# On the security of the initial tropical Stickel protocol and its modification based on Linde-de la Puente matrices

Sulaiman Alhussaini and Sergeĭ Sergeev

**Abstract**

Recently, a more efficient attack on the initial tropical Stickel protocol has been proposed, different from the previously known Kotov-Ushakov attack, yet equally guaranteed to succeed. Given that the Stickel protocol can be implemented in various ways, such as utilizing platforms beyond the tropical semiring or employing alternative commutative matrix "classes" instead of polynomials, we firstly explore the generalizability of this new attack across different implementations of the Stickel protocol. We then conduct a comprehensive security analysis of a tropical variant that successfully resists this new attack, namely the Stickel protocol based on Linde-de la Puente (LdlP) matrices. Additionally, we extend the concept of LdlP matrices beyond the tropical semiring, generalizing it to a broader class of semirings.

**Keywords:** public key cryptography; cryptographic attack; Stickel protocol
**Classification:** 94A60, 15A80

## 1 Introduction

Tropical linear algebra has been recently used as a platform for new supposedly more secure implementations of some cryptographic key exchange protocols including the Stickel protocol [18]. In this context, Grigoriev and Shpilrain [8] introduced the first tropical implementation of the Stickel protocol, which we refer to as the "initial tropical Stickel protocol". The widely accepted attack on this protocol is due to Kotov and Ushakov [12]. This attack successfully breaks the protocol by finding the whole solution set of the underlying tropical linear system imposed by the protocol by enumerating all minimal solutions of such system.

Then, recently, the authors in [16] proposed an alternative attack that breaks the protocol by finding only a single solution of this linear system, rather than enumerating all solutions, which significantly reduces the complexity in relation to the polynomial degree used in the protocol. This attack is possible because the polynomials chosen by Alice and Bob commute with the powers of the public matrices. Notably, this new attack is not guaranteed to succeed on all implementations of the Stickel protocol. Its applicability depends on specific conditions involving the underlying semiring and the "class" of the commuting matrices being used. Specifically, the attack successfully applies only when the one-sided linear systems

over the semiring are easily solvable and the matrices used by Alice and Bob have an obvious finite set of generators with which they commute (e.g., consider matrix powers as generators of matrix polynomials).

Consequently, certain tropical variants of the Stickel protocol prove resistant to this new attack, one notable example being the version based on Linde-de la Puente (LdlP) matrices [13] as proposed by [15]. This variant is also resistant to the Kotov-Ushakov attack which motivates a further investigation of its overall security by exploring the other heuristic means. It turns out that this class of matrices can also be constructed over a wider variety of semirings, possibly offering stronger cryptographic properties when utilized over alternative semirings.

This paper is organized as follows: Section 2 covers preliminaries and basic definitions, particularly those related to matrix algebra and the Stickel protocol over semirings. In Section 3, we present the conditions under which the new attack is applicable and provide its performance comparison with the Kotov-Ushakov attack. In Section 4, we analyze the security of the tropical Stickel protocol based on LdlP matrices against the new attack, the Kotov-Ushakov attack and some other heuristics that were suggested previously. All codes related to the numerical experiments have been made available on GitHub [1].

# 2 Preliminaries

In this section, we introduce the matrix algebra over semirings followed by the construction of the Stickel protocol over an arbitrary semiring, and how it is typically compromised by the Kotov-Ushakov attack and the new attack put forward in [16]. Note that we use the standard notation $[m] = \{1, \ldots, m\}$ and $[n] = \{1, \ldots, n\}$ for most common index sets. We start by recalling the definition of a semiring.

**Definition 2.1** (Semiring)**.** Let $S$ be a non-empty set equipped with two binary operations $\oplus$ and $\otimes$, which satisfy the following properties:

- $(S, \oplus)$ is an Abelian semigroup which means that it satisfies associativity, commutativity and existence of an additive identity element $\epsilon$.
- $(S, \otimes)$ is a semigroup which means that it satisfies associativity and existence of multiplicative identity element $e$.
- In $(S, \oplus, \otimes)$ multiplication $\otimes$ distributes over addition $\oplus$.
- The additive identity $\epsilon$ satisfies the absorbing property, that is $\epsilon \otimes e = e \otimes \epsilon = \epsilon$.

The semirings of primary interest, particularly for their cryptographic applications in implementing the Stickel protocol, are the tropical (max-plus), fuzzy (max-min), and the max-$T$ semirings. We now present their formal definitions.

[1] https://github.com/suliman1n/On-the-security-of-the-initial-tropical-Stickel-protocol-and-its-modification-based-on-LdlP-matrices

**Definition 2.2** (Tropical Semiring)**.** The tropical semiring $\mathbb{R}_{\max}$ is defined by $\mathbb{R}_{\max} = (\mathbb{R} \cup \{-\infty\}, \oplus, \otimes)$, where the tropical addition $\oplus$ and the tropical multiplication $\otimes$ are respectively defined by $a \oplus b = \max\{a, b\}$ and $a \otimes b = a + b$ for all $a, b \in \mathbb{R}_{\max}$.

**Definition 2.3** (Max-min Semiring)**.** The max-min semiring, denoted as $\mathbb{R}_{\max,\min}$, is defined by $\mathbb{R}_{\max,\min} = (\mathbb{R} \cup \{-\infty\} \cup \{\infty\}, \oplus, \otimes)$, with these two operations defined by $a \oplus b = \max\{a, b\}$ and $a \otimes b = \min\{a, b\}$ for all $a, b \in \mathbb{R}_{\max,\min}$.

**Definition 2.4** (Max-$T$ Semiring)**.** The max-$T$ semiring is defined as the unit interval $\mathcal{B} = [0, 1]$ equipped with the tropical addition $a \oplus b = \max(a, b)$ and the $T$-norm multiplication $a \otimes b = T(a, b)$ where $T : \mathcal{B}^2 \to \mathcal{B}$ is a $T$-norm (see Definition 2.5).

**Definition 2.5** ($T$-norm (e.g., [11]))**.** A T-norm is a binary operation on the unit interval that satisfies the following axioms for all $a, b, d \in [0, 1]$:

1. $T(a, 1) = a$ (boundary condition).
2. $b \leq d$ implies $T(a, b) \leq T(a, d)$ (monotonicity).
3. $T(a, b) = T(b, a)$ (commutativity).
4. $T(a, T(b, d)) = T(T(a, b), d)$ (associativity).

One notable example of a $T$-norm that has some interesting properties, which will be discussed later, is the Hamacher product, defined as

$$a \otimes b = T(a, b) = \begin{cases} 0, & \text{if } a = b = 0, \\ \frac{ab}{a+b-ab}, & \text{otherwise.} \end{cases} \tag{1}$$

The Stickel key exchange protocol is constructed using matrix algebra over an arbitrary semiring $S$. We hence present some of the relevant definitions.

