Public Key Cryptography Based on Tropical Algebra

by

Any Muanalifah

A thesis submitted to
The University of Birmingham
for the degree of
Doctor of Philosophy

Supervisor: Dr. Sergeĭ Sergeev
School of Mathematics
The University of Birmingham
June 2022

Abstract

We analyse some public keys cryptography in the classical algebra and tropical algebra. Currently one of the most secure system that is used is public key cryptography, which is based on discrete logarithm problem. The Dilfie-Helman public key and Stickel's key exchange protocol are the examples of the application of discrete logarithm problem in public key cryptography. This thesis will examine the possibilities of public key cryptography implemented within tropical mathematics. A tropical version of Stickel's key exchange protocol was suggested by Grigoriev and Sphilrain We suggest some modifications of this scheme use commuting matrices in tropical algebra and discuss some possibilities of attacks on them. We also generalise Kotov and Ushakov's attack and implement in our new protocols. In 2019, Grigoriev and Sphilrain [14] generated two new public key exchange protocols based on semidirect product. In this thesis we use some properties of CSR and ultimate periodicity in tropical algebra to construct an efficient attack on one of the protocols suggested in that paper.

Acknowledgements

I would like to thank my PhD supervisor Dr Sergeĭ Sergeev for helping me to create this thesis. He spent a lot of time to teach me how to conduct this research. His effort and his passion motivated me to analyse the security of existing protocols based on tropical algebra and to think of constructing some new ones.

I would also like thank my family (especially my Father Mukijan), closed friends (especially Dr. Arthur Kennedy-Cochran-Patrick and Dr. Asrul Harun Ismail), my beloved one Kashif Sharif who always stand by me and support me during my study and my sponsorship Ministry of Religion and Affairs who supported me during my study.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Tropical Cryptography is a new area that uses the structures of tropical mathematics as a new platform for classical public key exchange protocols in cryptography (such as the Diffie-Hellman and Stickel methods). The idea of using tropical algebra (and, more generally, tropical mathematics) was pioneered by Grigoriev and Shpilrain [13]. In this chapter, we provide an overview of the relevant concepts in public key cryptography, introduce tropical algebra and give an outline of this thesis.

1.1 Cryptography and tropical algebra

Cryptography studies security of communication over a public channel. For examples, suppose that two parties, Alice and Bob, need to communicate privately. There is a third party, Eve, who wants to know what they are communicating. Therefore, Alice and Bob need some secure system that will allow them to communicate with each other without Eve intercepting their information. To do so, in their communication, Alice and Bob need a key or a password to protect their information; therefore, the problem for Alice and Bob is how to generate their private key securely. A mathematical approach to this problem was put forward by Diffie and Hellman in 1976 [10] and led to the famous Diffie-Hellman public key exchange protocol.

The tropical (or max-plus) semiring is the set $\mathbb{R}_{\max} = \mathbb{R} \cup \{-\infty\}$ equipped with the operations $a \oplus b = \max(a, b)$ and $a \otimes b = a + b$ defined for all $a, b \in \mathbb{R}_{\max}$. The set $\mathbb{R}_{\max}$ equipped with operations $\oplus, \otimes$ is denoted by $(\mathbb{R}_{\max}, \oplus, \otimes)$. These operations can be extended to vectors and matrices in the usual way (see Definition 2.1.3 below), thus giving rise to tropical linear algebra.

Grigoriev and Shpilrain [13] were the first to use tropical linear algebra to develop a new implementation of a public key exchange protocol. The idea of using tropical linear algebra for this purpose is supported by the observation that matrices in tropical linear algebra are usually not invertible. They also developed two new protocols based on the semidirect product in 2019 [14].

In the following sections, we are going to review some of the relevant literature on cryptography and tropical linear algebra, and provide an overview of this thesis.

1.2 Literature review

The first known usage of cryptography in communication occurred around 2000 B.C., when hieroglyphics were used in ancient Egypt for communication. In principle, cryptography is used for hiding secret information or a secret message. To hide a message, the sender needs to encrypt the plaintext into unreadable text called ciphertext and the receiver needs to decrypt the ciphertext into plaintext. The earliest methods which were used for encryption were transposition and substitution ciphers. One of the oldest examples of transposition ciphers was the scytale, which was used by the ancient Greeks, and one of the most famous substitution ciphers was Caesar's cipher, which was used by Julius Caesar himself in his private communication [37].

In cryptography, there are two methods that are used to help us share the secret information, namely the symmetric key and the asymmetric key. The transposition cipher and the substitution cipher are classical examples of symmetric keys in cryptography. A

standard symmetric key uses a single key to encrypt and decrypt the message, and this means that Alice and Bob need to share their secret key over unsecured channel. To address this problem, Diffie and Hellman [10] introduced a new method in cryptography, allowing both parties to share a private document without sharing their secret key. This system is now known as public key cryptography or asymmetric key cryptography. Their concept has led to significant developments in the public key cryptography theories.

Most of the modern public key cryptography methods use groups, semigroups and other algebraic structures. In 1985 Wagner and Magyarik [39] used the word problem for groups and semigroups to generate a key exchange protocol. Stickel introduced a new key exchange protocol using non-Abelian groups. This protocol is based on the same idea as the Diffie-Hellman protocol and uses invertible matrices [38]. In 2005, Maze, Monico and Rosenthal suggested a generalisation of the Diffie-Hellman key exchange protocol based on semigroup action [25]. In 2016, Kahrobaei and Shpilrain described a modification of the Diffie-Hellman protocol based on the semidirect product of semigroups [21].

The use of tropical mathematics in cryptography was pioneered by Grigoriev and Shpilrain [13]. In particular, they developed a tropical implementation of Stickel's key exchange protocol that uses polynomials over tropical algebra. Their idea is that using tropical algebra instead of classical algebra is promising since matrices in tropical algebra are usually not invertible, and therefore the decomposition problem in tropical linear algebra cannot be simplified. They also introduced public key encryption using the automorphism semigroup in tropical algebra.

There are also some other works that use tropical mathematics in cryptography. Chauvet and Mahe [5] discussed the Diffie-Hellman key exchange protocol based on tropical Hessian pencil, and Grigoriev and Shpilrain [14] suggested two new implementations of public key exchange protocols that use semi-direct product in tropical algebra.

Some cryptanalysis of these protocols also has been published. Shpilrain [35] sug-

gested a linear algebra attack on Stickel's protocol for the case when it uses invertible matrices. Furthermore, Kotov and Ushakov [23] developed a rather successful attack on Grigoriev and Shpilrain's tropical implementation of Stickel's protocol [13]. In this thesis, we are going to discuss Kotov and Ushakov's attack more deeply and suggest a number of modifications of it.

In order to modify Stickel's key exchange protocol, we are going to study some classes of commuting matrices in tropical algebra. Existing literature on commuting matrices in tropical algebra is rather scarce. Some initial observations on them were made by Cuninghame-Green and Butkovič [9].

Later Katz, Schneider and Sergeev [22] observed some facts on common eigenvector, critical graphs and Frobenius normal forms of tropical commuting matrices. In this thesis we are going to make use of: 1) the work of Linde and de la Puente [24] who discovered some new classes of commuting normal matrices in tropical algebra, 2) the work of Jones [19], who discovered that tropical matrix roots exist for matrices over tropical semiring that satisfy a specific property (to be detailed later). We will show that tropical matrix roots commute with each other and the observations of Jones [19] can be generalised to give rise to new sets of pairwise commuting matrices.

In [14], Grigoriev and Shpilrain considered the semidirect product in tropical algebra. Using this new concept, they constructed two new protocols. They claimed that the resulting expression for the key in terms of the tropical matrix powers and their products becomes very intricate and presents a challenge for the attacker. However, in 2020 two papers analysing the security of new protocols of Grigoriev and Shpilrain were published. Rudy and Monico [32], observed the non-decreasing property of the sequence of powers based on the tropical semi-direct product and suggested an attack on one of the protocols of [14] based on binary search. This attack is guaranteed to work and can be efficiently implemented. However, its worst-case computational complexity is $O(K^2)$, where K is

an upper bound on the logarithm of the secret keys (power exponents) used by Alice and Bob to construct their messages.

Isaac and Kahrobaei [18] took a different approach to attack the same protocol of Grigoriev and Shpilrain [14]. They find the secret keys of Alice and Bob based on the assumption that the sequence of the powers based on tropical semi-direct product is ultimately periodic (although not providing a theoretical proof of that property). Not being dependent on the magnitude of the secret keys of Alice and Bob, this attack is more efficient in practice. Isaac and Kahrobei also prove that the second protocol suggested by Grigoriev and Shpilrain [14] is invalid, since the version of semi-direct product which is used in it does not satisfy associativity.

1.3 Thesis overview

There are two main achievements of this thesis. One of them is described in Chapter 5. There we construct a number of new tropical implementations of Stickel's protocol and consider some attacks on them: generalised Kotov-Ushakov attack and other more special attacks, which are called heuristic attacks. These new implementations are based on new classes of commuting tropical matrices described in Chapter 4. The second achievement is an attack on the protocol suggested by Grigoriev and Shpilrain [14]. This protocol is based on the tropical semidirect product, however we showed that the messages of Alice and Bob can be expressed via tropical matrix powers. This allows us to construct an attack on the protocol based on the ultimate periodicity properties of tropical matrix powers, more precisely on the ultimate periodicity of the columns with indices in the critical digraph [26] and the weak CSR expansions developed by Merlet et al [27]. To connect this results with cryptography we introduce and consider the tropical discrete logarithm problem in Chapter 3. There we suggest a polynomial algorithm for solving this problem and discuss the conditions under which it works.

Let us now describe the structure of this thesis in more detail.

In Chapter 2, we start with some basic definitions concerning tropical algebra and cryptography that are useful for our research.

In Chapter 3, we will give a basic definition of the discrete logarithm problem in classical algebra and suggest its analogue in tropical matrix algebra. The tropical discrete logarithm algorithm will be later applied to attack the protocol based on semidirect product [14]. We will also consider a two-sided extension of the tropical discrete logarithm in the last section of this chapter, which can potentially be used to construct a new attack on the tropical Stickel's key exchange protocol. We also implemented the two- sided tropical discrete logarithm problem to examine the success rate of the attack in the tropical version of Stickel's protocol.

Since we need new classes of tropical commuting matrices to construct the new implementations of Stickel's key exchange protocol, in Chapter 4 we will construct new classes of commuting matrices in tropical algebra. We start with the results of Jones [19], which we develop and extend in order to describe a new class of commuting matrices. Then, we consider two classes of commuting matrices that are due to Linde and De La Puente [24] and extend them. The first class of commuting matrices is comprised of matrices whose diagonal entries are equal to zero and non-diagonal entries lie in the interval $[2a, a]$ for some negative real number a, and we extend this class by allowing the diagonal entries to be equal to the same nonnegative number, so that they do not have to be equal to 0. The second class of commuting matrices is a combination of the matrix of all zeros and a tropical monomial matrix, and for this class we prove an extension of Theorem 22 from [24].

In Chapter 5, we start by constructing several new implementations of Stickel's protocol that use the new classes of commuting matrices that we described in Chapter 4. For one of these protocols we suggest a couple of simple attacks that, strictly speaking, work

only in special situations, but we can also use them as quite successful heuristic attacks in a general situation. Next, for all of these protocols we generalise the Kotov and Ushakov attack and describe how this generalised attack can be specialised to every protocol.

In Chapter 6, we first describe the new public key exchange protocol of Grigoriev and Shpilrain [14] (based on semidirect product). We analyse the security of Public Key Cryptography based on semidirect product [14] aiming to attack the protocol using our solution to the tropical discrete logarithm problem. The solution to that problem is based on the ultimate periodicity properties of tropical matrix powers, investigated previously by Merlet et al. [27, 26]. The attack on the protocol is then constructed as follows: first we explain how the powers based on the tropical semi-direct product can be conveniently expressed using tropical matrix powers and products, and then we use the solution to the tropical discrete logarithm problem to find the secret keys of Alice and Bob.

Various numerical experiments have been conducted to confirm the validity and investigate the efficiency of the attacks that are suggested in this thesis. For protocol using commutative matrices based on Linde and De La Puente matrices [24], we developed code for a heuristic attack with MATLAB version R2019b to analyse the efficiency of our attack we vary the bounds of the interval from which the parameters of the protocol instance are randomly chosen, conducting 1000 experiments for each value of the bound: see Chapter 5 for more details. We also developed code for modified Stickel's protocol (quasi-polynomials) using GAP (modifying Ushakov and Kotov code). For our attack on the protocol using semi-direct product, we developed a set of programs in Python where we used and modified parts of Isaac and Kahrobei's program for implementing the protocol and a C program implementing the policy iteration algorithm computing the maximum cycle mean due to Cochet-Terrasson et al. [6]. Our programs have been uploaded to GitHub[1]

[1]Python: https://www.github.com/anymath13/tropicalcryptographypython, MATLAB: https://github.com/anymath13/tropicalcryptographymatlab,

The main results of this thesis have been published in academic journals. Most of the material of Chapter 3 and Chapter 6 has appeared online in a joint publication with Dr S. Sergeev [29]. This paper is about our attack on the protocol suggested by Grigoriev and Shpilrain based on tropical semidirect product. Most of the results of Chapter 4 and Chapter 5 have been published in another joint article with Dr S. Sergeev [28]. This article is about new tropical implementations of Stickel's protocol based on some new classes of commuting matrices in tropical algebra. In both publications, the main ideas to consider new classes of commuting matrices and to formulate the tropical discrete logarithm problem and build an attack based on CSR expansion and ultimate periodicity emerged in discussions with Dr S. Sergeev. I developed those ideas, worked out the technical details of the proofs and was responsible for all numerical experiments.

GAP: `https://github.com/anymath13/tropicalcryptographyGAP`

Chapter 2

Preliminaries

This chapter gives some basic definitions and results in tropical algebra and cryptography, which will be used in this thesis.

2.1 Tropical algebra

Let us first give a formal definition of semiring. We are going to deal with a particular semiring in this thesis (called tropical semiring), but this more general definition is also of interest, since some of the protocols that we consider can be formulated over a wider class semirings.

Definition 2.1.1 (Semiring) *Let R be a non-empty set equipped with two binary operations $\oplus$ and $\otimes$, which satisfy the following properties:*

1. *$(R, \oplus)$ is an Abelian semigroup, which means that the following properties hold:*

   (i) ***associativity:***

   for all $a, b, c \in R$ we have $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

   (ii) ***existence of an identity element:***

   there exists $\varepsilon \in R$ such that for all $a \in R$ then $\varepsilon \oplus a = a \oplus \varepsilon = a$.

(iii) ***commutativity:***

for all $a, b \in R$ *then* $a \oplus b = b \oplus a$.

2. $(R, \otimes)$ *is a semigroup, which means:*

   (i) ***associativity:***

   for all $a, b, c \in R$ *then* $(a \otimes b) \otimes c = a \otimes (b \otimes c)$.

   (ii) ***existence of an identity element:***

   there exists $e \in R$ *such that for all* $a \in R$ *then* $e \otimes a = a \otimes e = a$.

3. $(R, \oplus, \otimes)$ *is* ***distributive:*** *for all* $a, b, c \in R$ *we have*

   (i) $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

   (ii) $(b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a)$.

4. ***absorbing property*** *of* ε: $\varepsilon \otimes e = e \otimes \varepsilon = \varepsilon$.

The following is a key example of semiring, to be considered throughout this thesis.

Example 2.1.1 (Tropical semiring (e.g.,[3]) Tropical semiring *is defined as the set* $\mathbb{R}_{\max} = \mathbb{R} \cup \{-\infty\}$ *we mean the set of equipped with two binary operations* $\oplus$ *and* $\otimes$ *defined by*

$$a \oplus b = \max(a, b),$$
$$a \otimes b = a + b.$$

The neutral element with respect to addition $\oplus$ *is* $-\infty$*, it is also called the* semiring zero*, and the neutral element with respect to multiplication is* 0*, it is the* semiring unit. *Inverse with respect to multiplication is defined for any* $a \in \mathbb{R}_{\max}$ *and is equal to* $a^{-} = -a$.

Example 2.1.2 *Let us illustrate some algebraic properties of the tropical arithmetics. First of all, we have* $2 \otimes 0 = 2 + 0 = 2$ *and* $-\infty \oplus 1 = 1$*, demonstrating the role of* 0 *and* $-\infty$ *as the unit and zero of the tropical semiring, respectively. The addition operation does not admit inverses but it is idempotent:* $2 \oplus 2 = 2$*. The multiplication is a group operation:* $5 \otimes (-5) = 0$*.*

The tropical semiring has a number of useful properties, which makes it rather special. We first note that, like in the field of real or complex numbers, the multiplication operation is a group operation, meaning that the tropical semiring is a semifield according to the following definition.

Definition 2.1.2 *If each element of a semiring* R *not equal to* ε *has an inverse with respect to* $\otimes$*, i.e., if for each* $a \in R \backslash \{\varepsilon\}$ *we have* a^- *with a property that* $a^- \otimes a = a \otimes a^- = e$*, then it is called a semifield.*

The tropical semiring (semifield) is also commutative ($a \otimes b = b \otimes a$ for all $a, b \in R$) and idempotent ($a \oplus a = a$ for all $a \in R$). Any idempotent semiring induces a partial order on its elements by the rule $a \oplus b = b \Leftrightarrow a \preceq b$, which in the case of tropical semiring is the usual total order on real numbers. Thus we have $a \oplus b = b \Leftrightarrow a \leqslant b$ for the tropical semiring and the usual order on real numbers (assuming that $-\infty$ is the smallest element).

The following definition reassures us that the basic operations with matrices are defined in the usual way (but using the new arithmetics). By $[m]$ and $[n]$ we denote $\{1, \ldots, m\}$ and $\{1, \ldots, n\}$.

Definition 2.1.3 (Tropical matrix addition and multiplication (e.g., [3])) *For an element* $c \in \mathbb{R}_{\max}$ *and* $A = (a_{ij}) \in \mathbb{R}_{\max}^{m \times n}$ *one defines* $c \otimes A$ *by*

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

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*

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

Equipped with these operations, matrices and vectors over $\mathbb{R}_{\max}$ form the tropical matrix algebra. Let us also remark that the semiring $\mathbb{R}_{\max}$ itself is also often called "tropical algebra" or "max-plus algebra" in the literature.

Example 2.1.3 *Suppose* $A = \begin{pmatrix} -2 & -1 & -\infty \\ 2 & 0 & -4 \\ 6 & -2 & -5 \end{pmatrix}$ *and* $B = \begin{pmatrix} -2 & -\infty & 0 \\ 1 & 4 & -2 \\ -\infty & 0 & 1 \end{pmatrix}$*. Then we have*

$$A \oplus B = \begin{pmatrix} \max(-2,-2) & \max(-1,-\infty) & \max(-\infty,0) \\ \max(2,1) & \max(0,4) & \max(-4,-2) \\ \max(6,-\infty) & \max(-2,0) & \max(-5,1) \end{pmatrix} = \begin{pmatrix} -2 & -1 & 0 \\ 2 & 4 & -2 \\ 6 & 0 & 1 \end{pmatrix},$$

$$A \otimes B = \begin{pmatrix} \max(-4,0,-\infty) & \max(-\infty,3,-\infty) & \max(-2,-3,-\infty) \\ \max(0,1,-\infty) & \max(-\infty,4,-4) & \max(2,-2,-3) \\ \max(4,-1,-\infty) & \max(-\infty,2,-5) & \max(6,-4,-4) \end{pmatrix} = \begin{pmatrix} 0 & 3 & -2 \\ 1 & 4 & 2 \\ 4 & 2 & 6 \end{pmatrix},$$

$$3 \otimes A = \begin{pmatrix} 3+(-2) & 3+(-1) & 3+(-\infty) \\ 3+2 & 3+0 & 3+(-4) \\ 3+6 & 3+(-2) & 3+(-5) \end{pmatrix} = \begin{pmatrix} 1 & 2 & -\infty \\ 5 & 3 & -1 \\ 9 & 1 & -2 \end{pmatrix}.$$

One of the central problems in tropical linear algebra is the eigenproblem.

Definition 2.1.4 (Tropical eigenproblem (e.g.,[3])) *Let $A \in \mathbb{R}_{\max}^{n\times n}$. Element $\lambda \in \mathbb{R}_{\max}$ is called a (tropical) eigenvalue of A if there exists a vector $x \in \mathbb{R}_{\max}^{n}$ with some components in $\mathbb{R}$ such that*

$$A \otimes x = \lambda \otimes x.$$

In this case x is called a (tropical) eigenvector of A associated with eigenvalue λ.
The greatest tropical eigenvalue of A will be denoted by $\lambda(A)$.

In general, a square matrix over tropical semiring always has an eigenvalue. It can have up to n different eigenvalues in the above sense, described in detail by Butkovič [3] (see also references therein).

The neutral element with respect to matrix multiplication (i.e., $I \in \mathbb{R}_{\max}^{n\times n}$ such that $A \otimes I = I \otimes A = A$ for all $A \in \mathbb{R}_{\max}^{n\times n}$) can be characterized as follows.

Definition 2.1.5 (Tropical identity matrix (e.g., [3])) *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 $-\infty$.

Tropical identity matrices are a special case of tropical diagonal matrices.

Definition 2.1.6 (Tropical diagonal matrices (e.g., [3])) *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 we have $D^- \otimes D = D \otimes D^- = I$. 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 $[n]$, 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 invertible $n \times n$ tropical monomial matrices is precisely the group of all invertible matrices in $\mathbb{R}_{\max}^{n \times n}$ (e.g., [3] Theorem 1.1.3).

Monomial matrices X can be used for performing similarity transformations (similarity scalings) in tropical algebra: $A \to X^- \otimes A \otimes X$. The following scaling is a useful special case of this.

Definition 2.1.7 (Tropical diagonal similarity scaling (e.g.,[3])) *Let* $A \in \mathbb{R}_{\max}^{n \times n}$ *and* D *be a tropical diagonal matrix, then we define a diagonal similarity scaling as the transformation* $A \mapsto D^- \otimes A \otimes D$*.*

The similarity scaling and, in particular, diagonal similarity scaling does not change the (tropical) eigenvalues of A. It is easy to see that if λ is an eigenvalue of A, then it is

also an eigenvalue of $D^- \otimes A \otimes D$ where D is an invertible diagonal matrix.

Any matrix over $\mathbb{R}_{\max}$ can be written as a tropical sum of what we will call tropical elementary matrices.

Definition 2.1.8 (Tropical 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 $i, j \in [n]$ and $k, l \in [n]$.

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

Let us now consider the tropical matrix powers.

Definition 2.1.9 (Tropical matrix powers (e.g.,[3])) *Let $A \in \mathbb{R}_{\max}^{n\times n}$. The kth tropical matrix power of A is defined as*

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

In tropical algebra, by analogy with linear algebra, we can define the zeroth power of A, denoted by $A^{\otimes 0}$, to be the identity matrix I of the same dimensions as A.

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

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

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

$$a^{\otimes r} = r \times a, \quad r, a \in \mathbb{R}; \quad (-\infty)^{\otimes r} = -\infty, \quad \forall r > 0; \quad (-\infty)^{\otimes 0} = 0.$$

Furthermore, we can also consider tropical polynomials.

Definition 2.1.10 (Tropical polynomials (e.g.,[3])) *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. Like 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.

Tropical matrix powers with different exponents can also be summed up together (tropically), and this gives rise to the following important objects.

Definition 2.1.11 (Metric Matrices and Kleene Stars (e.g.,[3])) *Let* $A \in \mathbb{R}_{\max}^{n \times n}$ *and consider the following formal sums:*

$$A^{+} = A \oplus A^{\otimes 2} \oplus A^{\otimes 3} \oplus \dots \tag{2.1.1}$$

and

$$A^{*} = I \oplus A \oplus A^{\otimes 2} \oplus \dots \tag{2.1.2}$$

If the series (2.1.1) *and* (2.1.2) *converge then they are called metric matrix and the Kleene star of* A *respectively.*

Note that the convergence of scalar sequences in $\mathbb{R}_{\max}$ is understood in the sense of the metric $d(x, y) = |e^x - e^y|$ defined for any $x, y \in \mathbb{R}_{\max}$, and the convergence of matrix series is understood entrywise.

Proposition 2.1.1 (e.g., [3]) *Let $A \in \mathbb{R}_{\max}^{n\times n}$. Series (2.1.1) and (2.1.2) converge if and only if $\lambda(A) \leqslant 0$, and then they can be truncated as follows:*

$$A^+ = A \oplus A^{\otimes 2} \oplus \ldots \oplus A^{\otimes n}, \tag{2.1.3}$$

and

$$A^* = I \oplus A \oplus A^{\otimes 2} \oplus \ldots \oplus A^{\otimes (n-1)}. \tag{2.1.4}$$

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

Proposition 2.1.2 (e.g., [3]) *Let $A \in \mathbb{R}_{\max}^{n\times n}$ and $\lambda(A) \leqslant 0$. Then $A = B^*$ if and only if $A = A^{\otimes 2}$ and $a_{ii} = 0$ for all i.*

Let us conclude this subsection by defining some classes of matrices that will be useful.

Definition 2.1.12 (Definite, increasing and strongly definite matrices [3]) *A square matrix $A \in \mathbb{R}_{\max}^{n\times n}$ then it is called definite if $\lambda(A) = 0$. Matrix A is called increasing if the diagonal entries of matrix A are nonnegative. If matrix A is increasing and definite then it is called strongly definite.*

2.2 Digraphs and Matrices

In this section we study the relationship between digraphs (directed graphs) and matrices over the tropical semiring. We will give some definitions concerning directed graphs that will be used in this thesis.

Definition 2.2.1 (Directed weighted graphs (e.g., [3])) *A directed graph (digraph) is formally defined as a pair of sets (N, E), where N is a finite set whose elements are called nodes, and the elements of $E \subseteq N \times N = \{(i, j) \mid i, j \in N\}$ are called edges.*

Consider a matrix $A = (a_{ij}) \in \mathbb{R}_{\max}^{n\times n}$. The weighted digraph associated with A is the digraph $\mathcal{G}_A = (N(A), E(A))$ where $N(A) = \{1, \ldots, n\}$ and $E(A) = \{(i, j) \mid i, j \in N,\ a_{ij} \neq -\infty\}$. Each edge $(i, j) \in E(A)$ has weight $w(i, j) = a_{ij}$.

Definition 2.2.2 (Length, walks,cycle and weights (e.g.,[3])) *A sequence of nodes $W = (i_0, ..., i_l)$, where l is called the length of W, is called a walk in $\mathcal{G} = (N, E)$ if $(i_{s-1}, i_s) \in E$ for each $1 \leqslant s \leqslant l$. A path ρ is a walk such that there are no two nodes in W that are the same. The weight of a path ρ is defined as $w(\rho) = a_{i_1 i_2} \otimes \cdots \otimes a_{i_{l-1} i_l}$. A cycle is a walk where the initial node i_0 is equal to the final node i_l, and such that the sequence $(i_0, i_1, \ldots, i_{l-1})$ is a path.*

Definition 2.2.3 (Strongly connected digraph (e.g.,[3])) *A digraph $\mathcal{G}_A$ is called strongly connected if there exists a path from node i to node j, for all $i \neq j$.*

Definition 2.2.4 (Tropical irreducible and reducible matrices (e.g.,[3])) *Matrix $A \in \mathbb{R}_{\max}^{n\times n}$ is an irreducible matrix if $\mathcal{G}_A$ is strongly connected and a reducible matrix otherwise.*

Example 2.2.1

Let us consider the following matrices:

$$A = \begin{pmatrix} -\infty & 3 & -\infty \\ 0 & 1 & 1 \\ -4 & -\infty & -\infty \end{pmatrix}, \quad B = \begin{pmatrix} -\infty & -\infty & 2 \\ -1 & -\infty & 0 \\ -\infty & -\infty & 0 \end{pmatrix}$$

Here A is irreducible and B is reducible.

Definition 2.2.5 (Maximum cycle mean (e.g.,[3])) *The maximum cycle mean of $\mathcal{G}_A$, denoted by $\lambda(A)$, is defined as the following number:*

$$\lambda(A) = \max_{\sigma} \ \mu(\sigma, A) \tag{2.2.1}$$

where the maximization is taken over all cycles in $\mathcal{G}_A$ *and* $\mu(\sigma, A) = \frac{w(A,\sigma)}{l(\sigma)}$*, where* σ *denotes a cycle and* $l(\sigma)$ *is the length of the cycle.*

The maximum cycle mean of $A \in \mathbb{R}_{\max}^{n\times n}$ is known to be the greatest tropical eigenvalue of A, and it is the unique tropical eigenvalue if A is irreducible.

Definition 2.2.6 (Critical digraph) *A cycle* σ *in digraph* $\mathcal{G}_A$ *is called critical, if* $\mu(\sigma, A) = \lambda(A)$*. Every node and edge that belongs to a critical cycle is called critical. The set of critical nodes is denoted by* $N_{\mathcal{C}}(A)$*, the set of critical edges is denoted by* $E_{\mathcal{C}}(A)$*. The critical digraph of* A*, further denoted by* $\mathcal{C}(A) = (N_{\mathcal{C}}(A), E_{\mathcal{C}}(A))$*, consists of all critical nodes and critical edges of* $\mathcal{G}_A$*.*

In general, the critical graph consists of a number of maximal strongly connected components (m.s.c.c.), which do not connect to each other by any path.

Example 2.2.2 *Consider the matrix*

$$A = \begin{pmatrix} 2 & -1 & -3 & -\infty \\ 1 & -\infty & -\infty & -2 \\ -\infty & -\infty & 0 & 3 \\ -\infty & 6 & -\infty & -\infty \end{pmatrix}$$

matrix A *has two critical cycles:* (1) *and* $(2, 4)$*. Entries of the matrix, which correspond to the critical edges, are marked in red. Thus the critical graph of* A *consists of two m.s.c.c., which are precisely the two critical cycles mentioned above.*

It appears that the critical digraph of a matrix can be "visualized" by means of a diagonal similarity scaling. The desired property is formally described as follows.

