Then the entries of the key $K = (k_{il})$ can be found as follows:*

$$k_{il} = w_{st}^{-} \otimes (v_{st} \otimes u_{il} \oplus u_{st} \otimes v_{il} \oplus u_{it} \otimes v_{sl} \oplus v_{it} \otimes u_{sl}). \tag{27}$$

Proof Using (23) and (26), we obtain for the entries k_{il} that

$$\begin{aligned} k_{il} = (l_1 \otimes l_2 \otimes u_{il}) \oplus (k_1 \otimes k_2 \otimes v_{il}) \oplus (l_1 \otimes k_2 \otimes a_{is}^{(1)} \otimes w_{st} \otimes b_{tl}^{(2)}) \\ \oplus (k_1 \otimes l_2 \otimes b_{is}^{(1)} \otimes w_{st} \otimes a_{tl}^{(2)}). \end{aligned} \tag{28}$$

The attacker can compute $l_1 \otimes l_2$ and $k_1 \otimes k_2$ as in Lemma 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 (26)

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

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

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

Substituting this into (28) 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 (27).

Now let us consider the formulae (25) and (27) as heuristic attacks on Protocol 3. To analyze the success of these attacks we consider 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 (25) or (27), 2) the **similarity rate**: the average percentage of the entries of the matrix computed by (25) or (27) which are equal to those in the secret key $K_a = K_b$ in the case of “no success” when the matrix computed by (25) or (27) does not coincide with the key. The results of our experiments are shown in Tables 2 and 3.

Table 2 Dependency of the success rate of the attacks based on (25) and (27) on the matrix dimension. Here the entries of W are chosen randomly in $[1, 1000000]$. Parameters a, b are in the range $[1, 20]$, and c, d are in the range $[60, 100]$, and k_1, k_2, l_1, l_2 are random positive number in the range $[0, 100]$.

Dimension of matrices	5	20	30	40
Success rate for the attack using (25)	22.8%	7%	6.2%	6%
Success rate for the attack using (27)	100%	99.8%	99.7%	99.1%

Table 3 Dependency of the similarity rate of the attacks based on (25) and (27) on the matrix dimension. The ranges of entries of W and all parameters are as in Table 2

Dimension of matrices	5	20	30	40
Similarity rate for the attack using (25)	60.2%	54.5%	49.35%	44.5 %
Similarity rate for the attack using (27)	-	97.11%	98.3%	98.5%

We see that the attack based on (27) is much more successful when the entries of W are within a much bigger range than all other important parameters. This is due to the fact that in this case W is highly likely to be dominant.

Let us now look at the case when the range of the entries of W is not so big compared to all other parameters. Considering the success rate and the similarity rate once again, we arrive at the following results shown in Tables 4 and 5.

Table 4 Dependency of the success rate of the attacks based on (25) and (27) on the matrix dimension. The entries of W are in the range $[-100, 100]$. Parameters a, b are in the range $[1, 20]$, parameters c, d are in the range $[60, 100]$, and k_1, k_2, l_1, l_2 are random positive number in the range $[0, 100]$.

Dimension of matrices	5	20	30	40
Success rate for the attack using (25)	85.4%	88.8%	90.4%	95.5%
Success rate for the attack using (27)	79.6%	50.8%	40.8 %	39.4%

Table 5 Dependency of the similarity rate of the attacks based on (25) and (27) on the matrix dimension. The ranges of the entries of W and all parameters are as in Table 4

Dimension of matrices	5	20	30	40
Similarity rate for the attack using (25)	78%	93%	98.45%	99.1%
Similarity rate for the attack using (27)	92%	97.125%	98.85%	99.45%

We see that in this case the simpler attack based on formula (25) is more efficient, and in particular, its success rate grows with the dimension while the success rate of the attack based on (27) decreases. However, the similarity rate remains overwhelming for both attacks and any dimension with which we experimentated.

In view of the success of simple heuristic attacks based on (25) and (27), it is still challenging to suggest W that would most often withstand these attacks 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

Previous subsection yields some simple but efficient enough heuristic attacks on Protocol 3. We now discuss how the Kotov-Ushakov attack can be generalized to apply to both Protocol 3 and 4. The main idea is to use tropical identity matrix and tropical elementary matrices to generate the matrices from 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

$$\begin{aligned}
&X=\bigoplus_{\alpha\in\mathcal{A}} x_\alpha\otimes A_\alpha,\quad Y=\bigoplus_{\beta\in\mathcal{B}} y_\beta\otimes B_\beta,\\
&X\otimes W\otimes Y=U,\\
&x_\alpha\in\mathcal{X}_\alpha(s),\quad y_\beta\in\mathcal{Y}_\beta(t).
\end{aligned}\tag{29}$$