**Definition 2.6** (Matrix Algebra over Semirings [7])**.** The arithmetic operations over a semiring $S$ are naturally extended to include matrices and vectors. In particular, the operation $A \otimes \alpha = \alpha \otimes A$, where $\alpha \in S, A \in S^{m \times n}$ and $(A)_{ij} = a_{ij}$ for $i \in [m]$ and $j \in [n]$, is defined by

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

The matrix addition $A \oplus B$ of two matrices $A \in S^{m \times n}$ and $B \in S^{m \times n}$, where $(A)_{ij} = a_{ij}$ and $(B)_{ij} = b_{ij}$ for $i \in [m]$ and $j \in [n]$, is defined by

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

The matrix multiplication of two matrices is also similar to the "traditional" algebra. Namely, we define $A \otimes B$ for two matrices, where $A \in S^{m \times p}$ and $B \in S^{p \times n}$, 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 2.7** (Matrix Powers)**.** For $M \in S^{n\times n}$, the $n$-th power of $M$ is denoted by $M^{\otimes n}$, and is equal to

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

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

**Definition 2.8** (Identity Matrix of a semiring)**.** The identity matrix $I \in S^{n\times n}$ is of the form $(I)_{ij} = \delta_{ij}$ where

$$\delta_{ij} = \begin{cases} e & \text{if } i = j \\ \epsilon & \text{otherwise} \end{cases}$$

**Definition 2.9** (Matrix Polynomials)**.** A matrix polynomial is a function of the form

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

where $a_k \in S$ for $k = 0, 1, \ldots, d$. Here $A \in S^{n\times n}$ is a square matrix of any dimension $n$.

Any two matrix polynomials of the same matrix over any semiring commute just like in the classical algebra [7], and this fact was utilized by Grigoriev and Shpilrain to construct an implementation of the Stickel protocol over the tropical semiring after successfully attacking the original implementation [8]. The Stickel protocol can clearly be implemented over any semiring, as this underlying commutativity property remains valid.

**Protocol 1** (Stickel Protocol over semirings)**.**

1. Alice and Bob agree on public matrices $A, B, W$.
2. Alice chooses two random 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 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 $K_b = q_1(A) \otimes U \otimes q_2(B)$.

The two parties end up with an identical key due to the commutativity of polynomials of the same matrix. Formally, we have $K_a = p_1(A) \otimes V \otimes p_2(B) = p_1(A) \otimes q_1(A) \otimes W \otimes q_2(B) \otimes p_2(B) = q_1(A) \otimes p_1(A) \otimes W \otimes p_2(B) \otimes q_2(B) = q_1(A) \otimes U \otimes q_2(B) = K_b$.

An intuitive way to attack this protocol is aiming to find the coefficients of two polynomials that can reconstruct the transmitted message ($U$ or $V$). This is achieved by scanning all solutions of the one-sided linear system corresponding to either message. (Note that

$U = p_1(A) \otimes W \otimes p_2(B)$ is essentially a one-sided linear system of the shape $A \otimes x = b$ with unknowns being the products of polynomial coefficients). The attacker then searches for a solution that satisfies a specific structure arising from the multiplication of two polynomials. This approach was proposed by Kotov and Ushakov to attack the tropical version of the Stickel protocol [12]. The ideas of the attack can be summarized as follows.

The aim is to find two matrices $X$ and $Y$, where they are expressed as

$$X = \bigoplus_{\alpha=0}^{D} \left(x_\alpha \otimes A^{\otimes\alpha}\right), Y = \bigoplus_{\beta=0}^{D} \left(y_\beta \otimes B^{\otimes\beta}\right),$$

such that $D$ is sufficiently large to exceed the maximal degree of any polynomial that Alice and Bob might use. Then, Alice's message $U$ can be expressed as

$$U = \bigoplus_{\alpha=0}^{D} \left(x_\alpha \otimes A^{\otimes\alpha}\right) \otimes W \otimes \bigoplus_{\beta=0}^{D} \left(y_\beta \otimes B^{\otimes\beta}\right),$$

or equivalently

$$\bigoplus_{\alpha,\beta=0}^{D} x_\alpha \otimes y_\beta \otimes \left(A^{\otimes\alpha} \otimes W \otimes B^{\otimes\beta}\right) = U.$$

We then denote $R^{\alpha\beta} = A^{\otimes\alpha} \otimes W \otimes B^{\otimes\beta}$ and therefore we can write

$$\bigoplus_{\alpha,\beta=0}^{D} x_\alpha \otimes y_\beta \otimes \left(R^{\alpha\beta}\right)_{\gamma\delta} = U_{\gamma\delta} \quad \forall\gamma,\delta \in [n] \times [n]. \tag{2}$$

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

$$\bigoplus_{\alpha,\beta=0}^{D} z_{\alpha\beta} \otimes \left(R^{\alpha\beta}\right)_{\gamma\delta} = U_{\gamma\delta} \quad \forall\gamma,\delta \in [n] \times [n]. \tag{3}$$

This is a system of linear equations of the shape $A \otimes x = b$ with coefficients $\left(R^{\alpha\beta}\right)_{\gamma\delta}$ and unknowns $z_{\alpha\beta}$.

The next goal of the attack is to scan all solutions to this system, and get the solution that satisfies $z_{\alpha\beta} = x_\alpha \otimes y_\beta$ for some $x_\alpha, y_\beta \in \mathbb{N} \quad \forall\alpha,\beta \in \{0, 1, \ldots, D\}$. The way how this is done may depend on the theory of $A \otimes x = b$ over the semiring in question. It is known that for the tropical (max-plus) semiring, the max-min semiring and, more generally, for any max-$T$ semiring where $T$ is a continuous $T$-norm, the system $A \otimes x = b$ has the greatest solution, a finite number of minimal solutions and each solution to $A \otimes x = b$ lies in the box defined by one of the minimal solutions and the greatest solution. For the attacker's puproses, we need to search for a vector $(z_{\alpha\beta})$ in the box defined by one of the minimal solutions and the greatest solution that satisfies $z_{\alpha\beta} = x_\alpha \otimes y_\beta$ for some $x_\alpha, y_\beta$. A formal description of the attack is due to Kotov and Ushakov [12] in the tropical case, and a max-min version (which has a straightforward generalization to the max-$T$ case) was suggested in [3].

Different variants of the Stickel protocol (protocol 1) can be implemented using alternative "classes" of commuting matrices. A number of these alternatives are explored in the literature (e.g., [15]). For these protocols using other kinds of commuting matrices, matrix powers can be replaced with other generators, although this may require imposing some mild constraints on the coefficients $x_\alpha, y_\beta$, and hence a generalized version of Kotov-Ushakov attack still applies [15]. Formally, $X$ and $Y$ are instead expressed as

$$X = \bigoplus_{\alpha \in \mathcal{A}} (x_\alpha \otimes A_\alpha), Y = \bigoplus_{\beta \in \mathcal{B}} (y_\beta \otimes B_\beta), \tag{4}$$

Here $\{A_\alpha : \alpha \in A\}$ and (respectively) $\{B_\beta : \beta \in B\}$ are finite sets of matrices such that any matrix that can be used by Alice and (respectively) by Bob can be represented as these $X$ and $Y$. The rest of the attack similarly follows, but may include additional conditions on the coefficients $x_\alpha, y_\beta$.