Definition 2.2.7 (Visualised matrices (e.g.,[3])) *Let A be a square matrix in $\mathbb{R}_{\max}^{n\times n}$ then A is called visualised if it satisfies the following conditions:*

$$\begin{cases} a_{ij} = \lambda(A), & \forall (i,j) \in E_{\mathcal{C}}(A), \\ a_{ij} \leqslant \lambda(A), & \forall (i,j) \notin E_{\mathcal{C}}(A). \end{cases} \tag{2.2.2}$$

The following known result states that a matrix can be brought to a visualized form by a diagonal similarity scaling.

Proposition 2.2.1 (e.g., [3]) *Let $A \in \mathbb{R}_{\max}^{n\times n}$ have $\lambda(A) \neq -\infty$ and $x \in \mathbb{R}^n$ be such that $A \otimes x \leqslant \lambda(A) \otimes x$ and $X = \operatorname{diag}(x)$, then $X^- \otimes A \otimes X$ is visualized.*

Note that such $x \in \mathbb{R}^n$ satisfying $A \otimes x \leqslant \lambda(A) \otimes x$ can always be found [3].

Let us now introduce the cyclicity of a strongly connected digraph and of a critical digraph.

Definition 2.2.8 (Cyclicity (e.g.,[3])) *The cyclicity of a strongly connected graph is defined as the greatest common divisor (g.c.d) of the lengths of all cycles.*

If the cyclicity is 1 *then the graph is called primitive, otherwise it is called imprimitive.*

The cyclicity of a critical digraph is defined as the least common multiple (l.c.m.) of all maximal strongly connected components of that digraph.

The cyclicity of a critical graph plays a crucial role in the following result. Cohen et al. [8] proved that if matrix $A \in \mathbb{R}_{\max}^{n\times n}$ is irreducible then the sequence of matrix powers $\{A^{\otimes k}\}_{k\geqslant 1}$ is ultimately periodic (with a shift), i.e., there exists a positive integer γ and a non negative transient time T such that

$$\forall k \geqslant T : A^{\otimes(k+\gamma)} = \lambda^{\otimes\gamma} \otimes A^{\otimes k}, \tag{2.2.3}$$

where $\lambda = \lambda(A)$ is the unique (tropical) eigenvalue of A. In particular we can take for γ the cyclicity of $\mathcal{G}^c(A)$.

Definition 2.2.9 *Let $\mathcal{G} = (N, E)$ be a digraph. Then we define two sets of walks as follows:*

(i) *$\mathcal{W}_{\mathcal{G}}(i \to j)$ is the set of walks over G connecting i to j;*

(ii) *$\mathcal{W}^k_{\mathcal{G}}(i \to j)$ is the set of walks over G with length k connecting i to j;*

For arbitrary set of walks $\mathcal{W}$, by $p(\mathcal{W})$ we denote the greatest weight of a walk in $\mathcal{W}$.

Using these sets of walks the following optimal walk interpretation of tropical matrix powers, Kleene stars and metric matrices can be stated.

Proposition 2.2.2 (Optimal walk interpretation (e.g.,[3])) *Let $A \in \mathbb{R}^{n\times n}_{\max}$ and $\mathcal{G}$ be the associated digraph of A. Then we have:*

$$A^{\otimes k}_{ij} = p\left(\mathcal{W}^k_{\mathcal{G}}(i \to j)\right), \quad \forall k \geqslant 1,\ 1 \leqslant i, j \leqslant n;$$
$$A^{+}_{ij} = p\left(\mathcal{W}_{\mathcal{G}}(i \to j)\right), \quad 1 \leqslant i, j \leqslant n;$$
$$A^{*}_{ij} = p\left(\mathcal{W}_{\mathcal{G}}(i \to j)\right), \quad 1 \leqslant i, j \leqslant n,\ i \neq j.$$

2.3 Cryptography

Cryptography studies the security of communication over open channel. Suppose that we have two parties, Alice and Bob, and that Alice needs to share her private document with Bob. Since Alice sends the document over unsecured network, Alice would like to protect her document with a secret password. In order to open the document, Bob needs Alice's secret password. The problem here is, how does Alice share her password securely to Bob? If Alice sends the password by email, it means that she allows an eavesdropper

(Eve) to steal the password. Therefore, we need a system to help Alice share her password in a secure way.

In cryptography, there are two methods to share a secret key: symmetric key and asymmetric key. Diffie and Hellman [10] introduced a new concept in cryptography that allowed Alice and Bob to share the private document without sharing their secret password. Their system became known as public key cryptography or asymmetric key.

2.3.1 Public Key Cryptography

In this section we discuss three main protocols, which are mostly relevant to our research: The Diffie-Hellman key exchange protocol, Stickel's protocol and protocol based on semidirect product.

The Diffie-Hellman protocol

As we mentioned before, Diffie and Hellman invented the concept of public key cryptography [10]. Let us denote Alice's secret key and Bob's secret key by K_a and K_b respectively and give a formal description of the Diffie-Hellman key exchange protocol.

Protocol 2.3.1 (The Diffie-Hellman Protocol [10])

1. *Alice and Bob agree on a finite cyclic group G and an element $g \in G$;*
2. *Alice chooses a random natural number a and sends $u = g^a$ to Bob;*
3. *Bob chooses a random natural number b and sends $v = g^b$ to Alice;*
4. *Alice computes $K_a = (g^b)^a$;*
5. *Bob computes $K_b = (g^a)^b$.*

We can see that both Alice and Bob now have the common secret key $K_a = (g^b)^a = g^{ba} = g^{ab} = (g^a)^b = K_b$.

The cryptanalysis of this protocol, i.e., the analysis of its security, is based on the analysis of the discrete logarithm problem, where Eve needs to find a if she is given g^a. However, the ultimate goal is to compute g^{ab} using the known data g, g^a and g^b. This is sometimes also referred to as the discrete logarithm problem.

Stickel's Protocol

Stickel's protocol is a public key exchange protocol closely related to the Diffie-Hellman protocol. We now give a formal description of this protocol.

Protocol 2.3.2 *[Stickel's protocol [38]] Let G be a non Abelian group.*

1. *Alice and Bob agree on public elements $A, B, W \in G$*
2. *Alice chooses two random natural numbers k, l and sends $U = A^k W B^l$ to Bob.*
3. *Bob chooses two random natural numbers m, n and sends $V = A^m W B^n$ to Alice.*
4. *Alice computes her secret key $K_a = A^k V B^l$.*
5. *Bob computes his secret key $K_b = A^m U B^n$.*

We can see that Alice and Bob end up with the same secret key $K_a = A^k V B^l = A^k A^m W B^n B^l = A^{k+m} W B^{n+l} = A^{m+k} W B^{l+n} = A^m A^k W B^l B^n = A^m U B^n = K_b$

In the case when this protocol uses invertible matrices it can be attacked by the following linear algebra attack [36], [35].
Assume that Eve knows matrices A, B, W, U, V. Eve needs to find matrices X and Y such that the following equations hold:

$$AX = XA, \quad BY = YB, \quad XWY = U. \tag{2.3.1}$$

Assuming that X is invertible, we observe that $XA = AX$ if and only if $X^{-1}A = AX^{-1}$ so we can rewrite (2.3.1) as follows:

$$AX^{-1} = X^{-1}A, \tag{2.3.2}$$

$$BY = YB, \tag{2.3.3}$$

$$WYU^{-1} = X^{-1}. \tag{2.3.4}$$

By substituting (2.3.4) into (2.3.3) we obtain

$$AWYU^{-1} = WYU^{-1}A, \quad YB = BY \tag{2.3.5}$$

Here we only need to find one unknown matrix, which is Y, and solving (2.3.5) means solving a system of linear equations. Hence Grigoriev and Shpilrain [13] suggested to use non-invertible matrices over tropical semiring to avoid the linear algebra attack. In the next section, we will discuss their tropical implementation of Stickel's protocol.

2.3.2 Tropical version of Stickel's Protocol

We next describe the following tropical version of Stickel's protocol.

Protocol 2.3.3 (Tropical Stickel protocol of [13])

Alice and Bob agree on $A, B \in \mathbb{R}_{\max}^{n\times n}$. *After this:*

1. *Alice chooses two random polynomial* $p_1(x)$ *and* $p_2(x)$ *with integer coefficients. Then Alice computes her public message* $U = p_1(A) \otimes W \otimes p_2(B)$ *and shares* U *to Bob.*

2. *Bob chooses two random polynomial* $q_1(x)$ *and* $q_2(x)$ *with integer coefficients. Then Bob computes his public message* $V = q_1(A) \otimes W \otimes q_2(B)$ *and shares* V *to Alice.*

3. *Alice computes* $K_a = p_1(A) \otimes V \otimes p_2(B)$.

4. Bob computes $K_b = q_1(A) \otimes U \otimes q_2(B)$.

We can see that both Alice and Bob have the common secret key because any two polynomials of the same matrix commute. Thus we have $K_a = p_1(A) \otimes V \otimes p_2(B) = p_1(A) \otimes q_1(A) \otimes W \otimes q_2(B) \otimes p_2(B) = q_1(A) \otimes p_1(A) \otimes W \otimes p_2(B) \otimes q_2(B) = q_1(A) \otimes U \otimes q_2(B) = K_b$

Grigoriev and Shpilrain's idea was that this modified protocol might be more secure in tropical algebra than in the usual algebra, with respect to the attack where Eve would like to find X and Y such that:

$$A \otimes X = X \otimes A, \quad B \otimes Y = Y \otimes B \tag{2.3.6}$$

and

$$X \otimes W \otimes Y = U \tag{2.3.7}$$

If X and Y satisfy (2.3.6) and (2.3.7), then Eve can find the common key $K = K_a = K_b$ by $X \otimes V \otimes Y$. Indeed,

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

In the tropical algebra, it is not immediately obvious how to solve (2.3.6) and (2.3.7) efficiently, especially since $X \otimes W \otimes Y = U$ is not tropically linear. However, Kotov and Ushakov [23] suggested the following solution of (2.3.6) and (2.3.7).

2.3.3 Kotov-Ushakov attack on the tropical version of Stickel's protocol

We first select a big enough number D such that it is bigger than the maximal degree of any tropical polynomial that can be used by Alice and Bob. Then we define

$$X = \bigoplus_{\alpha=0}^{D} x_\alpha \otimes A^{\otimes\alpha}, \quad Y = \bigoplus_{\beta=0}^{D} y_\beta \otimes B^{\otimes\beta}. \tag{2.3.8}$$

To satisfy (2.3.7) we impose

$$\begin{aligned} X \otimes W \otimes Y &= \bigoplus_{\alpha,\beta=0}^{D} x_\alpha \otimes A^{\otimes\alpha} \otimes W \otimes y_\beta \otimes B^{\otimes\beta} \\ &= \bigoplus_{\alpha,\beta=0}^{D} x_\alpha \otimes y_\beta \otimes A^{\otimes\alpha} \otimes W \otimes B^{\otimes\beta} = U. \end{aligned} \tag{2.3.9}$$

Equation (2.3.9) can be equivalently written as

$$\bigoplus_{\alpha,\beta=0}^{D} x_\alpha \otimes y_\beta \otimes (A^{\otimes\alpha} \otimes W \otimes B^{\otimes\beta} - U) = E, \tag{2.3.10}$$

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 (2.3.10) as

$$\bigoplus_{\alpha,\beta=0}^{D} (x_\alpha \otimes y_\beta \otimes T^{\alpha\beta}_{\gamma\delta}) = 0, \quad \forall \gamma, \delta \in [n]. \tag{2.3.11}$$

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 pairs $\gamma\delta$ play the role of rows and pairs $\alpha\beta$ play the role of columns. Such systems are considered, e.g., in [3], 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 [23]. The goal of this attack is to solve (2.3.11)

Attack 2.3.1 (Kotov-Ushakov [23])

1. *Compute* $c_{\alpha\beta} = \min_{\gamma,\delta}(-T^{\alpha\beta}_{\gamma\delta})$ *and* $S_{\alpha\beta} = \arg\min_{\gamma,\delta}(-T^{\alpha\beta}_{\gamma\delta})$.

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*

$$\bigcup_{(\alpha,\beta)\in\mathcal{C}} S_{\alpha\beta} = [n] \times [n]. \tag{2.3.12}$$

find a cover for which the system

$$\begin{cases} x_\alpha + y_\beta & = c_{\alpha\beta} \quad \textit{if}(\alpha,\beta) \in \mathcal{C} \\ x_\alpha + y_\beta & \leqslant c_{\alpha\beta} \quad \textit{otherwise.} \end{cases} \tag{2.3.13}$$

is solvable.

Theorem 2.3.1 (Validity of the Kotov-Ushakov attack[28]) *Let* $A, B, W \in \mathbb{R}^{n\times n}_{\max}$ *and* U *is the message sent by Alice to Bob in Protocol 2.3.3 . If* D *is bigger than the maximal degree of any tropical polynomial that can be used by Alice and Bob, then the Kotov-Ushakov attack yields*

$$X = \bigoplus_{\alpha=0}^{D} x_\alpha \otimes A^{\otimes\alpha}, \quad Y = \bigoplus_{\beta=0}^{D} y_\beta \otimes B^{\otimes\beta}. \tag{2.3.14}$$

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

Proof. Since D is bigger than the maximal degree as any tropical polynomial used by

Alice and Bob, it is clear from the Protocol 2.3.3 that $U = X \otimes W \otimes Y$ where

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

for some x_α and y_β, for $\alpha, \beta \in \{0, \ldots, D\}$. Therefore, there exist x_α and y_β that satisfy (2.3.9) or, equivalently, (2.3.11). It is also clear that any x_α and y_β that solve (2.3.11) yield X and Y that satisfy (2.3.8) and $X \otimes W \otimes Y = U$. Thus the protocol can be broken by solving (2.3.11) 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 (2.3.11) (provided that a solution exists, which is the case).

Consider the system

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

According to the theory of $A \otimes x = b$, and namely [3] Theorem 3.1.1 and Corollary 3.1.2, we have

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

2. 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 (2.3.12) 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 solvabilty of (2.3.11) amounts to finding at least one system (2.3.13) that is solvable with $\mathcal{C}$ being a minimal cover (i.e a set satisfying (2.3.12) that is minimal with respect to inclusion). This is what Attack 2.3.1 actually does. □

Note that Theorem 2.3.1 was not formally stated and proved in [23].

2.3.4 Protocol based on Semidirect Product

Habeeb, Kahrobei, Koupparis and Shpilrain [15] developed new concept of key exchange protocol based on the Diffie-Hellman protocol. In their protocol, they used noncommutative (semi)group as a platform and extended this semigroup by conjugating automorphism. However, this protocol can be attacked by "linear algebra attack" [35]. Therefore they tried to find another platform group which is a free nilpotent p-group with sufficiently large prime number p. They believed the protocol with this platform group is not easy to be attacked by "linear algebra attack".

Here, we give some basic definitions of semidirect product in the classical algebra and present the protocol of Habeeb et al.[15] using semidirect product.

Definition 2.3.1 (Semidirect product) *Suppose G and H are groups. Suppose that*

$$\psi : H \mapsto Aut(G)$$

is a homomorphism. Then we define the semidirect product of G and H as the set

$$G \rtimes H = \{(g, h) | g \in G, h \in H\}$$

equipped with the operation defined by

$$(g, h)(g', h') = (g^{\psi(h')} \cdot g', h \cdot h')$$

.

Protocol 2.3.4 (Protocol based on Semidirect Product [15])

Let G be a (semi)group. Alice and Bob agree on the following public information: an

element $g \in G$, an arbitrary automorphism $\psi \in Aut(G)$. Then Alice and Bob compute their secret key in the following steps:

1. *Alice chooses a private integer m and computes $(g, \psi^m) = (\psi^{m-1}(g) \cdot \cdots \cdot \psi^2(g) \cdot \psi(g), \psi^m)$. Then Alice sends the first part $A = \psi^{m-1}(g) \cdot \cdots \cdot \psi^2(g) \cdot \psi(g)$ to Bob.*

2. *Bob chooses a private integer n and computes $(g, \psi^n) = (\psi^{n-1}(g) \cdot \cdots \cdot \psi^2(g) \cdot \psi(g), \psi^n)$. Then Alice sends a pair (B, X) where $B = \psi^{n-1}(g) \cdot \cdots \cdot \psi^2(g) \cdot \psi(g)$ and $Y = \psi^n$ to Alice.*

3. *Alice computes $(B, X)(A, \psi^m) = (\psi^m(b) \cdot a, x \cdot \psi^m)$.*

4. *Bob computes $(A, Y)(B, \psi^n) = (\psi^(n)(a) \cdot b, y \cdot \psi^n)$.*

Since $(B, X)(A, \psi^m) = (A, Y)(B, \psi^m) = (g, \psi)^{m+n}$ then Alice and Bob have the same secret key $K_{Alice} = K_{Bob}$.

Chapter 3

Tropical Discrete Logarithm

In this chapter, we will introduce the new concept of tropical discrete logarithm problem that used to attack the protocol in the Chapter 6.

3.1 The Classical Discrete Logarithm Problem

Let G be a group. For any $a \in G$, $k \in \mathbb{N}$, the kth power of a is expressed as follows:

$$a^k = \underbrace{a \cdot a \cdot \ldots \cdot a}_{k}.$$

Let $b \in G$ satisfy $b = a^k$. The problem to find the smallest k such that $b = a^k$ is called the discrete logarithm problem.

There are several algorithms that are used for solving the discrete logarithm problem. For instance, Shank's Baby-Step Giant-Step Algorithm that requires running time $\mathcal{O}(\sqrt{n}\log n)$, Silver-Pohlig-Hellman Algorithm for solving the discrete logarithm problem over $GF(q)$ that requires running time $\mathcal{O}(\sqrt{p})$ where p is the largest prime number factor of $q-1$. There is also ρ -method, which requires the same running time as Baby-Step Giant-Step Algorithm, and Index Calculus Algorithm that has running time $\mathcal{O}(\exp(c(\sqrt{\log n \log\ \log n})))$ [40].

At present, no efficient algorithm can solve the discrete logarithm problem and public

key cryptography based on the tropical discrete logarithm problem. However, Shor showed that the discrete logarithm problem can be solved using Quantum Computer in polynomial time [34].

Since the discrete logarithm problem is hard to solve, it is used in public key cryptography and digital signature. The hardness of this problem is particularly important for the protocols discussed in [10],[11],[38],etc.

3.2 The Tropical Discrete Logarithm Problem and Ultimate Periodicity

In this section, we will discuss the algorithmic solution of the following problem, which we call the tropical discrete logarithm, for its similarity with the tropical discrete logarithm problem.

Problem 3.2.1 (Tropical Discrete Logarithm [29]) *Suppose that* $V \in \mathbb{R}_{\max}^{m\times d}$, $F \in \mathbb{R}_{\max}^{d\times d}$ *and secret key* $t \geqslant 1$ *are used to produce* $A = V \otimes F^{\otimes t}$. *Knowing* A, V *and* F *and that* t *is unique, find* t.

In the tropical mathematics, there is an important special case, in which the tropical discrete logarithm is well defined.

Proposition 3.2.1 ([29]) *Suppose that* V *has finite entries and* F *is irreducible. Then* $V \otimes F^{\otimes t_1} \neq V \otimes F^{\otimes t_2}$ *for any* t_1 *and* t_2 *if and only if* $\lambda(F) \neq 0$.

Proof. Suppose that we have $V \otimes F^{\otimes t_1} = V \otimes F^{\otimes t_2}$ for some $t_1 < t_2$. However, then each row of $V \otimes F^{\otimes t_1}$ (which has finite entries since so does V and since F is irreducible) is a left eigenvector of $F^{\otimes(t_2-t_1)}$ with eigenvalue 0. However, by [4] Corollary 5.5, $F^{\otimes(t_2-t_1)}$ has a unique eigenvalue, which is $(t_2 - t_1) \times \lambda(F) \neq 0$. This contradiction shows that $V \otimes F^{\otimes t_1} = V \otimes F^{\otimes t_2}$ implies $t_1 = t_2$, so the tropical discrete logarithm is well-defined.

If $\lambda(F) = 0$, then the sequence $(V \otimes F^{\otimes t})_{t \geqslant 1}$ is ultimately periodic [7, 8] (see also [1, 3, 16]), implying that the tropical discrete logarithm is not well-defined. □

As we mentioned before, there is no efficient algorithm that can solve the classical discrete logarithm problem without the Quantum Computer. But the situation with the tropical version described above is very different. In the tropical version, we can use the ultimate periodicity of tropical matrix powers, which means that the tropical discrete logarithm problem can be solved efficiently.

Now consider $F \in \mathbb{R}_{\max}^{d \times d}$ with $\lambda(F) \neq -\infty$. Recall that the critical graph of F, denoted by $\mathcal{G}^c(F)$, is the subgraph of $\mathcal{G}(F)$, which consists of all nodes and arcs of the cycles where the maximum cycle mean $\lambda(F)$ is attained. In general it consists of several maximal strongly connected components (abbreviated as m.s.c.c.), which do not have any connection to one another. Suppose that the critical graph $\mathcal{G}^c(F)$ has l m.s.c.c. $\mathcal{G}_1^c, \ldots, \mathcal{G}_l^c$ with corresponding cyclicities $\sigma_1, \ldots, \sigma_l$. For all $\nu \in \{1, ..., l\}$, each νth component gives rise to a CSR term via the following procedure described by Sergeev and Schneider [33] and Merlet, Nowak and Sergeev [27].

Let $\lambda = \lambda(F)$. Denote $U_\nu = ((\lambda^- \otimes F)^{\otimes \sigma_\nu})^+$ (using the metric matrix defined in (2.1.1)). Then, let matrices C_ν, R_ν and S_ν be defined by:

$$(C_\nu)_{ij} = \begin{cases} (U_\nu)_{ij} & \text{if } j \text{ is in } \mathcal{G}_\nu^c \\ -\infty & \text{otherwise,} \end{cases} \qquad (R_\nu)_{ij} = \begin{cases} (U_\nu)_{ij} & \text{if } i \text{ is in } \mathcal{G}_\nu^c \\ -\infty & \text{otherwise,} \end{cases}$$
$$(S_\nu)_{ij} = \begin{cases} \lambda^- \otimes F_{ij} & \text{if } (i,j) \in \mathcal{G}_\nu^c \\ -\infty & \text{otherwise.} \end{cases} \tag{3.2.1}$$

Define also matrices $B_\nu[F]$ and $B[F]$ by

$$(B_\nu[F])_{ij} = \begin{cases} -\infty, & \text{if } i \in \mathcal{G}_\nu^c \text{ or } j \in \mathcal{G}_\nu^c, \\ F_{ij}, & \text{otherwise,} \end{cases} \qquad (B[F])_{ij} = \begin{cases} -\infty, & \text{if } i \in \mathcal{G}^c(F) \text{ or } j \in \mathcal{G}^c(F), \\ F_{ij}, & \text{otherwise.} \end{cases} \tag{3.2.2}$$

Denote by $t(\operatorname{rem}\sigma)$ the remainder of t modulo σ (i.e., $r \in \{0, \dots, \sigma - 1\}$) such that $t = k\sigma + r$ for some k. Denote $C_\nu S_\nu^k R_\nu[F] = C_\nu \otimes S_\nu^k \otimes R_\nu$ and $C_\nu S_\nu^k[F] = C_\nu \otimes S_\nu^{\otimes k}$ for more brevity and to indicate the matrix (F) from which C_ν, S_ν and R_ν are defined.

The following claims can be derived from certain results of [27]. Their proofs are deferred to Section 3.3.

Proposition 3.2.2 (Coro. of [27] Theorem 4.1 and Corollary 4.3) *Let $F \in \mathbb{R}_{\max}^{d\times d}$ with $\lambda = \lambda(F) \neq -\infty$ and suppose that $\mathcal{G}^c(F)$ has components $\mathcal{G}_1^c, \dots, \mathcal{G}_l^c$ and σ_ν for $1 \leqslant \nu \leqslant l$ are their cyclicities. Then for any $\nu \in \{1, \dots, l\}$*

$$F^{\otimes t} = \lambda^{\otimes t} \otimes C_\nu S_\nu^{t(\operatorname{rem}\sigma_\nu)} R_\nu[F] \oplus (B_\nu[F])^{\otimes t}, \qquad \forall t \geqslant (d-1)^2 + 1. \tag{3.2.3}$$

Proposition 3.2.3 *Under the conditions of Proposition 3.2.2, we also have*

$$F^{\otimes t} = \lambda^{\otimes t} \otimes \left(\bigoplus_{\nu=1}^{l} C_\nu S_\nu^{t(\operatorname{rem}\sigma_\nu)} R_\nu[F] \right) \oplus (B[F])^{\otimes t} \qquad \forall t \geqslant (d-1)^2 + 1, \tag{3.2.4}$$

Furthermore, if F is irreducible then there exists $T(F)$ such that

$$F^{\otimes t} = \lambda^{\otimes t} \otimes \left(\bigoplus_{\nu=1}^{l} C_\nu S_\nu^{t(\operatorname{rem}\sigma_\nu)} R_\nu[F] \right), \qquad \forall t \geqslant T(F). \tag{3.2.5}$$

Equation (3.2.5) implies that after $T(F)$ the sequence of powers $(\lambda(F)^- \otimes F)^{\otimes t}$ is periodic, with period equal to the least common multiple of σ_ν for $\nu = 1, \dots, l$, a well-known fact established by Cohen et. al. [7, 8]. If we denote $CS^t R[F] = \bigoplus_{\nu=1}^{l} C_\nu S_\nu^{t(\operatorname{rem}\sigma_\nu)} R_\nu[F]$

then we can also rewrite (3.2.5) as

$$F^{\otimes t} = \lambda^{\otimes t} \otimes CS^t R[F], \quad \forall t \geqslant T(F). \tag{3.2.6}$$

It is not too difficult to compute the CSR terms. In particular, one needs to find λ, for which one can exploit Karp's method with complexity $O(d^3)$ [1, 3] or the policy iteration algorithm of Cochet-Terrasson et al. [6, 16], which works in general case and is very efficient in practice. The usual technique for powering up a matrix is to use repeated squaring, and this yields the addition of an $O(d^3 \log d)$ term (observing that $\sigma_\nu \leqslant d$). Further, the metric matrix can be computed by shortest path algorithms such as the Floyd-Warshall algorithm [1, 3, 16]. The complexity of finding the components of $\mathcal{G}^c(F)$ does not exceed $O(d^3)$ [1]. We also need to know the cyclicity of the components, which can be computed in $O(d^2)$ by Balcer and Veinott's digraph condensation [2]. However, below we are going to show how some of these problems can be avoided, as instead of the whole critical component we can use one critical cycle from that component, following an idea of Merlet et al. [27, Theorem 6.1]. The resulting complexity of computing CSR remains of the order $O(d^3 \log d)$, but we avoid the need for identifying the whole components of $\mathcal{G}^c(V)$ and the use of Balcer-Veinott digraph condensation.

Let us first give yet another definition of a CSR term, as below. Suppose that Z is a critical cycle, with length $l(Z)$. Denote $U_Z = ((\lambda^- \otimes F)^{\otimes l(Z)})^*$. Then, let matrices C_Z, R_Z and S_Z and $B_Z[F]$ be defined by:

$$(C_Z)_{ij} = \begin{cases} (U_Z)_{ij} & \text{if } j \text{ is in } Z \\ -\infty & \text{otherwise,} \end{cases} \quad (R_Z)_{ij} = \begin{cases} (U_Z)_{ij} & \text{if } i \text{ is in } Z \\ -\infty & \text{otherwise,} \end{cases}$$
$$(S_Z)_{ij} = \begin{cases} \lambda^- \otimes F_{ij} & \text{if } (i,j) \in Z \\ -\infty & \text{otherwise,} \end{cases} \tag{3.2.7}$$

The following claim can be seen as a corollary of [27, Theorem 6.1]. For the readers' convenience we give a proof of it in Section 3.3.

Proposition 3.2.4 (Coro. of [27], Theorem 6.1) *Let Z be a cycle belonging to a component $\mathcal{G}_\nu^c$ of the critical graph of a square matrix F with $\lambda(F) \neq -\infty$. Then $C_\nu S_\nu^t R_\nu[F] = C_Z S_Z^t R_Z[F]$ for any natural t, and therefore:*

$$F^{\otimes t} = \lambda^{\otimes t} \otimes C_Z S_Z^{t(\operatorname{rem} l(Z))} R_Z[F] \oplus (B_\nu[F])^{\otimes t}, \qquad \forall t \geqslant (d-1)^2 + 1. \tag{3.2.8}$$

for any critical cycle Z and component $\mathcal{G}_\nu^c$ in which it lies.

Here, equation (3.2.8) follows from (3.2.3) and the first part of the claim since σ_ν divides $l(Z)$ and $\{C_\nu S_\nu^t R_\nu[F]\}_{t \geqslant 0}$ is periodic with period σ_ν by [33, Prop. 3.2].

Let us now argue that the diagonal similarity scaling "commutes" with the computation of CSR. The claim below is also true for other CSR terms introduced and discussed earlier, but we will prove it for $C_Z S_Z^t R_Z[F]$, which is used in our solution of the tropical discrete logarithm problem.

Proposition 3.2.5 *Let D be a diagonal matrix with finite diagonal entries and let $F_D = D^- \otimes F \otimes D$. Then*

$$D^- \otimes C_Z S_Z^t R_Z[F] \otimes D = C_Z S_Z^t R_Z[F_D]. \tag{3.2.9}$$

Proof. It suffices to prove the following identities:

$$D^- \otimes C_Z[F] \otimes D = C_Z[F_D], \quad D^- \otimes S_Z[F] \otimes D = S_Z[F_D], \quad D^- \otimes R_Z[F] \otimes D = R_Z[F_D], \tag{3.2.10}$$

because then (3.2.9) can be obtained as a product of such identities. Here, the second identity follows since $S_Z[F]$ is obtained from the matrix $\lambda^-(F) \otimes F$ by setting some entries

to $-\infty$ and $S_Z[F_D]$ is obtained from the matrix $\lambda^-(F_D) \otimes F_D$ by setting the same entries to $-\infty$, and it is then implied by $\lambda^-(F_D) \otimes F_D = D^- \otimes (\lambda^-(F) \otimes F) \otimes D$ (using that $\lambda(F) = \lambda(F_D)$ since the diagonal similarity scaling does not change eigenvalues).