Here $\{A_\alpha\colon \alpha\in\mathcal{A}\}$ and (respectively) $\{B_\beta\colon \beta\in\mathcal{B}\}$ are the finite sets of matrices such that any matrix that can be used by Alice and (respectively) by Bob can be represented as in the first line of (29), provided that the coefficients x_α and y_β satisfy the conditions written in the last line of (29). 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 (29) is based on the same ideas from [5] that were already used in Subsection 5.2. After we substitute the first line of (29) into the decomposition problem $X\otimes W\otimes Y=U$ and denote

$$T^{\alpha\beta}=A_\alpha\otimes W\otimes B_\beta-U,\tag{30}$$

the decomposition problem reduces to solving the system

$$\max_{\alpha\in\mathcal{A},\beta\in\mathcal{B}}(x_\alpha\otimes y_\beta\otimes T_{kl}^{\gamma\delta})=0,\quad \forall\gamma,\delta\in[n].\tag{31}$$

Here, unlike in Subsection 5.2, x_α and y_β also satisfy the conditions in the last line of (29). As in Subsection 5.2, we denote

$$\begin{aligned}
c_{\alpha\beta}&=\min_{\gamma,\delta\in[n]}(-T_{\gamma\delta}^{\alpha\beta}),\\
S_{\alpha\beta}&=\arg\min_{\gamma,\delta\in[n]}(-T_{\gamma\delta}^{\alpha\beta}).
\end{aligned}\tag{32}$$

Then we need to find a minimal cover, i.e., a minimal subset $\mathcal{C}\subseteq\mathcal{A}\times\mathcal{B}$ such that

$$\bigcup_{(\alpha,\beta)\in\mathcal{C}} S_{\alpha\beta}=[n]\times[n],\tag{33}$$

and unknowns x_α, y_β with $\alpha\in\mathcal{A},\beta\in\mathcal{B}$ such that:

$$\begin{aligned}
&x_\alpha+y_\beta=c_{\alpha\beta}\quad \text{if}(\alpha,\beta)\in\mathcal{C}\\
&x_\alpha+y_\beta\le c_{\alpha\beta}\quad \text{otherwise},\\
&x_\alpha\in\mathcal{X}_\alpha(s),\quad y_\beta\in\mathcal{Y}_\beta(t),
\end{aligned}\tag{34}$$

where (as explained above) $\mathcal{X}_\alpha(s)$ and $\mathcal{Y}_\beta(t)$ are subsets of $\mathbb{R}$ whose specification depends on vectors s and t of unknown parameters.

The practical solvability of problem (34) 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 that problem (34) is still a linear programming problem.

6.3 Kotov-Ushakov attack on Protocol 3

In Protocol 3, we have $A_1 \in [2a, a]_n^{k_1}$ and $A_2 \in [2b, b]_n^{k_2}$ with unknown nonpositive a, b, and unknown nonnegative k_1 and k_2. Using tropical elementary matrices and I as A_α and B_β with α and β being pairs of indices from $[n]$, we can represent any matrix in $[2a, a]_n^{k_1}$ and $[2b, b]_n^{k_2}$ as in the first line of (29). However, for this we also need to restrict the coefficients x_α to belong to $[2a, a]$ for some $a \le 0$ if $\alpha = (i, j)$ with $i \ne j$ or to be equal to some $k_1 \ge 0$ if $i = j$. Similarly, the coefficients y_β should belong to $[2b, b]$ for some $b \le 0$ if $\beta = (i, j)$ with $i \ne j$ or to be equal to some $k_2 \ge 0$ if $i = j$.

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

$$A_\alpha = A^{ij} = B_\beta = B^{ij} = \begin{cases} E^{ij}, \text{ for } i \ne j \\ \;I, \;\;\text{ for } i = j. \end{cases} \tag{35}$$

where $(i, j) \in [n] \times [n]$, thus $\mathcal{A} = \mathcal{B} = [n] \times [n]$.

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

$$\mathcal{X}_{(i,j)}(a, k) = \begin{cases} [2a, a], \; i \ne j \\ \;\{k\}, \;\; i = j. \end{cases} \tag{36}$$

$$\mathcal{Y}_{(i,j)}(b, l) = \begin{cases} [2b, b], \; i \ne j \\ \;\{l\}, \;\; i = j, \end{cases} \tag{37}$$

where $k, l \ge 0$ and $a, b \le 0$.