Note that Kotov-Ushakov attack and its generalization [15] are guaranteed to succeed under the (not too restrictive) condition that any matrix used by Alice or Bob can be represented as linear combination of generators in $\mathcal{A}$ and $\mathcal{B}$; for a detailed proof, refer to [15]. However, a significant limitation of these attacks is that they require scanning the entire solution set of the underlying linear system, which involves finding all minimal solutions. As Alice and Bob use polynomials of higher degree (or larger $\mathcal{A}, \mathcal{B}$ in the case of the generalized Kotov-Ushakov attack), the number of minimal solutions in this system grows exponentially, resulting in a corresponding exponential increase in the attack's computational complexity. One way to circumvent this is to seek a particular minimal solution and then hope that the box defined by such solution and the greatest solution contains a solution of the desired structure. Then the resulting attack is of a polynomial time complexity, but the success rate of it may suffer. The heuristic attacks of such type were put forward by Mach [14] and in [1]. In the latter work it was found that a heuristic attack of this kind had 100% success rate when applied to the tropical Stickel protocol based on modified circulants and over 90% success rate when applied to the initial tropical Stickel protocol based on polynomials (the success of a similar attack in the max-min case was, however, much more modest [3]).

Recently, the authors in [16] came up with a better idea to attack the various versions of tropical Stickel protocols, which we next outline. Instead of searching for a special solution of system (3) among all possible solutions—the approach employed in the Kotov-Ushakov attack—it can be observed that any solution $(r_{\alpha\beta})$ to (3) suffices to break the protocol. Indeed, recalling that $V = q_1(A) \otimes W \otimes q_2(B)$ and using the commutation between $A^{\otimes\alpha}$ and $q_1(A)$ on one side and the commutation between $B^{\otimes\beta}$ and $q_2(B)$ on the other side we obtain that for any solution $(r_{\alpha\beta})$ to system (3), the shared secret key $K$ can be recovered by

$$K = \bigoplus_{\alpha,\beta=0}^{D} r_{\alpha\beta} \otimes A^{\otimes\alpha} \otimes V \otimes B^{\otimes\beta}. \tag{5}$$

To prove that, we simply need to verify whether this formula successfully recovers the

key. Given that $(r_{\alpha\beta})$ is any solution to (3), we have

$$\begin{aligned} K &= \bigoplus_{\alpha,\beta=0}^{D} r_{\alpha\beta} \otimes A^{\otimes\alpha} \otimes q_1(A) \otimes W \otimes q_2(B) \otimes B^{\otimes\beta} \\ &= \bigoplus_{\alpha,\beta=0}^{D} r_{\alpha\beta} \otimes q_1(A) \otimes A^{\otimes\alpha} \otimes W \otimes B^{\otimes\beta} \otimes q_2(B) \\ &= q_1(A) \otimes (\bigoplus_{\alpha,\beta=0}^{D} r_{\alpha\beta} \otimes A^{\otimes\alpha} \otimes W \otimes B^{\otimes\beta}) \otimes q_2(B) \\ &= q_1(A) \otimes U \otimes q_2(B) = K_b = K_a. \end{aligned}$$

This attack significantly reduces the burden on the attacker by eliminating the need to explore the entire solution set of system (3). Instead, any solution can be utilized. The new attack is formally described in the following algorithm.

**Attack 1** (Attacking Protocol 1 based on (5))**.**

1. Find a solution $r_{\alpha\beta}$ of system (3).
2. Compute the shared secret key $K$.

$$K = \bigoplus_{\alpha,\beta=0}^{D} r_{\alpha\beta} \otimes A^{\otimes\alpha} \otimes V \otimes B^{\otimes\beta}.$$

In the tropical case, as well as in the max-min case and, more generally, for max-$T$ semirings with lower-semicontinuous $T$-norms [3], [5], the greatest solution of system (3) can be easily found using an explicit formula and used in Attack 1. Note that the authors in [16] also give algebraic conditions for semirings over which (3) has the greatest solution that is easily computed by an explicit formula. Furthermore, for max-$T$ semirings with upper-semicontinuous $T$-norms one can find a minimal solution [5] and also use it in Attack 1. Although this may require more time than finding the greatest solution for which there is an explicit formula, it is still better than the Kotov-Ushakov attack where one needs to use a number of minimal solutions and the greatest solution.

Figure 1 compares the performance of the Kotov-Ushakov attack and this new attack (Attack 1) on the initial tropical Stickel protocol using the greatest solution to (3) with matrix dimensions of 10 and a range of polynomial degrees. As expected, the computational time of the Kotov-Ushakov attack increases exponentially due to the rapid growth of minimal solutions (enumerated minimal covers) with respect to the used polynomial degree. In contrast, the increase in computational time for the new attack remains relatively small. Note that at lower polynomial degrees, the two attacks show comparable performance, as the computational heavy part in the Kotov-Ushakov attack (enumerating all minimal covers) is not yet dominant.

Figure 2 also shows the computational time of this new attack and one of the previously proposed heuristics, namely the single cover heuristic from [1]. This may highlight that heuristic attacks can remain valuable, especially when they achieve high success rates, due to their higher efficiency when compared with the guaranteed attacks.

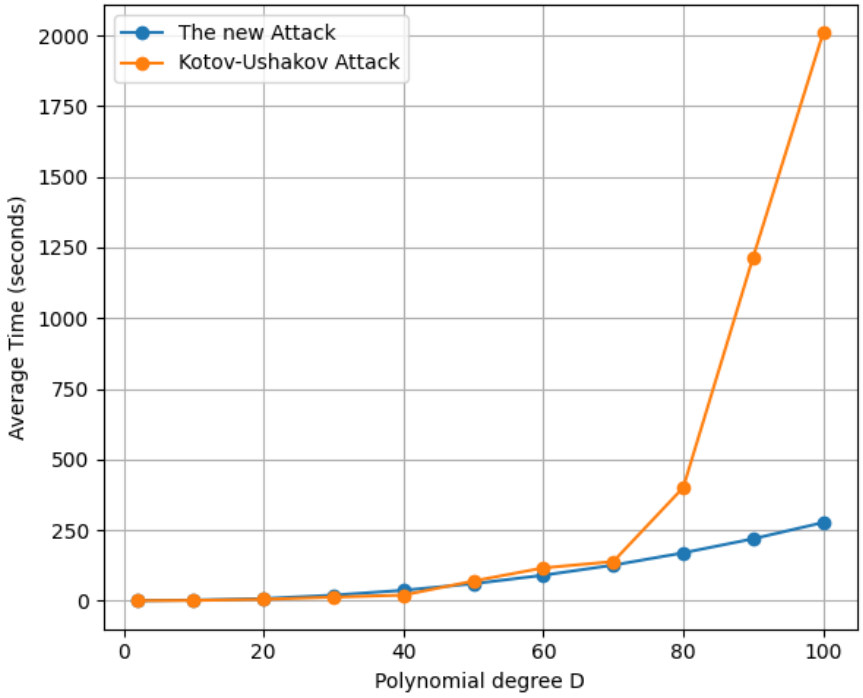


Figure 1: Computational time of Attack 1 vs. Kotov-Ushakov attack

The new attack also works for some other implementations of Stickel protocol such as the ones based on the modified circulants and Jones matrices [10], [15]. However, if Alice and Bob use a different implementation of Stickel protocol for which $A_\alpha$ in (4) do not commute with the matrices used by them on the left and/or $B_\beta$ do not commute with the matrices used by them on the right, then the Kotov-Ushakov attack is still guaranteed to work and the new attack becomes a heuristic. The next section will discuss the tropical Stickel protocol based on Linde-de la Puente matrices (shortly LdlP matrices) for which this is the case.