For the first identity and the third identities, we recall that $C_Z[F]$ is the matrix where the columns with indices in Z are the columns of $((\lambda(F)^- \otimes F)^{\otimes l(Z)})^+$ with indices in cycle Z, and $R_Z[F]$ is the matrix where the rows with indices in Z are the rows of $((\lambda(F)^- \otimes F)^{\otimes l(Z)})^+$ with indices in cycle Z. Then it suffices to prove the identity for $(G[F])^+$ and $(G[F_D])^+$, where $G[F] = (\lambda(F)^- \otimes F)^{\otimes l(Z)}$ and $G[F_D] = (\lambda(F_D)^- \otimes F_D)^{\otimes l(Z)}$. For this we first obtain the identity $D^- \otimes G[F] \otimes D = G[F_D]$ by taking the product of $l(Z)$ identities $D^- \otimes (\lambda(F)^- \otimes F) \otimes D = \lambda(F_D)^- \otimes F_D$ (recall that $\lambda(F) = \lambda(F_D)$). Next we recall that $(G[F])^+ = \bigoplus_{i=1}^{d} (G[F])^{\otimes i}$, and the identity $D^- \otimes (G[F])^+ \otimes D = (G[F_D])^+$ follows as we sum up the identities $D^- \otimes (G[F])^{\otimes i} \otimes D = (G[F_D])^{\otimes i}$. □

The next immediate corollary of above results will be used in practice, for solving the tropical discrete logarithm problem. It is closely related to an observation by Nachtigall [30] that critical rows and columns of matrix powers become periodic after $O(d^2)$, and the further more refined results of Merlet et al. [26].

Corollary 3.2.1 (Coro. of [27], Theorem 6.1) *Let $V \in \mathbb{R}_{\max}^{m \times d}$ and $F \in \mathbb{R}_{\max}^{d \times d}$ with $\lambda = \lambda(F) \neq -\infty$, and let Z be a cycle of $\mathcal{G}^c(F)$. Then for any $t \geqslant (d-1)^2 + 1$, the columns of $V \otimes F^{\otimes t}$ with indices in Z are equal to the corresponding columns in $\lambda^{\otimes t} \otimes V \otimes C_Z S_Z^{t(\operatorname{rem} l(Z))} R_Z[F]$.*

Proof. Equation (3.2.8) implies that the columns of $F^{\otimes t}$ with indices in Z are equal to the corresponding columns of $\lambda^{\otimes t} \otimes C_Z S_Z^{t(\operatorname{rem} l(Z))} R_Z[F]$. The claim now follows as we multiply the columns of $F^{\otimes t}$ and $\lambda^{\otimes t} \otimes C_Z S_Z^{t(\operatorname{rem} \sigma_1)} R_Z[F]$ with indices in Z by V. □

Corollary 3.2.1 suggests the following algorithm for finding t such that $A = V \otimes F^{\otimes t}$, that is, for solving Problem 3.2.1. In this algorithm, E will denote a matrix of appropriate

dimensions consisting of all zeros.

Algorithm 3.2.1 (Tropical Discrete Logarithm [29])

Input: A, $V \in \mathbb{R}_{\max}^{m\times d}$, $F \in \mathbb{R}_{\max}^{d\times d}$.

Output: t such that $A = V \otimes F^{\otimes t}$.

0. Find $\lambda = \lambda(F)$ and a critical cycle Z. Compute C_Z and S_Z.

1. For $t = 0,\ 1, \ldots, (d-1)^2$ check if $A = V \otimes F^{\otimes t}$ and return t if it is found;

2. For $k = 0, \ldots, l-1$ check if $A_{\cdot i} - V \otimes (C_Z S_Z^k R_Z[F])_{\cdot i} = \mu + E_{\cdot i}$ for all $i \in Z$ and some μ such that $t = \mu/\lambda(F)$ is a natural number and return the first such t that is found.

Proposition 3.2.6 ([29]) *Part 0., part 1. and part 2. of Algorithm 3.2.1 require at most* $O(d^3 \log l(Z))$, $O(md^4)$ *and* $O(ml(Z)(d + l(Z)))$ *operations, respectively.*

Proof. Complexity bounds:

0. Finding $\lambda(F)$ and a critical cycle Z needs at most $O(d^3)$ operations (Karp's algorithm and the methods described in [16, 31]. After this, C_Z can be found in $O(d^3 \log l(Z))$ operations (dominated by the repeated matrix squaring).

1. On step 1, the outer loop has size $(d-1)^2$, and the computationally dominant operation is that of repeated multiplication of an $m \times d$ matrix by an $d \times d$ matrix F, taking md^2 operations. Thus, the overall complexity is $O(md^4)$.

2. On step 2, the computational complexity can be decreased using the observation that the columns of $C_Z S_Z^{t(\operatorname{rem} l(Z))} R_Z[F]$ with indices in Z are equal to the corresponding columns $C_Z S_Z^{t(\operatorname{rem} l(Z))}[F]$ by [33, Corollary 3.7], and therefore we actually check if $A_{\cdot i} - (V \otimes C_Z \otimes S_Z^{\otimes k})_{\cdot i} = \mu + E_{\cdot i}$ for some μ such that $t = \mu/\lambda(F)$ is a natural number. The outer loop has size $l(Z)$ and we precompute the columns of $V \otimes C_Z$ with indices

in Z, which gives $O(mdl(Z))$ operations. The computationally dominant operation at each step is that of multiplying an $m \times l$ matrix by S_Z (done by a permutation of and adding some scalar values to the columns of that matrix), which is $O(ml(Z))$. Overall it gives $O(ml(Z)(d + l(Z)))$. □

Remark 3.2.1 Using [33, Corollary 3.7], $C_Z S_Z^{t \operatorname{rem}(l(Z))} R_Z[F]$ can be replaced with $C_Z S_Z^{t \operatorname{rem}(l(Z))}[F]$ in Corollary 3.2.1 and Algorithm 3.2.1.

Remark 3.2.2 If we are certain that $t \geqslant (d-1)^2 + 1$, then we can omit part 1. of the above algorithm. This gives rise to a "light" version of Algorithm 3.2.1, which will be tested in our numerical experiments.

Remark 3.2.3 We can also suggest another lighter but less reliable version of Algorithm 3.2.1 where $A_{\cdot i} - (V \otimes C_Z S_Z^{t(\operatorname{rem} l(Z))}[F])_{\cdot i} = \mu + E_{\cdot i}$ is checked just for one $i \in Z$. Then the complexity of Step 1. drops further.

Theorem 3.2.1 ([29]) *Suppose that matrices $V \in \mathbb{R}_{\max}^{m \times d}$, $F \in \mathbb{R}_{\max}^{d \times d}$ and critical cycle Z are such that any of the following equivalent conditions holds:*

1. *For any $t_1 \neq t_2$, we have $V \otimes \lambda^{\otimes t_1} \otimes C_Z S_Z^{t_1 \operatorname{rem} l(Z)}[F] \neq V \otimes \lambda^{\otimes t_2} \otimes C_Z S_Z^{t_2 \operatorname{rem} l(Z)}[F]$,*
2. *For no $t_1, t_2 \geqslant (d-1)^2 + 1$ and $t_1 \neq t_2$ we have that all columns of $V \otimes F^{\otimes t_1}$ with indices in Z are equal to the corresponding columns of $V \otimes F^{\otimes t_2}$.*

Then, for any $A = V \otimes F^{\otimes t}$ with $t \geqslant (d-1)^2 + 1$, part 2. of Algorithm 3.2.1 finds this t and it is unique.

Proof. The equivalence between 1. and 2. follows by Corollary 3.2.1 and Remark 3.2.1, which also imply that if $t \geqslant (d-1)^2 + 1$, then $A_{\cdot i} = t \times \lambda + V \otimes (C_Z S_Z^{t(\operatorname{rem} l(Z)}[F])_{\cdot i}$ and hence for $k \equiv t(\operatorname{rem}(l(Z))$ we have $A_{\cdot i} - V \otimes (C_Z S_Z^k[F])_{\cdot i} = \mu + E_{\cdot i}$ for all $i \in Z$, where μ

is such that $t = \mu/\lambda(F)$ is natural. Furthermore, if this holds for $t \geqslant (d-1)^2+1$, then we have $A_{\cdot i} = \lambda^{\otimes t} \otimes V \otimes (C_Z S_Z^{t(\operatorname{rem} l(Z))}[F])_{\cdot i}$ for all $i \in Z$, and hence $A_{\cdot i} = (V \otimes F^{\otimes t})_{\cdot i}$ for all such i by Proposition 3.2.4 and (3.2.3). Condition 2. of the theorem then implies that such t is unique and hence correct. □

Remark 3.2.4 The algorithm cannot work when $\lambda(F) = 0$. In this case, obviously, the sequence of columns $\{(V \otimes F^{\otimes t})_{\cdot i}\}_{t>(d-1)^2}$ is periodic for any $i \in Z$ with the same period, and there are infinitely many t such that $A_{\cdot i} = (V \otimes F^{\otimes t})_{\cdot i}$, if one such t exists. However, if F is irreducible with $\lambda(F) = 0$, then the tropical discrete logarithm problem is not well-defined, either.

Remark 3.2.5 *In the first part of the claim, we can replace* $t_1 \operatorname{rem} l(Z)$ *and* $t_2 \operatorname{rem} l(Z)$ *with* t_1 *and* t_2*, respectively.*

We now obtain the following previously not published result, which improves [29, Corollary 2.6].

Theorem 3.2.2 *Let* $\lambda(F) \neq 0$*, and let* Z *be a critical cycle of* $\mathcal{G}(F)$ *such that for each* $t \geqslant (d-1)^2+1$ *at least one column of* $V \otimes F^{\otimes t}$ *with index in* Z *has a finite entry. Then* $V \otimes \lambda^{\otimes t_1} \otimes C_Z S_Z^{t_1 \operatorname{rem} l(Z)}[F] \neq V \otimes \lambda^{\otimes t_2} \otimes C_Z S_Z^{t_2 \operatorname{rem} l(Z)}[F]$ *for any* t_1 *and* t_2 *with* $t_1 \neq t_2$*.*

Proof. Suppose that $V \otimes \lambda^{\otimes t_1} \otimes C_Z S_Z^{t_1 \operatorname{rem} l(Z)}[F] = V \otimes \lambda^{\otimes t_2} \otimes C_Z S_Z^{t_2 \operatorname{rem} l(Z)}[F]$, which is the same as

$$\lambda^{\otimes t_1} \otimes V \otimes C_Z S_Z^{t_1}[F] = \lambda^{\otimes t_2} \otimes V \otimes C_Z S_Z^{t_2}[F] \tag{3.2.11}$$

Let D be such that $F_D = D^- \otimes F \otimes D$ is visualised. Postmultiplying (3.2.11) by $R_Z[F]$ and D we obtain

$$\lambda^{\otimes t_1} \otimes (V \otimes D) \otimes D^- \otimes C_Z S_Z^{t_1} R_Z[F] \otimes D = \lambda^{\otimes t_2} \otimes (V \otimes D) \otimes D^- \otimes C_Z S_Z^{t_2} R_Z[F] \otimes D. \tag{3.2.12}$$

By Proposition 3.2.5, we have

$$D^- \otimes C_Z S_Z^t R_Z[F] \otimes D = C_Z S_Z^t R_Z[F_D]. \tag{3.2.13}$$

In words, the diagonal similarity scaling of the CSR term defined from F is equal to the CSR term defined from F_D. We then obtain:

$$(V \otimes D) \otimes C_Z S_Z^{t_1} R_Z[F_D] = \lambda^{\otimes(t_2-t_1)} \otimes (V \otimes D) \otimes C_Z S_Z^{t_2} R_Z[F_D]$$

Restricting this matrix equation to the columns with indices in Z we obtain

$$(V \otimes D) \otimes C_Z S_Z^{t_1}[F_D] = \lambda \times (t_2 - t_1) + (V \otimes D) \otimes C_Z S_Z^{t_2}[F_D] \tag{3.2.14}$$

Since F_D is visualized, the submatrix of $S_Z[F_D]$ extracted from the rows and columns in Z is a permutation matrix, and so is $S_Z^{\otimes(t_2-t_1)}[F_D]$. We see that

$$(V \otimes D) \otimes C_Z S_Z^{t_2}[F_D] = (V \otimes D) \otimes C_Z S_Z^{t_1}[F_D] \otimes S_Z^{t_2-t_1}[F_D],$$

and since $S_Z^{\otimes(t_2-t_1)}[F_D]$ is a permutation matrix, the greatest entries of $(V \otimes D) \otimes C_Z S_Z^{t_1}[F_D]$ and $(V \otimes D) \otimes C_Z S_Z^{t_2}[F_D]$ are the same. Since $V \otimes F^{\otimes t}$ for $t \geqslant (d-1)^2 + 1$ has at least one finite entry in one of the columns in Z and since these columns are equal to those of $V \otimes C_Z S_Z^{t \operatorname{rem} l(Z)}[F]$, the same property also holds for matrices $(V \otimes D) \otimes C_Z S_Z^{t_1}[F_D]$ and $(V \otimes D) \otimes C_Z S_Z^{t_2}[F_D]$ mentioned above, and therefore their greatest entries are finite. This implies that (3.2.14) is impossible, hence the claim follows. □

Remark 3.2.6 *It follows from the above that for any $t_2 \geqslant t_1 \geqslant (d-1)^2 + 1$ the $\{0, -\infty\}$ the pattern of each column of $V \otimes F^{\otimes t_2}$ with index in Z can be obtained as the $\{0, -\infty\}$ pattern of a (possibly different) column of $V \otimes F^{\otimes t_1}$ with index in Z, and hence the*

condition that for each $t \geqslant (d-1)^2+1$ *at least one column of* $V \otimes F^{\otimes t}$ *with index in* Z *has a finite entry can be replaced with the condition that a column with index in* Z *and a finite entry should exist in* $V \otimes F^{\otimes d^2}$.

We then have the following immediate corollaries of the above results.

Corollary 3.2.2 *Let* $\lambda(F) \notin \{0, -\infty\}$, *and suppose that there exists a node of* $\mathcal{G}^c(F)$ *such that the corresponding column of* $V \otimes F^{\otimes d^2}$ *has a finite entry. Then part 2. of Algorithm 3.2.1, which uses any cycle* Z *containing such node and is applied to* $V \otimes F^{\otimes t}$, *finds that* t, *which is unique.*

Corollary 3.2.3 *Under the conditions of Corollary 3.2.2 the discrete logarithm problem is well defined for* V, F *and any* $t \geqslant (d-1)^2+1$.

Corollary 3.2.4 *Let* $\lambda(F) \notin \{0, -\infty\}$ *and let* V *have only finite entries. Then the discrete logarithm problem is well-defined for these* V *and* F *and any* $t \geqslant (d-1)^2+1$, *and part 2. of Algorithm 3.2.1, which uses any critical cycle* Z *and is applied to* $V \otimes F^{\otimes t}$, *finds that* t.

3.3 Proofs of some results on CSR expansions

In this section we will give the previously deferred proofs of some results on the CSR expansion.

3.3.1 Proof of Proposition 3.2.2 [29]

Here we deduce these propositions from results of Merlet et al. [27]. To do this, we need to introduce other versions of CSR decomposition and expansion, which appeared in that work. First of all, we can define the "big" CSR terms by considering the whole critical graph instead of individual components. For this, let σ be the l.c.m. of all $\sigma_1, \ldots, \sigma_l$ and

define $U = ((\lambda^- \otimes F)^{\otimes\sigma})^+$. Then let matrices C, R and S be defined by

$$C_{ij} = \begin{cases} U_{ij} & \text{if } j \text{ is in } \mathcal{G}^c(F) \\ -\infty & \text{otherwise,} \end{cases} \qquad R_{ij} = \begin{cases} U_{ij} & \text{if } i \text{ is in } \mathcal{G}^c(F) \\ -\infty & \text{otherwise,} \end{cases}$$
$$S_{ij} = \begin{cases} \lambda^- \otimes F_{ij} & \text{if } (i,j) \in \mathcal{G}^c(F) \\ -\infty & \text{otherwise.} \end{cases} \tag{3.3.1}$$

We will denote $CS^tR[F] = C \otimes S^{\otimes t} \otimes R$. By Wielandt's bound (15) in [27][Theorem 4.1], we have

$$F^{\otimes t} = \lambda^{\otimes t} \otimes CS^tR[F] \oplus (B[F])^{\otimes t} = \lambda^{\otimes t} \otimes CS^{t(\operatorname{rem}\sigma)}R[F] \oplus (B[F])^{\otimes t}, \quad t \geqslant (d-1)^2 + 1 \tag{3.3.2}$$

Let us now discuss how the CSR term appearing in (3.3.2) can be decomposed into smaller CSR terms. For this, assume some numbering of the critical components and for $\mu\colon 1 \leqslant \mu \leqslant l-1$, define matrix $F_{\mu+1}$ by

$$(F_{\mu+1})_{ij} = \begin{cases} -\infty, & \text{if } i \in \mathcal{G}_\mu^c \text{ or } j \in \mathcal{G}_\mu^c, \\ (F_\mu)_{ij}, & \text{otherwise,} \end{cases} \tag{3.3.3}$$

with $F_1 = F$. Observe that $\lambda(F_\mu) = \lambda$ for any such μ, and that the critical graph of F_μ consists of components $\mathcal{G}_\mu^c, \ldots, \mathcal{G}_l^c$. Denote $U'_\mu = ((\lambda^- \otimes F_\mu)^{\otimes\sigma_\mu})^+$. Then, let matrices C'_μ,

R'_μ and S'_μ for $\mu = 1, \dots, l$ be defined by:

$$(C'_\mu)_{ij} = \begin{cases} (U'_\mu)_{ij} & \text{if } j \text{ is in } \mathcal{G}_\nu^c \\ -\infty & \text{otherwise,} \end{cases} \qquad (R'_\mu)_{ij} = \begin{cases} (U'_\mu)_{ij} & \text{if } i \text{ is in } \mathcal{G}_\nu^c \\ -\infty & \text{otherwise,} \end{cases}$$
$$(S'_\mu)_{ij} = (S_\mu)_{ij} = \begin{cases} \lambda^- \otimes (F_\mu)_{ij} & \text{if } (i,j) \in \mathcal{G}_\nu^c \\ -\infty & \text{otherwise.} \end{cases} \tag{3.3.4}$$

Let us also compare C'_μ, S'_μ and R'_μ with the matrices introduced in (3.2.1). Notice that $S'_\mu = S_\mu$, for all μ and also $C'_1 = C_1$ and $R'_1 = R_1$, but in general only $C'_\mu \leqslant C_\mu$ and $R'_\mu \leqslant R_\mu$. We further denote $C'_\mu S_\mu^{t(\operatorname{rem}\sigma_\nu)} R_\mu[F] = C'_\mu \otimes S_\mu^{t(\operatorname{rem}\sigma_\mu)} \otimes R'_\mu$, similarly to the CSR notation before. According to [27][Corollary 4.3], the following decomposition holds:

$$CS^{t(\operatorname{rem}\sigma)} R[F] = \bigoplus_{\mu=1}^{l} C'_\mu S_\mu^{t(\operatorname{rem}\sigma_\mu)} R'_\mu[F], \qquad \forall t. \tag{3.3.5}$$

Combining (3.3.2) and (3.3.5), we obtain

$$F^{\otimes t} = \lambda^{\otimes t} \otimes \bigoplus_{\mu=1}^{l} C'_\mu S_\mu^{t(\operatorname{rem}\sigma_\mu)} R'_\mu[F] \oplus (B[F])^{\otimes t}, \quad \forall t \geqslant (d-1)^2 + 1. \tag{3.3.6}$$

Observing that $C'_1 S_1^{t(\operatorname{rem}\sigma_1)} R'_1[F] = C_1 S_1^{t \operatorname{rem}\sigma_1} R_1[F]$ we can also write:

$$F^{\otimes t} = \lambda^{\otimes t} \otimes C_1 S_1^{t(\operatorname{rem}\sigma_1)} R_1[F] \oplus \lambda^{\otimes t} \otimes \bigoplus_{\mu=2}^{l} C'_\mu S_\mu^{t(\operatorname{rem}\sigma_\mu)} R'_\mu[F] \oplus (B[F])^{\otimes t}, \quad \forall t \geqslant (d-1)^2 + 1. \tag{3.3.7}$$

But by a similar combination of [27] Theorem 4.1 and Corollary 4.3, we also have:

$$(B_1[F])^{\otimes t} = \lambda^{\otimes t} \otimes \bigoplus_{\mu=2}^{l} C'_\mu S_\mu^{t(\operatorname{rem}\sigma_\mu)} R'_\mu[F] \oplus (B[F])^{\otimes t}, \quad \forall t \geqslant (d-1)^2 + 1, \tag{3.3.8}$$

where $B_1[F]$ is defined as in (3.2.2) with $\nu = 1$. Substituting (3.3.8) into (3.3.7) we obtain

$$F^{\otimes t} = \lambda^{\otimes t} \otimes C_1 S_1^{t(\operatorname{rem}\sigma_1)} R_1[F] \oplus (B_1[F])^{\otimes t}, \tag{3.3.9}$$

which is the same as (3.2.3) for $\nu = 1$

3.3.2 Proof of Proposition 3.2.3 [29]

Observe that (3.3.6) holds for any numbering of critical components. In other words, for any numbering of critical components we get the corresponding CSR decomposition of the form (3.3.6). Depending on which of these components is the first one, the first term in (3.3.6) can be equal to any of the terms $C_\nu S_\nu^{t(\operatorname{rem}\sigma_\nu)} R_\nu[F]$, while any other term in (3.3.6) is less than or equal to one of these $C_\nu S_\nu^{t(\operatorname{rem}\sigma_\nu)} R_\nu[F]$. This implies that taking the tropical sum of all CSR decompositions (3.3.6) written for all possible numberings of the critical components we obtain (3.2.4):

$$F^{\otimes t} = \lambda^{\otimes t} \otimes \bigoplus_{\nu=1}^{l} C_\nu S_\nu^{t(\operatorname{rem}\sigma_\nu)} R_\nu[F] \oplus (B[F])^{\otimes t}, \quad \forall t \geqslant (d-1)^2 + 1, \tag{3.3.10}$$

For the irreducible matrices, the existence of $T(F)$ such that

$$F^{\otimes t} = \lambda^{\otimes t} \otimes C S^{t(\operatorname{rem}\sigma)} R[F], \qquad \forall t \geqslant T(F) \tag{3.3.11}$$

follows from [33][Theorem 5.6], and a number of upper bounds on $T(F)$ have been established in [27]. Recall also that

$$C S^t R[F] = \bigoplus_{\mu=1}^{l} C'_\mu S_\mu^{t(\operatorname{rem}\sigma_\mu)} R'_\mu[F] \leqslant \bigoplus_{\nu=1}^{l} C_\nu S_\nu^{t(\operatorname{rem}\sigma_\nu)} R_\nu[F], \quad \forall t. \tag{3.3.12}$$

It follows from (3.3.10), (3.3.11) and (3.3.12) that

$$\bigoplus_{\nu=1}^{l} C_\nu S_\nu^{t(\operatorname{rem}\sigma_\nu)} R_\nu[F] \leqslant C S^{t(\operatorname{rem}\sigma)} R[F], \quad \forall t \geqslant T(F). \tag{3.3.13}$$

Combining (3.3.12), (3.3.13) and the periodicity of CSR terms, we can replace inequalities in (3.3.12) and (3.3.13) with equalities, and we can write (3.3.11) as

$$F^{\otimes t} = \lambda^{\otimes t} \otimes \bigoplus_{\nu=1}^{l} C_\nu S_\nu^{t(\operatorname{rem}\sigma_\nu)} R_\nu[F],$$

establishing (3.2.5) and completing the proof of Proposition 3.2.3.

3.3.3 Proof of Proposition 3.2.4 [29]

Let us recall the notation introduced in Definition 2.2.9 and the result of Proposition 2.2.2, according to which, in particular,

$$A_{ij}^{\otimes k} = p\left(\mathcal{W}^k(i \to j)\right), \quad A_{ij}^{+} = p\left(\mathcal{W}(i \to j)\right).$$

Here and below, we will omit the subscript G as the walks will be always defined on G being the graph associated with A.

Let us also introduce some extra notation, following [27]. We are also going to use the following sets of walks:

- $\mathcal{W}^{t,l}(i \to j)$: set of walks connecting node i to node j and having length $t(\operatorname{rem} l)$;
- $\mathcal{W}^{t,l}(i \xrightarrow{\mathcal{G}} j)$: set of walks connecting node i to node j, going through a node in subgraph $\mathcal{G}$ and having length $t(\operatorname{rem} l)$.

The proof given below is a simplified version of the proof of [27][Theorem 6.1]. For the sake of this proof we assume without loss of generality that the critical graph is strongly

connected, i.e., it consists of one component, and let C, S and R be defined from it. We will show that for arbitrary i and j

$$(C \otimes S^{\otimes t} \otimes R)_{ij} = (C_Z \otimes S_Z^{\otimes t} \otimes R_Z)_{ij} = p(\mathcal{W}^{t,l(Z)}(i \xrightarrow{Z} j)). \tag{3.3.14}$$

We first show

$$(C_Z \otimes S_Z^{\otimes t} \otimes R_Z)_{ij} \leqslant p(\mathcal{W}^{t,l(Z)}(i \xrightarrow{Z} j)), \quad (C \otimes S^{\otimes t} \otimes R)_{ij} \leqslant p(\mathcal{W}^{t,l(Z)}(i \xrightarrow{Z} j)). \tag{3.3.15}$$

For the first inequality, we have $(C_Z \otimes S_Z^{\otimes t} \otimes R_Z)_{ij} = (C_Z)_{is_1} \otimes (S_Z^{\otimes t})_{s_1 s_2} \otimes (R_Z)_{s_2 j}$, for some $s_1, s_2 \in Z$, which means that in terms of walks, there is a walk V such that $p(V) = (C_Z \otimes S_Z^{\otimes t} \otimes R_Z)_{ij}$ and decomposed as $V = V_1 V_2 V_3$, where $V_1 \in \mathcal{W}^{0,l(Z)}(i \to s_1)$, $V_2 \in \mathcal{W}^{t}(s_1 \to s_2)$ and $V_3 \in \mathcal{W}^{0,l(Z)}(s_2 \to j)$. It is then obvious that $V \in \mathcal{W}^{t,l(Z)}(i \xrightarrow{Z} j)$, and the first inequality of (3.3.15) follows.

As for the second inequality, $(C \otimes S^{\otimes t} \otimes R)_{ij}$ is the weight of a walk W that can be decomposed as $W = W_1 W_2 W_3$, where $W_1 \in \mathcal{W}^{0,\sigma}(i \to k_1)$, $W_2 \in \mathcal{W}^{t}(k_1 \to k_2)$ and $W_3 \in \mathcal{W}^{0,\sigma}(k_2 \to j)$ and $k_1, k_2 \in \mathcal{G}_1^c$. We now introduce a walk W_4 connecting k_1 to a node $k_3 \in Z$ and a walk W_5 going back to k_1. The composition $W_4 W_5$ forms a closed walk on $\mathcal{G}^c(F)$, and its length is a multiple of σ. In k_3, we insert a closed walk W_6 of a big enough length, whose all arcs belong to $\mathcal{G}^c(F)$ and whose length is such that the sum of lengths of W_1, W_3, W_4, W_5 and W_6 is a multiple of $l(Z)$. Then for the walk $\tilde{W} = W_1 W_4 W_6 W_5 W_2 W_3$, we have $\tilde{W} \in \mathcal{W}^{t,l(Z)}(i \xrightarrow{Z} j)$. We thus have $p(W) = p(\tilde{W}) \leqslant p(\mathcal{W}^{t,l(Z)}(i \xrightarrow{Z} j))$, hence the second inequality of (3.3.15).

We now prove:

$$(C_Z \otimes S_Z^{\otimes t} \otimes R_Z)_{ij} \geqslant p(\mathcal{W}^{t,l(Z)}(i \xrightarrow{Z} j)), \quad (C \otimes S^{\otimes t} \otimes R)_{ij} \geqslant p(\mathcal{W}^{t,l(Z)}(i \xrightarrow{Z} j)). \tag{3.3.16}$$

For this, consider a walk W such that $p(W) = p(\mathcal{W}^{t,l(Z)}(i \xrightarrow{Z} j))$. Then we decompose it as $W = V_1V_2$, where V_1 connects i to a node $k \in Z \subseteq \mathcal{G}^c(F)$, and V_2 connects k to j. At node k we insert mZ: a number of copies of Z such that $ml(Z) \geqslant t + l(Z)$. We then find V_3, W_2 and V_4 such that $mZ = V_3W_2V_4$, W_2 has length t and both $l(V_1) + l(V_3)$ and $l(V_4) + l(V_2)$ are multiples of $l(Z)$. Since $\tilde{W} = V_1V_3W_2V_4V_2 \in \mathcal{W}^{t,l(Z)}(i \xrightarrow{Z} j)$ and m is big enough, such walks V_3, W_2 and V_4 can be found. Denoting by k_1 the end of walk V_3 and by k_2 the beginning of walk V_4, we see that

$$p(V_1) + p(V_3) \leqslant (C_Z)_{ik_1}, \quad p(V_1) + p(V_3) \leqslant C_{ik_1}, \quad p(W_2) \leqslant (S_Z^{\otimes t})_{k_1k_2}, \quad p(W_2) \leqslant S_{k_1k_2}^{\otimes t},$$
$$p(V_4) + p(V_2) \leqslant (R_Z)_{k_2j}, \quad p(V_4) + p(V_2) \leqslant R_{k_2j},$$

and this implies both inequalities of (3.3.16).

3.4 Two-sided Tropical Discrete Logarithm Problem

In this section, we will generalise the two-sided tropical discrete logarithm problem to attack heuristically the tropical version of Stickel's protocol.

