Generalized Kotov-Ushakov Attack on Tropical Stickel Protocol Based on Modified Tropical Circulant Matrices

Sulaiman Alhussaini, Craig Collett and Sergeĭ Sergeev

Abstract

After the Kotov-Ushakov attack on the tropical implementation of Stickel protocol, various attempts have been made to create a secure variant of such implementation. Some of these attempts used a special class of commuting matrices resembling tropical circulants, and they have been proposed with claims of resilience against the Kotov-Ushakov attack, and even being potential post-quantum candidates. This paper, however, reveals that a form of the Kotov-Ushakov attack remains applicable and, moreover, there are heuristic implementations of that attack which have a polynomial time complexity and show an overwhelmingly good success rate.

Keywords: public-key cryptography; key exchange protocol; cryptographic attack; tropical cryptography
Classification: 94A60, 15A80

1 Introduction

Tropical cryptography, a relatively new and promising area in cryptography, is aiming to use various structures of tropical mathematics to redefine the classical public key exchange protocols in cryptography, such as those put forward by Diffie and Hellman, and Stickel. Grigoriev and Shpilrain were pioneers in introducing the tropical algebra as an alternative framework for cryptographic protocols [7]. Their work involved developing a tropical implementation of the Stickel key exchange protocol, replacing the initial classical version suggested by Stickel since it was shown to be susceptible to the conventional linear algebraic attacks. This was motivated by the generally non-invertible nature of matrices in tropical algebra providing resistance against any obvious analogue of the linear algebraic attack on the original Stickel protocol.

Kotov and Ushakov later suggested an attack on Grigoriev and Shpilrain's tropical implementation of the Stickel protocol [11]. They managed to transform the underlying mathematical problem into the problem of solving a tropical linear equation of the form $A \otimes x = b$ where x should have a special structure. This enabled them to employ the tropical linear system solvability theory (see, e.g., Theorem 3.1.1 and Corollary 3.1.2 [4]).

Subsequently [14] proposed several modifications to the original Stickel protocol in an attempt to make it resistant against the Kotov-Ushakov attack, where different classes of commuting matrices were suggested instead of tropical polynomials. For example, a modification was suggested where the commutative property of tropical matrix roots was utilized, along with some other variations, in the hope of enhancing the resistance of the key exchange protocols compared to the original Stickel protocol. Unfortunately, it was also observed that all these modifications appeared to exhibit vulnerability to a form of Kotov-Ushakov attack. Specifically, a generalized version of the Kotov-Ushakov attack was proposed, and it was proved that it applied to all proposed modifications of Stickel protocol.

Grigoriev and Shpilrain [8] also proposed two tropical implementations of the Diffie-Hellman protocols based on the semi-direct product, but one of them was shown to be invalid by Isaac and Kahrobaei [10] and the other successfully attacked by the same authors as well as in [15]. See also a recent survey of Ahmed et al. [1] for a number of other interesting protocols based on tropical matrix algebra and the cryptanalysis of such protocols.

The main idea of this paper is to present an attack on variants of the Stickel protocol that are based on modified tropical circulants. We attack the proposed protocols using the generalized Kotov-Ushakov attack similar to the one described in [14], and we also make an observation that there is a heuristic implementation of this attack which is much faster and shows an overwhelming success rate. More specifically, the paper is organized as follows. In Section 2 we start with some preliminaries and basic definitions of tropical matrix algebra. In Section 3 we define the tropical circulants and the different forms of modified tropical circulants and present the previously proposed key exchange protocols based on them. In Section 4 we cryptanalyze the proposed protocols using the generalized Kotov-Ushakov attack, and present some numerical experiments showing the attack's efficiency and performance. In Section 5 we construct a heuristic efficient implementation of the generalized Kotov-Ushakov attack, employing it to attack the protocols based on modified circulants as well as the tropical Stickel protocol of [7] and present some numerical experiments showing that this heuristic implementation is indeed much faster and has a very good (and, in the case of modified circulants, excellent) success rate. Throughout this paper, we denote the "modified tropical circulant matrices" as simply "modified circulants". Our codes have been uploaded to GitHub [1].

While revising this paper we learned of an IACR preprint by Buchinskiy, Kotov and Treier [3] where an attack very similar to our Attack 4.1 on Stickel protocols based on circulants and modified circulants was suggested. Interestingly, in [3] this attack is also applied to the TrES protocol of Durcheva [5]. In turn, the present paper suggests much more efficient heuristic implementations of this attack (see Section 5), which avoid the hard problem of enumerating all minimal covers and makes an observation that these heuristic implementations have an overwhelming success rate (100%) for the protocols based on modified circulants. We also observe a much easier way to attack the protocol based on the anti-*s*-*p* circulants described in [2]. Then, yet another related publication by Mach [13] was brought to our attention during the revision process. Part of publication [13] has a similar goal of trying to efficiently attack Stickel protocol (although not the implementation based on circulants which is considered in the present paper), and one of our proposed heuristic forms of Kotov-Ushakov attack (namely, Algorithm 2 in Section 5) shares certain idea with [13], Algorithm 9. The similarities and differences will be discussed in Section 5 in more detail.

2 Preliminaries

In this section, we present fundamental definitions in tropical algebra that will be utilized in the subsequent sections.

Definition 2.1. (Tropical Semiring). We define the tropical/max-plus semiring as $\mathbb{R}_{\max} = (\mathbb{R} \cup$

[1]https://github.com/suliman1n/Generalized-KotovUshakov-Attack-on-Tropical-Stickel-Protocol-Based-on-Modified-Circulants

$\{-\infty\}, \oplus, \otimes)$, where traditional addition $+$ and multiplication $\times$ are replaced by tropical addition $\oplus$ and tropical multiplication $\otimes$ respectively. These new arithmetical operations are defined by $x \oplus y = \max\{x, y\}$ and $x \otimes y = x + y$ for all $x, y \in \mathbb{R}_{\max}$

The tropical operations can also be extended to include matrices and vectors. In particular, the operation $A \otimes \alpha = \alpha \otimes A$, where $\alpha \in \mathbb{R}_{\max}, A \in \mathbb{R}_{\max}^{m \times n}$ and $(A)_{ij} = a_{ij}$ is defined by

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

where $[m]$ and $[n]$ denote $\{1, \ldots, m\}$ and $\{1, \ldots, n\}$ respectively.

The tropical addition $A \oplus B$ of two matrices $A \in \mathbb{R}_{\max}^{m \times n}$ and $B \in \mathbb{R}_{\max}^{m \times n}$, where $(A)_{ij} = a_{ij}$ and $(B)_{ij} = b_{ij}$ is defined by

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

The multiplication of two matrices is also similar to the "traditional" algebra. Namely, we define $A \otimes B$ for two matrices, where $A \in \mathbb{R}_{\max}^{m \times p}$ and $B \in \mathbb{R}_{\max}^{p \times n}$, as follows:

$$(A \otimes B)_{ij} = \bigoplus_{k=1}^{p} a_{ik} \otimes b_{kj} = (a_{i1} \otimes b_{1j} \oplus a_{i2} \otimes b_{2j} \oplus \ldots \oplus a_{in} \otimes b_{nj}) \quad \forall i \in [m] \text{ and } \forall j \in [n].$$

Definition 2.2. (Matrix Power). For $M \in \mathbb{R}_{\max}^{n \times n}$, the n-th tropical power of M is denoted by $M^{\otimes n}$, and expressed as,

$$M^{\otimes n} = \underbrace{M \otimes M \otimes \ldots \otimes M}_{n \text{ times}}$$

By definition, any tropical square matrix to the power 0 is the tropical identity.