In order to implement the attack, we define the matrices $T^{\alpha\beta}$ by (30) where $\alpha = (i, j)$ and $\beta = (s, t)$ with $i, j, s, t \in [n]$, and we define A_α and B_β by (35). We further define $c_{\alpha\beta} = c_{ijst}$ and $S_{\alpha\beta} = S_{ijst}$ by (32), and among the minimal sets $\mathcal{C} \subseteq [n]^2 \times [n]^2$ that satisfy (33) we seek those which satisfy

$$\begin{aligned} & x_{ij} + y_{st} = c_{ijst}, \quad \text{for} \quad (i, j, s, t) \in \mathcal{C} \\ & x_{ij} + y_{st} \le c_{ijst}, \quad \text{otherwise}, \\ & 2a \le x_{ij} \le a, \quad 2b \le y_{st} \le b, \quad \forall i \ne j, \;\; s \ne t, \\ & x_{ii} = k_1, \quad y_{ss} = k_2, \quad \forall i, s, \\ & a, b \le 0, \quad k_1, k_2 \ge 0. \end{aligned} \tag{38}$$

6.4 Kotov-Ushakov attack on Protocol 4

In Protocol 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 $\{1, \ldots, n\}$, we can represent any matrix in $[2a, a]_n^k$ and $[0, l]_n$ as in the first line of (29). However, for this we also need to restrict the coefficients x_α to belong to $[2a, a]$ for some $a \le 0$ if $\alpha = (i, j)$ with $i \ne j$ 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 $\alpha = \beta = (i,j)$ to be:

$$\begin{aligned} A_\alpha &= A^{ij} = \begin{cases} E^{ij}, \text{ for } i \neq j, \\ I, \quad \text{for } i = j, \end{cases} \\ B_\beta &= B^{ij} = E^{ij}. \end{aligned} \tag{39}$$

Here $(i,j) \in [n] \times [n]$, thus again $\mathcal{A} = \mathcal{B} = [n] \times [n]$.

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

$$\mathcal{X}_{(i,j)}(a) = \begin{cases} [2a, a], \; i \neq j \\ \{k\}, \quad i = j. \end{cases} \tag{40}$$

$$\mathcal{Y}_{(i,j)} = [0, l] \quad \forall i, j. \tag{41}$$

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 $a \leq 0$.

In order to implement the attack, we define the matrices $T^{\alpha\beta}$ by (30) where $\alpha = (i,j)$ and $\beta = (s,t)$ with $i, j, s, t \in [n]$, and we define A_α and B_β by (39). We further define $c_{\alpha\beta} = c_{ijst}$ and $S_{\alpha\beta} = S_{ijst}$ by (32), and among the minimal sets $\mathcal{C} \subseteq [n]^2 \times [n]^2$ that satisfy (33) we seek those which satisfy

$$\begin{aligned} & x_{ij} + y_{st} = c_{ijst}, \quad \text{for} \quad (i,j,s,t) \in \mathcal{C} \\ & x_{ij} + y_{st} \leq c_{ijst}, \quad \text{otherwise}, \\ & 2a \leq x_{ij} \leq a, \quad x_{ii} = k, \quad \forall i \neq j, \\ & 0 \leq y_{st} \leq l \quad \forall s, t, \quad a \leq 0. \end{aligned} \tag{42}$$

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 can be rather successfully used as heuristic attacks 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 1) as well as when too large subsets of rational numbers in $[0, 1]$ are used in the protocol with quasi-polynomials (Protocol 2). We also do not expect it to be successful for large n in the protocols with $[2r, r]_n^k$ matrices (Protocols 3 and 4). Therefore, it still makes sense to search for alrternative attacks on our new protocols. For

Protocol 3, since some rather successful heuristic attacks have been found, it is neccessary to look for a new 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 semidirect product, and therefore they are immune to Kotov-Ushakov attack and present a new interesting object of study.

Acknowledgements The authors would like to thank Dr. Daniel Jones for discussing with them the roots of tropical matrices and results that he obtained in his PhD Thesis, and also Dr. Matvei Kotov for help with GAP and useful advice on how to use the code which was written for [5]. The first author is supported by Ministry of Religion and Affair (MORA) Scholarship, Indonesia.

References

1. Butkovič, P.: Max-linear Systems: Theory and Algorithms. Springer Science & Business Media (2010)
2. Grigoriev, D., Shpilrain, V.: Tropical cryptography. Communications in Algebra **42**(6), 2624–2632 (2014)
3. Grigoriev, D., Shpilrain, V.: Tropical cryptography II: extensions by homomorphisms. arXiv preprint arXiv:1811.06386 (2018)
4. Jones, D.: Special and structured matrices in max-plus algebra. Ph.D. thesis, University of Birmingham (2017)
5. Kotov, M., Ushakov, A.: Analysis of a key exchange protocol based on tropical matrix algebra. IACR Cryptology ePrint Archive **2015**, 852 (2015)
6. Linde, J., de la Puente, M.: Matrices commuting with a given normal tropical matrix. Linear Algebra and its Applications **482**, 101–121 (2015)
7. Shpilrain, V.: Cryptanalysis of Stickel's key exchange scheme. Lecture Notes in Computer Science **5010**, 283–288 (2008)