3.4.1 Theoretical observations and algorithms

Recall the original Stickel's Protocol 2.3.2 in Chapter 2. Here we consider the following tropical version of Stickel's protocol:

Protocol 3.4.1 (Tropical Version of Stickel's Protocol) *Alice and Bob agree on public matrices $A, B, W \in \mathbb{R}_{\max}^{n\times n}$ then they do the following steps:*

1. *Alice chooses a pair of positive integer numbers (m, n). Then Alice sends $U = A^{\otimes m} \otimes W \otimes B^{\otimes n}$ to Bob,*

2. *Bob chooses a pair positive integer numbers (p, q). Then Bob sends $V = A^{\otimes p} \otimes W \otimes B^{\otimes q}$ to Alice,*

3. *Alice computes her private key* $K_a = A^{\otimes m} \otimes V \otimes B^{\otimes n}$,

4. *Bob computes his private key* $K_b = A^{\otimes p} \otimes W \otimes A^{\otimes q}$.

Note that here we are not considering the tropical Stickel protocol with tropical polynomials as in [13], but a simpler version of it.

To break Protocol 3.4.1, it is desirable to have a method of finding t_1 and t_2 such that $A^{\otimes t_1} \otimes W \otimes B^{\otimes t_2} = U$, for given matrices A, B, W and U. However, unlike the one-sided problem discussed earlier in this chapter, such problem is quite likely to have multiple solutions, as we can see from experiments.

Example 3.4.1 *Let*

$$A = \begin{pmatrix} 595 & 432 & -120 & -959 & -755 \\ 444 & -901 & 395 & 389 & 793 \\ -387 & -990 & 357 & 211 & 474 \\ 558 & -482 & 897 & 307 & -233 \\ 81 & 186 & 27 & -246 & -829 \end{pmatrix}, \quad B = \begin{pmatrix} 607 & 476 & 749 & -244 & -775 \\ 310 & -496 & -74 & 917 & -677 \\ -270 & 479 & 103 & -939 & 394 \\ -105 & -661 & -999 & 500 & 67 \\ -133 & -172 & -163 & -508 & 935 \end{pmatrix},$$

and

$$W = \begin{pmatrix} -831 & 931 & 287 & 790 & -250 \\ -990 & -901 & -411 & -424 & -588 \\ 229 & -989 & -474 & 106 & -714 \\ 141 & -376 & 454 & 666 & 688 \\ -450 & 820 & -997 & -699 & -858 \end{pmatrix}$$

Consider the following pairs: $(m_1, n_1) = (68, 72)$, $(m_2, n_2) = (35, 93)$, $(m_3, n_3) =$

$(46,\ 86)$, $(m_4,\ n_4) = (90,\ 58)$ *Then it can be seen that:*

$$A^{\otimes m_1} \otimes W \otimes A^{\otimes n_1} = A^{\otimes m_2} \otimes W \otimes B^{\otimes n_2} = A^{\otimes m_3} \otimes W \otimes B^{\otimes n_3}$$
$$= A^{\otimes m_4} \otimes W \otimes B^{\otimes n_4} =$$
$$= \begin{pmatrix} 107031 & 106992 & 107001 & 106974 & 108099 \\ 106880 & 106841 & 106850 & 106823 & 107948 \\ 106610 & 106571 & 106580 & 106553 & 107678 \\ 106994 & 106955 & 106964 & 106937 & 108062 \\ 106517 & 106478 & 106487 & 106460 & 107585 \end{pmatrix}.$$

Let us also consider the following pairs: $(p_1,\ q_1) = (53,\ 53)$, $(p_2,\ q_2) = (31,\ 67), (p_3,\ q_3) = (64,\ 46)$ *and* $(p_4,\ q_4) = (42,\ 60)$. *Then*

$$A^{\otimes p_1} \otimes W \otimes A^{\otimes q_1} = A^{\otimes p_2} \otimes W \otimes B^{\otimes q_2} = A^{\otimes p_3} \otimes W \otimes B^{\otimes q_3} = A^{\otimes p_4} \otimes W \otimes B^{\otimes q_4}$$
$$= \begin{pmatrix} 80341 & 80302 & 80311 & 80284 & 81409 \\ 80190 & 80151 & 80160 & 80133 & 81258 \\ 79920 & 79881 & 79890 & 79863 & 80988 \\ 80304 & 80265 & 80274 & 80247 & 81372 \\ 79827 & 79788 & 79797 & 79770 & 80895 \end{pmatrix}$$

For the purpose of breaking Stickel's protocol we can find arbitrary t_1' and t_2' such that $A^{\otimes t_1'} \otimes W \otimes B^{\otimes t_2'} = U$, and guessing the "true" t_1 and t_2 is not necessary. Therefore, for that purpose we are satisfied with the following relaxed formulation of the two-sided discrete logarithm problem.

Problem 3.4.1 (Two-sided Tropical Discrete Logarithm) *Given matrices A, W, B and U of appropriate dimensions such that $A^{\otimes t_1} \otimes W \otimes B^{\otimes t_2} = U$ for some t_1 and t_2, find t_1' and t_2' such that $A^{\otimes t_1'} \otimes W \otimes B^{\otimes t_2'} = U$.*

For irreducible A and B the solution to this problem can be based on the CSR expansion, as it follows from (3.2.6) that:

$$A^{\otimes t_1}\otimes W\otimes B^{\otimes t_2}=\lambda^{\otimes t_1}(A)\otimes\lambda^{\otimes t_2}\otimes CS^{t_1}R[A]\otimes W\otimes CS^{t_2}R[B],\quad \forall t_1\geqslant T(A),\ \forall t_2\geqslant T(B), \tag{3.4.1}$$

where $T(A)$ and $T(B)$ are the periodicity transients of the sequences of tropical matrix powers of A and B. If, moreover, $\mathcal{G}^c(A)$ and $\mathcal{G}^c(B)$ consist just of one component then (3.4.1) simplifies to

$$A^{\otimes t_1}\otimes W\otimes B^{\otimes t_2}=\lambda^{\otimes t_1}(A)\otimes\lambda^{\otimes t_2}(B)\otimes C_{Z_1}S_{Z_1}^{t_1}R_{Z_1}[A]\otimes W\otimes C_{Z_2}S_{Z_2}^{t_2}R_{Z_2}[B],\quad \forall t_1\geqslant T(A),\ \forall t_2\geqslant T(B), \tag{3.4.2}$$

where Z_1 is an arbitrary critical cycle of $\mathcal{G}_A$ and Z_2 is an arbitrary critical cycle of $\mathcal{G}_B$.

We will also suggest a heuristic method for solving this problem, based on the following proposition.

Proposition 3.4.1 *Let $A,B,W\in\mathbb{R}_{\max}^{d\times d}$, Z_1 be a critical cycle in $\mathcal{G}_A$ with set of nodes N_1 and Z_2 be a critical cycle in $\mathcal{G}_B$ with set of nodes N_2. Then*

$$\left(A^{\otimes t_1}\otimes W\otimes B^{\otimes t_2}\right)_{N_1N_2}=\lambda^{\otimes t_1}(A)\otimes\lambda^{\otimes t_2}(B)\otimes\left(C_{Z_1}S_{Z_1}^{t_1}R_{Z_1}[A]\otimes W\otimes C_{Z_2}S_{Z_2}^{t_2}R_{Z_2}[B]\right)_{N_1N_2},\quad \forall t_1,t_2\geqslant (d-1)^2+1. \tag{3.4.3}$$

Proof. By Theorem (3.2.2) we know that for any $t_1,t_2\geqslant(d-1)^2+1$ the rows of $A^{\otimes t_1}$ with indices in N_1 are equal to the rows of $\lambda^{\otimes t_1}\otimes C_{Z_1}S_{Z_1}^{t_1}R_{Z_1}[A]$ with the same indices and the columns of $B^{\otimes t_2}$ with indices in N_2 are equal to the columns of $C_{Z_2}S_{Z_2}^{t_2}R_{Z_2}[B]$ with the same indices. Next, the submatrix of $A^{\otimes t_1}\otimes W\otimes B^{\otimes t_2}$ extracted from the rows in N_1

and columns in N_2 can be obtained as the (tropical) product of: 1) the submatrix of $A^{\otimes t_1}$ extracted from the rows in N_1, 2) matrix W and 3) the submatrix of $A^{\otimes t_2}$ extracted from the columns in N_2. The claim results from a direct combination of these two ideas. $\square$

Using a result of [33] we can simplify (3.4.3) as follows:

$$\left(A^{\otimes t_1} \otimes W \otimes B^{\otimes t_2}\right)_{N_1 N_2} = \lambda^{\otimes t_1}(A) \otimes \lambda^{\otimes t_2}(B) \otimes (S_{Z_1}^{t_1} R_{Z_1}[A] \otimes W \otimes C_{Z_2} S_{Z_2}^{t_2}[B])_{N_1 N_2}, \quad \forall t_1, t_2 \geqslant (t-1)^2 + 1 \tag{3.4.4}$$

Let us first formulate an algorithm based on (3.4.2). It is guaranteed to solve the two-sided logarithm problem in the case where A and B are irreducible and $\mathcal{G}^c(A)$ and $\mathcal{G}^c(B)$ consist just of one component.

Algorithm 3.4.1 (Two-sided Tropical Discrete Logarithm (exact))

Input: A, B, W, $U \in \mathbb{R}_{\max}^{d \times d}$.

Output: t_1 and t_2 such that $U = A^{\otimes t_1} \otimes W \otimes B^{\otimes t_2}$.

0. Find $\lambda_1 = \lambda(A)$, $\lambda_2 = \lambda(B)$, critical cycle Z_1 of A and critical cycle Z_2 of B. Compute $C_{Z_1}[A]$, $S_{Z_1}[A]$, $R_{Z_1}[A]$, $C_{Z_2}[B]$, $S_{Z_2}[B]$ and $R_{Z_2}[B]$. Determine T_1 and T_2: upper bounds on $T(A)$ and $T(B)$.

1. For each $t_1 = 0, 1, \ldots, T_1$, using Algorithm 3.2.1, try to find t_2 such that $U = A^{\otimes t_1} \otimes W \otimes B^{\otimes t_2}$. If t_2 is never found, try to find t_1 such that the same equation holds for some $t_2 = 0, 1, \ldots, T_2$.

2. Let l_1 and l_2 be the lengths of Z_1 and Z_2, respectively. For $k_1 = 1, \ldots, l_1$ and $k_2 = 1, \ldots, l_2$ check if $U - C_{Z_1} S_{Z_1}^{k_1} R_{Z_1}[A] \otimes W \otimes C_{Z_2} S_{Z_2}^{k_2} R_{Z_2}[B] = \mu + E$, where $\mu = \lambda_1 t_1 + \lambda_2 t_2$ for some natural t_1 and t_2 such that $k_1 \equiv t_1 (\operatorname{rem} l_1)$ and $k_2 \equiv t_2 (\operatorname{rem} l_2)$. Return these t_1 and t_2 when they are found.

The following heuristic version of this algorithm is based on Proposition 3.4.1 and will be studied in our numerical experiments.

Algorithm 3.4.2 (Two-sided Tropical Discrete Logarithm (heuristic))

Input: A, B, W, $U \in \mathbb{R}_{\max}^{d\times d}$.

Output: t_1 and t_2 such that $U \approx A^{\otimes t_1} \otimes W \otimes B^{\otimes t_2}$.

1. Find $\lambda_1 = \lambda(A)$, $\lambda_2 = \lambda(B)$, critical cycle Z_1 of A and critical cycle Z_2 of B. Compute $S_{Z_1}[A]$, $R_{Z_1}[A]$, $C_{Z_2}[B]$, $S_{Z_2}[B]$.

2. Let l_1 and l_2 be the lengths of Z_1 and Z_2, respectively. For $t_1 = 1, \ldots, l_1$ and $t_2 = 1, \ldots, l_2$ check if $U_{N_1N_2} - \left(S_{Z_1}^{k_1} R_{Z_1}[A] \otimes W \otimes C_{Z_2} S_{Z_2}^{k_2}[B]\right)_{N_1N_2} = \mu + E_{N_1N_2}$, where $\mu = \lambda_1 t_1 + \lambda_2 t_2$ for some natural t_1 and t_2 such that $k_1 \equiv t_1 (\operatorname{rem} l_1)$ and $k_2 \equiv t_2 (\operatorname{rem} l_2)$. Return these t_1 and t_2 when they are found.

Efficient implementation of these algorithms relies on efficient solution of the following problems. For the first algorithm, we would have to find the transients $T(A)$ and $T(B)$ or some upper bounds on them that are not too big. Finding the transients is essentially the same problem as the one solved in the attack of Isaac and Kahrobaei [17], where the length of the preperiodic part of an ultimately periodic sequence is found. For better bounds on $T(A)$ and $T(B)$, the results of Merlet et al. [27] can give some guidance. However both the transients and the bounds in general depend on the matrix entries and can be arbitrarily big (see, e.g., [27]).

Also, in both algorithms we need to find t_1 and t_2 with certain properties, satisfying $\mu = \lambda_1 t_1 + \lambda_2 t_2$, where μ is the difference between the entries of the matrix and the entries of a CSR product. Finding such t_1 and t_2 is more difficult than just dividing μ by λ as in the solution of the (one-sided) tropical discrete logarithm.

On the other hand, however, if the problem is very degenerate as in Example 3.4.1, then it will not take too much effort for the attacker to find one such pair (which does

not have to be the same as the one used by Alice and Bob).

3.4.2 Numerical Experiments

In this section, we examine the success rate of our heuristic algorithm to break the tropical version of Stickel's protocol. We implemented Algorithm 3.4.2 in Matlab R2019b and run the test on 1.2 GHz Dual-Core Intel Core m3 Macbook retina 2017 with 8 GB of RAM.

We performed a series of experiments for Algorithm 3.4.2. For each dimension we performed 100 experiments. More precisely, the following parameters were used:

- The dimension of matrices $d = 5$ to $d = 50$,
- The entries of public matrices A, B and W in the range $[-1000, 1000]$,
- The private exponents of Alice and Bob in the range $[d^2, 3 \times d^2]$.

The result which we obtained is shown in Figure 3.1.

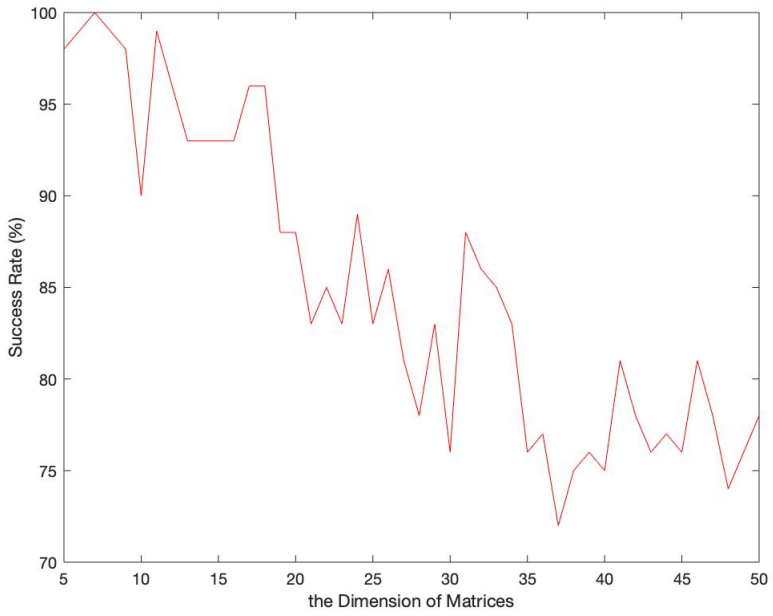

Figure 3.1: Success rate of Algorithm 3.4.2 depending on dimension

From this figure we can see that the success rate of algorithm 3.4.2 depends on the dimension of public matrices. The success rate decreases when the dimension of public matrices increases, but still stays well above 70% as the dimension of matrices approaches 50.

Chapter 4

Commuting Matrices in Tropical Algebra

In this chapter, we study three sets of commuting matrices in tropical algebra which are used to generate new public key exchange protocols (in the next chapter). The first set of commuting matrices is based on a set of special matrices considered by Jones [19], which we call generalised Kleene stars (Section 4.1). More precisely, we consider the set of deformations of such matrices (Definition 4.1.2) generalising Jones' results on tropical matrix roots of those special matrices. Two other sets of commuting matrices are based on our generalisation of some results of Linde and de la Puente [24] (Section 4.2).

4.1 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 [19], for which the notion of polynomial can be extended.

Definition 4.1.1 (Generalized Kleene Stars) *Let $A = (a_{ij})$ be a $n \times n$ tropical matrix*

which satisfies the following property:

$$a_{ij} \otimes a_{jk} \leqslant a_{ik} \otimes a_{jj} \quad \forall i, j, k. \tag{4.1.1}$$

We call A a generalized Kleene star.

Note that any Kleene star is a generalized Kleene star where we have $a_{jj} = 0$ for all $j \in [n]$ in (4.1.1).

We will consider the following operation. It is an extended version of tropical matrix roots, which were considered by Jones [19].

Definition 4.1.2 (Deformation [28]) *Let A be a generalized Kleene star and $\alpha \in \mathbb{R}$. Matrix $A^{(\alpha)} = (a_{ij}^{(\alpha)})$ defined by*

$$a_{ij}^{(\alpha)} = a_{ij} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)} \tag{4.1.2}$$

is called a deformation *of A.*

The proof techniques of the following two theorems are very close to those in Jones [19]. 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 $\alpha \leqslant 1$.

Theorem 4.1.1 ([28]) *$A^{(\alpha)}$ satisfies (4.1.1) for any $\alpha \leqslant 1$.*

Proof. We have

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

Hence the inequality which we want to prove is

$$\begin{aligned} &a_{ij} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)} \otimes a_{jk} \otimes (a_{jj} \oplus a_{kk})^{\otimes(\alpha-1)} \\ &\leqslant a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\alpha-1)} \otimes a_{jj}^{\otimes\alpha}. \end{aligned} \tag{4.1.3}$$

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 (4.1.3) is equivalent to

$$\begin{aligned} &a_{ij} \otimes a_{jk} \otimes (a_{ii} \oplus a_{kk})^{\otimes(1-\alpha)} \\ &\leqslant a_{ik} \otimes a_{jj}^{\otimes\alpha} \otimes (a_{ii} \oplus a_{jj})^{\otimes(1-\alpha)} \otimes (a_{jj} \oplus a_{kk})^{\otimes(1-\alpha)}. \end{aligned} \tag{4.1.4}$$

To prove (4.1.4) we observe that

$$\begin{aligned} &a_{ij} \otimes a_{jk} \otimes (a_{ii} \oplus a_{kk})^{\otimes(1-\alpha)} = a_{ij} \otimes a_{jk} \otimes (a_{ii}^{\otimes(1-\alpha)} \oplus a_{kk}^{\otimes(1-\alpha)}) \\ &\leqslant a_{ik} \otimes a_{jj} \otimes (a_{ii}^{\otimes(1-\alpha)} \oplus a_{kk}^{\otimes(1-\alpha)}) = a_{ik} \otimes a_{jj} \otimes a_{ii}^{\otimes(1-\alpha)} \oplus a_{ik} \otimes a_{jj} \otimes a_{kk}^{\otimes(1-\alpha)} \end{aligned} \tag{4.1.5}$$

and that

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

which implies

$$\begin{aligned} &a_{ik} \otimes a_{jj}^{\otimes\alpha} (a_{ii} \oplus a_{jj})^{\otimes(1-\alpha)} \otimes (a_{jj} \oplus a_{kk})^{\otimes(1-\alpha)} \\ &\geqslant a_{ik} \otimes a_{jj}^{\otimes\alpha} \otimes (a_{ii}^{\otimes(1-\alpha)} \otimes a_{jj}^{\otimes(1-\alpha)} \oplus a_{jj}^{\otimes(1-\alpha)} \otimes a_{kk}^{\otimes(1-\alpha)}) \\ &= a_{ik} \otimes a_{jj} \otimes a_{ii}^{\otimes(1-\alpha)} \oplus a_{ik} \otimes a_{jj} \otimes a_{kk}^{\otimes(1-\alpha)}. \end{aligned} \tag{4.1.6}$$

Combining (4.1.5) and (4.1.6) yields (4.1.4). □

Note that in Theorem 4.1.1 α can be negative.

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

Example 4.1.1 *Let us consider matrix*

$$A = \begin{pmatrix} 0 & 1 & -1 \\ -1 & 0 & -2 \\ -1 & 0 & -2 \end{pmatrix}$$

then we compute:

$$A^{(-\frac{2}{3})} = \begin{pmatrix} 0 & 1 & -1 \\ -1 & 0 & -2 \\ -1 & 0 & \frac{4}{3} \end{pmatrix}$$

and

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

.

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

and

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

.

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.

Proposition 4.1.1 ([28]) *For any $\alpha, \beta \in \mathbb{R}$ such that $0 \leqslant \alpha \leqslant 1$, $0 \leqslant \beta \leqslant 1$ and $0 \leqslant \alpha + \beta \leqslant 1$, 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

$$\bigoplus_{j=1}^{n} a_{ij} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)} \otimes a_{jk} \otimes (a_{jj} \oplus a_{kk})^{\otimes(\beta-1)} = a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\alpha+\beta-1)}. \quad (4.1.7)$$

We have

$$\begin{aligned} &\bigoplus_{j=1}^{n} a_{ij} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)} \otimes a_{jk} \otimes (a_{jj} \oplus a_{kk})^{\otimes(\beta-1)} \\ &= a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\alpha-1)} a_{kk}^{\otimes\beta} \oplus a_{ii}^{\otimes\alpha} \otimes a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\beta-1)} \\ &\oplus \bigoplus_{j \notin \{i,k\}} a_{ij} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)} \otimes a_{jk} \otimes (a_{jj} \oplus a_{kk})^{\otimes(\beta-1)}. \end{aligned} \quad (4.1.8)$$

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

$$\begin{aligned} &a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\alpha-1)} \otimes a_{kk}^{\otimes\beta} \oplus a_{ii}^{\otimes\alpha} \otimes a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\beta-1)} \\ &= a_{ik} \otimes a_{kk}^{\otimes\beta} \otimes a_{ii}^{\otimes(\alpha-1)} \oplus a_{ik} \otimes a_{ii}^{\otimes(\alpha+\beta-1)} = a_{ik} \otimes a_{ii}^{\otimes(\alpha+\beta-1)} \\ &= a_{ik} \otimes (a_{ii} \oplus a_{kk})^{\otimes(\alpha+\beta-1)}. \end{aligned} \quad (4.1.9)$$

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

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

it remains to show that

$$a_{jj} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)} \otimes (a_{jj} \oplus a_{kk})^{\otimes(\beta-1)} \leqslant (a_{ii} \oplus a_{kk})^{\otimes(\alpha+\beta-1)}. \tag{4.1.10}$$

which is equivalent to

$$a_{jj} \leqslant (a_{ii} \oplus a_{kk})^{\otimes(\alpha+\beta-1)} \otimes (a_{ii} \oplus a_{jj})^{\otimes(1-\alpha)} \otimes (a_{jj} \oplus a_{kk})^{\otimes(1-\beta)}. \tag{4.1.11}$$

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

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

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

In particular, $A^{(0)}$ is an idempotent and plays the role of unity for $A^{(\alpha)}$ for $0 \leqslant \alpha \leqslant 1$. For the tropical matrix roots, this property was established by Jones [19], see also [20].

Corollary 4.1.1 ([19]) *Matrix $A^{(0)}$ 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 [19].

Corollary 4.1.2 ([19]) *$A^{(k/l)} = (A^{(1/l)})^{\otimes k}$ holds for any integer $l > 0$ and integer $k\colon 1 \leqslant k \leqslant l$.*

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

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

Theorem 4.1.2 ([28]) *$A^{(\alpha)} \otimes A^{(\beta)} = A^{(\beta)} \otimes A^{(\alpha)}$ 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 $\alpha = \frac{k_1}{l_1}$ 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 max-algebraic 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 4.1.2 ([28]) *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 $a_{ij} \otimes a_{jk} \leqslant a_{ik} \otimes a_{jj}$ is equivalent to

$$d_i \otimes a_{ij} \otimes f_j \otimes d_j \otimes a_{jk} \otimes f_k \leqslant d_i \otimes a_{ik} \otimes f_k \otimes d_j \otimes a_{jj} \otimes f_j. \tag{4.1.12}$$

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 (4.1.12) is the same as $b_{ij} \otimes b_{jk} \leqslant b_{ik} \otimes b_{jj}$. □

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 4.1.3 (Generalised Kleene Star [28]) *Let A be a Kleene star and D and F be arbitrary diagonal matrices. Then $D \otimes A$, $A \otimes F$ are generalized Kleeme stars.*

Proof. By Proposition 4.1.2, $D \otimes A \otimes F$ is a generalized Kleene star for arbitrary diagonal matrices D and F. Taking $F = I$ we obtain that $D \otimes A$ is a generalized Kleene star and taking $D = I$ we obtain that $A \otimes F$ is a generalized Kleene star. □

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 4.1.3 ([28]) *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 $a_{ij}a_{jk} \leqslant a_{ik}$ is a special case of (4.1.1) when $a_{ii} = 0$. By Proposition 4.1.2, matrices A_1, A_2 and A satisfy (4.1.1). Then it suffices to observe that all diagonal entries of these matrices are equal to 0. □

4.2 Other sets of commuting matrices

In this section we will extend two sets of pairwise commuting matrices that were described by Linde and De La Puente [24].

4.2.1 Matrices of the form $[2r, r]_n^k$

Let us consider the following set of matrices, which extends a set of matrices considered by Linde and de la Puente [24].

Definition 4.2.1 *For arbitrary real number $r \leqslant 0$ and real number $k \geqslant 0$, we denote by $[2r, r]_n^k$ the set of matrices A such that $a_{ii} = k$, for all i and $a_{ij} \in [2r, r]$ for $i \neq j$.*

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

Theorem 4.2.1 ([28], extension of [24] Theorem 21) *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*

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

Proof. For all i, j we have

$$\begin{aligned}(A \otimes B)_{ij} &= a_{ii} \otimes b_{ij} \oplus a_{ij} \otimes b_{jj} \oplus \bigoplus_{l \notin \{i,j\}} a_{il} \otimes b_{lj} \\ &= k_1 \otimes b_{ij} \oplus k_2 \otimes a_{ij} \oplus \bigoplus_{l \notin \{i,j\}} a_{il} \otimes b_{lj}.\end{aligned} \tag{4.2.1}$$

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

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

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

$$\begin{aligned}(A \otimes B)_{ij} &= k_1 \otimes b_{ij} \oplus a_{ij} \otimes k_2 \oplus \bigoplus_{l \notin \{i,j\}} a_{il} \otimes b_{lj} \\ &= k_1 \otimes b_{ij} \oplus a_{ij} \otimes k_2 \\ &= (k_2 \otimes A \oplus k_1 \otimes B)_{ij} \\ &= (B \otimes A)_{ij},\end{aligned} \tag{4.2.2}$$

which shows the claim. □

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

Let us define a matrix with entries belong to $[0, k]$.

Definition 4.2.2 *For arbitrary real number $k \geqslant 0$, we denote by $[0, k]_n$ the set of matrices*

A such that $0 \leqslant a_{ij} \leqslant k$, *forall* i, j.

We also observe the following commutativity property.

Theorem 4.2.2 ([28]) *Let* $A \in [2a, a]_n^k$ *with* $a \leqslant 0$, $k \geqslant 0$ *and* $B \in [0, k]_n$ *then* $A \otimes B = B \otimes A = k \otimes b_{ij}$.

Proof.

$$\begin{aligned}(A \otimes B)_{ij} &= a_{ii} \otimes b_{ij} \oplus a_{ij} \otimes b_{jj} \oplus \bigoplus_{l \notin \{i,j\}} a_{il} \otimes b_{lj} \\ &= k \otimes b_{ij}.\end{aligned} \tag{4.2.3}$$

$$\begin{aligned}(B \otimes A)_{ij} &= b_{ii} \otimes a_{ij} \oplus b_{ij} \otimes a_{jj} \oplus \bigoplus_{l \notin \{i,j\}} b_{il} \otimes a_{lj} \\ &= b_{ij} \otimes k.\end{aligned} \tag{4.2.4}$$

Hence $A \otimes B = B \otimes A$. □

4.2.2 Matrices of the form $\mathfrak{A}(p, a)$

Let us introduce other special commuting matrices from [24]. By $\mathbb{R}_-^n$ we denote the set of real n-vectors with nonpositive components.

Definition 4.2.3 *Let* $p = (p_1, ..., p_n) \in \mathbb{R}_-^n$ *and* $a \leqslant 0$. *Then for* $n \geqslant 3$ *we define*

$$\mathfrak{A}(-p, -a) := \begin{pmatrix} 0 & p_1 & \dots & a & a \\ a & 0 & p_2 & \dots & a \\ a & a & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & p_{n-1} \\ p_n & \dots & a & a & 0 \end{pmatrix}$$

In [24] if we take two matrices $A = \mathfrak{A}(p, a)$ and $B = \mathfrak{A}(p, b)$ where $a + b \geqslant p_i$ for all i then we have $A \otimes B = B \otimes A$. Our next goal is to get rid of this condition thus extending this result to the case when we have just $a, b \leqslant 0$ as in the following Theorem.

Theorem 4.2.3 ([28], extending Theorem 22 in [24]) *Let* $A = \mathfrak{A}(p, a)$ *and* $B = \mathfrak{A}(p, b)$ *for all* $p \in \mathbb{R}^n_-$ *and* $a, b \leqslant 0$ *then* $A \otimes B = B \otimes A$.

Proof. To prove the theorem, we identify four cases for $A \otimes B$ as follows:

Case 1 When $i = j$ (diagonal entries)

$(A \otimes B)_{ij} = (a_{ii} \otimes b_{jj}) = 0$ for all $i = j$.

Case 2 When $j - i = 1(mod\ n)$

$(A \otimes B)_{ij} = (a_{ii} \otimes b_{ij}) \oplus (a_{ij} \otimes b_{jj}) \oplus \bigoplus_{k \notin \{i,j\}} (a_{ik} \otimes b_{kj}) = \max(p_i, a + b)$.