Definition 2.3. (Tropical Identity). The tropical identity matrix $I \in \mathbb{R}_{\max}^{n \times n}$ is of the form $(I)_{ij} = \delta_{ij}$ where

$$\delta_{ij} = \begin{cases} 0 & \text{if } i = j \\ -\infty & \text{otherwise} \end{cases}$$

Subsequently, we define the tropical matrix polynomials.

Definition 2.4. (Tropical Matrix Polynomials). Tropical matrix polynomial is a function of the form

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

where $a_k \in \mathbb{R}_{\max}$ for $k = 0, 1, \ldots, d$. Here A is a square matrix of any dimension.

Notice that any two tropical matrix polynomials of the same matrix commute as in the classical algebra, and this fact was utilized by Grigoriev and Shpilrain [7] to construct the following tropical implementation of the Stickel protocol.

Protocol 1. Original Tropical Stickel Protocol

1. Alice and Bob agree on public matrices $A, B, W \in \mathbb{R}_{\max}^{n \times n}$.

2. Alice chooses two random tropical polynomials $p_1(x)$ and $p_2(x)$ and sends $U = p_1(A) \otimes W \otimes p_2(B)$ to Bob.

3. Bob chooses two random tropical polynomials $q_1(x)$ and $q_2(x)$ and sends $V = q_1(A) \otimes W \otimes q_2(B)$ to Alice.

4. Alice computes her secret key using a public key V obtained from Bob, which is $K_a = p_1(A) \otimes V \otimes p_2(B)$.

5. Bob also computes his secret key using Alice's public key U, which is $K_b = q_1(A) \otimes U \otimes q_2(B)$.

We notice that the protocol utilizes the commutativity of tropical polynomials of the same matrix, and this is why the two parties end up with an identical key.

3 Public-Key Cryptography Using Modified Tropical Circulant Matrices

In this section, we introduce the definition of tropical circulant matrices and their various modified forms. We also present the key exchange protocols based on these modified circulants.

3.1 Modified Tropical Circulant Matrices

Modified tropical circulants, as suggested by their name, are modifications of circulant matrices, which are well known in "traditional" algebra over fields as well as in tropical algebra, where some of their properties were studied in [6], [16] and [17]. Here is a formal definition of tropical circulants.

Definition 3.1. (Tropical Circulants). Let $C \in \mathbb{R}_{\max}^{n \times n}$. We say that C is a circulant matrix with entries $c_0, c_1, \ldots, c_{n-1}$ if it is of the form

$$\begin{pmatrix} c_0 & c_{n-1} & c_{n-2} & \cdots & c_1 \\ c_1 & c_0 & c_{n-1} & \cdots & c_2 \\ c_2 & c_1 & c_0 & \cdots & c_3 \\ \vdots & \vdots & \vdots & \ddots & \cdots \\ c_{n-1} & c_{n-2} & c_{n-3} & \cdots & c_0 \end{pmatrix}$$

where $c_0, c_1, c_2 \ldots, c_{n-1} \in \mathbb{R}_{\max}$.

We now present the modified forms of tropical circulants introduced in [9],[2] and [18].

Definition 3.2. (Upper s-Circulants [9]). Let $T \in \mathbb{R}_{\max}^{n \times n}$. We say that T is an upper-s-circulant if it is of the form

$$\begin{pmatrix} c_0 & c_{n-1} \otimes s & c_{n-2} \otimes s & \cdots & c_1 \otimes s \\ c_1 & c_0 & c_{n-1} \otimes s & \cdots & c_2 \otimes s \\ c_2 & c_1 & c_0 & \cdots & c_3 \otimes s \\ \vdots & \vdots & \vdots & \ddots & \cdots \\ c_{n-1} & c_{n-2} & c_{n-3} & \cdots & c_0 \end{pmatrix}$$

where $c_0, c_1, c_2 \ldots, c_{n-1}, s \in \mathbb{R}_{\max}$.

Definition 3.3. (Lower s-Circulants [2]). Let $T \in \mathbb{R}_{\max}^{n\times n}$. We say that T is a lower s-circulant if it is of the form

$$\begin{pmatrix} c_0 & c_{n-1} & c_{n-2} & \cdots & c_1 \\ c_1 \otimes s & c_0 & c_{n-1} & \cdots & c_2 \\ c_2 \otimes s & c_1 \otimes s & c_0 & \cdots & c_3 \\ \vdots & \vdots & \vdots & \ddots & \cdots \\ c_{n-1} \otimes s & c_{n-2} \otimes s & c_{n-3} \otimes s & \cdots & c_0 \end{pmatrix}$$

where $c_0, c_1, c_2 \ldots, c_{n-1}, s \in \mathbb{R}_{\max}$.

Definition 3.4. Denote the set of all tropical upper or lower s-circulant matrices of dimension $(n \times n)$ as C_n^s. Thus $C_n^s = \{A \in \mathbb{R}_{\max}^{n\times n} \mid A$ is an upper s-circulant matrix$\}$ or $C_n^s = \{A \in \mathbb{R}_{\max}^{n\times n} \mid A$ is a lower s-circulant matrix$\}$. We will use the same notation for both matrix classes, distinguishing between them based on the context when necessary.

Proposition 3.1. ([2]) The set of all tropical upper or lower s-circulant matrices C_n^s of $\mathbb{R}_{max}^{n\times n}$ is a commutative tropical subsemiring of $\mathbb{R}_{max}^{n\times n}$.

Proposition 3.1 was proved in [2] only for lower s-circulant matrices, but the same claim for upper s-circulnat matrices easily follows by transposition.

Definition 3.5. (Anti-s-Circulants [2]). Let $T \in \mathbb{R}_{\max}^{n\times n}$. We say that T is an anti-s-circulant if it is of the form

$$\begin{pmatrix} c_0 \otimes s & c_{n-1} \otimes s & \cdots & c_2 \otimes s & c_1 \\ c_1 \otimes s & c_0 \otimes s & \cdots & c_3 & c_2 \otimes s \\ c_2 \otimes s & c_1 \otimes s & \cdots & c_4 \otimes s & c_3 \otimes s \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{n-2} \otimes s & c_{n-3} & \cdots & c_0 \otimes s & c_{n-1} \otimes s \\ c_{n-1} & c_{n-2} \otimes s & \cdots & c_1 \otimes s & c_0 \otimes s \end{pmatrix}$$

where $c_0, c_1, c_2 \ldots, c_{n-1}, s \in \mathbb{R}_{\max}$.

Note that anti-s-circulants do not generally commute and hence they can not be directly used to construct a variant of tropical Stickel protocol. They, however, commute in a special case which will be described soon. Example 3.1 shows that anti-s-circulants do not generally commute.