# 3 Security analysis of tropical Stickel protocol based on Linde-de la Puente matrices

The tropical Stickel protocol based on Linde-de la Puente matrices closely resembles the original tropical implementation in [8], but replaces tropical polynomials with matrices of the form $[2r, r]_n^k$ as introduced in [15]. We firstly introduce the concept of elementary matrices, which will serve as the generators $A_\alpha$ and $B_\beta$ in the tropical Stickel protocol based on LdlP matrices.

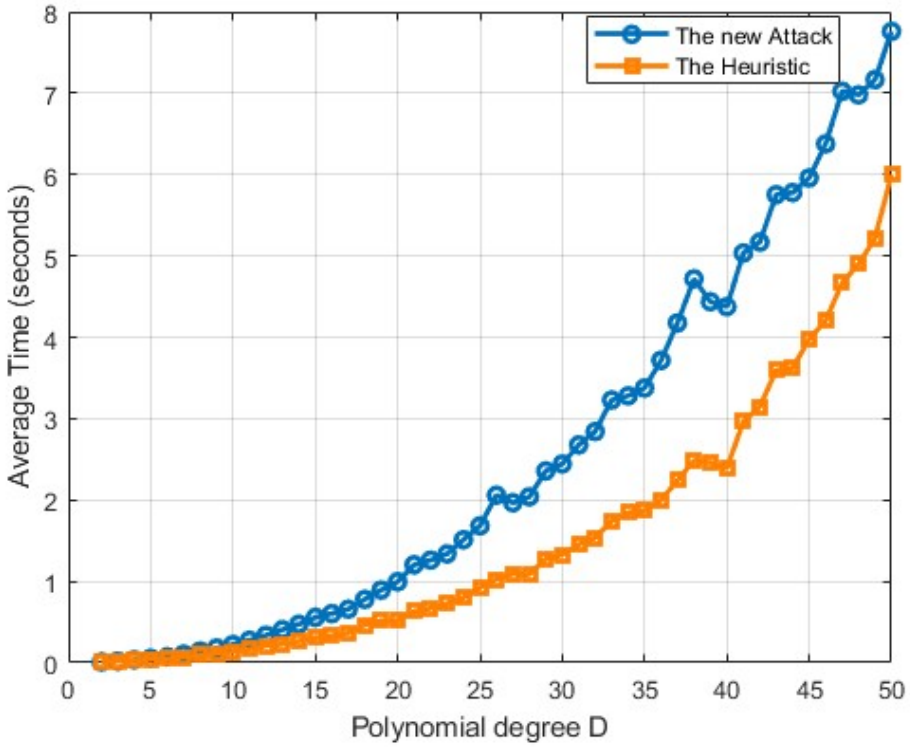


Figure 2: Computational time of Attack 1 vs. the heuristic attack in [1]

**Definition 3.1** (Tropical Elementary Matrices)**.** Let $E^{ij} \in \mathbb{R}_{\max}^{n\times n}$ be a matrix with entries

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

for $i, j \in [n]$ and $k, l \in [n]$. Any matrix of this form is called a tropical elementary matrix.

Let us then present the definition of LdlP matrices.

**Definition 3.2** ([15], generalizing [13])**.** 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 $i \neq j$.

Note that any two matrices of this form commute due to the following theorem.

**Theorem 3.1** (LdlP Matrices Commutativity [15])**.** *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*

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

Let us observe that Linde-de la Puente matrices also allow for semiring generalizations. Consider any semiring with idempotent addition ($a \oplus a = a$) in which the order $\leq$ is defined canonically ($a \oplus b = b \Leftrightarrow a \leq b$), the property $a \otimes b \leq a^{\otimes 2} \oplus b^{\otimes 2}$ holds and in which there

exists at least one element $a$ with $a^{\otimes 2} \leq a$. In particular, the property $a \otimes b \leq a^{\otimes 2} \oplus b^{\otimes 2}$ (to which we further refer as to the *squares property*) holds in commutative semirings with cancellative condition ($a \otimes b = a \otimes c$ and $a \neq \mathbf{0}$ implies $b = c$) as shown in [6]. The latter condition is sufficient but not necessary: for example, the max-min semiring also satisfies the squares property without being cancellative. Then we can modify the above definition to the following one. Here and below, $\mathbf{0}$ and $\mathbf{1}$ will denote the zero and the unity elements of the semiring.

**Definition 3.3.** For arbitrary element $r$ such that $r^{\otimes 2} \leq r$ we denote by $[r^{\otimes 2}, r]_n$ the set of matrices $A$ such that $a_{ii} = \mathbf{1}$ for all $i$ and $r^{\otimes 2} < a_{ij} < r$ for $i \neq j$.

Let us show that any two matrices of this form commute, adopting and generalizing an argument of [13].

**Theorem 3.2** (LdlP Matrices Commutativity over Semirings)**.** *Consider an idempotent semiring in which the squares property holds, and let $A \in [r^{\otimes 2}, r]_n, B \in [s^{\otimes 2}, s]_n$ for any $r, s$ such that $r^{\otimes 2} \leq r$ and $s^{\otimes 2} \leq s$. Then*

$$A \otimes B = B \otimes A = A \oplus B$$

*Proof.* We observe that $(A \otimes B)_{ik}$ can be written as

$$\bigoplus_j a_{ij} \otimes b_{jk} = a_{ik} \oplus b_{ik} \oplus \bigoplus_{j \neq i,k} a_{ij} \otimes b_{jk} \tag{6}$$

Then, note that

$$a_{ij} \otimes b_{jk} \leq r \otimes s \leq r^{\otimes 2} \oplus s^{\otimes 2} \leq a_{ik} \oplus b_{ik},$$

implying that $(A \otimes B)_{ik} = a_{ik} \oplus b_{ik}$, and $(B \otimes A)_{ik} = b_{ik} \oplus a_{ik}$ can be shown similarly. □

As written above, the max-min semiring satisfies the squares property and therefore the above theorem holds for LdlP matrices over it. However, here we have $a^{\otimes 2} = a$ for all $a$, which trivializes the class of LdlP matrices making it less attractive for cryptographic purposes. We can also consider the max-$T$ semiring with $T$ being the Hamacher product. It can be shown that the Hamacher product is commutative and cancellative and therefore the squares property holds in the max-Hamacher semiring. Furthermore, the intervals $(a^{\otimes 2}, a)$ are non-empty for any $a\colon 0 < a < 1$ (we have $\mathbf{0} = 0$ and $\mathbf{1} = 1$ in any max-$T$ semiring).

The protocol that utilizes the commutativity property of LdLP matrices over tropical semiring is outlined below. Its generalization to commutative idempotent semirings satisfying the squares property ($a \otimes b \leq a^{\otimes 2} \oplus b^{\otimes 2}$) is also obvious, but we will restrict our cryptanalysis to the tropical case in what follows.

**Protocol 2** (Tropical Stickel Protocol based on LdlP matrices [15])**.**

1. Alice and Bob agree on a public matrix $W \in \mathbb{R}_{\max}^{n \times n}$.
2. Alice chooses two random matrices $A_1$ and $A_2$, where $A_1 \in [2a_1, a_1]_n^{k_1}$ and $A_2 \in [2a_2, a_2]_n^{k_2}$ such that $a_1, a_2 \leq 0$ and $k_1, k_2 \geq 0$ and sends $U = A_1 \otimes W \otimes A_2$ to Bob.