Case 3 When $j - i = 2\ (mod\ n)$

$(A \otimes B)_{ij} = (a_{ii} \otimes b_{ij}) \oplus (a_{ij} \otimes b_{jj}) \oplus (a_{il} \otimes b_{lj}) \oplus \bigoplus_{k \notin \{i,j,l\}} (a_{ik} \otimes b_{kj}) = \max(a, b, p_i + p_{i+1}, a + b)$.

Case 4 Otherwise

$(A \otimes B)_{ij} = (a_{ii} \otimes b_{ij}) \oplus (a_{ij} \otimes b_{jj}) \oplus (a_{it} \otimes b_{tj}) \oplus (a_{is} \otimes b_{sj}) \oplus \bigoplus_{k \notin \{i,j,t,s\}} (a_{ik} \otimes b_{kj}) = \max(a, b, p_i + b, a + p_s, a + b) = \max(a, b)$.

and for $B \otimes A$ we also identify four cases below:

Case 1 When $i = j$ (diagonal entries)

$(B \otimes A)_{ij} = (b_{jj} \otimes a_{ii}) = 0$ for all $i = j$.

Case 2 When $j - i = 1\ (mod\ n)$

$(B \otimes A)_{ij} = (a_{ij} \otimes b_{ii}) \oplus (b_{ij} \otimes a_{jj}) \oplus \bigoplus_{k \notin \{i,j\}} (b_{ik} \otimes a_{kj}) = \max(p_i, p_i, b + a)$.

Case 3 When $j - i = 2 \ (mod \ n)$

$(B \otimes A)_{ij} = (b_{ii} \otimes a_{ij}) \oplus (b_{ij} \otimes a_{jj}) \oplus (b_{il} \otimes a_{lj}) \oplus \bigoplus_{k \notin \{i,j,l\}} (b_{ik} \otimes a_{kj}) = \max(b, a, p_i + p_{i+1}, b + a)$.

Case 4 Otherwise

$(B \otimes A)_{ij} = (b_{ii} \otimes a_{ij}) \oplus (b_{ij} \otimes a_{jj}) \oplus (b_{it} \otimes a_{tj}) \oplus (b_{is} \otimes a_{sj}) \oplus \bigoplus_{k \notin \{i,j,t,s\}} (b_{ik} \otimes a_{kj}) = \max(b, a, p_i + a, b + p_s, b + a) = \max(b, a)$.

We can see that $A \otimes B = B \otimes A$. □

Chapter 5

Protocols Based on Commuting Matrices in Tropical Algebra

In Chapter 4 we introduced and studied new sets of pairwise commuting matrices in tropical linear algebra. In this Chapter, we will introduce new tropical implementations of Stickel's protocol based on those sets of commuting matrices. In Section 5.1 we suggest some heuristic attacks on one of these implementations (Section 5.2) and a generalised Kotov-Ushakov attack whose specifications apply to all protocols that we are going to introduce in Section 5.4. We also performed some numerical experiments for heuristic attack on Protocol 5.1.2 and give some toy examples in Section 5.3.

5.1 New implementations of Stickel's Protocol

In this section, we are going to describe a number of protocols using the commuting matrices from Chapter 4. In Protocols 5.1.1, 5.1.2 and 5.1.4 we make use of tropical quasi-polynomials of generalised Kleene stars, and matrices belonging to sets $[2r, r]_n^k$ and $\mathfrak{A}(p, a)$, respectively. Protocols 5.1.3 and 5.1.5 give two examples how one can combine two different kinds of commuting matrices.

5.1.1 Using tropical quasi-polynomials

By Theorem 4.1.2, 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 $\alpha, \beta \colon 0 \leqslant \alpha, \beta \leqslant 1$. Using this we can define a quasi-polynomial, where the role of monomials is played by deformations.

Definition 5.1.1 (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 5.1.1 ([28])

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 $K_a = K_b$.

5.1.2 Using matrices of the form $[2r, r]_n^k$

The protocol that we next describe are based on Theorem 4.2.1 and 4.2.2.

Protocol 5.1.2 ([28])

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* $a \leqslant 0$, $b \leqslant 0$, $k_1 \geqslant 0$ *and* $k_2 \geqslant 0$. *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* $c \leqslant 0$, $d \leqslant 0$, $l_1 \geqslant 0$ *and* $l_2 \geqslant 0$. *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 5.1.3 *[[28]]*

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

1. *Alice chooses matrix* $A_1 \in [2a, a]_n^g$ *for* $a \leqslant 0$ *and* $g \geqslant 0$ *and sends* g *to Bob.*

2. *Bob chooses* $B_2 \in [2b, b]_n^h$ *for* $b \leqslant 0$ *and* $h \geqslant 0$ *and sends* h *to Alice.*

3. *Alice chooses matrix* A_2 *with entries in* $[0, h]_n$, *computes* $U = A_1 \otimes W \otimes A_2$ *and sends it to Bob.*

4. *Bob chooses matrix* B_1 *with entries in* $[0, g]_n$, *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 $K_a = K_b$.

5.1.3 Using matrices of the form $\mathfrak{A}(p, a)$

Next, we introduce protocol based on Theorem 4.2.3.

Protocol 5.1.4 ([28])

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

1. *Alice chooses a random vector $p \geqslant 0$ and a non negative real number a. Then Alice constructs a matrix $A_1 = \mathfrak{A}(-p, -a)$ and sends p to Bob.*

2. *Bob chooses a random vector $q \geqslant 0$ and $b \geqslant 0$. Then Bob constructs matrix $B_2 = \mathfrak{A}(-q, -b)$ and sends q to Alice.*

3. *Alice selects a matrix $A_2 = \mathfrak{A}(-q, -c)$ for $c \geqslant 0$ and sends to Bob $U = A_1 \otimes W \otimes A_2$.*

4. *Bob selects a matrix $B_1 = \mathfrak{A}(-p, -d)$ for $d \geqslant 0$ and sends to Alice $V = B_1 \otimes W \otimes B_2$.*

5. *Alice computes $K_a = A_1 \otimes V \otimes A_2 = A_1 \otimes B_1 \otimes W \otimes B_2 \otimes A_2$.*

6. *Bob computes $K_b = B_1 \otimes U \otimes B_2 = B_1 \otimes A_1 \otimes W \otimes A_2 \otimes B_2$.*

Hence, since $A_1 \otimes B_1 = B_1 \otimes A_1$ and $A_2 \otimes B_2 = B_2 \otimes A_2$ then Alice and Bob have the common key $K_a = K_b$.

5.1.4 Using polynomials and matrices of the form $[2r, r]_n^k$

Protocol 5.1.5 ([28])

Alice and Bob agree on public matrix $W \in \mathbb{R}_{\max}^{n\times n}$. Then Alice and Bob exchange the messages in the following steps:

1. *Alice chooses matrix $A \in [2a, a]_n^{k_1}$ and a random tropical polynomial $p(x)$. Then Alice sends $U = A \otimes p(W)$.*

2. *Bob chooses matrix* $B \in [2b, b]_n^{k_2}$ *and a random tropical polynomial* $q(x)$. *Then Bob sends* $V = B \otimes q(W)$.

3. *Alice computes* $K_a = A \otimes V \otimes p(W)$ *and Bob computes* $K_b = B \otimes U \otimes q(W)$.

It can be seen immediately that Alice and Bob have the common secret key $K_a = A \otimes V \otimes p(W) = A \otimes B \otimes q(W) \otimes p(W) = B \otimes A \otimes p(W) \otimes q(W) = K_b$.

5.2 Heuristic attacks on Protocol 5.1.2

In this Section we will look closely at Protocol 5.1.2, which exploits matrices belonging to $[2a, a]_n^k$ for $a \leqslant 0$ and $k \geqslant 0$. We observe that there are two special cases, in which the key can be reconstructed easily, by means of an explicit formula. We then use the two formulae that are guaranteed in these special cases as heuristic attacks on the protocol analysing their performance in the general case.

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 4.2.1, we obtain

$$\begin{aligned} K_a &= (l_1 \otimes A_1 \oplus k_1 \otimes B_1) \otimes W \otimes (k_2 \otimes B_2 \oplus l_2 \otimes A_2) \\ &= (l_1 \otimes k_2 \otimes A_1 \otimes W \otimes B_2) \oplus (l_1 \otimes l_2 \otimes A_1 \otimes W \otimes A_2) \\ &\quad \oplus (k_1 \otimes k_2 \otimes B_1 \otimes W \otimes B_2) \oplus (k_1 \otimes l_2 \otimes B_1 \otimes W \otimes A_2) \\ &= \underline{(l_1 \otimes l_2 \otimes U) \oplus (k_1 \otimes k_2 \otimes V)} \oplus (l_1 \otimes k_2 \otimes A_1 \otimes W \otimes B_2) \\ &\quad \oplus (k_1 \otimes l_2 \otimes B_1 \otimes W \otimes A_2). \end{aligned} \tag{5.2.1}$$

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 5.2.1 ([28]) *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

$$\begin{aligned} u_{st} &= k_1 \otimes w_{st} \otimes k_2 \oplus \bigoplus_{(s',t')\neq(s,t)} (A_1)_{ss'} \otimes w_{s't'} \otimes (A_2)_{t't}, \\ v_{st} &= l_1 \otimes w_{st} \otimes l_2 \oplus \bigoplus_{(s',t')\neq(s,t)} (B_1)_{ss'} \otimes w_{s't'} \otimes (B_2)_{t't}. \end{aligned} \tag{5.2.2}$$

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 5.2.1 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 5.2.1 (W is vanishing [28]) *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 5.2.1 (Attack when W is vanishing [28]) *If W is vanishing in $A_1 \otimes W \otimes A_2$ and $B_1 \otimes W \otimes B_2$, then*

$$K_a = K_b = l_1 \otimes l_2 \otimes U \oplus k_1 \otimes k_2 \otimes V, \tag{5.2.3}$$

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 4.2.1 we find that

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

The expressions for $k_1 \otimes k_2$ and $l_1 \otimes l_2$ follow from Lemma 5.2.1. □

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 $B^{(2)}$). Then we can assume that the following property holds.

Definition 5.2.2 (W is dominant [28]) *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* (s,t)-dominant *in $A^{(1)} \otimes W \otimes A^{(2)}$ and $B^{(1)} \otimes W \otimes A^{(2)}$, if the following properties hold:*

$$\begin{aligned} (A^{(1)} \otimes W \otimes A^{(2)})_{il} &= a_{is}^{(1)} \otimes w_{st} \otimes a_{tl}^{(2)}, \quad \forall i,l, \\ (B^{(1)} \otimes W \otimes B^{(2)})_{il} &= b_{is}^{(1)} \otimes w_{st} \otimes b_{tl}^{(2)}, \quad \forall i,l, \end{aligned} \tag{5.2.4}$$

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 5.2.2 (Attack when W is dominant [28]) *Suppose that W is (s,t)-dominant in $A^{(1)} \otimes W \otimes A^{(2)}$ and $B^{(1)} \otimes W \otimes B^{(2)}$. Then the entries of the key $K_a = K_b = (k_{il})$ can be found as follows:*

$$k_{il} = w_{st}^{-} \otimes (v_{st} \otimes u_{il} \oplus u_{st} \otimes v_{il} \oplus u_{it} \otimes v_{sl} \oplus v_{it} \otimes u_{sl}). \tag{5.2.5}$$

Proof. Using (5.2.1) and (5.2.4), we obtain that

$$\begin{aligned} k_{il} = (l_1 \otimes l_2 \otimes u_{il}) \oplus (k_1 \otimes k_2 \otimes v_{il}) \oplus (l_1 \otimes k_2 \otimes a_{is}^{(1)} \otimes w_{st} \otimes b_{tl}^{(2)}) \\ \oplus (k_1 \otimes l_2 \otimes b_{is}^{(1)} \otimes w_{st} \otimes a_{tl}^{(2)}). \end{aligned} \tag{5.2.6}$$

The attacker can compute $l_1 \otimes l_2$ and $k_1 \otimes k_2$ as in Lemma 5.2.1: $l_1 \otimes l_2 = v_{st} \otimes w_{st}^{-}$

and $k_1 \otimes k_2 = u_{st} \otimes w_{st}^-$. To compute the rest, we observe that by (5.2.4)

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

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 (5.2.1) 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 (5.2.5). □

Let us describe both attacks formally.

Attack 5.2.1 (W vanishing)

Input: *Public matrix* $W \in \mathbb{R}_{\max}^{n\times n}$, *messages* $U, V \in \mathbb{R}_{\max}^{n\times n}$.

Output: *Secret key of Alice* K_a *or secret key of Bob* K_b.

1. *Compute* $l_1 \otimes l_2 = v_{st} \otimes w_{st}^-$ *and* $k_1 \otimes k_2 = u_{st} \otimes w_{st}^-$.

2. *Compute* $K = l_1 \otimes l_2 \otimes U \oplus k_1 \otimes k_2 \otimes V$.

This attack works well when the range of matrix W is small enough. More precise results can be seen in Table 5.1, see in particular the case when entries of W belong to $[-10, 10]$.

Attack 5.2.2 (W dominant)

Input: *Public matrix* $W \in \mathbb{R}_{\max}^{n\times n}$, *messages* $U, V \in \mathbb{R}_{\max}^{n\times n}$.

Output: *Secret key of Alice* K_a *or secret key of Bob* K_b.

1. *Compute* $l_1 \otimes l_2 = v_{st} \otimes w_{st}^{-}$ *and* $k_1 \otimes k_2 = u_{st} \otimes w_{st}^{-}$.

2. *Compute* K *using formula* (5.2.5).

5.3 Numerical Experiments and Toy Examples

In this section, we perform various numerical experiments for heuristic attacks on Protocol 5.1.2

5.3.1 Numerical Experiments

Now let us consider the formulae (5.2.3) and (5.2.6) as heuristic attacks on Protocol 5.1.2. 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 (5.2.3) or (5.2.6), 2) the **similarity rate**: the average percentage of the entries of the matrix computed by (5.2.3) or (5.2.6) which are equal to those in the secret key $K_a = K_b$ in the case of "no success" when the matrix computed by (5.2.3) or (5.2.6) does not coincide with the key. We implemented the attacks in Matlab R2019b and run the test on 1.2 GHz Dual-Core Intel Core m3 Macbook retina 2017 with 8 GB of RAM. The parameters that we use in our experiments as follows:

- the maximum dimension of matrices is 50×50;
- the range of k_1, k_2, l_1 and l_2 is integer number between 0 and 100;
- the entries of matrix W are integer numbers in the range from $[-10, 10]$ to $[-10^6, 10^6]$ (depending on the series of experiments, see Table 5.1).

We see that the attack based on (5.2.6) 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. We also consider the case when the range of the entries of W is not so big compared to all other parameters, in which the attack working in the case of vanishing W has better chance. Considering the success rate and the similarity rate once again, we arrive at the following results shown in Table 5.1. Note that here we revised the results previously obtained in [28] and improved them.

We see that in this case the simpler attack based on formula (5.2.3) is more efficient, and in particular, its success rate grows with the dimension while the success rate of the attack based on (5.2.6) decreases. However, the similarity rate remains overwhelming for both attacks and any dimension with which we experimented.

In view of the success of simple heuristic attacks based on (5.2.3) and (5.2.6), 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 section.

The results of our experiments are shown in Table 5.1.

Dimension of matrices	5	20	30	40	50
Success rate, entries of W in $[-10, 10]$ using attack 5.2.1 (%)	100	100	100	100	100
Success rate, entries of W in $[-10, 10]$ using attack 5.2.2 (%)	17.54	0.06	0.1	0.2	0
Success rate, entries of W in $[-10^2, 10^2]$ using attack 5.2.1 (%)	99.02	100	100	100	100
Success rate, entries of W in $[-100, 100]$ using attack 5.2.2 (%)	54.10	8.22	4.08	2.21	1.35
Success rate, entries of W in $[-10^3, 10^3]$ using attack 5.2.1 (%)	31.57	28.28	32.89	38.9	45.28
Success rate, entries of W in $[-10^3, 10^3]$ using attack 5.2.2 (%)	89.36	27.21	24.05	22.7	23.07
Success rate, entries of W in $[-10^4, 10^4]$ using attack 5.2.1 (%)	23.10	9.96	10.1	13.68	15.62
Success rate, entries of W in $[-10^4, 10^4]$ using attack 5.2.2 (%)	98.54	52.04	28.01	21.17	18.03
Success rate, entries of W in $[-10^5, 10^5]$ using attack 5.2.1 (%)	22.62	8.32	7.15	8.68	5.43
Success rate, entries of W in $[-10^5, 10^5]$ using attack 5.2.2 (%)	99.91	93.27	82.65	71.78	61.32
Success rate, entries of W in $[-10^6, 10^6]$ using attack 5.2.1 (%)	22.06	8.30	6.6	8.58	7.71
Success rate, entries of W in $[-10^6, 10^6]$ using attack 5.2.2 (%)	99.98	99.25	98.12	96.38	95.67

Table 5.1: Dependency of the success and similarity rate on dimension and the range of entries of W for the attack based on (5.2.6). 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 $[0, 100]$.

5.3.2 Toy Examples

The following examples demonstrate that all of the following four situations are possible: (1) when both Attack 5.2.1 and Attack 5.2.2 work; (2) only Attack 5.2.1 succeeds; (3) only Attack 5.2.2 succeeds; (4) none of these attacks succeed.

Example 5.3.1 *Alice and Bob agree on public matrix*

$$W = \begin{pmatrix} 6 & -8 & -5 & -7 \\ -3 & 1 & -4 & 2 \\ -6 & 2 & 4 & -6 \\ 1 & -9 & 3 & 4 \end{pmatrix}$$

Then they generate the secret key in the following steps:

1. *Alice picks some integer numbers* $a = 5, b = 78, k_1 = 69$ *and* $k_2 = 39$.

   She generates matrix A_1 *and* A_2 *as follows:*

   $$A_1 = \begin{pmatrix} 69 & -10 & -9 & -8 \\ -5 & 69 & -6 & -10 \\ -5 & -6 & 69 & -9 \\ -9 & -9 & -6 & 69 \end{pmatrix} \text{ and } A_2 = \begin{pmatrix} 39 & -87 & -83 & -135 \\ -126 & 39 & -116 & -135 \\ -139 & -99 & 39 & -111 \\ -90 & -133 & -149 & 39 \end{pmatrix}.$$

   She then sends $U = A_1 \otimes W \otimes A_2 = \begin{pmatrix} 98 & 101 & 107 & 112 \\ 109 & 112 & 106 & 113 \\ 107 & 106 & 111 & 102 \\ 115 & 114 & 100 & 108 \end{pmatrix}$.

2. *Bob picks some integer numbers* $c = 6, d = 87, l_1 = 64$ *and* $l_2 = 15$. *He generates matrices* B_1 *and* B_2 *as follows:*

$$B_1 = \begin{pmatrix} 64 & -8 & -7 & -12 \\ -7 & 64 & -7 & -8 \\ -10 & -7 & 64 & -9 \\ -10 & -12 & -6 & 64 \end{pmatrix} \text{ and } B_2 = \begin{pmatrix} 15 & -134 & -158 & -93 \\ -87 & 15 & -121 & -95 \\ -99 & -144 & 15 & -148 \\ -102 & -166 & -130 & 15 \end{pmatrix}.$$

Then Bob sends $V = B_1 \otimes W \otimes B_2 = \begin{pmatrix} 69 & 72 & 78 & 83 \\ 80 & 83 & 77 & 84 \\ 78 & 77 & 82 & 73 \\ 86 & 85 & 71 & 79 \end{pmatrix}$

3. *Alice computes her secret key* $K_{Alice} = A_1 \otimes V \otimes A_2 = \begin{pmatrix} 177 & 180 & 186 & 191 \\ 188 & 191 & 185 & 192 \\ 186 & 185 & 190 & 181 \\ 194 & 193 & 179 & 187 \end{pmatrix}$

4. *Bob computes his secret keys* $K_{Bob} = B_1 \otimes U \otimes W = \begin{pmatrix} 177 & 180 & 186 & 191 \\ 188 & 191 & 185 & 192 \\ 186 & 185 & 190 & 181 \\ 194 & 193 & 179 & 187 \end{pmatrix}$

We can see immediately that K_{Alice} *is equal to* K_{Bob}.

As an attacker, Eve needs to find Alice's or Bob's secret key. Therefore, she uses the public matrices to attack the protocol. In this example we will implement Attack 5.2.2 and Attack 5.2.1. First, we perform Attack 5.2.1:

1. *Using the information from public matrices* W, V *and* U*, Eve computes* $k_1 \otimes k_2 = 108$ *and* $l_1 \otimes l_2 = 79$.

2. *Eve computes* $K_{Attack} = l_1 \otimes l_2 \otimes U \oplus k_1 \otimes k_2 \otimes V = \begin{pmatrix} 177 & 180 & 186 & 191 \\ 188 & 191 & 185 & 192 \\ 186 & 185 & 190 & 181 \\ 194 & 193 & 179 & 187 \end{pmatrix}$.

We have $K_{Alice} = K_{Bob} = K_{Attack}$. *So Eve can reveal Alice's or Bob secret keys easily. Second, we will attack the protocol using attack* 5.2.2. *Eve attacks the protocol as in the following step:*

(a) *Using the information from public matrices* W, V *and* U, *Eve computes* $k_1 \otimes k_2 = 108$ *and* $l_1 \otimes l_2 = 79$.

(b) *Eve computes each components of* K_{attack} *using Theorem* 5.2.2 *and gets* $K_{attack} = \begin{pmatrix} 177 & 180 & 186 & 191 \\ 188 & 191 & 185 & 192 \\ 186 & 185 & 190 & 181 \\ 194 & 193 & 179 & 187 \end{pmatrix}$

In this example we can see that both Attack 5.2.1 *and Attack* 5.2.1 *can break the protocol to get the secret key.*

Example 5.3.2 *Alice and Bob agree on public matrix* $W = \begin{pmatrix} 9 & -8 & -6 & -6 \\ -4 & -3 & -10 & -5 \\ -5 & 1 & 7 & 0 \\ 8 & -3 & -5 & 10 \end{pmatrix}$

Then they generate the secret key in the following steps:

1. *Alice picks some integer numbers* $a = 9, b = 70, k_1 = 54$ *and* $k_2 = 70$. *She generate matrix* A_1 *and* A_2 *as follows:*

$$A_1 = \begin{pmatrix} 54 & -16 & -18 & -11 \\ -16 & 54 & -13 & -12 \\ -18 & -16 & 54 & -17 \\ -11 & -15 & -11 & 54 \end{pmatrix} \text{ and } A_2 = \begin{pmatrix} 70 & -101 & -80 & -100 \\ -103 & 70 & -108 & -77 \\ -113 & -75 & 70 & -102 \\ -129 & -73 & -88 & 70 \end{pmatrix}.$$

She then sends $U = A_1 \otimes W \otimes A_2 = \begin{pmatrix} 133 & 116 & 118 & 118 \\ 120 & 121 & 114 & 119 \\ 119 & 125 & 131 & 124 \\ 132 & 121 & 119 & 134 \end{pmatrix}$.

2. *Bob picks some integer numbers* $c = 18, d = 75, l_1 = 88$ *and* $l_2 = 80$. *He generate matrix* B_1 *and* B_2 *as follows:*

$$B_1 = \begin{pmatrix} 88 & -26 & -29 & -33 \\ -24 & 88 & -29 & -27 \\ -30 & -25 & 88 & -33 \\ -24 & -20 & -35 & 88 \end{pmatrix} \text{ and } B_2 = \begin{pmatrix} 80 & -138 & -130 & -149 \\ -97 & 80 & -75 & -132 \\ -86 & -113 & 80 & -123 \\ -114 & -148 & -143 & 80 \end{pmatrix}.$$

Then Bob sends $V = B_1 \otimes W \otimes B_2 = \begin{pmatrix} 177 & 160 & 162 & 162 \\ 164 & 165 & 158 & 163 \\ 163 & 169 & 175 & 168 \\ 176 & 165 & 163 & 178 \end{pmatrix}$

3. *Alice computes her secret key* $K_{Alice} = A_1 \otimes V \otimes A_2 = \begin{pmatrix} 301 & 284 & 286 & 286 \\ 288 & 289 & 282 & 287 \\ 287 & 293 & 299 & 292 \\ 300 & 289 & 287 & 302 \end{pmatrix}$

4. *Bob computes his secret keys* $K_{Bob} = B_1 \otimes U \otimes W = \begin{pmatrix} 301 & 284 & 286 & 286 \\ 288 & 289 & 282 & 287 \\ 287 & 293 & 299 & 292 \\ 300 & 289 & 287 & 302 \end{pmatrix}$

We can see immediately that K_{Alice} *is equal to* K_{Bob}.

As attacker, Eve needs to find Alice's or Bob's secret key. Therefore, she uses the public matrices to attack the protocol. In this example we will implement Attack 5.2.2 and Attack 5.2.1. First, we perform Attack 5.2.1:

1. *Using the information from public matrices* W, V *and* U*, Eve computes* $k_1 \otimes k_2 = 124$ *and* $l_1 \otimes l_2 = 168$.

2. *Eve computes* $K_{Attack} = l_1 \otimes l_2 \otimes U \oplus k_1 \otimes k_2 \otimes V = \begin{pmatrix} 301 & 284 & 286 & 286 \\ 288 & 289 & 282 & 287 \\ 287 & 293 & 299 & 292 \\ 300 & 289 & 287 & 302 \end{pmatrix}$

   We have $K_{Alice} = K_{Bob} = K_{Attack}$*. So Eve can reveal Alice's or Bob secret keys easily. Second, we will attack the protocol using Attack 5.2.2. Eve attacks the protocol as follows:*

   (a) *Using the information from public matrices* W, V *and* U*. Eve computes* $k_1 \otimes k_2 = 108$ *and* $l_1 \otimes l_2 = 79$.

   (b) *Eve computes each components of* K_{attack} *using Theorem (5.2.2) and gets* $K_{attack} = \begin{pmatrix} 301 & 284 & 286 & 286 \\ 288 & 289 & 282 & 287 \\ 290 & 293 & 299 & 292 \\ 300 & 289 & 287 & 302 \end{pmatrix}$

   We can see that $K_{Alice} \neq K_{Attack}$*, therefore this attack fails to break the protocol.*

However, the similarity of K_{Alice} and K_{Attack} is quite big. In this example only element (3,1) is different from K_{Alice}.

In this example we can see that both Attack 5.2.1 and Attack 5.2.1 can break the protocol to get the secret key.

Example 5.3.3 *Alice and Bob agree on public matrix*

$$W = \begin{pmatrix} 819 & 128 & 794 & 312 \\ 609 & 898 & 908 & 58 \\ 248 & 984 & 252 & 640 \\ 409 & 836 & 338 & 292 \end{pmatrix}.$$

Then they generate the secret key in the following steps:

1. *Alice picks some integer numbers $a = 11, b = 74, k_1 = 6$ and $k_2 = 15$. She generates matrices A_1 and A_2 as follows:*

$$A_1 = \begin{pmatrix} 64 & -21 & -18 & -11 \\ -16 & 64 & -16 & -17 \\ -14 & -17 & 64 & -20 \\ -17 & -12 & -21 & 64 \end{pmatrix} \text{ and } A_2 = \begin{pmatrix} 15 & -81 & -128 & -136 \\ -88 & 15 & -78 & -122 \\ -123 & -88 & 15 & -101 \\ -90 & -119 & -101 & 15 \end{pmatrix}.$$

She then sends $U = A_1 \otimes W \otimes A_2 == \begin{pmatrix} 898 & 981 & 902 & 844 \\ 880 & 983 & 987 & 871 \\ 960 & 1063 & 970 & 926 \\ 875 & 978 & 911 & 841 \end{pmatrix}$.

2. *Bob picks some integer numbers $c = 16, d = 955, l_1 = 47$ and $l_2 = 22$. He generates matrix B_1 and B_2 as follows:*

$$B_1 = \begin{pmatrix} 47 & -25 & -27 & -21 \\ -17 & 47 & -27 & -16 \\ -19 & -30 & 47 & -18 \\ -20 & -25 & -22 & 47 \end{pmatrix} \text{ and } B_2 = \begin{pmatrix} 22 & -143 & -115 & -105 \\ -164 & 22 & -183 & -152 \\ -179 & -187 & 22 & -126 \\ -138 & -98 & -151 & 22 \end{pmatrix}. \text{ Then}$$

$$\text{Bob sends } V = B_1 \otimes W \otimes B_2 = \begin{pmatrix} 888 & 979 & 905 & 805 \\ 824 & 979 & 977 & 829 \\ 867 & 1053 & 900 & 879 \\ 821 & 984 & 905 & 810 \end{pmatrix}$$

3. *Alice computes her secret key* $K_{Alice} = A_1 \otimes V \otimes A_2 = \begin{pmatrix} 967 & 1058 & 984 & 921 \\ 955 & 1058 & 1056 & 940 \\ 1029 & 1132 & 1039 & 995 \\ 960 & 1063 & 984 & 926 \end{pmatrix}$.

4. *Bob computes his secret keys* $K_{Bob} = B_1 \otimes U \otimes W = \begin{pmatrix} 967 & 1058 & 984 & 921 \\ 955 & 1058 & 1056 & 940 \\ 1029 & 1132 & 1039 & 995 \\ 960 & 1063 & 984 & 926 \end{pmatrix}$.

We can see immediately that K_{Alice} *is equal to* K_{Bob}.

As an attacker, Eve needs to find Alice's or Bob's secret key. Therefore, she uses the public matrices to attack the protocol. In this example we will implement Attack 5.2.2 and Attack 5.2.1. First, we perform Attack 5.2.1:

1. *Using the information from public matrices* W, V *and* U*, Eve computes* $k_1 \otimes k_2 = 21$ *and* $l_1 \otimes l_2 = 69$.