Example 3.1. let A be an anti-2-circulant with parameters $c_0 = 1, c_1 = 2, c_2 = 3$ and $s = 2$:

$$A = \begin{pmatrix} 1 \otimes 2 & 3 \otimes 2 & 2 \\ 2 \otimes 2 & 1 & 3 \otimes 2 \\ 3 & 2 \otimes 2 & 1 \otimes 2 \end{pmatrix} = \begin{pmatrix} 3 & 5 & 2 \\ 4 & 1 & 5 \\ 3 & 4 & 3 \end{pmatrix}.$$

Let B be an anti-2-circulant with parameters $c_0 = 5, c_1 = 7, c_2 = 4$ and $s = 2$:

$$B = \begin{pmatrix} 5 \otimes 2 & 4 \otimes 2 & 7 \\ 7 \otimes 2 & 5 & 4 \otimes 2 \\ 4 & 7 \otimes 2 & 5 \otimes 2 \end{pmatrix} = \begin{pmatrix} 7 & 6 & 7 \\ 9 & 5 & 6 \\ 4 & 9 & 7 \end{pmatrix}.$$

Then

$$A \otimes B = \begin{pmatrix} 14 & 11 & 11 \\ 11 & 14 & 12 \\ 13 & 12 & 10 \end{pmatrix} \neq B \otimes A = \begin{pmatrix} 10 & 12 & 11 \\ 12 & 14 & 11 \\ 13 & 11 & 14 \end{pmatrix}.$$

We note that anti-s-circulants can not be generally used to construct a variant of Stickel protocol.

We now recall the definitions of upper triangular and lower triangular Toeplitz matrices which were used for the Stickel protocol in [18].

Definition 3.6. (Upper Triangular Toeplitz Matrices [18]). Let $T \in \mathbb{R}_{\max}^{n\times n}$. We say that T is an upper triangular Toeplitz matrix if the matrix is of the form

$$\begin{pmatrix} c_0 & c_{n-1} & c_{n-2} & \cdots & c_1 \\ -\infty & c_0 & c_{n-1} & \cdots & c_2 \\ -\infty & -\infty & c_0 & \cdots & c_3 \\ \vdots & \vdots & \vdots & \ddots & \cdots \\ -\infty & -\infty & -\infty & \cdots & c_0 \end{pmatrix}$$

where $c_0, c_1, c_2 \ldots, c_{n-1} \in \mathbb{R}_{\max}$.

Definition 3.7. (Lower Triangular Toeplitz Matrices [18]). Let $T \in \mathbb{R}_{\max}^{n\times n}$. We say that T is a lower triangular Toeplitz matrix if the matrix is of the form

$$\begin{pmatrix} c_0 & -\infty & -\infty & \cdots & -\infty \\ c_1 & c_0 & -\infty & \cdots & -\infty \\ c_2 & c_1 & c_0 & \cdots & -\infty \\ \vdots & \vdots & \vdots & \ddots & \cdots \\ c_{n-1} & c_{n-2} & c_{n-3} & \cdots & c_0 \end{pmatrix}$$

where $c_0, c_1, c_2 \ldots, c_{n-1} \in \mathbb{R}_{\max}$.

Note that the Toeplitz matrices also already appeared in the tropical context before, see, e.g., [6] and [12]. For our purpose, it is sufficient to observe, however, that lower triangular Toeplitz matrices and, respectively, upper triangular Toeplitz matrices are upper s-circulants and, respectively, lower s-circulants with $s = -\infty$. This also implies, in view of Proposition 3.1, that any two lower triangular Toeplitz matrices as well as any two upper triangular Toeplitz matrices commute. One could also prove this by representing lower and upper triangular Toeplitz matrices as matrix polynomials.

Example 3.2 illustrates the commutativity properties of the modified tropical circulants.

Example 3.2. Let $A_1 \in C_3^3$ be an upper 3-circulant matrix with parameters $c_0 = 1, c_1 = -1, c_2 = 2$ and $s = 3$:

$$A_1 = \begin{pmatrix} 1 & 2\otimes 3 & -1\otimes 3 \\ -1 & 1 & 2\otimes 3 \\ 2 & -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 2 \\ -1 & 1 & 5 \\ 2 & -1 & 1 \end{pmatrix}.$$

Let B_1 be an upper 3-circulant matrix with parameters $c_0 = 5, c_1 = 6, c_2 = 0$ and $s = 3$:

$$B_1 = \begin{pmatrix} 5 & 0\otimes 3 & 6\otimes 3 \\ 6 & 5 & 0\otimes 3 \\ 0 & 6 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 3 & 9 \\ 6 & 5 & 3 \\ 0 & 6 & 5 \end{pmatrix}$$

We have

$$A_1 \otimes B_1 = \begin{pmatrix} 11 & 10 & 10 \\ 7 & 11 & 10 \\ 7 & 7 & 11 \end{pmatrix} = B_1 \otimes A_1.$$

Similarly, let $A_2 \in C_3^3$ be a lower 3-circulant matrix with parameters $c_0 = 1, c_1 = -1, c_2 = 2$ and $s = 3$:

$$A_2 = \begin{pmatrix} 1 & 2 & -1 \\ -1 \otimes 3 & 1 & 2 \\ 2 \otimes 3 & -1 \otimes 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & -1 \\ 2 & 1 & 2 \\ 5 & 2 & 1 \end{pmatrix}.$$

Let B_2 be a lower 3-circulant matrix with parameters $c_0 = 5, c_1 = 6, c_2 = 0$ and $s = 3$:

$$B_2 = \begin{pmatrix} 5 & 0 & 6 \\ 6 \otimes 3 & 5 & 0 \\ 0 \otimes 3 & 6 \otimes 3 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 0 & 6 \\ 9 & 5 & 0 \\ 3 & 9 & 5 \end{pmatrix}.$$

We have

$$A_2 \otimes B_2 = \begin{pmatrix} 11 & 8 & 7 \\ 10 & 11 & 8 \\ 11 & 10 & 11 \end{pmatrix} = B_2 \otimes A_2.$$

We see that upper or lower s-circulant matrices and upper or lower triangular Toeplitz matrices can be used in cryptographic protocols in order to compute shared keys.

3.2 Stickel Protocols Based on Modified Tropical Circulants

We now recall the tropical cryptographic Stickel protocols based on the different forms of modified tropical circulants introduced in the previous section. The commutativity property of these modified circulants ensures the success of the protocols.

Protocol 2. Stickel Protocol Based on Tropical Upper or Lower s-Circulant Matrices

1. Alice and Bob agree on $s, t \in \mathbb{R}_{\max}$ and a publicly known matrix $M \in \mathbb{R}_{\max}^{n \times n} \setminus (C_n^s \cup C_n^t)$.
2. Alice generates two matrices $A_1 \in C_n^s$ and $A_2 \in C_n^t$.
3. Bob generates two matrices $B_1 \in C_n^s$ and $B_2 \in C_n^t$.
4. Alice calculates $U = A_1 \otimes M \otimes A_2$ and sends it to Bob.
5. Bob calculates $V = B_1 \otimes M \otimes B_2$ and sends it to Alice.
6. Alice calculates $K_a = A_1 \otimes V \otimes A_2$.
7. Bob calculates $K_b = B_1 \otimes U \otimes B_2$.
8. They both have the same key, $K_a = K = K_b$.

We notice that the keys are identical due to the property of $A_1 \otimes B_1 = B_1 \otimes A_1$ and $B_2 \otimes A_2 = A_2 \otimes B_2$ from Proposition 3.1:

$$\begin{aligned} K_a &= A_1 \otimes V \otimes A_2 = A_1 \otimes B_1 \otimes M \otimes B_2 \otimes A_2 \\ &= B_1 \otimes A_1 \otimes M \otimes A_2 \otimes B_2 = B_1 \otimes U \otimes B_2 = K_b. \end{aligned}$$

In [2], the authors proposed a key exchange protocol based on a specific class of matrices known as anti-s-p-circulant matrices. These matrices are anti-s-circulants with the property that $c_i - c_{i-1} = p \quad \forall i \in \{1, 2, \cdots n-1\}$ where $p \in \mathbb{N}$ and $c_0, c_1, c_2 \ldots, c_{n-1}$ are the parameters of the underlying circulant matrix. It is proved in [2] that any two anti-s-p-circulant matrices commute, and therefore one can consider a Stickel protocol based on such matrices.