3. Bob chooses two random matrices $B_1$ and $B_2$, where $B_1 \in [2b_1, b_1]_n^{l_1}$ and $A_2 \in [2b_2, b_2]_n^{l_2}$ such that $b_1, b_2 \leq 0$ and $l_1, l_2 \geq 0$ and sends $V = B_1 \otimes W \otimes B_2$ to Bob.

4. Alice computes her secret key using a public key $V$ obtained from Bob, which is $K_a = A_1 \otimes V \otimes A_2$.

5. Bob also computes his secret key using Alice's public key $U$, which is $K_b = B_1 \otimes U \otimes B_2$.

The two parties end up with an identical key due to the commutativity of Linde-de la Puente matrices. Formally, we have $K_a = A_1 \otimes V \otimes A_2 = A_1 \otimes B_1 \otimes W \otimes B_2 \otimes A_2 = B_1 \otimes A_1 \otimes W \otimes A_2 \otimes B_2 = B_1 \otimes U \otimes B_2 = K_b$.

Given that the new attack (Attack 1) is not guaranteed to succeed against this protocol, we firstly analyze the effectiveness of both this attack and the Kotov-Ushakov attack (or more precisely their generalized forms). Subsequently, we evaluate other heuristic attacks that have previously demonstrated promising results against other tropical implementations of the Stickel protocol. For all numerical experiments, unless stated otherwise, the values of $k_1, k_2, l_1, l_2$ are chosen randomly from $[0, 100]$, while $a_1, a_2, b_1, b_2$ are selected from $[-100, 0]$, and the entries of $W$ are from $[-100, 100]$.

- **Kotov-Ushakov attack**
  Lets firstly describe a generalized version of Kotov-Ushakov attack that applies to this protocol followed by an evaluation of its performance. Note that any matrix $A \in [2a, a]_n^k$ chosen in the protocol can be represented as a tropical linear combination of elementary matrices with some restrictions on the coefficients $(x, y)$. Therefore, to break the protocol, we need to find

$$X = \bigoplus_{i,j=0}^{n} \left(x_{ij} \otimes E^{ij}\right), Y = \bigoplus_{s,t=0}^{n} \left(y_{st} \otimes E^{st}\right),$$

  Then, Alice's message $U$ can be expressed as

$$U = \bigoplus_{i,j=0}^{n} \left(x_{ij} \otimes E^{ij}\right) \otimes W \otimes \bigoplus_{s,t=0}^{n} \left(y_{st} \otimes E^{st}\right),$$

  or equivalently

$$\bigoplus_{i,j,s,t}^{n} x_{ij} \otimes y_{st} \otimes \left(E^{ij} \otimes W \otimes E^{st}\right) = U.$$

  We then denote $R^{ijst} = E^{ij} \otimes W \otimes E^{st}$ and therefore we can write

$$\bigoplus_{i,j,s,t=0}^{n} x_{ij} \otimes y_{st} \otimes \left(R^{ijst}\right)_{\gamma\delta} = U_{\gamma\delta} \quad \forall \gamma, \delta \in [n] \times [n]. \tag{7}$$

  If we additionally denote $z_{ijst} = x_{ij} \otimes y_{st}$, we have

$$\bigoplus_{i,j,s,t=0}^{n} z_{ijst} \otimes \left(R^{ijst}\right)_{\gamma\delta} = U_{\gamma\delta} \quad \forall \gamma, \delta \in [n] \times [n]. \tag{8}$$

We then similarly scan the whole solution of this tropical linear system searching for an appropriate solution through the following attack.

**Attack 2** (Kotov-Ushakov attack on tropical Stickel protocol based on LdlP matrices [15])**.**

1. Compute

$$c_{ijst} = \min_{\gamma,\delta\in[n]} \left(U_{\gamma\delta} - R^{ijst}_{\gamma\delta})\right), \quad S_{ijst} \ = \arg\min_{\gamma,\delta\in[n]} \left(U_{\gamma\delta} - R^{ijst}_{\gamma\delta})\right).$$

2. Among all minimal covers of $[n] \times [n]$ by $S_{ijst}$, that is, all minimal subsets $\mathcal{C} \subseteq [n^2] \times [n^2]$ such that

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

find a cover for which the system

$$\begin{aligned}
&x_{ij} + y_{st} = c_{ijst}, \quad \text{if } (i,j,s,t) \in \mathcal{C},\\
&x_{ij} + y_{st} \leqslant c_{ijst}, \quad \text{if otherwise.}\\
&2a_1 \leqslant x_{ij} \leqslant a_1, \quad 2a_2 \leqslant y_{st} \leqslant a_2, \quad \forall i \neq j, \quad s \neq t,\\
&x_{ii} = k_1, \quad y_{ss} = k_2, \quad \forall i, s,\\
&a_1, a_2 \leqslant 0, \quad k_1, k_2 \geq 0.
\end{aligned} \tag{9}$$

is solvable.

Figure 3 illustrates the computational time required to execute Attack 2, showing that the attack is impractical due to the excessively high time consumption, even for relatively low-dimensional cases. This inefficiency arises from the extremely high number of minimal covers, which happens because each $S_{ijst}$ contains only one element (as $R^{ijst}$ has only a single finite element). As a result, the total number of minimal covers becomes $(n^2)^{n^2}$, since each entry is covered by $n^2$ components. Specifically, for each $(\gamma, \delta) \in [n] \times [n]$, there are $n^2$ sets $S_{ijst}$ that satisfy $(\gamma, \delta) \in S_{ijst}$.

- **The greatest solution attack**

We now explore the applicability of an analogous version of Attack 1, which leverages the greatest solution of system (8) to break the protocol. The attack follows a similar structure, which involves finding the greatest solution to system (8), followed by the key recovery formula.

**Attack 3** (The greatest solution attack on tropical Stickel protocol based on LdlP matrices)**.**

1. Compute the greatest solution $(c_{ijst})$ of system (8).

$$c_{ijst} = \min_{\gamma,\delta\in[n]} \left(U_{\gamma\delta} - R^{ijst}_{\gamma\delta})\right) \quad \forall i,j,s,t \in [n].$$

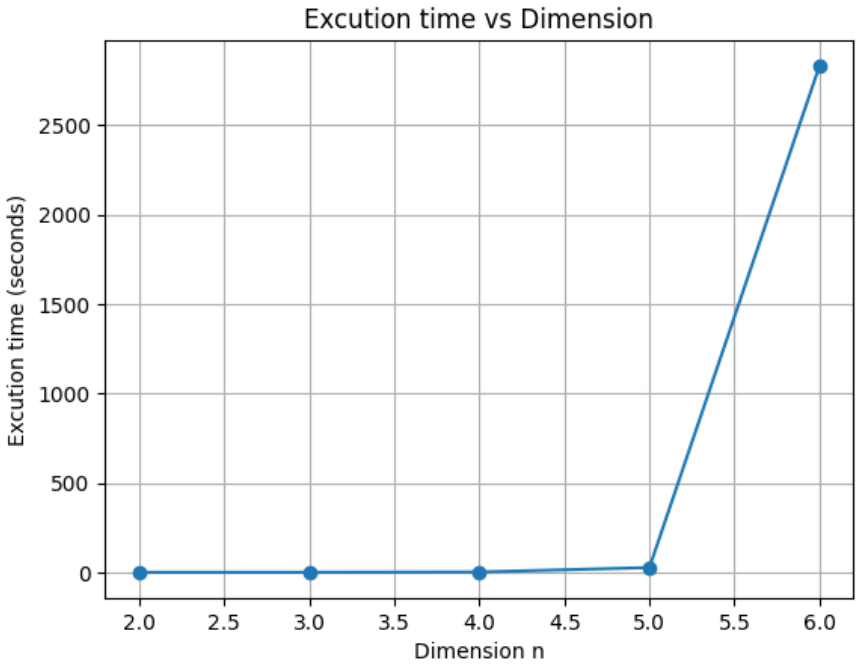


Figure 3: Computional time of Attack 2

2. Compute the shared secret key $K$.

$$K = \bigoplus_{i,j,s,t=0}^{n} c_{ijst} \otimes E^{ij} \otimes V \otimes E^{st}.$$

Although the attack is unlikely to succeed generally since the protocol violates the generators' commutativity condition, we investigate how frequently it does. Figure 4 shows the observed success rate. The attack showed high success rate with smaller $W$ values, but its success rate rapidly approaches zero as $W$ becomes sufficiently large.