2. *Eve computes* $K_{Attack} = l_1 \otimes l_2 \otimes U \oplus k_1 \otimes k_2 \otimes V = \begin{pmatrix} 967 & 1058 & 984 & 913 \\ 949 & 1058 & 1056 & 940 \\ 1029 & 1132 & 1039 & 995 \\ 944 & 1063 & 984 & 910 \end{pmatrix}$. *We have* $K_{Alice} = K_{Bob} = K_{Attack}$. *So Eve can reveal Alice's or Bob secret keys easily. Second, we will attack the protocol using Attack 5.2.2. Eve attacks the protocol follows:*

   (a) *Using the information from public matrices* W, V *and* U, *Eve computes* $k_1 \otimes k_2 = 108$ *and* $l_1 \otimes l_2 = 79$.

   (b) *Eve computes* K_{attack} *using Theorem 5.2.2 and gets* $K_{attack} = \begin{pmatrix} 967 & 1058 & 984 & 921 \\ 955 & 1058 & 1056 & 940 \\ 1029 & 1132 & 1039 & 995 \\ 960 & 1063 & 984 & 926 \end{pmatrix}$.

   We can see that $K_{Alice} = K_{Attack}$.

In this example we can see that only Attack 5.2.2 can break the protocol. However, Attack 5.2.1 cannot break the protocol but the entries of K_{attack} *are similar with the entries of* K_{Alice}

Example 5.3.4 *Alice and Bob agree on public matrix*

$$W = \begin{pmatrix} 982 & 621 & 293 & 369 \\ 552 & 584 & 343 & 157 \\ 805 & 468 & 667 & 967 \\ 677 & 797 & 980 & 979 \end{pmatrix}.$$

Then they generate the secret key in the following steps:

1. *Alice picks some integer numbers* $a = 16, b = 97, k_1 = 9$ *and* $k_2 = 63$. *She generates matrices* A_1 *and* A_2 *as follows:*

$$A_1 = \begin{pmatrix} 9 & -30 & -17 & -16 \\ -23 & 9 & -25 & -17 \\ -22 & -26 & 9 & -24 \\ -30 & -16 & -24 & 9 \end{pmatrix} \text{ and } A_2 = \begin{pmatrix} 63 & -131 & -154 & -188 \\ -117 & 63 & -170 & -109 \\ -115 & -111 & 63 & -101 \\ -182 & -159 & -109 & 63 \end{pmatrix}.$$ *She then sends* $U = A_1 \otimes W \otimes A_2 == \begin{pmatrix} 1054 & 860 & 1027 & 1026 \\ 1022 & 852 & 1026 & 1025 \\ 1023 & 845 & 1019 & 1039 \\ 1015 & 878 & 1052 & 1051 \end{pmatrix}$.

2. *Bob picks some integer numbers* $c = 18, d = 81, l_1 = 43$ *and* $l_2 = 40$. *He generates matrix* B_1 *and* B_2 *as follows:*

$$B_1 = \begin{pmatrix} 43 & -18 & -33 & -31 \\ -31 & 43 & -19 & -28 \\ -18 & -30 & 43 & -35 \\ -23 & -27 & -21 & 43 \end{pmatrix} \text{ and } B_2 = \begin{pmatrix} 40 & -136 & -108 & -157 \\ -135 & 40 & -126 & -128 \\ -103 & -97 & 40 & -121 \\ -138 & -131 & -123 & 40 \end{pmatrix}.$$ *Then Bob sends* $V = B_1 \otimes W \otimes B_2 = \begin{pmatrix} 1065 & 889 & 989 & 988 \\ 991 & 855 & 992 & 991 \\ 1004 & 879 & 985 & 1050 \\ 999 & 926 & 1063 & 1062 \end{pmatrix}$.

3. *Alice computes her secret key* $K_{Alice} = A_1 \otimes V \otimes A_2 = \begin{pmatrix} 1137 & 973 & 1110 & 1109 \\ 1105 & 972 & 1109 & 1108 \\ 1106 & 965 & 1102 & 1122 \\ 1098 & 998 & 1135 & 1134 \end{pmatrix}$.

4. *Bob computes his secret key* $K_{Bob} = B_1 \otimes U \otimes W = \begin{pmatrix} 1137 & 973 & 1110 & 1109 \\ 1105 & 972 & 1109 & 1108 \\ 1106 & 965 & 1102 & 1122 \\ 1098 & 998 & 1135 & 1134 \end{pmatrix}$.

We can see immediately that K_{Alice} *is equal to* K_{Bob}.

As an attacker, Eve needs to find Alice's or Bob's secret key. Therefore, she uses the public matrices to attack the protocol. In this example we will implement Attack 5.2.2 and Attack 5.2.1. First, we perform attack 5.2.1 as follows:

1. *Usiing the information from public matrices* W, V *and* U*, Eve computes* $k_1 \otimes k_2 = 72$ *and* $l_1 \otimes l_2 = 83$.

2. *Eve computes* $K_{Attack} = l_1 \otimes l_2 \otimes U \oplus k_1 \otimes k_2 \otimes V = \begin{pmatrix} 1137 & 961 & 1110 & 1109 \\ 1105 & 935 & 1109 & 1108 \\ 1106 & 951 & 1102 & 1122 \\ 1098 & 998 & 1135 & 1134 \end{pmatrix}$.

   We have $K_{Alice} \neq K_{Attack}$. *Eve fails to break the protocol.*

   Second, Eve attacks the protocol using Attack 5.2.2. Eve attacks the protocol as follows:

   (a) *Using the information from public matrices* W, V *and* U*, Eve computes* $k_1 \otimes k_2 = 72$ *and* $l_1 \otimes l_2 = 83$.

   (b) *Eve computes each components of* K_{attack} *using Theorem (5.2.2) and get* $K_{attack} = \begin{pmatrix} 1137 & 961 & 1110 & 1109 \\ 1105 & 935 & 1109 & 1108 \\ 1106 & 951 & 1102 & 1122 \\ 1098 & 998 & 1135 & 1134 \end{pmatrix}$

   We can see that $K_{Alice} \neq K_{Attack}$. *Eve cannot break protocol using this attack.*

In this example we can see that both Attack 5.2.1 and Attack 5.2.1 cannot break the protocol to get the secret key. However, the similarity between K_{attack} and K_{Alice} is quite big. In this example also, we have that K_{attack} when W vanishing and K_{attack} when W dominant are the same.

5.4 Cryptanalysis using the Kotov-Ushakov attack

In this section we focus on the Kotov-Ushakov attack: how to modify it so that it applies to all protocols that were described in Section 5.1. To solve this problem we first describe a generalisation of the Kotov-Ushakov attack in Subsection 5.4.1. Then we describe specifications of this generalised attack to Protocol 5.1.1 (in Subsection 5.4.2), Protocol 5.1.2, (in Subsection 5.4.4), Protocol 5.1.3 (in Subsection 5.4.5) Protocol 5.1.4 (in Subsection 5.4.6), and Protocol 5.1.5 (in Subsection 5.4.7).

5.4.1 Generalisation of the Kotov-Ushakov attack

Previous section yields some simple but efficient enough heuristic attacks on Protocol 5.1.2. We now discuss how the Kotov-Ushakov attack can be generalized to apply to all protocols described in Section 5.1. The main idea is that for the protocols using other kinds of commuting matrices, tropical matrix powers can be replaced with other generators at the expense of some mild conditions imposed on coefficients.

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

$$\begin{aligned} &X = \bigoplus_{\alpha\in\mathcal{A}} x_\alpha \otimes A_\alpha, \quad Y = \bigoplus_{\beta\in\mathcal{B}} y_\beta \otimes B_\beta, \\ &X \otimes W \otimes Y = U, \\ &x_\alpha \in \mathcal{X}_\alpha(s), \quad y_\beta \in \mathcal{Y}_\beta(t). \end{aligned} \tag{5.4.1}$$

Here $\{A_\alpha \colon \alpha \in \mathcal{A}\}$ and (respectively) $\{B_\beta \colon \beta \in \mathcal{B}\}$ are 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 (5.4.1), provided that the coefficients x_α and y_β satisfy the conditions written in the last line of (5.4.1). 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 (5.4.1) is based on the same ideas from [23] that were already used in Subsection 5.4.2. After we substitute the first line of (5.4.1) into the decomposition problem $X \otimes W \otimes Y = U$ and denote

$$T^{\alpha\beta} = A_\alpha \otimes W \otimes B_\beta - U, \tag{5.4.2}$$

the decomposition problem reduces to solving the system

$$0 = \max_{\alpha\in\mathcal{A},\beta\in\mathcal{B}} (x_\alpha \otimes y_\beta \otimes T^{\alpha\beta}_{\gamma\delta}), \quad \forall \gamma, \delta \in [n]. \tag{5.4.3}$$

Here, unlike in Subsection 5.4.2, x_α and y_β also satisfy the conditions in the last line of (5.4.1). Our attack then aims to solve equation (5.4.3) with these conditions.

Attack 5.4.1 (Generalized Kotov-Ushakov)

1. *Compute*

$$\begin{aligned} c_{\alpha\beta} &= \min_{\gamma,\delta\in[n]} (-T^{\alpha\beta}_{\gamma\delta}) \\ S_{\alpha\beta} &= \arg\min_{\gamma,\delta\in[n]} (-T^{\alpha\beta}_{\gamma\delta}). \end{aligned} \tag{5.4.4}$$

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*

$$\bigcup_{(\alpha,\beta)\in\mathcal{C}} S_{\alpha\beta} = [n]\times[n], \tag{5.4.5}$$

find a cover for which the system

$$\begin{aligned} &x_\alpha + y_\beta = c_{\alpha\beta}, \quad \textit{if } (\alpha,\beta) \in \mathcal{C}, \\ &x_\alpha + y_\beta \leqslant c_{\alpha\beta}, \quad \textit{if otherwise.} \\ &x_\alpha \in \mathcal{X}_\alpha(s), y_\beta \in \mathcal{Y}_\beta(t) \end{aligned} \tag{5.4.6}$$

is solvable.

Note that we do not generally know the nature and the complexity of the conditions $x_\alpha \in \mathcal{X}_\alpha(s), \quad y_\beta \in \mathcal{Y}_\beta(t)$, and vectors s and t can themselves be constrained. However, in the specifications of Attack 5.4.1 that will follow in the next subsections, system (5.4.6) is always linear, so that its solvability can be checked by the simplex method.

The proof that Attack 5.4.1 is almost the same as that of Theorem 2.3.1, the only differences being that we have more general sets $\mathcal{A}$ and $\mathcal{B}$ instead of $\{0,\dots,D\}$, and that we have to respect the new conditions $x_\alpha \in \mathcal{X}_\alpha(s)$ and $y_\beta \in \mathcal{Y}_\beta(t)$.

Theorem 5.4.1 ([28]) *Attack 5.4.1 yields*

$$X = \bigoplus_{\alpha\in\mathcal{A}} x_\alpha \otimes A_\alpha, \quad Y = \bigoplus_{\beta\in\mathcal{B}} y_\beta \otimes B_\beta.$$

that satisfy $X \otimes W \otimes Y = U$ and $x_\alpha \in \mathcal{X}_\alpha(s)$, $y_\beta \in \mathcal{Y}_\beta(t)$ if such X and Y exists.

Proof. It remains to show that the Kotov-Ushakov attack actually finds a solution to (5.4.3) with conditions $x_\alpha \in \mathcal{X}_\alpha(s)$, $y_\beta \in \mathcal{Y}_\beta(t)$ (provided that such solution exists, which is the case).

Consider the system

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

where $z_{\alpha\beta} = x_\alpha + y_\beta$ and $x_\alpha \in \mathcal{X}_\alpha(s)$, $y_\beta \in \mathcal{Y}_\beta(t)$.

According to the theory $A \otimes x = b$ (see [3] Theorem 3.1.1 and Corollary 3.1.2) we can use the following results:

1. If the solution exists then vector $\mathcal{C} = (c_{\alpha\beta})$ where $c_{\alpha\beta} = \min\limits_{\gamma,\delta\in[n]}(-T^{\alpha\beta}_{\gamma\delta})$ is the greatest solution.

2. Vector $Z = (z_{\alpha\beta})$ is a solution if and only if there exists a set $\mathcal{C} \subseteq \mathcal{A} \times \mathcal{B}$ such that (5.4.5) 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 where $x_\alpha \in \mathcal{X}_\alpha(s)$, $y_\beta \in \mathcal{Y}_\beta(t)$, it follows that checking the solvability of (5.4.3) amounts to finding at least one system (5.4.6) that is solvable with $\mathcal{C}$ being a minimal cover (i.e a set satisfying (5.4.5) that is minimal with respect to inclusion).

5.4.2 Attack on Protocol 5.1.1

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

$$\begin{aligned} X &= \bigoplus_{\alpha\in\mathcal{T}} x_\alpha \otimes A^{(\alpha)}, \\ Y &= \bigoplus_{\beta\in\mathcal{T}} y_\beta \otimes B^{(\beta)}. \end{aligned} \tag{5.4.7}$$

Comparing this with (5.4.1) we see that here we have $A_\alpha = A^{(\alpha)}$, $B_\beta = B^{(\beta)}$ and $\mathcal{A} = \mathcal{B} = \mathcal{T}$. In this case the coefficients x_α and y_β are unrestricted, so the conditions in the last line of (5.4.1) are absent.

Following the idea of Attack 5.4.1, we can write the following attack:

Attack 5.4.2 *[[28]]*

Input: *Public matrices* $W, A, B \in \mathbb{R}_{\max}^{n\times n}$ *and the messages* $U, V \in \mathbb{R}_{\max}^{n\times n}$

Output: *The secret key of Alice* K_a *or the secret key of Bob* K_b

1. *Compute* $c_{\alpha\beta} = c_{ijst}$ *and* $S_{\alpha\beta} = S_{ijst}$ *by* (5.4.4)*, where* $A_\alpha = A^{(\alpha)}$*,* $B_\beta = B^{(\beta)}$ *and* $T^{\alpha\beta}$ *by* (5.4.2) *where* $\alpha, \beta \in \mathcal{T}$*.*

2. *Among the minimal sets* $\mathcal{C} \subseteq \mathcal{T} \times \mathcal{T}$ *that satisfy* (5.4.5) *we seek those which satisfy*

$$\begin{aligned} x_\alpha + y_\beta &= c_{\alpha\beta}, \quad \text{if } (\alpha,\beta) \in \mathcal{C}, \\ x_\alpha + y_\beta &\leqslant c_{\alpha\beta}, \quad \text{if } (\alpha,\beta) \notin \mathcal{C}. \end{aligned} \tag{5.4.8}$$

Thus the Kotov-Ushakov attack on the protocol with tropical quasi-polynomials is very similar to the original one.

We now present a theorem about the validity of Attack 5.4.2.

Theorem 5.4.2 ([28]) *Let* $A, B, W \in \mathbb{R}_{\max}^{n\times n}$ *and* U *be the message sent by Alice to Bob in Protocol 5.1.1. 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*

$$X = \bigoplus_{\alpha\in\mathcal{T}} x_\alpha \otimes A^{(\alpha)}, \quad Y = \bigoplus_{\beta\in\mathcal{T}} y_\beta \otimes B^{(\beta)}. \tag{5.4.9}$$

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

The proof of this theorem is very similar to that of Theorem 2.3.1 and will be omitted. It can be also obtained as a corollary of Theorem 5.4.1 where (as explained above) $A_\alpha = A^{(\alpha)}$, $B_\beta = B^{(\beta)}$ and $\mathcal{A} = \mathcal{B} = \mathcal{T}$.

5.4.3 Implementation of the attacks 2.3.1 and 5.4.2

We implemented Attack 2.3.1 and Attack 5.4.2 using the computational algebra software GAP version 4.10.2 on MacBook Retina 1.2 GHz Intel Core m3 by modifying the existing code from [23].

In their paper Kotov and Ushakov [23] run experiments using the parameters described in [13]. In their experiments the maximal degree of the tropical polynomials is in the interval $[1, 10]$, the entries of matrices are in the interval $[-10^{10}, 10^{10}]$ and the coefficients of tropical polynomial are in the interval $[-1000, 1000]$. We use the same dimension of matrices as in the experiments of Kotov and Ushakov . For Protocol 2.3.3 and Attack 2.3.1, we use the following parameters:

- The dimension of matrices are 10×10.
- The entries of matrices and the coefficients of tropical polynomial are integer numbers in the interval $[-100, 100]$.
- The degree of polynomial in this experiment is from 1 to 50.

The growth of running time for attacking the protocol and generating a secret key is shown on Figure 5.1. Each point on the graph results from a single instance experiment, hence the random character of these graphs. We can see that the running time for Attack 2.3.1 is likely to be polynomial and the average computation time grows in practice as we increase the maximal degree of monomials in tropical polynomial. 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 [23]. Note that acording to [23] the attacker generates all minimal covers and sorts them by criteria $|\{\alpha|\exists(\alpha,\beta) \in \mathcal{C}\}.|\{\beta|\exists(\alpha,\beta) \in \mathcal{C}\}$. We could generate one minimal cover after another instead, but the efficiency of this is arguable. With this sorting, we need to check 1 or 2 covers in practice so that the

complexity of Attack 2.3.1 similar to the complexity of simplex method, after the covers are generated and sorted. We can also see that to generate a secret key we only need much less time than to attack the protocol. For instance to generate a secret key with degree of polynomial is 50 we only need 2.152 seconds but to attack it we need 7242.807 seconds.

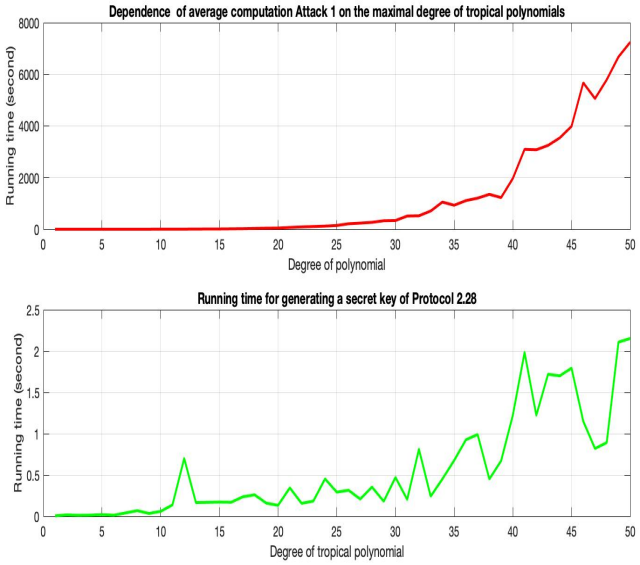

Figure 5.1: (a) Dependence of average computation Attack 2.3.1 on the maximal degree of tropical polynomials and (b) running time for generating a secret key of Protocol 2.3.3

For Protocol 2.3.3 and Attack 5.4.2, we use the following parameters:

- The dimension of matrices are 10×10.
- The entries of matrices and the coefficients of tropical quasi-polynomial are integer numbers in the interval $[-100, 100]$.
- The denominator of degree of tropical quasi-polynomial that is used in this experiment is from 1 to 50 for generating a secret key and from 1 to 13 for attacking Protocol 5.1.1.

The growth of running time for attacking the protocol and generating a secret key is shown on Figure 5.2. We can also see that the running time for Attack 5.4.2 is likely to be polynomial similar to the running time for Attack 2.3.1 and the average computation time grows in practice as we increase the maximal denominator of the degree of tropical quasi-polynomial. Since the running time of Attack 5.4.2 grows more rapidly than that of Attack 2.3.1 as we increase the maximal denominator, for Attack 5.4.2 we only investigate the running time until maximal denominator is equal to 13. We also can see that when we select the maximal denominator equal to 13, we only need 0.043 seconds for generating a secret key and 9147.872 seconds for attacking.

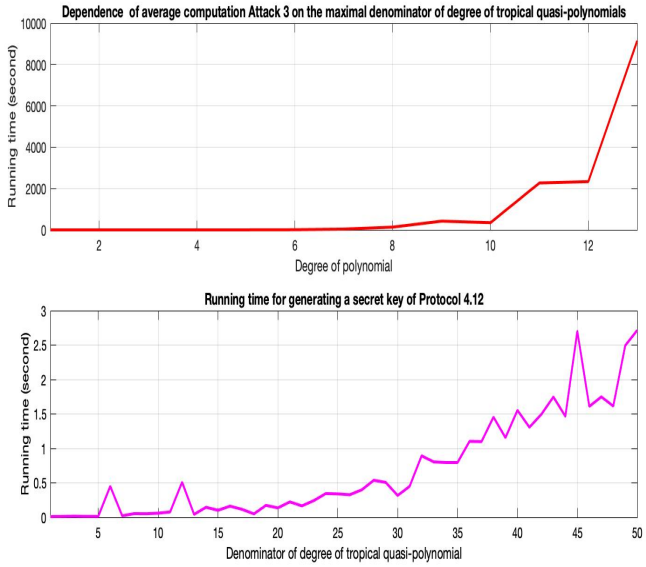

Figure 5.2: (a) Dependence of average computation Attack 5.4.2 on the maximal degree of tropical quasi-polynomials and (b) running time for generating a secret key of Protocol 5.1.1

We conclude that our modified Protocol 5.1.1 requires more time to attack it using a Kotov-Ushakov attack rather than Protocol 2.3.3.

5.4.4 Attack on Protocol 5.1.2

In Protocol 5.1.2, 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 as A_α and B_β with α and β being pairs of indices from $[n]$ (see equation (5.4.10)), we can represent any matrix in $[2a, a]_n^{k_1}$ and $[2b, b]_n^{k_2}$ as in the first line of (5.4.1). However, for this we also need to restrict the coefficients x_α to belong to $[2a, a]$ if $\alpha = (i, j)$ with $i \neq j$ or to be equal to k_1 if $i = j$. Similarly, the coefficients y_β should belong to $[2b, b]$ if $\beta = (i, j)$ with $i \neq j$ or to be equal to k_2 if $i = j$.

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

$$A_\alpha = A^{ij} = B_\beta = B^{ij} = E^{ij}, \quad \text{for all } i, j \tag{5.4.10}$$

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

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

$$\mathcal{X}_{(i,j)}(a, k_1) = \begin{cases} [2a, a], & i \neq j \\ \{k_1\}, & i = j. \end{cases} \tag{5.4.11}$$

$$\mathcal{Y}_{(i,j)}(b, k_2) = \begin{cases} [2b, b], & i \neq j \\ \{k_2\}, & i = j. \end{cases} \tag{5.4.12}$$

Unknown parameters k_1, k_2, a and b satisfy $k_1, k_2 \geqslant 0$ and $a, b \leqslant 0$.

Attack 5.4.3 *([28])*

Input: *public matrix* $W \in \mathbb{R}_{\max}^{n \times n}$ *and messages* $U, V \in \mathbb{R}_{\max}^{n \times n}$.

Output: *the secret key of Alice* K_a *or the secret key of Bob* K_b.

1. *Compute* $c_{\alpha\beta} = c_{ijst}$ *and* $S_{\alpha\beta} = S_{ijst}$ *by* (5.4.4)*, where* A_α*,* B_β *are defined by* (5.4.10) *and* $T^{\alpha\beta}$ *by* (5.4.2) *where* $\alpha = (i,j)$*,* $\beta = (s,t)$ *with* $i,j,s,t \in [n]$*.*

2. *Among the minimal sets* $\mathcal{C} \subseteq [n]^2 \times [n]^2$ *that satisfy* (5.4.5) *we seek those which satisfy*

$$\begin{aligned} & x_{ij} + y_{st} = c_{ijst}, \quad \textit{for} \quad (i,j,s,t) \in \mathcal{C} \\ & x_{ij} + y_{st} \leqslant c_{ijst}, \quad \textit{otherwise}, \\ & 2a \leqslant x_{ij} \leqslant a, \quad 2b \leqslant y_{st} \leqslant b, \quad \forall i \neq j,\ s \neq t, \\ & x_{ii} = k_1, \quad y_{ss} = k_2, \quad \forall i, s, \\ & a, b \leqslant 0, \quad k_1, k_2 \geqslant 0. \end{aligned} \tag{5.4.13}$$

Note that this is a linear system of equalities and inequalities whose solvability can be checked by the simplex method. Then attack works since it is a special case of Attack 5.4.2.

We now explain why the attack is valid.

Theorem 5.4.3 ([28]) *Let* $W \in \mathbb{R}_{\max}^{n\times n}$ *and let* U *be the message sent by Alice to Bob in Protocol* 5.1.2*. Then Attack 4 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* $X \otimes W \otimes Y = U$*.*

Proof. In this case we have to solve system (5.4.1) with $\mathcal{A} = \mathcal{B} = [n] \times [n]$, with A_α and B_β being tropical elementary matrices, and with the sets that contain x_α and y_β taking the forms of (5.4.11) and (5.4.12) 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 5.1.2.

Since (5.4.6) in this case becomes (5.4.13), Attack 4 is indeed a specialization of Attack 3, and by Theorem 5.4.1 it finds a solution to the above described specialization

of system 5.4.1, and hence it finds matrices X and Y which satisfy $X \otimes W \otimes Y = U$ and are of the required form. □

5.4.5 Attack on Protocol 5.1.3

In Protocol 5.1.3, we have $A_1 \in [2a, a]_n^g$ and $A_2 \in [0, h]_n$ (see Definition 4.2.2)with unknown nonpositive a and known nonnegative g and h. 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 $[n]$, we can represent any matrix in $[2a, a]_n^g$ and $[0, h]_n$ as in the first line of (5.4.1). However, for this we also need to restrict the coefficients x_α to belong to $[2a, a]$ if $\alpha = (i, j)$ with $i \neq j$ or to be equal to g if $i = j$. The coefficients y_β should belong to $[0, h]_n$ for any $\beta = (i, j)$ for $i, j \in [n]$

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

$$A_\alpha = A^{ij} = \begin{cases} E^{ij}, & \text{for } i \neq j, \\ I, & \text{for } i = j, \end{cases} \tag{5.4.14}$$

$$B_\beta = B^{ij} = E^{ij}.$$

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

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

$$\mathcal{X}_{(i,j)} = \begin{cases} [2a, a], & i \neq j \\ \{g\}, & i = j. \end{cases} \tag{5.4.15}$$

$$\mathcal{Y}_{(i,j)} = [0, h] \quad \forall i, j. \tag{5.4.16}$$

Observe that g and h 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 $a \leqslant 0$.

Attack 5.4.4 ([28])

Input: *public matrix* W*, public integer number* g, h *and messages* $U, V \in \mathbb{R}_{\max}^{n\times n}$

Output: *the secret key of Alice* K_a *and the secret key of Bob* K_b

1. *Compute* $c_{\alpha\beta} = c_{ijst}$ *and* $S_{\alpha\beta} = S_{ijst}$ *by;* (5.4.4)*, where* A_α *and* B_β *are defined by* (5.4.14) *and* $T^{\alpha\beta}$ *by* (5.4.2) *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* (5.4.5) *we seek those which satisfy*

$$\begin{aligned} &x_{ij} + y_{st} = c_{ijst}, \quad \textit{for} \quad (i,j,s,t) \in \mathcal{C} \\ &x_{ij} + y_{st} \leqslant c_{ijst}, \quad \textit{otherwise}, \\ &2a \leqslant x_{ij} \leqslant a, \forall i \neq j, \quad x_{ii} = g, \forall i \\ &0 \leqslant y_{st} \leqslant h \quad \forall s, t, \quad a \leqslant 0. \end{aligned} \tag{5.4.17}$$

Note that this is a linear system of equalities and inequalities whose solvability can be checked by the simplex method. This attack works since it is a special case of Attack 5.4.2. The detailed explanation of this, which we omit here, is fully analogous to the proof of Theorem 5.4.3.

5.4.6 Attack on Protocol 5.1.4

In Protocol 5.1.4 we have $A_1 = \mathfrak{A}(p, a)$ and $A_2 = \mathfrak{A}(q, b)$ with known vectors $p, q \leqslant 0$ and unknown non positive scalars $a, b \leqslant 0$. We can represent any matrix in $A_1 = \mathfrak{A}(p, a)$ and

$A_2 = \mathfrak{A}(q, b)$ as in the first line of (5.4.1), if we define

$$M = \begin{bmatrix} -\infty & -\infty & \dots & 0 & 0 \\ 0 & -\infty & -\infty & \dots & 0 \\ 0 & 0 & -\infty & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & -\infty \\ -\infty & \dots & 0 & 0 & -\infty \end{bmatrix}$$

and let A_α and B_β be:

$$\begin{aligned} &A_0 = B_0 = I, \quad A_{n+1} = B_{n+1} = M, \\ &A_k = E^{ij}, k \in [n], \text{ for } i = k, j \equiv k+1 (\text{mod } n) \end{aligned} \tag{5.4.18}$$

thus $\mathcal{A} = \mathcal{B} = \{0, \dots, n+1\}$.

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

$$\begin{aligned} &\mathcal{X}_0 = \mathcal{Y}_0 = \{0\}, \\ &\mathcal{X}_k = \{p_k\}, \quad \mathcal{Y}_k = \{q_k\}, \quad \text{for } k \in [n], \\ &\mathcal{X}_{n+1}(a) = (-\infty, a], \quad \mathcal{Y}_{n+1}(b) = (-\infty, b]. \end{aligned} \tag{5.4.19}$$

Observe that vectors p and q are known in this case, since Alice and Bob are sending them to one another in the public area, so we have to assume that Eve can intercept vectors p and q. However, a, b are unknown parameters satisfying $a, b \leqslant 0$.

Attack 5.4.5 ([28])

Input: public Matrix $W \in \mathbb{R}_{\max}^{n \times n}$ and the messages $U, V \in \mathbb{R}_{\max}^{n \times n}$

Output: Alice's secret key K_a or Bob secret's key K_b.

1. Compute $c_{\alpha\beta}$ and $S_{\alpha\beta}$ by (5.4.4), where A_α and B_β are defined by (5.4.18) and $T^{\alpha\beta}$ by (5.4.2) .