However, such protocol is easy to attack as it essentially reduces to the two parties choosing a single random integer for each generated matrix. More precisely, the matrices generated by Alice or Bob are of the form

$$\begin{pmatrix} c_0 \otimes s & c_0 + (n-1)p \otimes s & \cdots & c_0 + 2p \otimes s & c_0 + p \\ c_0 + p \otimes s & c_0 \otimes s & \cdots & c_0 + 3p & c_0 + 2p \otimes s \\ c_0 + 2p \otimes s & c_0 + p \otimes s & \cdots & c_0 + 4p \otimes s & c_0 + 3p \otimes s \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_0 + (n-2)p \otimes s & c_0 + (n-3)p & \cdots & c_0 \otimes s & c_0 + (n-1)p \otimes s \\ c_0 + (n-1)p & c_0 + (n-2)p \otimes s & \cdots & c_0 + p \otimes s & c_0 \otimes s \end{pmatrix}$$

This implies that Alice and Bob each choose only one secret integer c_0 for their respective matrices, as s and p must be publicly known or sent by a transmission that can be intercepted (since both Alice and Bob have to use these parameters). The attacker can then easily find the sum of the two integers used by Alice by intercepting Alice's message U, and use it to reconstruct the secret shared key. Hence, there is no need to apply any form of Kotov-Ushakov attack or other advanced methods, and we will not discuss the Stickel protocol based on tropical anti-s-p-circulants in what follows.

Let us also present the following protocol from [18], although it can be seen as a special case of the previous protocol.

Protocol 3. Stickel Protocol Based on Tropical Upper and Lower Triangular Toeplitz Matrices

1. Alice and Bob agree on a publicly known matrix $M \in \mathbb{R}_{\max}^{n \times n}$.
2. Alice generates an upper triangular Toeplitz matrix A_1 and a lower triangular Toeplitz matrix A_2.
3. Bob generates an upper triangular Toeplitz matrix B_1 and a lower triangular Toeplitz matrix B_2.
4. Alice calculates $U = A_1 \otimes M \otimes A_2$ and sends it to Bob.
5. Bob calculates $V = B_1 \otimes M \otimes B_2$ and sends it to Alice.
6. Alice calculates $K_a = A_1 \otimes V \otimes A_2$.
7. Bob calculates $K_b = B_1 \otimes U \otimes B_2$.
8. They both have the same key, $K_a = K = K_b$.

Alice and Bob end up with the same shared key due to the commutativity properties of the upper and lower triangular Toeplitz matrices. Note that the authors of this protocol [18] proposed it using the max-times semiring, while we present it here using the max-plus semiring. The two approaches are equivalent due to the following remark.

Remark 3.1. Both the max-times and min-plus semirings are isomorphic to the max-plus semiring (see, e.g., [4] Section 1.4), and therefore the claim that the max-times semiring is not a tropical semiring is false.

4 Cryptanalysis of The Proposed Protocols Using The Generalized Kotov-Ushakov Attack

In this section, we present our attacks on the protocols introduced in the previous section. Subsequently, we implement the attacks showing their efficiency and performance.

4.1 Generalized Kotov-Ushakov Attack on Modified Tropical Circulant Stickel Protocols

It is claimed in [9],[2] and [18] that these protocols are resistant to the Kotov-Ushakov attack since the modified tropical circulants cannot be represented as tropical polynomials of any matrix. However we aim to show that, while this claim is true, we can in fact represent these matrices in a nice algebraic manner as seen in the upcoming example, and therefore (similarly to how it is done in [14]) we can implement a form of the generalized Kotov-Ushakov attack to cryptanalyze all existing Stickel protocols based on modified tropical circulants.

Example 4.1. Consider the set of upper s-circulant matrices of size 3, in particular C_3^s. Let $A \in C_3^s$ with parameters c_0, c_1, c_2 and s. We can express A as

$$A = \begin{pmatrix} c_0 & c_2 \otimes s & c_1 \otimes s \\ c_1 & c_0 & c_2 \otimes s \\ c_2 & c_1 & c_0 \end{pmatrix} = c_0 \otimes \begin{pmatrix} 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \end{pmatrix} \oplus$$

$$c_1 \otimes \begin{pmatrix} -\infty & -\infty & s \\ 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \end{pmatrix} \oplus c_2 \otimes \begin{pmatrix} -\infty & s & -\infty \\ -\infty & -\infty & s \\ 0 & -\infty & -\infty \end{pmatrix}.$$

Proposition 4.1. We can express any modified tropical circulant matrix of dimension $n \times n$ with entries $c_0, c_1, \ldots, c_{n-1}$ as

$$A = \bigoplus_{\alpha=0}^{n-1} (c_\alpha \otimes \Gamma_\alpha^s),$$

where we have the following definition for the upper circulant case

$$(\Gamma_\alpha^s)_{ij} = \begin{cases} 0 & \text{if } \alpha \equiv (i-j)(\text{mod} n) \text{ and } i \geq j \\ s & \text{if } \alpha \equiv (i-j)(\text{mod} n) \text{ and } i < j \\ -\infty & \text{otherwise} \end{cases} \tag{1}$$

and the following definition for the lower circulant case

$$(\Gamma_\alpha^s)_{ij} = \begin{cases} 0 & \text{if } \alpha \equiv (i-j)(\text{mod} n) \text{ and } i \leq j \\ s & \text{if } \alpha \equiv (i-j)(\text{mod} n) \text{ and } i > j \\ -\infty & \text{otherwise} \end{cases} \tag{2}$$

We are going to use these formulas to generate a form of Kotov-Ushakov attack on the proposed protocols. We begin by providing a theoretical description of the attack. Recall from Protocol 2 or Protocol 3 that M, U, V, s, t are public values known to the attacker while A_1, A_2, B_1, B_2 are secrets. The attacker aims to find two unknown matrices X and Y such that $X \otimes M \otimes Y = U$ where X is a modified s-circulant and Y is a modified t-circulant. We know that X commutes with B_1 since they are both modified s-circulants, and similarly Y commutes with B_2 since they are both modified t-circulants. Thus, the attacker can compute $K_{attack} = X \otimes V \otimes Y = X \otimes B_1 \otimes M \otimes B_2 \otimes Y = B_1 \otimes X \otimes M \otimes Y \otimes B_2 = B_1 \otimes U \otimes B_2 = K_b = K_a$. To find such X and Y, the equation $X \otimes M \otimes Y = U$ can be expressed as a tropical linear system of equation of the shape $A \otimes x = b$ after representing X and Y as in Proposition 4.1. Then, utilizing the theory of solving such a system, the attacker can find the entries of X and Y, and hence recover the shared key. The details of these processes are described below.