- **The single cover heuristic attack**
Kotov and Ushakov observed in their experiment [12] that smaller minimal covers are significantly more likely to "work". A heuristic attack that construct a small sized single minimal cover by iteratively selecting the largest $S_{\alpha\beta}$ until all elements of $[n] \times [n]$ are covered showed to be highly effective against multiple implementations of the Stickel protocol [1]. An adaptation of this attack on protocol 2 is described in Attack 4.

**Attack 4** (The single minimal cover heuristic on tropical Stickel protocol based on LdlP matrices)**.**

1. Compute

$$c_{ijst} = \min_{\gamma,\delta\in[n]} \left(U_{\gamma\delta} - R^{ijst}_{\gamma\delta})\right), \quad S_{ijst} = \arg\min_{\gamma,\delta\in[n]} \left(U_{\gamma\delta} - R^{ijst}_{\gamma\delta})\right).$$

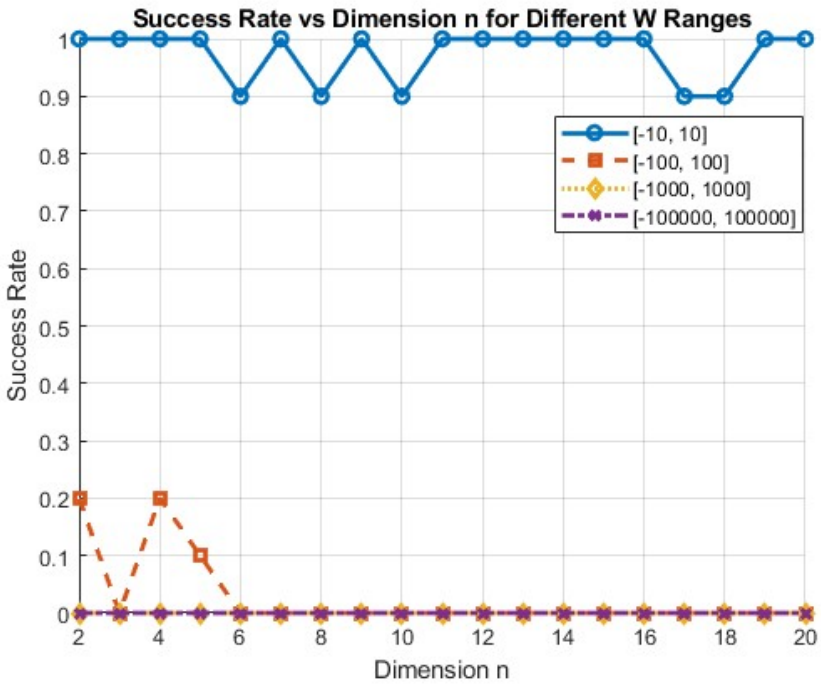


Figure 4: Success rate of Attack 3

2. For each uncovered $(\gamma, \delta) \in [n] \times [n]$, select the largest $S_{ijst}$ that includes it, and add the indices $i, j, s, t$ to the cover.
3. Solve the system

$$\begin{aligned}
&x_{ij} + y_{st} = c_{ijst}, \quad \text{if } (i,j,s,t) \text{ is in the cover,}\\
&x_{ij} + y_{st} \leqslant c_{ijst}, \quad \text{if otherwise,}\\
&2a_1 \leqslant x_{ij} \leqslant a_1, \quad 2a_2 \leqslant y_{st} \leqslant a_2, \quad \forall i \neq j, \quad s \neq t,\\
&x_{ii} = k_1, \quad y_{ss} = k_2, \quad \forall i, s,\\
&a_1, a_2 \leqslant 0, \quad k_1, k_2 \geq 0.
\end{aligned}$$

Figure 5 shows the success rate of this attack, which performs poorly probably due to the fact that all minimal covers of system (8) are of equal size (specifically $n^2$ since each $S_{ijst}$ contains only a single element). As a result, there is no smaller cover that offers a higher probability of solving the linear system (9). Additionally, the large number of minimal covers,as explained in the generalized Kotov-Ushakov attack (Attack 2), probably further reduces the likelihood of finding an appropriate cover.

- **Tropical Shpilrain attack**
We now explore the effectiveness of the tropical version of Shpilrain attack [17], building on the approach outlined in [2]. Similar to the other heuristics, this attack aims to avoid the impracticality of the guaranteed attack (Attack 2). The objective of the attack is to find $X$ and $Y$ such that

$$X \otimes W \otimes Y = U$$

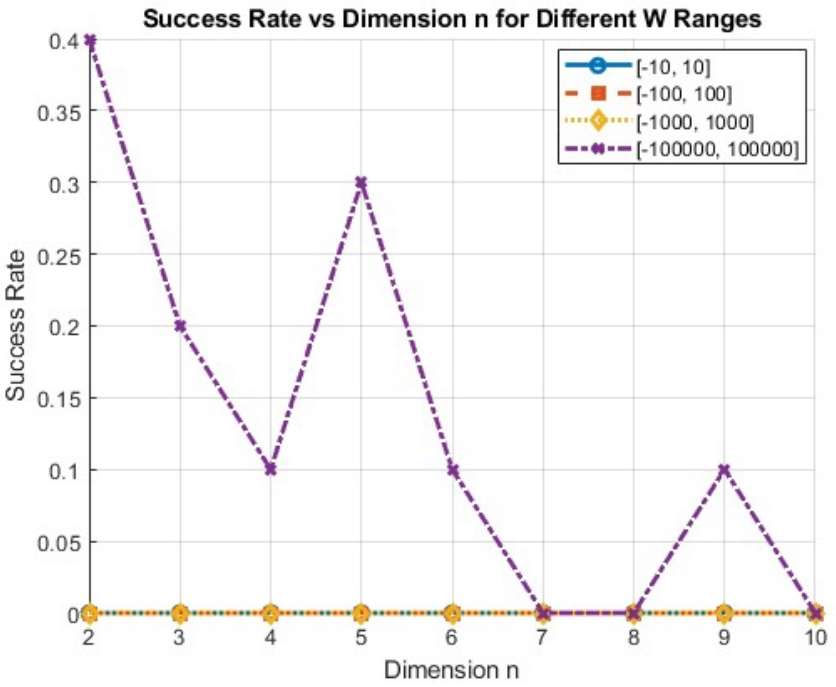


Figure 5: Success rate of Attack 4

where $X$ and $Y$ follow the forms of $[2a_1, a_1]_n^{k1}$ and $[2a_2, a_2]_n^{k2}$ respectively. Then, a Mixed-Integer Linear Program (MILP) can be formulated by converting the disjunctive constraints into linear constraints with Boolean variables [4], and solved using a MILP solver (e.g. [9]). In particular, with $x_{ij}, w_{ij}, y_{ij}$ and $u_{ij}$ being respectively the entries of $X, W, Y$ and $U$, we have