2. Among the minimal sets $\mathcal{C} \subseteq \{0,\dots,n+1\} \times \{0,\dots,n+1\}$ that satisfy (5.4.5) we seek those which satisfy

$$\begin{aligned} &x_\alpha + y_\beta = c_{\alpha\beta}, \quad \text{for} \quad (\alpha,\beta) \in \mathcal{C} \\ &x_\alpha + y_\beta \leqslant c_{\alpha\beta}, \quad \text{otherwise}, \\ &x_0 = y_0 = 0, \quad x_k = p_k, \quad y_k = q_k \quad \text{for } k \in [n], \\ &x_{n+1} \leqslant 0, \quad y_{n+1} \leqslant 0. \end{aligned} \tag{5.4.20}$$

Note that this is a linear system of equalities and inequalities whose solvability can be checked by the simplex method. This attack works since it is a special case of Attack 5.4.2.

5.4.7 Attack on Protocol 5.1.5

As in the case of the original Kotov-Ushakov attack [23], we first select a big enough number D such that it is bigger than the maximal degree of any tropical polynomial that can be used by Alice and Bob.

Then we use the tropical elementary matrices and I as A_α and the matrix power $W^{\otimes\beta}$ as B_β. Here α are pairs of indices from $[n]$ and $\beta \in \{0,\dots,D\}$. Thus we can represent any matrix in $[2a,a]_n^g$ and tropical polynomial $p(W)$ as in the first line of (5.4.1). However, for this we also need to restrict the coefficients x_α to belong to $[2a,a]$ if $\alpha = (i,j)$ with $i \neq j$ or to be equal to g if $i = j$. The coefficients y_β are unrestricted.

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

$$\begin{aligned} A_\alpha = A^{ij} &= \begin{cases} E^{ij}, & \text{for } i \neq j, \\ I, & \text{for } i = j, \end{cases} \\ B_\beta &= W^{\otimes\beta}, \quad \text{for } \beta \in \{0,\dots,D\}. \end{aligned} \tag{5.4.21}$$

Thus $\mathcal{A} = [n] \times [n]$ and $\mathcal{B} = \{0, \ldots, D\}$

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

$$\mathcal{X}_{(i,j)} = \begin{cases} [2a, a], & i \neq j \\ \{g\}, & i = j. \end{cases} \tag{5.4.22}$$

$$\mathcal{Y}_\beta = \mathbb{R}_{\max}. \tag{5.4.23}$$

Here, we have two unknown parameters a and g such that $a \leqslant 0$ and $g \geqslant 0$.

Hence, we formulate attack for protocol 5.1.6 as follows:

Attack 5.4.6 ([28])

Input: *Public Matrix* $W \in \mathbb{R}_{\max}^{n\times n}$ *and messages* $U, V \in \mathbb{R}_{\max}^{n\times n}$

Output: *Alice's secret key* K_a *or Bob secret's key* K_b*. In order to reveal* K_a *or* K_b*, the attacker need to solve decomposition problem* (5.4.2) *in the following steps:*

1. *Compute* $c_{\alpha\beta} = c_{ij\beta}$ *and* $S_{\alpha\beta} = S_{ij\beta}$ *by* (5.4.4)*, where* A_α *and* B_β *are defined by* (5.4.21)*,* $T^{\alpha\beta}$ *by* (5.4.2) *where* $\alpha = (i, j)$ *for all* $i, j \in [n]$*and* $\beta \in \{0, \ldots D\}$*.*

2. *Among the minimal sets* $\mathcal{C} \subseteq [n]^2 \times \{0, \ldots, D\}$ *that satisfy* (5.4.5) *we seek those which satisfy*

$$\begin{aligned} &x_{ij} + y_\beta = c_{ij\beta}, \quad \textit{for} \quad (i, j, \beta) \in \mathcal{C} \\ &x_{ij} + y_\beta \leqslant c_{ij\beta}, \quad \textit{otherwise}, \\ &2a \leqslant x_{ij} \leqslant a, \quad \forall i \neq j, \quad x_{ii} = g, \forall i. \end{aligned} \tag{5.4.24}$$

3. *Since* $\mathcal{X}$ *and* $\mathcal{Y}$ *can be found then Eve as an attacker can compute* $K_{Alice} = \mathcal{X} \otimes V \otimes \mathcal{Y}$*.*

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

Chapter 6

Cryptography Based on Tropical Semidirect Product and Its Security

6.1 Tropical Semidirect Product

In this section we are going to give a definition of the semidirect product in tropical algebra, following [14].

Definition 6.1.1 (Tropical Group Action) *Let G be a semigroup (a non empty set equipped with a binary operation and associative). Then we say that G acting on tropical algebra $\mathbb{R}_{\max}$, if it satisfies the following conditions:*

- *there is a well defined element $x^g \in \mathbb{R}_{\max}$ for any $x \in \mathbb{R}_{\max}$ and $g \in G$,*
- *$(x \otimes y)^g = (x^g \otimes y^g)$ and $x^{gh} = (x^g)^h$ for any $x, y \in \mathbb{R}_{\max}$ and $g, h \in G$.*

Definition 6.1.2 (Tropical Semidirect Product) *Let G be semigroup acting on $\mathbb{R}_{\max}$. Then define the set of pairs as follow:*

$$\Gamma = \mathbb{R}_{\max} \rtimes G = \{(x, g) | x \in \mathbb{R}_{\max}, g \in G\}$$

. *Then* Γ *is a semidirect products if it is a semigroup under the following operation:*

$$(x, g)(y, h) = (x^h \otimes y, gh)$$

. *for any* $x, y \in \mathbb{R}_{\max}$ *and* $g, h \in G$.

Example 6.1.1 (Tropical Semidirect Product [14]) *Grigoriev and Shpilrain [14] consider the following* semidirect products *of the pairs of matrices over tropical semiring*

$$(M, G)(A, H) = ((M \circ H) \oplus A, G \circ H) \tag{6.1.1}$$

We will consider one of the protocols in [14], where $\circ$ *is defined as the* adjoint product:

$$A \circ B = A \oplus B \oplus A \otimes B, \tag{6.1.2}$$

defined for any square matrices A *and* B *of the same size. It has the following properties:*

- $(A \circ B) \circ C = A \circ (B \circ C)$ *(associativity),*
- $A \circ (B \oplus C) = A \circ B \oplus A \circ C$ *and* $(B \oplus C) \circ A = B \circ C \oplus B \circ A$ *(distributivity).*

Adjoint product (6.1.5) can be used to define *adjoint powers* inductively: $A^{\circ(k+1)} = A^{\circ k} \circ A$ for all k. Moreover, the associativity implies that for any nonzero numbers $m_1, \ldots, m_s \in \mathbb{N}$ such that $m_1 + \ldots + m_s = k$ we have

$$A^{\circ k} = A^{\circ m_1} \circ A^{\circ m_2} \circ \ldots \circ A^{\circ m_s}. \tag{6.1.3}$$

Thus the adjoint powers $A^{\circ n} = \underbrace{A \circ \ldots \circ A}_{n}$ are well-defined and can be quickly computed using (6.1.3).

Using (6.1.4) we also observe the following:

Proposition 6.1.1 *Let $A \in \mathbb{R}_{\max}^{d\times d}$ have $\lambda(A) \leqslant 0$ and $n \geqslant d$. Then $A^{\circ n} = A^{+}$.*

Here A^{+} is the *metric matrix* of A defined in (2.1.1)

Proof. We start by proving the following identity:

$$A^{\circ n} = A \oplus A^{\otimes 2} \oplus \dots A^{\otimes n}. \tag{6.1.4}$$

Indeed, $A^{\circ 2} = A \oplus A^{\otimes 2}$ is obvious, and for general n we can use a simple induction:

$$\begin{aligned} A^{\circ n} &= A^{\circ(n-1)} \circ A = A \oplus A^{\circ(n-1)} \oplus (A^{\circ(n-1)} \otimes A) \\ &= A \oplus (A \oplus A^{\otimes 2} \oplus \dots \oplus A^{\otimes(n-1)}) \oplus (A^{\otimes 2} \oplus \dots \oplus A^{\otimes n}) \\ &= A \oplus A^{\otimes 2} \oplus \dots \oplus A^{\otimes n}. \end{aligned}$$

When $\lambda(A) \leqslant 0$ and $n \geqslant d$, the above series is equal to A^{+}, which completes the claim.□

With $\circ$ being the adjoint multiplication, the semidirect product of (M, G) and (A, H) given by (6.1.1) becomes

$$(M, G)(A, H) = (M \oplus A \oplus H \oplus M \otimes H, G \otimes H \oplus G \oplus H). \tag{6.1.5}$$

This semidrect product is associative as the following lemma proves:

Lemma 6.1.1 *Let A, B, M, G, H, J in $\mathbb{R}_{\max}^{n\times n}$ and then we have $[(M, G)\cdot(A, H)]\cdot(B, J) = (M, G)\cdot[(A, H)\cdot(B, J)]$*

Proof. Indeed, on the left-hand side we have:

$$\begin{aligned}
[(M,G)\cdot(A,H)]\cdot(B,J) &= (M\circ H\oplus A,\ G\circ H)\cdot(B,J)\\
&= ((M\oplus H\oplus(M\otimes H)\oplus A)\circ J\oplus B,\ G\circ H\circ J)\\
&= (M\circ J\oplus H\circ J\oplus(M\otimes H)\circ J\oplus A\circ J\oplus B, G\circ H\circ J)\\
&= (M\oplus J\oplus(M\otimes J)\oplus H\oplus J\oplus(H\otimes J)\oplus(M\otimes H)\oplus J\\
&\quad\oplus(M\otimes H\otimes J)\oplus A\oplus J\oplus(A\otimes J)\oplus B, G\circ H\circ J)\\
&= (M\oplus H\oplus J\oplus A\oplus B\oplus(M\otimes J)\oplus(M\otimes H)\oplus(H\otimes J)\oplus(A\otimes J)\\
&\oplus(M\otimes H\otimes J),\ G\circ H\circ J)
\end{aligned}$$

On the right-hand side:

$$\begin{aligned}
(M,G)\cdot[(A,H)\cdot(B,J)] &= (M,G)\cdot(A\circ J\oplus B, H\circ J)\\
&= (M,G)\cdot(A\oplus J\oplus A\otimes J\oplus B, H\oplus J\oplus H\otimes J)\\
&= (M\circ(H\oplus J\oplus H\otimes J)\oplus A\oplus J\oplus A\otimes J\oplus B, G\circ H\circ J)\\
&= (M\circ H\oplus M\circ J\oplus M\circ(H\otimes J)\oplus A\oplus J\oplus A\otimes J\oplus B, G\circ H\circ J)\\
&= (M\oplus H\oplus(M\otimes H)\oplus M\oplus J\oplus(M\otimes J)\oplus M\oplus(H\otimes J)\oplus\\
&(M\otimes H\otimes J)\oplus A\oplus J\oplus(A\otimes J)\oplus B, G\circ H\circ J)\\
&= (M\oplus H\oplus J\oplus A\oplus B\oplus(M\otimes J)\oplus(M\otimes H)\oplus(H\otimes J)\\
&\oplus(A\otimes J)\oplus M\otimes H\otimes J, G\circ H\circ J),
\end{aligned}$$

which is identical with what we obtained for the left-hand side. □

Example 6.1.2 (Tropical Semidirect Product) *Grigoriev and Sphilrain also intro-*

duced another action of the multiplicative semigroup of $\mathbb{R}_{\max}^{n\times n}$ *as follows:*

$$M^H = (H \otimes M^T) \oplus (M^T \otimes H) \tag{6.1.6}$$

where M^T *is the transpose of matrix* M*.*

The semidirect product assiciated with this action is a semigroup with the following operation:

$$(M, G)(S, H) = ((H \otimes M^T) \oplus (M^T \otimes H) \oplus S, G \otimes H) \tag{6.1.7}$$

However, Isaac and Kahrobei observed that the operation (6.1.5) is not associative and consequently this is not a semidirect product, contrary to the claim of Grigoriev and Shpilrain [14].

Let us consider the following counterexample to the associativity of operation defined by (6.1.5). This example is different from the one given by [17], but still very similar to their example.

Example 6.1.3 *Let us consider two matrices as follows:*

$$M = \begin{pmatrix} 1 & 2 \\ -1 & 2 \end{pmatrix}$$

and

$$H = \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix}$$

. *Then we have*

$$
\begin{aligned}
(M,H)^2 &= (M,H)(M,H) \\
&= \left(\begin{pmatrix} 1 & 2 \\ -1 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix}\right)\left(\begin{pmatrix} 1 & 2 \\ -1 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix}\right) \\
&= \left(\begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix} \oplus \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix} \otimes \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 1 & 2 \\ -1 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix}\right) \\
&= \left(\begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix} \oplus \begin{pmatrix} 5 & 1 \\ 6 & 2 \end{pmatrix} \oplus \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 8 & 4 \\ 4 & 0 \end{pmatrix}\right) \\
&= \left(\begin{pmatrix} 5 & 3 \\ 6 & 2 \end{pmatrix}, \begin{pmatrix} 8 & 4 \\ 4 & 0 \end{pmatrix}\right).
\end{aligned}
$$

We need to show that $(M,H)(M,H)^2 \neq (M,H)^2(M,H)$. *Let us start with the left side as the following step:*

$$
\begin{aligned}
(M,H)(M,H)^2 &= \left(\begin{pmatrix} 1 & 2 \\ -1 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix}\right)\left(\begin{pmatrix} 5 & 3 \\ 6 & 2 \end{pmatrix}, \begin{pmatrix} 8 & 4 \\ 4 & 0 \end{pmatrix}\right) \\
&= \left(\begin{pmatrix} 8 & 4 \\ 4 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix} \oplus \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix} \otimes \begin{pmatrix} 8 & 4 \\ 4 & 0 \end{pmatrix} \oplus \begin{pmatrix} 5 & 3 \\ 6 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 8 & 4 \\ 4 & 0 \end{pmatrix}\right) \\
&= \left(\begin{pmatrix} 9 & 7 \\ 5 & 3 \end{pmatrix} \oplus \begin{pmatrix} 9 & 5 \\ 10 & 6 \end{pmatrix} \oplus \begin{pmatrix} 5 & 3 \\ 6 & 2 \end{pmatrix}, \begin{pmatrix} 12 & 8 \\ 8 & 4 \end{pmatrix}\right) \\
&= \left(\begin{pmatrix} 9 & 7 \\ 10 & 6 \end{pmatrix}, \begin{pmatrix} 12 & 8 \\ 8 & 4 \end{pmatrix}\right)
\end{aligned}
\tag{6.1.8}
$$

$$
\begin{aligned}
(M,H)^2(M,H) &= \left(\begin{pmatrix} 5 & 3 \\ 6 & 2 \end{pmatrix}, \begin{pmatrix} 8 & 4 \\ 4 & 0 \end{pmatrix}\right)\left(\begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}\right) \\
&= \left(\begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 5 & 6 \\ 3 & 2 \end{pmatrix} \oplus \begin{pmatrix} 5 & 6 \\ 3 & 2 \end{pmatrix} \otimes \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 1 & 2 \\ -1 & 2 \end{pmatrix}, \begin{pmatrix} 8 & 4 \\ 4 & 0 \end{pmatrix} \otimes \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix}\right) \\
&= \left(\begin{pmatrix} 9 & 10 \\ 5 & 6 \end{pmatrix} \oplus \begin{pmatrix} 9 & 6 \\ 7 & 3 \end{pmatrix} \oplus \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 12 & 8 \\ 8 & 4 \end{pmatrix}\right) \\
&= \left(\begin{pmatrix} 9 & 10 \\ 7 & 6 \end{pmatrix}, \begin{pmatrix} 12 & 8 \\ 8 & 4 \end{pmatrix}\right)
\end{aligned}
\tag{6.1.9}
$$

From (6.1.8) *and* (6.1.9) *we can see that this operation is not associative.*

Since the operation is not associative (i.e is not a semigroup), it cannot be a semidirect product and we will not consider it further.

6.1.1 The protocol based on tropical semidirect product

Grigoriev and Shpilrain[14] introduced a new tropical version of the public key exchange protocol based on the tropical semidirect product. Their work is based on public key protocol using semidirect product in classical algebra by Kahrobaei and Shpilrain [21]. The new protocol uses the tropical semidirect product (6.1.1).

Protocol 6.1.1 *Suppose that Alice and Bob agree on matrices* $M, H \in \mathbb{R}_{\max}^{n\times n}$. *Then Alice and Bob do the following steps:*

1. *Alice chooses a random positive integer number* m *and computes* $(M,H)^m = (A, H^m)$. *Then Alice sends* A *to Bob.*

2. *Bob chooses a random positive integer number* n *and computes* $(M,H)^n = (B, H^n)$. *Then Bob sends* B *to Alice.*

3. *Alice computes* $K_{Alice} = A \oplus B \oplus H^{\circ m} \oplus (B \otimes H^{\circ m})$.

4. *Bob computes* $K_{Bob} = A \oplus B \oplus H^{\circ n} \oplus (A \otimes H^{\circ n})$.

6.1.2 Correctness of Protocol 6.1.1. Relation to tropical matrix powers.

Semidirect product (6.1.5) can be used to define semidirect powers of matrix pairs inductively: $(M,H)^{k+1} = (M,H)^k \cdot (M,H)$ for all k. Moreover, the associativity implies that for $m_1, \ldots, m_s \in \mathbb{N}$ such that $m_1 + \ldots + m_s = k$ we have

$$(M,H)^k = (M,H)^{m_1}(M,H)^{m_2} \ldots (M,H)^{m_s}. \tag{6.1.10}$$

This property assures that the semidirect powers $(M,H)^k = \underbrace{(M,H) \cdot \ldots \cdot (M,H)}_{k}$ are well-defined. We now express the semidirect powers in terms of the tropical matrix powers.

Proposition 6.1.2 ([29]) *Let* $M, H \in \mathbb{R}_{\max}^{d\times d}$. *Then*

$$(M,H)^k = ((M \otimes \bigoplus_{i=0}^{k-1} H^{\otimes i}) \oplus (H \otimes \bigoplus_{i=0}^{k-2} H^{\otimes i}), H^{\circ k})$$

for all $k \geqslant 2$.

Proof. We first consider $k = 2$ to check the base of induction. We obtain:

$$(M,H)(M,H) = (M \oplus H \oplus M \oplus M \otimes H,\ H^{\circ 2}) = (M \otimes (I \oplus H) \oplus H,\ H^{\circ 2}).$$

We now assume that the statement holds for $k = t$ and prove it for $k = t + 1$. Indeed:

$$(M,H)^{t+1} = (M,H)^t \cdot (M,H) = ((M \otimes \bigoplus_{i=0}^{t-1} H^{\otimes i}) \oplus (H \otimes \bigoplus_{i=0}^{t-2} H^{\otimes i}), H^{\circ t}) \cdot (M,H)$$
$$= ((M \otimes \bigoplus_{i=0}^{t-1} H^{\otimes i}) \oplus (H \otimes \bigoplus_{i=0}^{t-2} H^{\otimes i}) \oplus M \oplus H \oplus (M \otimes \bigoplus_{i=1}^{t} H^{\otimes i}) \oplus (H \otimes \bigoplus_{i=1}^{t-1} H^{\otimes i}), H^{\circ(t+1)})$$
$$= ((M \otimes \bigoplus_{i=0}^{t} H^{\otimes i}) \oplus (H \otimes \bigoplus_{i=0}^{t-1} H^{\otimes i}), H^{\circ(t+1)}).$$

The induction is complete. □

Note that we can also use that $\bigoplus_{i=0}^{k} H^{\otimes i} = (I \oplus H)^{\otimes k}$ for any k, and then the result of the previous lemma can be reformulated as follows:

$$\begin{aligned}(M,H)^k &= (M \otimes (I \oplus H)^{\otimes(k-1)} \oplus H \otimes (I \oplus H)^{\otimes(k-2)}, H^{\circ k}) \\ &= ((M \otimes (I \oplus H) \oplus H) \otimes (I \oplus H)^{\otimes(k-2)}, H^{\circ k}).\end{aligned} \tag{6.1.11}$$

Property (6.1.10) implies that $K_a = K_b$, since both of them are the first component of $(M,H)^{m+n}$. For the protocol recalled above, we immediately obtain

$$\begin{aligned}A &= \left(M \otimes \bigoplus_{i=0}^{m-1} H^{\otimes i}\right) \oplus \left(H \otimes \bigoplus_{i=0}^{m-2} H^{\otimes i}\right) = (M \otimes (I \oplus H) \oplus H) \otimes (I \oplus H)^{\otimes(m-2)}, \\ B &= \left(M \otimes \bigoplus_{i=0}^{n-1} H^{\otimes i}\right) \oplus \left(H \otimes \bigoplus_{i=0}^{n-2} H^{\otimes i}\right) = (M \otimes (I \oplus H) \oplus H) \otimes (I \oplus H)^{\otimes(n-2)},\end{aligned} \tag{6.1.12}$$

for the messages exchanged between Alice and Bob ($m \geqslant 2$ and $n \geqslant 2$), using Proposition 6.1.2.

6.2 Cryptanalysis of Protocol 6.1.1

In this section, we will present three attack methods for Protocol 6.1.1. The first method is proposed by Rudy and Monico [32], the second method is introduced by Isaac and Kahrobei [18], and the last attack is due to Muanalifah and Sergeev [29], which uses the ultimate periodicity of tropical matrix powers and the previously discussed connection between tropical matrix powers and powers resulting from the tropical semidirect product.

6.2.1 Binary Search Attack

This attack is based on Rudy and Monico [32]. The focus of this attack is to find m from the first component of $(M, H)^m$ and then use this m to compute the secret key K_{Alice}. Using the fact that $A \oplus B \geqslant A$ and $A \oplus B \geqslant B$ for any matrices A and B of the same size, one can obtain the following claim.

Proposition 6.2.1 ([32]) *Let $(M_m, H_m) := (M, H)^m$. Then the sequence $\{M_m\}$ is monotonically increasing, meaning that $M_1 \leqslant M_2 \leqslant M_3 \leqslant \dots M_m$ for all $m \in \mathbb{N}$.*

Proof. For every $m \geqslant 2$, we can observe the following:

$$\begin{aligned}(M, H)_m &= (M, H)_{m-1} \circ (M, H) \\ &= (M_{m-1} \oplus M \oplus H \oplus (M_{m-1} \otimes H), H_{m-1} \oplus H \oplus (H_{m-1} \otimes H))\end{aligned} \tag{6.2.1}$$

From equation (6.2.1), we can see that $M_m = (M_{m-1} \oplus M \oplus H \oplus (M_{m-1} \otimes H))$, and therefore $M_m \geqslant M_{m-1}$ for any $m \geqslant 2$. □

The problem to find a positive integer m can be solved by using binary search algorithm. Rudy and Monico successfully attack the Protocol 6.1.1. The attack of Rudy and Monico [32] requires $\mathcal{O}(N^2)$, where N is the maximum of the logarithms of the secret keys (exponents) used by Alice and Bob.

6.2.2 Isaac and Kahrobei's Attack

The attack on Protocol (6.1.1) developed by Isaac and Kahrobaei [17] is based on the ultimate periodicity property of the tropical semidirect powers, which was observed experimentally. In their attack, based on the property that the sequence $\{M_n\}_{n\geqslant 1}$ is ultimately periodic (where M_n is the first component of $(M,H)^n$), the attacker can compute the exponent a using the public matrices M, H and A. Then the attacker can find the secret key using the formula by which it is computed in Protocol 6.1.1. The attack consist of two parts:

- Attacker computes d and ρ for the sequence $\{M_n\}_{n\geqslant 1}$, where ρ is the period of that sequence after the periodicity starts and d is the length of the pre-periodic part.
- Using d and ρ, the attacker computes the private key (exponent) a.

Isaac and Kahrobei successfully attack the protocol with the parameters suggested by Grogoriev and Sphilrain [14]. They performed 1000 instances protocol using Python 3.76 on single core of an i7 CPU at 2.9GHz, with 8GB of RAM, running Windows 10. Experimentally, their attack is better in time than the Binary Search attack of Rudy and Monico [32].

6.2.3 the Tropical Discrete Logarithm Problem Attack

We now explain the attack on the Grigoriev-Shpilrain protocol, which depends on the sign of $\lambda(H)$. This attack was developed in a joint article with my supervisor S. Sergeev [29].

Proposition 6.2.2 ([29]) *Let $M, H \in \mathbb{R}_{\max}^{d\times d}$ and $\lambda(H) \leqslant 0$. If $m \geqslant d+1$ then $A = (M \oplus H) \otimes H^*$, and if $n \geqslant d+1$ then $B = (M \oplus H) \otimes H^*$.*

Proof. From (6.1.12) we recall that

$$A = \left(M \otimes \bigoplus_{i=0}^{m-1} H^{\otimes i}\right) \oplus \left(H \otimes \bigoplus_{i=0}^{m-2} H^{\otimes i}\right), \quad B = \left(M \otimes \bigoplus_{i=0}^{n-1} H^{\otimes i}\right) \oplus \left(H \otimes \bigoplus_{i=0}^{n-2} H^{\otimes i}\right)$$

Since $\lambda(H) \leqslant 0$, we have

$$H^* = I \oplus H \oplus \ldots \oplus H^{\otimes(t-1)} \quad \text{for } t \geqslant d.$$

Using this property and the identities for A and B, we obtain the claim. □

Proposition 6.2.3 ([29]) *Let $M, H \in \mathbb{R}_{\max}^{d\times d}$ and $\lambda(H) \leqslant 0$ and let $m \geqslant d+1$, $n \geqslant d+1$, $A = (M \oplus H) \otimes H^*$ or $B = (M \oplus H) \otimes H^*$. Then*

$$K_a = K_b = A \oplus B = (M \oplus H) \otimes H^*.$$

Proof. Using Proposition 6.2.2 and (6.1.4), if $m \geqslant d+1$ or if $A = (M \oplus H) \otimes H^*$, then we obtain

$$\begin{aligned} A \otimes H^{\circ n} &= (M \oplus H) \otimes (H^* \otimes H^{\circ n}) \\ &= (M \oplus H) \otimes \left(H^* \otimes \bigoplus_{i=1}^{n} H^{\otimes i} \right) \leqslant (M \oplus H) \otimes H^* = A, \\ H^{\circ n} &= \bigoplus_{i=1}^{n} H^{\otimes i} \leqslant A, \end{aligned}$$

and also $B \leqslant A$, using (6.1.12).

Similarly, if $n \geqslant d+1$ or if $B = (M \oplus H) \otimes H^*$ then we have

$$\begin{aligned} B \otimes H^{\circ m} &= (M \oplus H) \otimes (H^* \otimes H^{\circ m}) \\ &= (M \oplus H) \otimes \left(H^* \otimes \bigoplus_{i=1}^{m} H^{\otimes i} \right) \leqslant (M \oplus H) \otimes H^* = B, \\ H^{\circ m} &= \bigoplus_{i=1}^{m} H^{\otimes i} \leqslant B \end{aligned}$$

and $A \leqslant B$. Therefore, we have

$$K_a = B \oplus A \oplus H^{\circ m} \oplus B \otimes H^{\circ m} = A \oplus B = B, \quad \text{if } n \geqslant d+1$$
$$K_b = A \oplus B \oplus H^{\circ n} \oplus A \otimes H^{\circ n} = A \oplus B = A, \quad \text{if } m \geqslant d+1.$$

Thus in this case the key can be computed simply as $A \oplus B$. □

6.2.4 Computing the key knowing m and n

If we have m and n then the key can be obviously computed as

$$K_a = K_b = A \oplus B \oplus H^{\circ m} \oplus (B \otimes H^{\circ m}) = A \oplus B \oplus H^{\circ n} \oplus (A \otimes H^{\circ n}), \tag{6.2.2}$$

where $H^{\circ m}$ and $H^{\circ n}$ can be computed as adjoint powers, using (6.1.3) or (6.1.4).

Let us also consider how to simplify expression (6.2.2). Assume first that $m > n$. Then $A \geqslant B$ and $A \geqslant H^{\circ n}$, since any power $H^{\otimes i}$ for $1 \leqslant i \leqslant n$ appears as one of the terms in

$$A = (M \otimes (I \oplus H) \oplus H)(I \oplus H \oplus \ldots \oplus H^{\otimes(m-2)}),$$

when we multiply it out. Then the key simplifies to

$$K_a = K_b = A \otimes (I \oplus H^{\circ n}) = A \otimes (I \oplus H \oplus \ldots \oplus H^{\otimes n}) = A \otimes (I \oplus H)^{\otimes n}. \tag{6.2.3}$$

In the case $n > m$ we similarly obtain

$$K_a = K_b = B \otimes (I \oplus H \oplus \ldots \oplus H^{\otimes m}) = B \otimes (I \oplus H)^{\otimes m}. \tag{6.2.4}$$

In the case $m = n$ we have $B = A$ and therefore

$$K_a = K_b = A \otimes (I \oplus H)^{\otimes n} \oplus H \otimes (I \oplus H)^{\otimes(n-1)}. \tag{6.2.5}$$

6.2.5 Formulation of the attack

Let us now give a more formal description of the attack on Protocol 6.1.1, in the form of an algorithm.

Algorithm 6.2.1 (Attacking Protocol 6.1.1 [29])

Input: public matrices $M, H \in \mathbb{Z}_{\max}^{d\times d}$ and messages $A, B \in \mathbb{Z}_{\max}^{d\times d}$ of Alice and Bob.

Output: the secret key K_a and the secret key K_b

0. Compute $\lambda(H)$, $F = I \oplus H$ and $V = (M \otimes (I \oplus H) \oplus H)$.

1. If $\lambda(H) \leqslant 0$ then check if $A = (M \oplus H) \otimes H^*$ or $B = (M \oplus H) \otimes H^*$. If any of these two conditions is true then return $K = (M \oplus H) \otimes H^*$.

   If none of these conditions are true, check if $A = M$ or $B = M$ or find $l_1, l_2 = 0, \dots d-2$ such that $A = V \otimes F^{\otimes l_1}$ and $B = V \otimes F^{\otimes l_2}$. Then set $m = l_1 + 2$ or $m = 1$ if $A = M$, and $n = l_2 + 2$ or $n = 1$ if $B = M$, and go to 3.