Let D_s and D_t be arbitrary modified tropical circulants, assuming different forms of the modified circulants depending on the specific protocol targeted by the attack. Similarly to the original Kotov-Ushakov attack [11], we are aiming to find modified tropical circulants X and Y that solve

$$\begin{cases} X \otimes D_s = D_s \otimes X \\ Y \otimes D_t = D_t \otimes Y \\ X \otimes M \otimes Y = U \end{cases} \tag{3}$$

Using Proposition 4.1 we can express X and Y as

$$X = \bigoplus_{\alpha=0}^{n-1} (x_\alpha \otimes \Gamma_\alpha^s), \quad Y = \bigoplus_{\beta=0}^{n-1} \left(y_\beta \otimes \Gamma_\beta^t\right).$$

We now substitute these into the third equation of (3) to obtain

$$U = \bigoplus_{\alpha=0}^{n-1} (x_\alpha \otimes \Gamma_\alpha^s) \otimes M \otimes \bigoplus_{\beta=0}^{n-1} \left(y_\beta \otimes \Gamma_\beta^t\right).$$

Combining the tropical summations, we obtain

$$U = \bigoplus_{\alpha,\beta=0}^{n-1} (x_\alpha \otimes \Gamma_\alpha^s) \otimes M \otimes \left(y_\beta \otimes \Gamma_\beta^t\right).$$

Rearranging those using the distributivity law will give

$$\bigoplus_{\alpha,\beta=0}^{n-1} x_\alpha \otimes y_\beta \otimes \left(\Gamma_\alpha^s \otimes M \otimes \Gamma_\beta^t - U\right) = E,$$

where E is a matrix of the correct dimension with zeros in all entries. We denote $T^{\alpha\beta} = \Gamma_\alpha^s \otimes M \otimes \Gamma_\beta^t - U$ and therefore we can write

$$\bigoplus_{\alpha,\beta=0}^{n-1} x_\alpha \otimes y_\beta \otimes \left(T^{\alpha\beta}\right)_{\gamma\delta} = 0 \quad \forall \gamma, \delta \in [n].$$

If we additionally denote $z_{\alpha\beta} = x_\alpha \otimes y_\beta$, we have

$$\bigoplus_{\alpha,\beta=0}^{n-1} z_{\alpha\beta} \otimes \left(T^{\alpha\beta}\right)_{\gamma\delta} = 0 \quad \forall \gamma, \delta \in [n]. \tag{4}$$

We have arrived at a system of tropical linear one-sided equations with coefficients $\left(T^{\alpha\beta}\right)_{\gamma\delta}$ and unknowns $z_{\alpha\beta}$.
Now we describe a generalized form of the Kotov-Ushakov attack similar to [14]. Here and below, $\arg\min_{\gamma,\delta\in[n]}\left(-T^{\alpha\beta}_{\gamma\delta}\right)$ denotes the set of pairs (γ, δ) at which the minimum of $-T^{\alpha\beta}_{\gamma\delta}$ is attained.

Attack 4.1. Generalized Kotov-Ushakov attack against the tropical Stickel protocol based on modified circulants.

1. Compute
$$c_{\alpha\beta} = \min_{\gamma,\delta\in[n]}\left(-T^{\alpha\beta}_{\gamma\delta}\right)$$
$$S_{\alpha\beta} = \arg\min_{\gamma,\delta\in[n]}\left(-T^{\alpha\beta}_{\gamma\delta}\right).$$

2. Among all minimal covers of $[n] \times [n]$ by $S_{\alpha\beta}$, that is, all minimal subsets $\mathcal{C} \subseteq \{0, \ldots, n-1\} \times \{0, \ldots, n-1\}$ such that
$$\bigcup_{(\alpha,\beta)\in\mathcal{C}} S_{\alpha\beta} = [n] \times [n],$$
find a cover for which the system
$$\begin{aligned} x_\alpha + y_\beta &= c_{\alpha\beta}, && \text{if } (\alpha, \beta) \in \mathcal{C}, \\ x_\alpha + y_\beta &\leqslant c_{\alpha\beta}, && \text{if otherwise.} \end{aligned} \tag{5}$$
is solvable.

We now prove that this attack works, due to it producing X and Y that satisfy equations (3). (The proof is quite similar to the proof of [14], Theorem 5.1, but we include it here for reader's convenience.)

Proposition 4.2. Let U be the message that Alice sent to Bob in Protocol 2 or Protocol 4. Then Attack 4.1 yields

$$X = \bigoplus_{\alpha=0}^{n-1} \left(x_\alpha \otimes \Gamma^s_\alpha\right), \quad Y = \bigoplus_{\beta=0}^{n-1} \left(y_\beta \otimes \Gamma^t_\beta\right),$$

where Γ^s_α and Γ^t_β are the generators of X and Y defined in (1) or (2) depending on which modified circulants are used in the protocol, such that X and Y satisfy $X \otimes M \otimes Y = U$.

Proof. Since $U = X \otimes M \otimes Y$ where X and Y are modified circulants, it is clear that Equation (4) is solvable with $z_{\alpha\beta} = x_\alpha \otimes y_\beta$ and x_α and y_β such that $X = \bigoplus_{\alpha=0}^{n-1}\left(x_\alpha \otimes \Gamma^s_\alpha\right)$ and $Y = \bigoplus_{\beta=0}^{n-1}\left(y_\beta \otimes \Gamma^t_\beta\right)$. We are now left to show that the method described in Attack 4.1 does find a solution.

We utilize the following results from the theory of tropical linear equation of the shape $A \otimes x = b$ (see [4] Theorem 3.1.1 and Corollary 3.1.2):

1. We have that $c_{\alpha\beta} = \min\left(-T^{\alpha\beta}_{\gamma\delta}\right) = -\max\left(T^{\alpha\beta}_{\gamma\delta}\right)$ is the greatest solution.
2. We recall that $S_{\alpha\beta} = \arg\min_{\alpha\beta}\left(-T^{\alpha\beta}_{\gamma\delta}\right) = \arg\max\left(T^{\alpha\beta}_{\gamma\beta}\right)$. Therefore, $Z = (z_{\alpha\beta})$ is a solution if and only if there exists a set $\mathcal{C} \subseteq \{0,\dots,n-1\} \times \{0,\dots,n-1\}$ such that

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

and also

$$\begin{aligned} &z_{\alpha\beta} = c_{\alpha\beta} \text{ for all } (\alpha,\beta) \in \mathcal{C} \text{ and } z_{\alpha\beta} \leq c_{\alpha\beta} \text{ for all } (\alpha,\beta) \notin \mathcal{C}, \\ &z_{\alpha\beta} = x_\alpha \otimes y_\beta \qquad \forall \alpha, \beta. \end{aligned}$$

If there is a solution (x, y) that satisfies these set of equalities and inequalities, then there is a minimal cover $C' \subseteq C$ of $[n] \times [n]$ for which it is of this form with C being replaced with C'. Therefore, the solvability is checked by finding at least one linear system (5) that is solvable with $\mathcal{C}$ being a minimal cover (i.e a set satisfying $\bigcup_{(\alpha,\beta)\in\mathcal{C}} S_{\alpha\beta} = [n] \times [n]$ that is minimal with respect to inclusion). As Attack 4.1 performs this procedure, it will break the proposed protocol, provided that a solution exists (which in the case that the protocol has been applied is true). □

4.2 Implementation of The Attack With a Comparison Between The Modified Circulant Protocols And The Original Stickel Protocol

We implemented Attack 4.1 and applied it to the Stickel protocols based on modified circulants and performed the experiments for a matrix size ranging from 2 to 50 and the entries of the matrix in the interval [-1000,1000]. We have computed the time taken for the attack to recover the secret shared key for each matrix size. We also computed the time taken to generate the key between the two authorized parties (Alice and Bob) in order to compare it with the attacker's time. Each point in the figures corresponds to attacking or generating a single instance by the protocols. The code was executed on GAP-V4.12.2 running on Windows 11 64-bit, equipped with an Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz and 16.0 GB RAM.

Firstly, we performed the attack on Protocol 2 and compared its time with the key generation time as seen in Figure 1.