$$\max_{k,l\in[n]}(x_{ik} \otimes w_{kl} \otimes y_{lj}) = u_{ij} \quad \forall (i,j) \in [n] \times [n],$$

which can be represented as the following set of inequalities

$$x_{ik} \otimes w_{kl} \otimes y_{lj} \leq u_{ij} \quad \forall i,j,k,l \in [n],$$

and with $M$ being a sufficiently large number

$$x_{ik} \otimes w_{kl} \otimes y_{lj} + (1 - z_{klij})M \geq u_{ij} \quad \forall i,j,k,l \in [n],$$

$$\sum_k z_{klij} = 1, \quad z_{kij} \in \{0,1\} \quad \forall i,j,k,l \in [n].$$

The details of the attack is described below in Attack 5.

**Attack 5** (Shpilrain attack on tropical Stickel protocol based on LdlP matrices)**.**

Solve the following system using a MILP solver

$$
\begin{aligned}
&x_{ik} + w_{kl} + y_{lj} \leq u_{ij} \quad \forall i, j, k, l \in [n], \\
&x_{ik} + w_{kl} + y_{lj} + (1 - z_{klij})M \geq u_{ij} \quad \forall i, j, k, l \in [n], \\
&z_{5klij} \in \{0, 1\}, \\
&\sum_{k,l} z_{klij} = 1 \quad \forall i, j \in [n],
\end{aligned}
$$

$$
\begin{aligned}
&2a_1 \leqslant x_{ij} \leqslant a_1, \quad 2a_2 \leqslant y_{st} \leqslant a_2, \quad \forall i \neq j, \quad s \neq t, \\
&x_{ii} = k_1, \quad y_{ss} = k_2, \quad \forall i, s, \\
&a_1, a_2 \leqslant 0, \quad k_1, k_2 \geq 0.
\end{aligned}
$$

This attack has a perfect success rate and shows significantly better time efficiency compared to the Kotov-Ushakov attack (Attack 2), as shown in Figure 6. However, one major limitation of this attack is its high memory usage, which increases with the dimension. The attack demands a substantial amount of memory to encode all the required equations, and in environments like Matlab, it becomes impractical for dimensions larger than 13. Specifically, the attack requires encoding $2n^4+n^2$ equations with $n^4 + 2n^2 + 4$ variables. This also shows that Protocol 2 offers greater resistance to the Shpilrain attack compared to the initial tropical implementation (Protocol 1) since the computational time of the attack increases with the dimension, while in the initial implementation, the attack time remains unchanged, as it does not depend on the polynomial degrees used in the protocol as presented in [2].

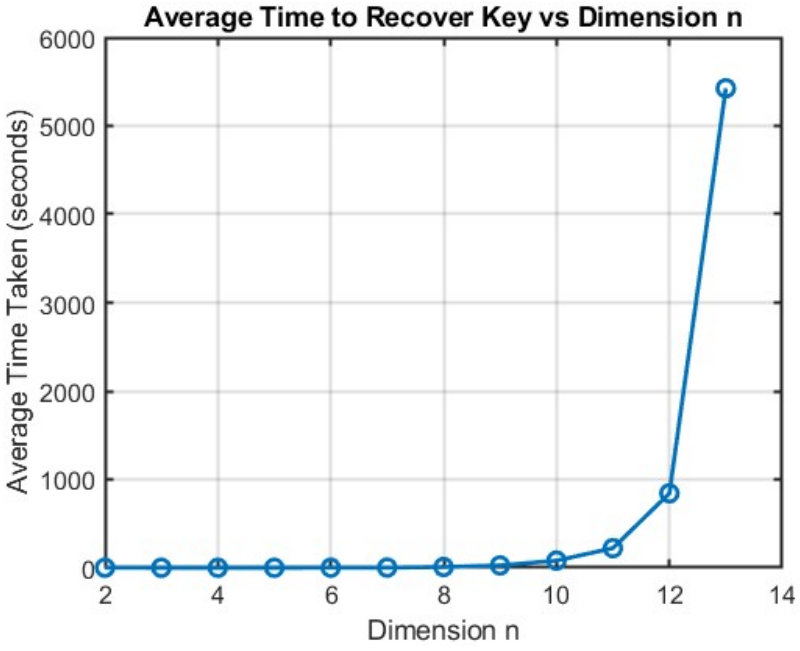


Figure 6: Computational time of Attack 5

- **Vanishing and dominant $W$ heuristic attacks**
  It is occasionally possible to recover the shared secret key using only the public parameters by leveraging the theory of vanishing or dominant $W$, as outlined in [15], when applicable. The two heuristic approaches for this are illustrated in the following two attacks, where $w_{st}$ denotes the largest entry in $W$.

  **Attack 6** (Vanishing $W$ attack on tropical Stickel protocol based on LdlP matrices)**.**

  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 the key $K$ as $K = l_1 \otimes l_2 \otimes U \oplus k_1 \otimes k_2 \otimes V$.

  **Attack 7** (Dominant $W$ attack on tropical Stickel protocol based on LdlP matrices)**.**

  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 the key $K$ as $K_{ij} = -w_{st} \otimes (v_{st} \otimes u_{ij} \oplus u_{st} \otimes v_{ij} \oplus u_{it} \otimes v_{sj} \oplus v_{it} \otimes u_{sj})$.

  The success rate of the two attacks is illustrated in Figure 7. A notable trend is observed: when one attack performs poorly, the other tends to perform well across different ranges of $W$. As a result, the overall combined success rate is generally high. However, there are specific ranges of $W$ where both attacks underperform, suggesting that Alice and Bob can still effectively resist these two heuristics by carefully selecting certain values of $W$. For example, Figure 8 highlights a range of $W$ where the performance of both attacks noticeably weakens.