2. If $\lambda(H) > 0$ then check $A = M$ or $B = M$ or find l_1 and l_2 satisfying $A = V \otimes F^{\otimes l_1}$ and $B = V \otimes F^{\otimes l_2}$ using Algorithm 3.2.1. Then set $m = l_1 + 2$ or $m = 1$ if $A = M$, and $n = l_2 + 2$ or $n = 1$ if $B = M$, and go to 3.

3. Compute the key using (6.2.3), (6.2.4) or (6.2.5).

The following result improves the claim which we obtained in [29], as we dispense with the assumption that the critical graph should be strongly connected. We could also omit the irreducibility, but we need to make sure that the conditions of Theorem 3.2.2 hold.

Theorem 6.2.1 *Suppose that H is irreducible. Then the attacker can compute the key using Algorithm 6.2.1.*

Proof. Since H is irreducible, so is $F = I \oplus H$ and $V = (M \otimes (I \oplus H) \oplus H) \neq \mathcal{E}$, each column of $V \otimes F^{\otimes t}$ has a finite entry, and Corollary 3.2.2 applies and establishes the

validity of Algorithm 3.2.1 for $t \geqslant (d-1)^2 + 1$. The increasing property of $F = I \oplus H$ means that the sequence of matrices $\{M,\ V,\ V \otimes F,\ V \otimes F^2 \ldots\}$ is non-decreasing, and it either stabilises so that $V \otimes F^{\otimes t} = (M \oplus H) \otimes H^*$ for $t \geqslant T$ for some $T \leqslant d-1$, or it grows in such a way that

$$M < V < V \otimes F^{\otimes t_1} < V \otimes F^{\otimes t_2} < \ldots$$

In particular, we have $V \otimes F^{\otimes t_1} \neq V \otimes F^{\otimes t_2}$ for $t_1 \neq t_2$, unless both are equal to $(M \oplus H) \otimes H^*$. These observations, together with the validity of Algorithm 3.2.1 for $t \geqslant (d-1)^2 + 1$, imply the validity of the claim. □

Let us analyse how many operations the algorithm requires.

0. Computation of $\lambda(H)$ and V requires no more than $O(d^3)$ operations.

1. Checking if $A = (M \oplus H) \otimes H^*$ or $B = (M \oplus H) \otimes H^*$ requires $O(d^3)$ operations. Straightforward checking for powers less than $d-1$ requires $O(d^4)$ operations.

2. Here we apply Algorithm 3.2.1, whose complexity is analysed in Proposition 3.2.6.

3. Computation of the key (unless it has been computed on step 1) requires no more than $O(d^3 \log \max(m, n))$. This is done using repeated tropical matrix squaring and has the same computational complexity as the protocol itself.

6.3 Toy examples

In this section we give a couple of toy examples to demonstrate how the attack on the protocol works in the cases when $\lambda(H) \leqslant 0$ and $\lambda(H) > 0$.

Example 6.3.1 ($(\lambda(H) \leqslant 0)$)

Let Alice and Bob agree on two public matrices as follows:

$$M = \begin{pmatrix} 8 & 7 & 2 \\ 10 & 3 & 6 \\ -10 & -1 & 3 \end{pmatrix}, \quad H = \begin{pmatrix} 0 & -3 & -5 \\ -1 & -2 & 2 \\ 1 & -3 & -4 \end{pmatrix}.$$

Bob and Alice pick two random integer numbers $m = 5$ and $n = 8$ respectively. Alice and Bob compute

$$A = B = \begin{pmatrix} 10 & 7 & 9 \\ 10 & 7 & 9 \\ 4 & 1 & 3 \end{pmatrix} = K_a = K_b.$$

Since $\lambda(H) = 0$, we cannot use the tropical discrete logarithm method to find m and n. However, Eve can check that $A = B = (M \oplus H) \otimes H^*$, hence she concludes that $K_a = K_b = (M \oplus H) \otimes H^*$.

Example 6.3.2 ($(\lambda(H) > 0)$)

Alice and Bob agree on two public matrices as follows:

$$M = \begin{pmatrix} -75 & -45 & -69 & 60 \\ 83 & 52 & 9 & -72 \\ 27 & 92 & 92 & -16 \\ 87 & 93 & -3 & 84 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 7 & 2 & 5 \\ -1 & -2 & 2 & 4 \\ 3 & 4 & 2 & 2 \\ -5 & -10 & 10 & 0 \end{pmatrix}.$$

Then they follow the protocol 6.1.1 in the following steps:

- Alice and Bob pick two random integer numbers $m = 15$ and $n = 16$ respectively.
- Alice computes $(M, H)^m = (A, H^{\circ m})$ and Bob computes $(M, H)^n = (B, H^{\circ n})$. They

exchange the following messages:

$$A = \begin{pmatrix} 145 & 146 & 148 & 144 \\ 176 & 177 & 179 & 175 \\ 175 & 176 & 178 & 174 \\ 176 & 177 & 179 & 175 \end{pmatrix}, \quad B = \begin{pmatrix} 151 & 152 & 154 & 150 \\ 182 & 183 & 185 & 181 \\ 181 & 182 & 184 & 180 \\ 182 & 183 & 185 & 181 \end{pmatrix}.$$

- Alice computes $K_a = A \oplus B \oplus H^{\circ m} \oplus (B \otimes H^{\circ m})$ and Bob computes $K_b = B \oplus A \oplus H^{\circ n} \oplus (A \otimes H^{\circ n})$. They thus obtain the common secret key:

$$K_a = K_b = \begin{pmatrix} 241 & 242 & 244 & 240 \\ 272 & 273 & 275 & 271 \\ 271 & 272 & 274 & 270 \\ 272 & 273 & 275 & 271 \end{pmatrix}.$$

Attacking the protocol

Eve as an attacker only knows public matrices M and H and public keys A and B. To attack the protocol Eve needs to find m and n and compute K_a or K_b. Using Algorithm 5.3, Eve obtains Alice's private key by the following:

1. Eve computes $\lambda(H) = 6$ and

$$F = I \oplus H = \begin{pmatrix} 1 & 7 & 2 & 5 \\ -1 & 0 & 2 & 4 \\ 3 & 4 & 2 & 2 \\ -5 & -10 & 10 & 0 \end{pmatrix}, \quad V = \begin{pmatrix} 55 & 50 & 70 & 60 \\ 98 & 99 & 97 & 97 \\ 95 & 96 & 94 & 96 \\ 92 & 93 & 95 & 97 \end{pmatrix}.$$

2. Since $\lambda(H) > 0$, Eve needs to find m_a satisfying $A = V \otimes F^{\otimes(m_a-2)}$. For this Eve

finds a critical cycle $Z = (1\ 2\ 4\ 3)$ and computes

$$C_Z = R_Z = \begin{pmatrix} 0 & 1 & 3 & -1 \\ -5 & 0 & 2 & -2 \\ -1 & -2 & 0 & -4 \\ 1 & 2 & 4 & 0 \end{pmatrix}, \quad S_Z = \begin{pmatrix} -\infty & 1 & -\infty & -\infty \\ -\infty & -\infty & -\infty & -2 \\ -3 & -\infty & -\infty & -\infty \\ -\infty & -\infty & 4 & -\infty \end{pmatrix}.$$

3. The dimension is $d = 4$, hence for $t = 0, \ldots, (4-1)^2 = 9$, Eve first tries to find t such that $A = V \otimes F^{\otimes t}$. Here we cannot find t satisfying $A = V \otimes F^{\otimes t}$ for these low exponents.

4. Now Eve uses the CSR method. The length of critical cycle is $l = 4$, but it turns out that

$$C_Z S_Z^k R_Z[F] = \begin{pmatrix} 0 & 1 & 3 & -1 \\ -1 & 0 & 2 & -2 \\ -3 & -2 & 0 & -4 \\ 1 & 2 & 4 & 0 \end{pmatrix} \quad \text{for all } k.$$

   For $k = 0$ Eve finds that $A = V \otimes (C_Z R_Z[F]) = \mu + E$ with $\mu = 78$. Eve then finds that $m_a = \mu/\lambda(F) + 2 = \frac{78}{6} + 2 = 15$.

5. Eve computes $K_a = B \otimes (I \otimes H)^{\otimes 15} = \begin{pmatrix} 241 & 242 & 244 & 240 \\ 272 & 273 & 275 & 271 \\ 271 & 272 & 274 & 270 \\ 272 & 273 & 275 & 271 \end{pmatrix}$.

6.4 Numerical experiments

In this section we will describe the numerical experiments which we performed with the tropical discrete logarithm and attack on Protocol 1 of [14]. We will mostly follow the de-

scription that we gave in [29] and then will give a brief summary of some new experiments which we did not describe in that paper.

We first discuss how we generated matrix F, which gets powered up in the discrete logarithm problem, or matrix H for Protocol 1 of [14]. If we generate matrix F by random and all of its entries are real, then it is irreducible and generically we have only one critical cycle and therefore the critical graph is strongly connected. This is the case for which the validity of our attack was proved in [29]. To study the problem under more general conditions we also generated matrices F (and H) in such a way that the critical graph is guaranteed to have at least three components.

In more detail, we did it according to the following procedure:

(a) We determined two random integer numbers k_1 and k_2, where k_1 is approximately $\frac{1}{3}$ of the dimension of matrix d and k_2 is a random integer numbers between k_1 and k_2. Then we generated three random matrices with entries 0 and $-\infty$. Each matrix has dimension k_1, $[k_1+1, k_2]$ and $[k_2+1, d]$ respectively. The frequency of 0 entries is approximately $\frac{1}{3}$ and we made sure that each of these matrices contains a cycle and there is $-\infty$ on the diagonal.

(b) We composed a $d \times d$ matrix with entries in $\{0, -\infty\}$, which has the three matrices generated above as as its principal submatrices. The rest of entries in this matrix are set to $-\infty$.

(c) We substituted all $-\infty$ entries in step (b) with a random negative number in the interval $[-100, 0]$ and add to the whole matrix a nonzero random number λ.

(d) We applied a diagonal similarity scaling $A \mapsto D^{-1} \otimes A \otimes D$ where D is a diagonal matrix (with all off-diagonal entries equal to $-\infty$) and the diagonal entries being randomly selected in the interval $[-100, 100]$.

As a result, we would obtain a "random" matrix F, whose critical graph contains three components, and such that $\lambda(F) = \lambda$.

Such matrix was also used as matrix H in [14] Protocol 1, however here we also had to make sure that $\lambda(H) > 0$, otherwise we would be in the very easy case treated in Propositions 6.2.2 and 6.2.3 This could be guaranteed by taking $\lambda > 0$ at step (c).

For the tropical discrete logarithm problem as well as for the protocol, we ran similar experiments using the following parameters:

- Dimension d was in the interval $[6, 500]$;
- The entries of matrix M were random integer numbers in the interval $[-100, 100]$;
- Exponents m, n used by Alice and Bob, and the secret key t in the tropical discrete logarithm were random integer numbers in the interval $[(d-1)^2 + 1, d^2]$.

We then performed experiments using MATLAB R2019/b, also using supercomputer Bluebear system (University of Birmingham) for dimensions between 400 and 500. We ran 100 experiments for each dimension d:

1. We solved the tropical discrete logarithm by Algorithm 3.2.1 where we skipped step (1): straightforward "catching" powers powers up to $(d-1)^2$. In this experiment we find 100% success rate.
2. We attacked Protocol 1 of [14] using Algorithm 6.2.1 In this experiment we also found 100% success rate.

For the dimensions up to 100, the average computation times are given on Figure 6.1. We distinguish between the cases where H is randomly generated and where $F = I \oplus H$ is guaranteed to have three critical components. However, the average time that it takes is similar (being slightly less for the case of special matrices), and it does not exceed 6 seconds for dimensions up to 100 in both cases.

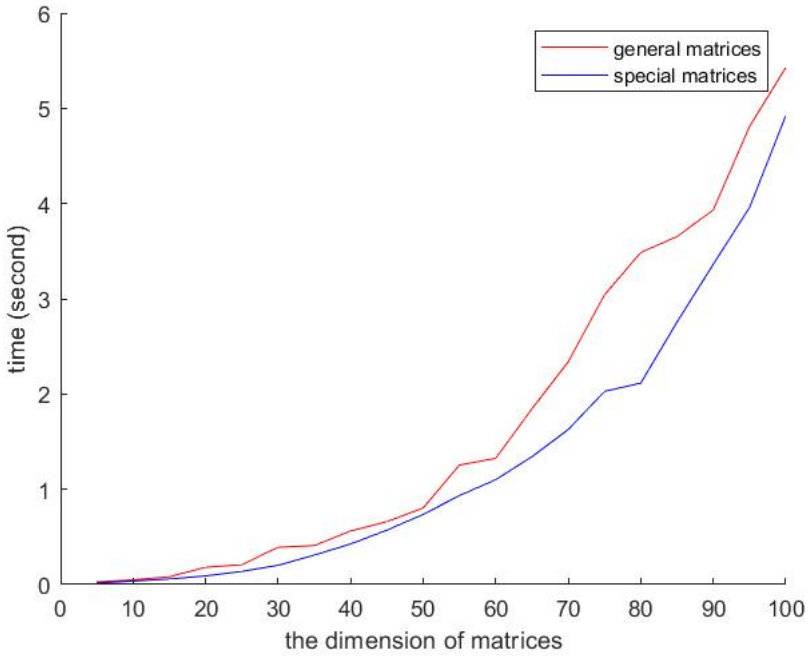

Figure 6.1: Time required by Algorithm 6.2.1 in the case where H is randomly generated ("general matrices") and in the case where (F) is guaranteed to have at least three critical components and $\lambda(F) > 0$ ("special matrices)"

We then observed that Rudy and Monico [32] as well as Isaac and Kahrobaei [17] use much bigger exponents in their experiments, following the setup of Grigoriev and Shpilrain [14]. To make a better comparison with their results, we implemented Algorithm 3.2.1 and Algorithm 6.2.1 also in Python, thus enabling our attacks to work with very high exponents of Alice and Bob, of the order 2^{200}. We also increased the range of matrices H and M to $[-1000, 1000]$.

This required some other improvements and upgrades in the code, such as: 1) the use of fast powering to generate the protocol instances (for which we utilized parts of the code written by Isaac and Kahrobaei [17], 2) we "translated" into Python the program (written by S. Gaubert) for computing the maximum cycle mean based on the Howard policy iteration algorithm of Cochet-Terrasson et al. [6]. Another upgrade was done to enable us to experimentate with matrices that have $-\infty$ entries.

We then performed a series of numerical experiments, where we attacked the protocol with the public matrices being randomly generated matrices (with range $[1000, 1000]$. We implemented our attack using Python 3.8 and performed 1000 instances of the protocol on Macbook Retina 1.2 GHz Dual-Core Intel Core m3, with 8GB of RAM. The results are shown below, first for a "light" version of the algorithm where we omit the "catching power" part of it, and then for Algorithm 6.2.1 as it is stated.

We decided that performing experiments where all entries are finite and the critical graph is guaranteed to have three components is not necessary, as due to the improved results of this Thesis, Algorithm 6.2.1 is also guaranteed to work in this case and Figure 6.1 indicates that its performance does not differ significantly.

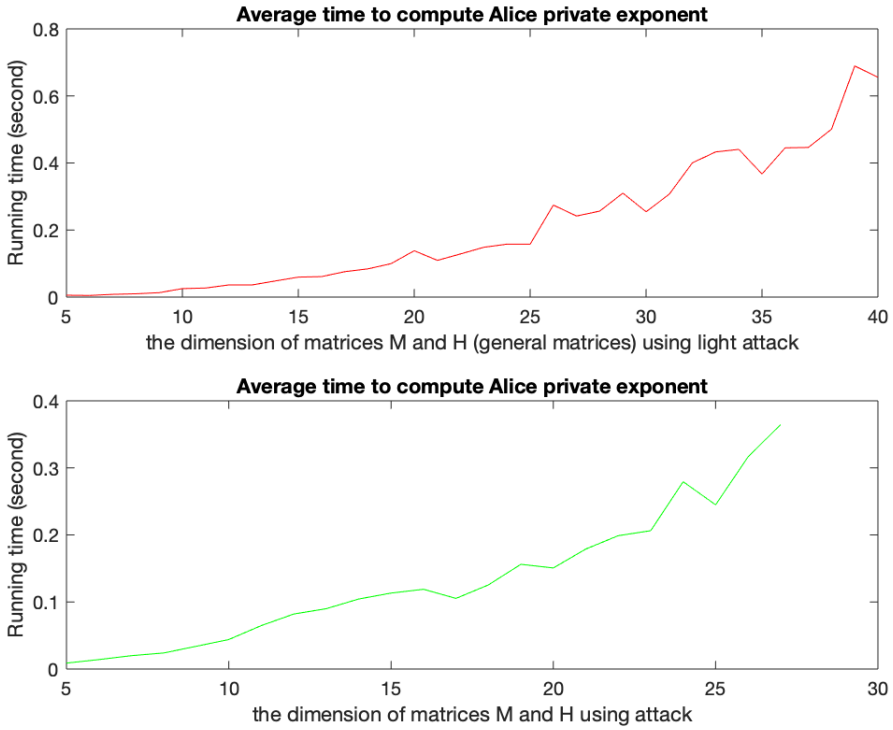

Figure 6.2: Time required by Algorithm 6.2.1 (green) and its light version (red) in the case where all public matrices are randomly generated

We performed similar series of experiments where matrix H has $-\infty$ entries and each row has at least one finite entry. Note that policy iteration algorithm of Cochet-Terrasson et al. [6] allows us to compute the maximum mean value (λ) for general matrices with $-\infty$ entries (however, we introduced the assumption that each row of H has a $-\infty$ entry for simplicity of application of that algorithm). We next implemented Algorithm 6.2.1 on Python 3.9. Using similar parameters, we generate random 1000 instances experiments for each dimension of public matrices. The results of the average running times are shown on Figure 6.3.

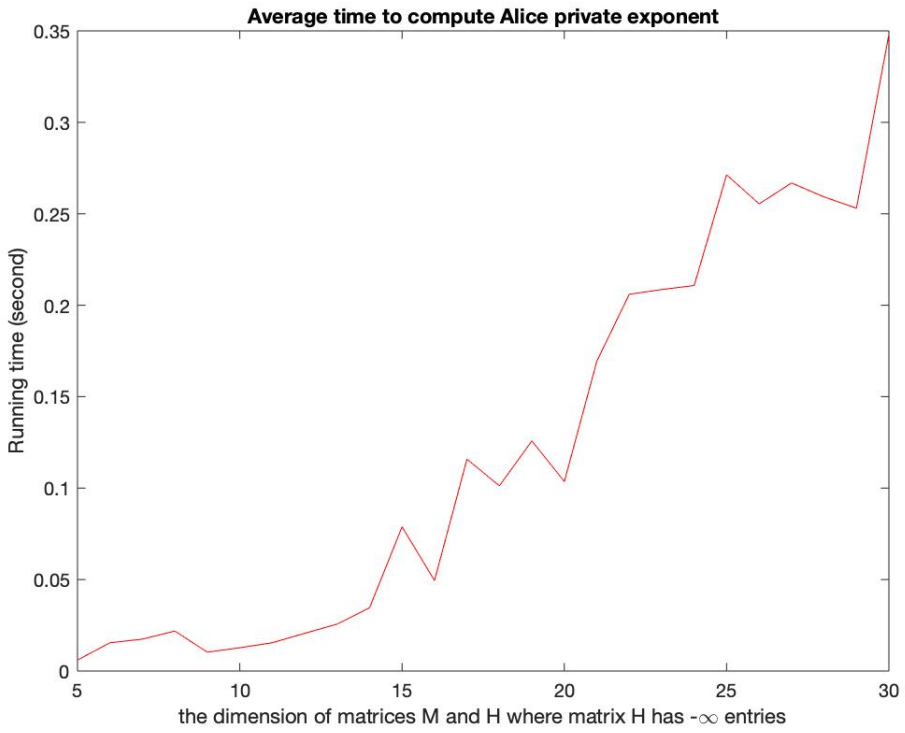

Figure 6.3: Time required by Algorithm 6.2.1 in the case where H is randomly generated ("has at least one finite entries each row and $-\infty$ entries.")

From Figure 6.3 we can see that the average time to attack the protocol is similar to that on Figure 6.2, where matrix H does not have $-\infty$ entries. So far we do not have any counterexample or indication that Algorithm 6.2.1 could fail in the case where $-\infty$ entries are allowed, unless the conditions of Theorem 3.2.2 are violated.

Chapter 7

Conclusion and Future Work

The starting point for this thesis are two papers by Grigoriev and Shpilrain [13, 14], where it was suggested to use the tropical linear algebra as a platform for some public key protocols. In the first paper, one of the most prominent suggestions was to use tropical matrix polynomials in the tropical version of Stickel's protocol, and this idea naturally led us to search for some classes of tropical commuting matrices which could be used with the same purpose.

Using the results previously obtained in [19] and [24] 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 generalised to apply to all our protocols. We analysed the performance of this attack on the tropical Stickel protocol suggested by [13] 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 guaranteed to be successful for big D in the tropical

Stickel protocol of [13] (Protocol 2.3.3) and even more so when too large subsets of rational numbers in $[0, 1]$ are used in the protocol with quasi-polynomials (Protocol 5.1.1). We also do not expect it to be successful for large n in the protocols with $[2r, r]_n^k$ matrices (Protocols 5.1.2 and 5.1.3). However, the complexity and efficiency of this attack requires more rigorous analysis. It still makes sense to search for alternative attacks on our new protocols. For Protocol 5.1.2, since some rather successful heuristic attacks have been found, it is desirable 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.

Some new protocols using tropical algebra were suggested in [14]. 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 Kotov-Ushakov attack.

Grigoriev and Sphilrain proposed two new key exchange protocols. However, Isaac and Kahrobei [18] showed that one of the protocols fails to work because the product on which it is based is not associative. We are then left with Protocol 6.1.1 which uses an assosiative operation and thus a true tropical version of the semidirect product. Isaac and Kahrobei already suggested an efficient attack on Protocol 6.1.1 using the ultimate periodicity properties. Before that, Rudy and Monico [32] also introduced binary search methods to attack Protocol 6.1.1.

Motivated by the discrete logarithm problem, which plays an important role in the classical cryptography, we introduced a new concept of the tropical discrete logarithm problem and its two-sided version. Using the CSR expansion of [33] and [27] we can find an efficient solution of the tropical discrete logarithm problem. This method and the connection between the tropical semidirect product and the tropical matrix powers

which we found allowed us to attack Protocol 6.1.1 using a different approach from Rudy and Monico, and Isaac and Kahrobei methods. For the same parameters as suggested in [14], our attack needs less time than the attack of Rudy and Monico [32] and Isaac and Kahrobaei [17]. For instance, for the matrix with dimension 30×30, the average time that is needed by our attack to find the exponent used by Alice and Bob is equal to $0.2544478195s$, compared to Isaac and Kahrobaei's attack [17] needing $3.9s$ on average for the same dimension and the same order of exponents used by Alice and Bob.

We also included in this dissertation some results on the extended two-sided version of tropical discrete logarithm, which could help to develop an alternative to the Kotov-Ushakov attack on the tropical Stickel protocol of Grigoriev and Shpilrain [13]. However, there are still some obstacles to this, which we hope to overcome in the future.

At present, it seems that there are no protocols that are immune to attacks based on the ultimate periodicity of tropical matrix powers or on the efficient enough solution of the tropical one-sided systems (possibly, with some extra conditions). The search for successful protocols using tropical linear algebra only may be not the best possible direction for future research, but the abundance of semirings on which new protocols can be based (such as described in Golan [12]) leads one to consider "tougher" semirings and linear algebra over them as a possible platform for implementing Diffie-Hellman and Stickel protocols.

List of References

[1] François Baccelli, Guy Cohen, Geert Jan Olsder, and Jean Pierre Quadrat. *Synchronization and linearity: an algebra for discrete event systems*. John Wiley & Sons Ltd, 1992.

[2] Yves Balcer and A.F. Veinott. Computing a graph's period quadratically by node condensation. *Discrete Math.*, 4:295–303, 1973.

[3] Peter Butkovič. *Max-linear systems: theory and algorithms*. Springer Science & Business Media, 2010.

[4] Peter Butkovič, Hans Schneider, Sergeĭ Sergeev, and Bit-Shun Tam. Two cores of a nonnegative matrix. *Linear Algebra Appl.*, 439:1929–1954, 2013.

[5] Jean-Marie Chauvet and Eric Mahé. Cryptography from the tropical hessian pencil. *Groups Complexity Cryptology*, 9(1):19–29, 2017.

[6] Jean Cochet-Terrasson, Guy Cohen, Stéphane Gaubert, Michael M. Gettrick, and Jean-Pierre Quadrat. Numerical computation of spectral elements in max-plus algebra. In *Proceedings of the IFAC conference on systems structure and control*, pages 699–706, IRCT, Nantes, France, 1998.

[7] Guy Cohen, Didier Dubois, Jean-Pierre Quadrat, and Michel Viot. A linear system theoretic view of discrete event processes and its use for performance evaluation in manufacturing. *IEEE Trans. on Automatic Control*, AC–30:210–220, 1985.

[8] Guy Cohen, Didier Dubois, Jean-Pierre Quadrat, and Michel Viot. Analyse du comportement périodique de systèmes de production par la théorie des dioïdes. Technical report, INRIA, Février 1983. Rapport de Recherche no. 191.

[9] RA Cuninghame-Green and P Butkovic. Generalised eigenproblem in max-algebra. In *2008 9th International Workshop on Discrete Event Systems*, pages 236–241. IEEE, 2008.

[10] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

[11] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, 31(4):469–472, 1985.

[12] J.S. Golan. *Semirings and Their Applications*. 2013.

[13] Dima Grigoriev and Vladimir Shpilrain. Tropical cryptography. *Communications in Algebra*, 42(6):2624–2632, 2014.

[14] Dima Grigoriev and Vladimir Shpilrain. Tropical cryptography II. extensions by homomorphisms. *Communications in Algebra*, 47:4224–4229, 2018.

[15] Maggie Habeeb, Delaram Kahrobaei, Charalambos Koupparis, and Vladimir Shpilrain. Public key exchange using semidirect product of (semi) groups. In *International Conference on Applied Cryptography and Network Security*, pages 475–486. Springer, 2013.

[16] Bernd Heidergott, Geert Jan Olsder, and Jacob Van der Woude. *Max Plus at Work*. Princeton University Press, 2006.

[17] Steve Isaac and Delaram Kahrobaei. A closer look at the tropical cryptography. *International Journal of Computer Mathematics: Computer Systems Theory*, 6(2):137–142, 2021.

[18] Steve Isaac and Delaram Kahrobaei. A closer look at the tropical cryptography. Arxiv preprint 2011.14163v1, November 2020.

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

[20] D. Jones. Matrix roots in the max-plus algebra. 2018.

[21] Delaram Kahrobaei and Vladimir Shpilrain. Using semidirect product of (semi) groups in public key cryptography. In *Conference on Computability in Europe*, pages 132–141. Springer, 2016.

[22] Ricardo D Katz, Hans Schneider, et al. On commuting matrices in max algebra and in classical nonnegative algebra. *Linear Algebra and its Applications*, 436(2):276–292, 2012.

[23] Matvei Kotov and Alexander Ushakov. Analysis of a key exchange protocol based on tropical matrix algebra. *IACR Cryptology ePrint Archive*, 2015:852, 2015.

[24] J Linde and MJ de la Puente. Matrices commuting with a given normal tropical matrix. *Linear Algebra and its Applications*, 482:101–121, 2015.

[25] Gérard Maze, Chris Monico, and Joachim Rosenthal. Public key cryptography based on semigroup actions. *arXiv preprint cs/0501017*, 2005.

[26] Glenn Merlet, Thomas Nowak, Hans Schneider, and Sergeĭ Sergeev. Generalizations of bounds on the index of convergence to weighted digraphs. *Discrete Applied Mathematics*, 178:121–134, 2014.

[27] Glenn Merlet, Thomas Nowak, and Sergeĭ Sergeev. Weak CSR expansions and transience bounds in max-plus algebra. *Linear Algebra and its Applications*, 461:163–199, 2014.

[28] Any Muanalifah and Sergeĭ Sergeev. Modifying the tropical version of stickels key exchange protocol. *Applications of Mathematics*, 65(6):727–753, 2020.

[29] Any Muanalifah and Sergeĭ Sergeev. On the tropical discrete logarithm problem and security of a protocol based on tropical semidirect product. *Communications in Algebra*, 0(0):1–19, 2021.

[30] Karl Nachtigall. Powers of matrices over an extremal algebra with applications to periodic graphs. *Mathematical Methods of Operations Research*, 46:87–102, 1997.

[31] Geert-Jan Olsder, Kees Roos, and R.J. van Egmond. An efficient algorithm for critical circuits and finite eigenvectors in the max-plus algebra. *Linear Algebra and its Applications*, 295(1):231–240, 1999.

[32] Dylan Rudy and Chris Monico. Remarks on a tropical key exchange system. Arxiv preprint 2005.04363, May 2020.

[33] Sergeĭ Sergeev and Hans Schneider. CSR expansions of matrix powers in max algebra. *Transactions of the American Mathematical Society*, 364(11):5969–5994, 2012.

[34] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[35] Vladimir Shpilrain. Cryptanalysis of stickel's key exchange scheme. *Lecture Notes in Computer Science*, 5010:283–288, 2008.

[36] Vladimir Shpilrain and Alexander Ushakov. A new key exchange protocol based on the decomposition problem. *arXiv preprint math/0512140*, 2005.

[37] Laurence Dwight Smith. *Cryptography: The science of secret writing*. Courier Corporation, 1955.

[38] Eberhard Stickel. A new method for exchanging secret keys. In *Information Technology and Applications, 2005. ICITA 2005. Third International Conference on*, volume 2, pages 426–430. IEEE, 2005.

[39] Neal R Wagner and Marianne R Magyarik. A public-key cryptosystem based on the word problem. In *Workshop on the Theory and Application of Cryptographic Techniques*, pages 19–36. Springer, 1984.

[40] Song Y Yan. *Quantum attacks on public-key cryptosystems*. Springer, 2013.