As expected, the attacker takes more time to recover the shared secret as the dimension of the matrix increases. This is due to a high number of generators (i.e., Γ matrices) in the generalized Kotov-Ushakov attack, leading to a big number of minimal covers to be checked. Note that all of these minimal covers are generated by the attack, as it also was in the case of the original implementation by Kotov and Ushakov [11].

Thus, on the one hand, generating these covers and then sorting them and looking for an appropriate cover can be very time-consuming. On the other hand, generating the shared key between the authorized parties is obviously very fast, since it only requires generating random

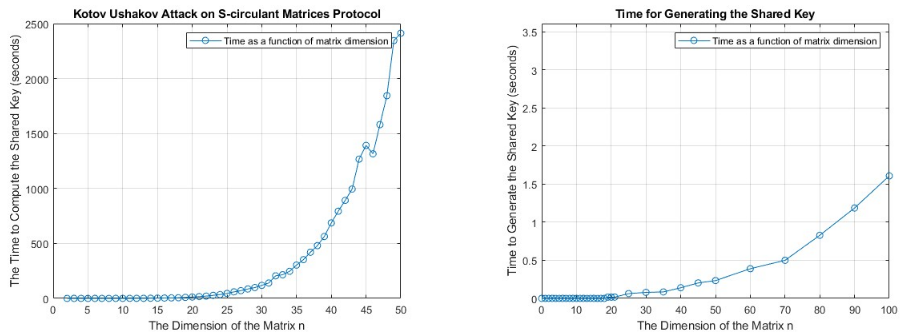

Figure 1: Attacking vs. performing Protocol 2

matrices and multiplying them. For example, it only takes Alice and Bob 1.6 sec to exchange a shared key for a matrix size of 100.

We also applied the same attack to Protocol 3 and compared its time with the generation of the shared key, and we obtained very similar results in the performance of the triangular Toeplitz protocol against the attack when compared with the s-circulants protocol, with the Toeplitz protocol requiring less time to attack (23 minutes for 50×50 Toeplitz matrices compared to 40 minutes for s-circulant matrices of the same dimension).
Since both the modified circulants protocols and the original Stickel protocol are susceptible to a form of Kotov-Ushakov attack, it makes sense to compare their resilience and performance against their attacks. Figure 2 shows the performance of the tropical Stickel protocol of [7] against the Kotov-Ushakov attack and the time required for the generation of the shared key. Similarly, the matrix entries and polynomial coefficients are from the interval $[-1000, 1000]$ and each point in the figures corresponds to attacking or generating a single instance of the protocol.

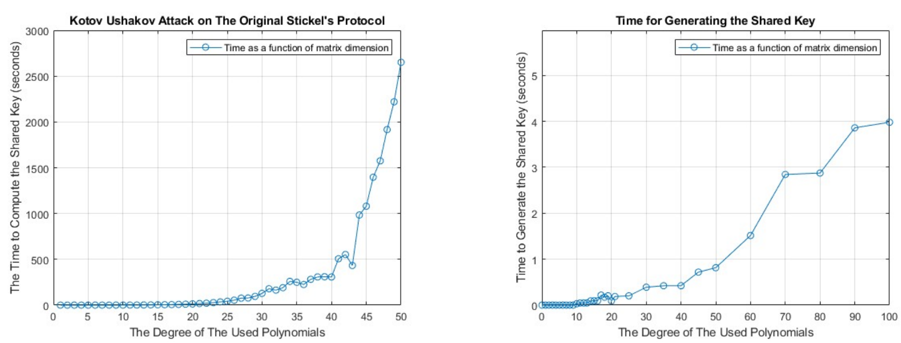

Figure 2: Attacking vs. performing Protocol 1

We observe that both the modified circulant protocols and the original Stickel protocol exhibit comparable resistance to the Kotov-Ushakov attacks, with an advantage of the original Stickel protocol. For example, original Stickel protocol required the Kotov-Ushakov attack 44.188 minutes to successfully recover the shared key for a 50-sized polynomial, whereas the generalized Kotov-Ushakov attack on the s-circulant and the triangular Toeplitz protocols took 40.203 and 25.83

minutes respectively for a 50-dimensional matrix. Notably, enhancing the security of original Stickel protocol is achievable by employing larger matrices, as we employed only a 10-dimensional matrix in this experiment, as suggested by the authors of the protocol [7].
Note that the process of key generation between authorized parties proves to be more efficient in the modified circulant protocols, as they do not require the evaluation of polynomials and matrix powers. However, the difference in efficiency is relatively subtle and might not be noticeable to users. Consequently, the proposed modified circulant protocols do not provide any significant additional advantages over the original Stickel protocol.

5 A More Efficient Implementation of the Kotov-Ushakov Attack

In this section, we present an alternative implementation of the Kotov-Ushakov attack that requires less time to attack the proposed modified circulant protocols as well as the tropical Stickel protocol of [7].

5.1 Details of The Attack

The number of enumerated covers in Kotov-Ushakov attack appears to grow exponentially with the polynomial degree in the original Stickel protocol and similarly with the matrix size in the modified circulant protocols. This makes the attack highly time-consuming for large values of these parameters, as illustrated in the preceding figures. Consequently, there is a compelling need to seek a more efficient implementation of the attack. In their work [11], Kotov and Ushakov observed that smaller-sized covers are more likely to be appropriate and lead to a consistent solvable linear system. In their experiment they only had to test for at most 2 covers after sorting all covers by size and then another criteria. This inspired us to implement an efficient version of the attack where we only try to find the smallest cover instead of enumerating all possible covers using a greedy algorithm where we iteratively select the largest set $S_{\alpha,\beta}$ containing the pair (γ, δ).
In particular, we firstly compute $c_{\alpha\beta}$ and $S_{\alpha\beta}$ as in the original Kotov-Ushakov attack. Then, for every pair (γ, δ) in $[n] \times [n]$, we have $(\gamma, \delta) \in S_{\alpha\beta}$ for some (α, β) pairs. We identify the largest sized set among them and add the associated (α, β) to our cover. We then repeat the process for all possible uncovered (γ, δ) pairs in $[n] \times [n]$. In practice, this procedure quite often yields the smallest sized cover. The process is described in Algorithm 1.

Remark 5.1. Algorithm 1 has polynomial complexity. Indeed, the initialization in line 2 takes $O(n^4)$ operations. It can be also seen that the loops in lines 3-10 take at most $O(n^6)$ operations. Lastly, the system in line 11 can be formulated as a linear programming problem, which is known to be polynomially solvable.

5.2 Implementation of The Attack With Success Rate and Efficiency Analysis

We expect this attack to have a high success rate against Protocol 1 since the smallest cover almost always succeeds in the original implementation of the Kotov-Ushakov attack. We will firstly apply it on a special case of Protocol 2 where M is the tropical identity matrix I, Figure 3 shows the success rate of the attack. The code was executed on MATLAB R2023b running on Windows 11

Algorithm 1 Heuristic Implementation of Kotov-Ushakov Attack Using a Cover

Initialize $Final\_Cover = [\ ]$

Compute $c_{\alpha\beta} = \min\limits_{\gamma,\delta\in[n]} \left(-T^{\alpha\beta}_{\gamma\delta}\right)$ and $S_{\alpha\beta} = \arg\min\limits_{\gamma,\delta\in[n]} \left(-T^{\alpha\beta}_{\gamma\delta}\right)$

for $(\gamma,\delta) \in [n]\times[n]$ and $(\gamma,\delta) \notin \bigcup S_{\alpha\beta}\ \forall \alpha,\beta \in Final\_Cover$: **do**

  Initialize $Possible\_Covers = [\ ]$

  for $(\alpha,\beta) \in \{0,1,\ldots,n-1\}\times\{0,1,\ldots,n-1\}$ **do**

    if $(\gamma,\delta) \in S_{\alpha\beta}$ **then**

      Append (α,β) to $Possible\_Covers$

  for $(\alpha,\beta) \in Possible\_Covers$ **do**

    find largest sized $S_{\alpha\beta}$ and assign (α',β')=(α,β)

  Append (α',β') to $Final\_Cover$

Solve the system

$$\begin{aligned} x_\alpha + y_\beta &= c_{\alpha\beta}, && \text{if } (\alpha,\beta)\in Final\_Cover,\\ x_\alpha + y_\beta &\leqslant c_{\alpha\beta}, && \text{if otherwise.} \end{aligned}$$

64-bit, equipped with an Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz and 16.0 GB RAM. The parameters used in the experiment are:
- The matrix entries are chosen randomly from -10000 to 10000 in every trail.
- The protocol parameters s and t are chosen randomly from -10000 to 10000 in every trail.
- 1000 trails are performed for every matrix dimension.