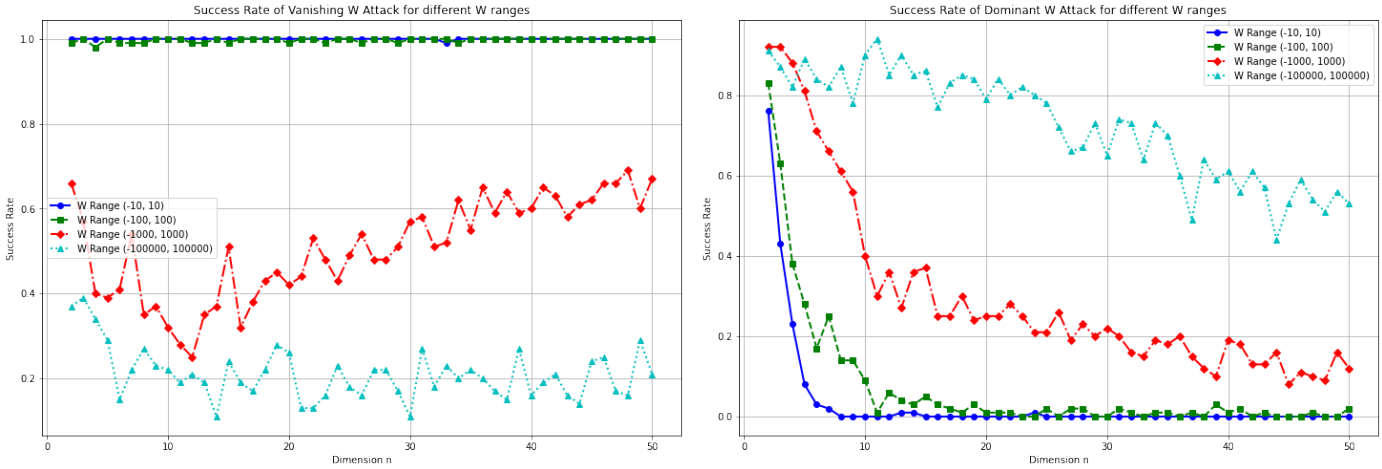


Figure 7: Success rate of Attack 6 and Attack 7

# 4 Conclusion

The Kotov-Ushakov attack could now be considered largely obsolete by the introduction of the new attack (Attack 1), which can replace it to attack various implementations of the Stickel protocol. However, the Kotov-Ushakov may still be valuable against some variants

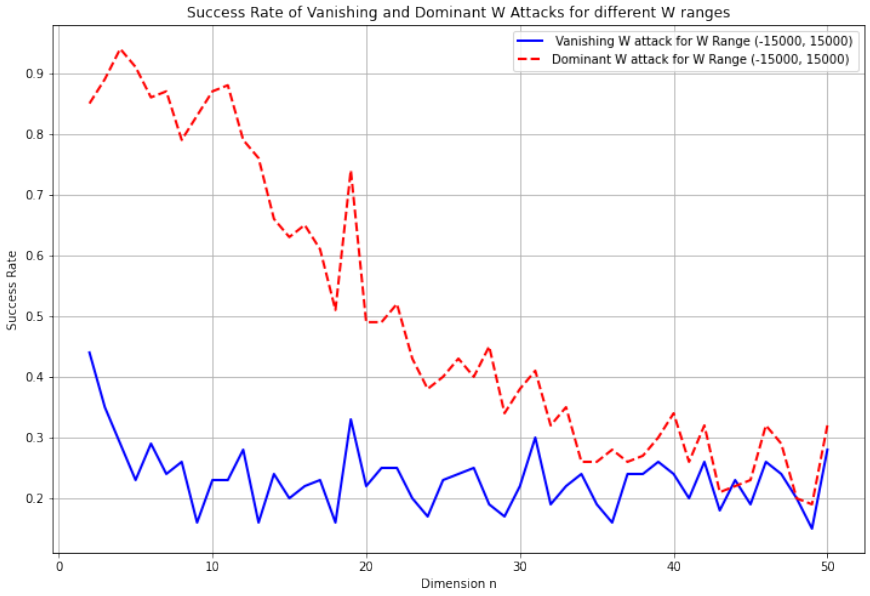


Figure 8: Suboptimal performance of Attack 6 and Attack 7

that are resistant to the new attack, though it would likely be inefficient due to the significant computations involved in enumerating all solutions of the underlying linear system. For the Kotov-Ushakov attack to remain relevant, new classes of commuting matrices over semirings have to be found. For such cases, the Kotov-Ushakov attack might be the only feasible attack.

While Attack 1 offers a clear advantage over the Kotov-Ushakov attack, it still encounters some of the same challenges. Firstly, in the case of the Stickel protocol based on polynomials, Alice and Bob can use sparse polynomials with sufficiently large degree $D$. This is especially easy for them in the case of the implementation based on Jones matrices [10, 15] since they would use rational exponents with high denominator, and the corresponding deformations $A^{(\alpha)}$ and $B^{(\beta)}$ are easy to compute. Secondly, there may still exist semirings over which $A \otimes x = b$ is hard to solve, and in such cases, the new attack is not applicable. Identifying such semirings, however, requires further exploration.

In the case of the tropical semiring, the Stickel protocol based on LdlP matrices resists the new attack. It also resists the Kotov-Ushakov attack, primarily due to its impracticality as it requires enumerating an exceedingly high number of minimal solutions in this case. Moreover, other heuristic attacks that previously demonstrated promising results against other variants of Stickel protocol showed only limited success here. This indicates that the tropical Stickel protocol based on LdlP matrices requires further cryptanalysis to validate its resistance. If so, this could indicate that tropical cryptography still holds potential and may remain a viable platform for implementing secure cryptographic key exchange protocols.

# References


[1] S. Alhussaini, C. Collett, and S. Sergeev. Generalized Kotov-Ushakov attack on tropical Stickel protocol based on modified tropical circulant matrices. Cryptology ePrint Archive, Paper 2023/1904, 2023. `https://eprint.iacr.org/2023/1904`.

[2] S. Alhussaini and S. Sergeev. Attacking tropical Stickel protocol by MILP and heuristic optimization techniques. Cryptology ePrint Archive, Paper 2024/1169, 2024. `https://eprint.iacr.org/2024/1169`.

[3] S. Alhussaini and S. Sergeev. On implementation of Stickel's key exchange protocol over max-min and max-$T$ semirings. Cryptology ePrint Archive, Paper 2024/519, 2024. `https://eprint.iacr.org/2024/519`.

[4] B. De Schutter, W.P.M.H. Heemels, and A. Bemporad. On the equivalence of linear complementarity problems. *Operational Research Letters*, 30(4):211–222, 2002.

[5] A. Di Nola, W. Pedrycz, and S. Sessa. Fuzzy relation equations under LSC and USC $t$-norms and their Boolean solutions. *Stochastica*, 11(2-3), 1987.

[6] P. I. Dudnikov and S. N. Samborskiĭ. Endomorphisms of finitely generated free semimodules. In V.P. Maslov and S.N. Samborskiĭ, editors, *Advances in Soviet Mathematics*, volume 13 of *Contemporary Mathematics*, pages 65–85. AMS, 1992.

[7] J.S. Golan. *Semirings and their Applications*. Springer, 2000.

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

[9] Gurobi Optimization, LLC. Gurobi Optimizer Reference Manual, 2023.

[10] D. Jones. *Special and structured matrices in max-plus algebra*. Phd thesis, University of Birmingham, 2017.

[11] G.J. Klir and B. Yuan. *Fuzzy Sets and Fuzzy Logic. Theory and Applications*. Prentice Hall, 1995.

[12] 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.

[13] J. Linde and M.J. de la Puente. Matrices commuting with a given normal tropical matrix. *Linear Algebra and its Applications*, 482:101–121, 2015.

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

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

[16] Á. Otero Sánchez, D. Camazón Portela, and J.A. López-Ramos. On the solutions of linear systems over additively idempotent semirings. *Mathematics*, 12(18), 2024.

[17] V. Shpilrain. Cryptanalysis of Stickel's key exchange scheme. In E.A. Hirsch, A.A. Razborov, A. Semenov, and A. Slissenko, editors, *Computer Science - Theory and Applications*, volume 5010 of *LNTCS*, pages 283–288. Springer, 2008.

[18] E. Stickel. A new method for exchanging secret keys. In *Third International Conference on Information Technology and Applications (ICITA'05)*, volume 2, pages 426–430, 2005.

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

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