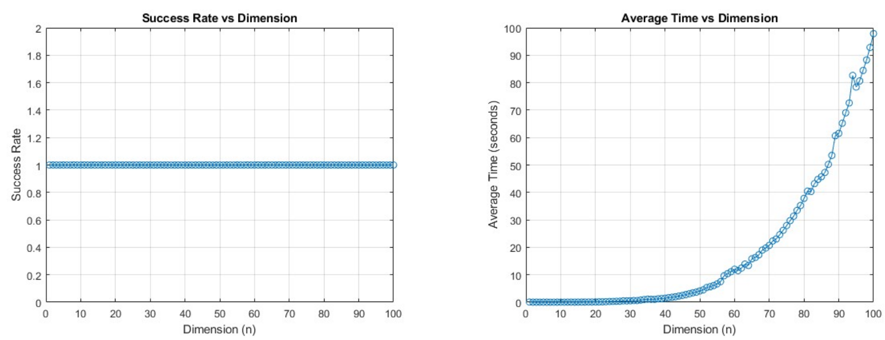

Figure 3: Algorithm 1 attacking Protocol 2 when $M = I$: success rate and efficiency

We observe that the algorithm maintains a perfect success rate even for higher dimensions, which are the most important cases since the original implementation is not efficient for them. Figure 3 illustrates the average time for the attack to recover the secret key as a function of matrix dimension. Comparing this with Figure 1, this attack implementation is over 500 times faster for the matrices of dimension 50×50 than the original implementation. We also applied the attack on the triangular Toeplitz matrices protocol, and similarly the attack achieved a perfect success rate and a much faster execution time compared to the original implementation of the generalized Kotov-Ushakov attack.

However, when M is included in the circulant protocols with sufficiently high entries, the algorithm occasionally fails. Thus, we need an alternative method to carefully select a minimal cover that breaks the protocol. One way is to add an extra step to Algorithm 1. After extracting the minimal cover using Algorithm 1, we check if there are any pairs $(\alpha', \beta') \in \{0, 1, \ldots, n-1\} \times \{0, 1, \ldots, n-1\}$ such that $S_{\alpha'\beta'} = S_{\alpha\beta}$ for some $(\alpha, \beta) \in Final\_Cover$. We then examine all possible minimal covers formed by the components of $Final\_Cover$ and these new (α', β') pairs. We observed that this approach achieved a perfect success rate but still involves enumerating and testing multiple minimal covers, which adds substantial complexity, especially in high dimensions. This enumeration and testing are precisely the issues we aim to avoid.

We then considered that using a complete minimal cover might not be necessary; a partial cover could suffice to recover the key. Therefore, we will relax our goal from strictly extracting a complete minimal cover to identifying any successful sub-cover. One way is that, after extracting the minimal cover by Algorithm 1, we simply delete those components $(\alpha, \beta) \in Final\_Cover$ where $S_{\alpha\beta} = S_{\alpha'\beta'}$ for some $(\alpha', \beta') \in \{0, 1, \ldots, n-1\} \times \{0, 1, \ldots, n-1\}$. This approach achieves a very high success rate with only a slight increase in execution time compared to Algorithm 1.

Following this route of using a sub-cover, yet another approach is to select a sub-cover that is guaranteed to be part of every possible minimal cover (Algorithm 2). Specifically, we pick the pairs (α, β) such that for some $(\gamma, \delta) \in [n] \times [n]$ we have $(\gamma, \delta) \in S_{\alpha\beta}$ and $(\gamma, \delta) \notin S_{\alpha'\beta'}$ for any other $(\alpha', \beta') \in \{0, 1, \ldots, n-1\} \times \{0, 1, \ldots, n-1\}$. This approach achieves a perfect success rate and preserves the same order of computational time as Algorithm 1, which is $O(n^6)$ + the computational complexity of solving the linear program. The success rate and time consumption of Algorithm 2 are shown in Figure 4.

Algorithm 2 Heuristic Implementation of Kotov-Ushakov Attack Using a Sub-cover

Initialize $Sub\_Cover = [\,]$

Compute $c_{\alpha\beta} = \min\limits_{\gamma,\delta \in [n]} \left(-T^{\alpha\beta}_{\gamma\delta}\right)$ and $S_{\alpha\beta} = \arg\min\limits_{\gamma,\delta \in [n]} \left(-T^{\alpha\beta}_{\gamma\delta}\right)$

for $(\gamma, \delta) \in [n] \times [n]$: **do**

  for $(\alpha, \beta) \in \{0, 1, \ldots, n-1\} \times \{0, 1, \ldots, n-1\}$ **do**

    if $(\gamma, \delta) \in S_{\alpha\beta}$ and $(\gamma, \delta) \notin S_{\alpha'\beta'} \quad \forall (\alpha', \beta') \neq (\alpha, \beta)$ **then**

      Append (α, β) to Sub_Cover

Solve the system

$$\begin{aligned} x_\alpha + y_\beta &= c_{\alpha\beta}, &&\text{if } (\alpha, \beta) \in Sub\_Cover, \\ x_\alpha + y_\beta &\leqslant c_{\alpha\beta}, &&\text{if otherwise.} \end{aligned}$$

Let us compare Algorithm 2 to [13], Algorithm 9. Both algorithms use a similar idea of picking (α, β) that need to be in any cover of $[n] \times [n]$. Also, similarly to the initial Kotov-Ushakov attack, they aim to correctly formulate system (5) to break the targeted protocols. The primary difference is that Algorithm 2 uses only a specially formed sub-cover to formulate and solve the linear program, while Algorithm 9 in [13] forms a complete minimal cover of $[n] \times [n]$ before using it to set up and solve the linear program.

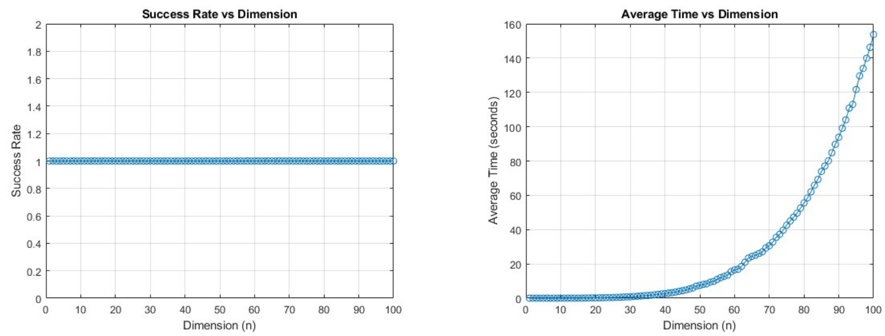

Figure 4: Algorithm 2 attacking Protocol 2: success rate and efficiency

We also applied some of these proposed heuristics on the original tropical Stickel protocol. Specifically, we applied Algorithm 1 but with replacing $(\alpha, \beta) \in \{0, 1, \dots, n-1\} \times \{0, 1, \dots, n-1\}$ in the 5th line of the algorithm by $(\alpha, \beta) \in \{0, 1, \dots, D\} \times \{0, 1, \dots, D\}$ where D is the maximum polynomial degree that can be used by Alice and Bob. Figure 5 illustrates the success rate and the time consumption of this attack on the original Stickel protocol, in which we similarly notice a high success rate with a faster computation compared to the original implementation by Kotov and Ushakov.
The parameters used in the experiment are:
- The matrix dimension is 10 for all trails.
- The matrix entries are chosen randomly from -10000 to 10000 in every trail.
- The polynomial coefficients are chosen randomly from -10000 to 10000 in every trail.
- 1000 trails are performed for every polynomial degree.

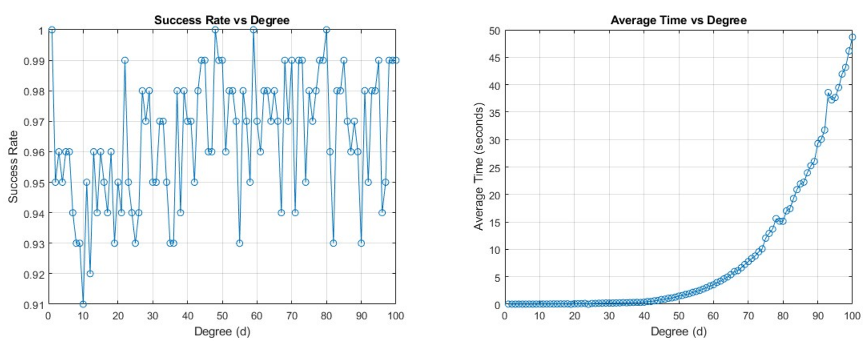

Figure 5: Algorithm 1 attacking Protocol 1 : success rate and efficiency

We note that this heuristic implementation achieved a high success rate and much less computational time when applied to the original Stickel protocol. Thus it is outperforming the computational efficiency of the original attack implementation by Kotov and Ushakov, but losing a bit in terms of success rate.

6 Conclusions

In this paper, we analyzed some versions of the tropical Stickel protocol that are based on the modified tropical circulant matrices. We showed that a form of Kotov-Ushakov attack applies to these protocols and is able to successfully recover the shared secret key. Since the matrix dimension in these protocols is equivalent to the polynomial degree in the original Stickel protocol, Kotov-Ushakov attack becomes less efficient as the matrix dimension increases. To address this, we implemented several heuristic forms of the attack, demonstrating both exceptional speed and a remarkably high success rate. These implementations achieved a supreme success rate when applied to the Stickel protocols based on modified circulants, and Algorithm 1 achieved an extremely high success rate when applied to the tropical Stickel protocol of [7].

Therefore, our findings lead to the conclusion that the proposed protocols do not confer any advantage over the original version of tropical Stickel protocol. All protocols are vulnerable to a form of Kotov-Ushakov attack. The original tropical Stickel protocol, however, enjoys the advantage of having two user-controllable parameters (matrix dimension and polynomial degree), enhancing its resistance. In contrast, the proposed protocols feature only one parameter (matrix dimension), implying that the Kotov-Ushakov attack would require less time to compromise it under extreme parameter values.

Acknowledgement

We are grateful to our anonymous referees for suggesting a number of corrections which helped to improve our paper. One of the referees made us aware of the preprint by Buchinskiy, Kotov and Treier [3], in which a very similar attack is presented (see the end of Introduction for more detailed discussion). We also wish to thank Dr. Any Muanalifah for bringing M. Mach's Master Thesis [13] to our attention.

References

[1] K. Ahmed, S. Pal, and R. Mohan. A review of the tropical approach in cryptography. *Cryptologia*, 47(1):63–87, 2023.

[2] B. Amutha and R. Perumal. Public key exchange protocols based on tropical lower circulant and anti circulant matrices. *AIMS Mathematics*, 8(7):17307–17334, 2023.

[3] I. Buchinskiy, M. Kotov, and A. Treier. Analysis of four protocols based on tropical circulant matrices. Cryptology ePrint Archive, Paper 2023/1707, 2023. `https://eprint.iacr.org/2023/1707`.

[4] P. Butkovič. *Max-linear Systems: Theory and Algorithms.* Springer, London, 2010.

[5] M.I. Durcheva. TrES: tropical encryption scheme based on double key exchange. *Eur. J. Inf. Tech. Comp. Sci.*, 2(4), 2022.

[6] M. Gavalec. *Periodicity in Extremal Algebras.* Gaudeamus, Hradec Králové, 2004.

[7] D. Grigoriev and V. Shpilrain. Tropical cryptography. *Communications in Algebra*, 42:2624 – 2632, 2013.

[8] D. Grigoriev and V. Shpilrain. Tropical cryptography ii: Extensions by homomorphisms. *Communications in Algebra*, 47(10):4224–4229, 2019.

[9] H. Huang, C. Li, and L. Deng. Public-key cryptography based on tropical circular matrices. *Applied Sciences*, 12(15), 2022.

[10] S. Isaac and D. Kahrobaei. A closer look at the tropical cryptography. *International Journal of Computer Mathematics: Computer Systems Theory*, 6(2):137–142, 2021.

[11] M. Kotov and A. Ushakov. Analysis of a key exchange protocol based on tropical matrix algebra. *Journal of Mathematical Cryptology*, 12(3):137–141, 2018.

[12] G.L. Litvinov, A.Ya. Rodionov, S.N. Sergeev, and A.N. Sobolevski. Universal algorithms for solving the matrix bellman equations over semirings. *Soft Computing*, 17(10):1767–1785, October 2013.

[13] M. Mach. Cryptography based on semirings. Master's thesis, Univerzita Karlova, Matematicko-fyzikální fakulta, 2019.

[14] A. Muanalifah and S. Sergeev. Modifying the tropical version of Stickel's key exchange protocol. *Applications of Mathematics*, 65:727–753, 12 2020.

[15] A. Muanalifah and S. Sergeev. On the tropical discrete logarithm problem and security of a protocol based on tropical semidirect product. *Communications in Algebra*, 50(2):861–879, 2022.

[16] J. Plávka. On eigenproblem for circulant matrices in max algebra. *Optimization*, 50:477–483, 2001.

[17] J. Plávka and S. Sergeev. Reachability of eigenspaces for interval circulant matrices in max-algebra. *Linear Algebra and its Applications*, 550:59–86, 2018.

[18] A. Ponmaheshkumar and R. Perumal. Toeplitz matrices based key exchange protocol for the internet of things. *International Journal of Information Technology*, 65, 11 2023.

Sulaiman Alhussaini
University of Birmingham, School of Mathematics, Birmingham, Edgbaston B15 2TT, UK
saa399@student.bham.ac.uk

Craig Collett
University of Birmingham, School of Mathematics, Birmingham, Edgbaston B15 2TT, UK
CRC957@student.bham.ac.uk

Sergeĭ Sergeev
University of Birmingham, School of Mathematics, Birmingham, Edgbaston B15 2TT, UK
s.sergeev@bham.ac.uk