Attacking Tropical Stickel Protocol by MILP and Heuristic Optimization Techniques

Sulaiman Alhussaini and Sergeĭ Sergeev

Abstract

Known attacks on the tropical implementation of Stickel protocol involve solving a minimal covering problem, and this leads to an exponential growth in the time required to recover the secret key as the used polynomial degree increases. Consequently, it can be argued that Alice and Bob can still securely execute the protocol by utilizing very high polynomial degrees, a feasible approach due to the efficiency of tropical operations. The same is true for the implementation of Stickel protocol over some other semirings with idempotent addition (such as the max-min or fuzzy semiring). In this paper, we propose alternative methods to attacking Stickel protocol that avoid this minimal covering problem and the associated exponential time complexity. These methods involve framing the attacks as a mixed integer linear programming (MILP) problem or applying certain global optimization techniques.

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

1 Introduction

A key exchange protocol is a process where two parties, commonly referred to as Alice and Bob, collaboratively generate a shared secret key using public information and messages exchanged over a public channel. The security of a protocol is determined by its ability to prevent an attacker from easily recovering the shared secret key using these public information and intercepted messages, typically by ensuring that the attacker must solve a computationally hard problem to succeed. These protocols often rely on various algebraic tools to achieve the desired security properties.

Polynomials over the tropical (max-plus) semiring are one of the recent tools utilized in key exchange protocols, appearing inthe tropical implementation of the Stickel protocol proposed by Grigoriev and Shpilrain [6]. This new implementation followed Shpilrain's successful attack [13] on the initial Stickel protocol [14] and has become one of the most popular key exchange protocols utilizing tropical operations. The rationale behind suggesting a tropical implementation of the protocol was to avoid obvious attacks involving linear algebra and matrix inverses, which were effective against the original protocol. The Stickel

protocol can be similarly implemented over any semiring, and its implementation over max-min and max-T semirings (where the symbol T stands for arbitrary T-norm [8]) is analyzed in [2].

Kotov and Ushakov [9] later suggested an attack on the tropical Stickel protocol by transforming the underlying problem into finding a special solution to the protocol's associated system of equations of the form $A \otimes x = b$. Despite this, the attacker still faces a significant challenge: solving a minimal covering problem to find a minimal cover that satisfies certain conditions. Therefore, this approach is less effective when Alice and Bob use high-degree polynomials, which can be efficiently managed by Alice and Bob with minimal computational resources due to the efficient nature of tropical operations. An analogue of the Kotov-Ushakov attack against the max-min and, more generally, max-T implementations of the Stickel protocol can be similarly proposed [2]. However, it encounters a similar challenge of finding a minimal solution with special properties, resulting in an exponential increase in complexity.

The main idea of this paper is to introduce alternative attack strategies that avoid the hard problem or exponential complexity encountered in the conventional Kotov-Ushakov attack. Specifically, we propose an attack where we instead find a solution x that minimizes the protocol's associated objective function $\sum_i((A \otimes x)_i - b_i)^2$ using a heuristic optimization technique. We will compare this with a different approach where some of the known attacks are formulated as mixed integer linear programs, allowing the shared key to be recovered using MILP solver.

This paper is organized as follows: Section 2 covers preliminaries and basic definitions, particularly those related to the matrix algebra over the tropical and max-min semirings, as well as the targeted key exchange protocols based on these semirings. In Section 3, we present our alternative attacks, provide numerical implementations demonstrating their performance, and compare them with the typical Kotov-Ushakov attack. Our code implementations have been made available on GitHub [1].

2 Preliminaries

In this section we are going to introduce the matrix algebra over the *tropical* and *max-min* semirings, followed by the Stickel protocol over these semirings and two versions of the Kotov-Ushakov attack. Note that we use the standard notation $[m] = \{1, \ldots, m\}$ and $[n] = \{1, \ldots, n\}$ for most common index sets.

Definition 2.1 (Matrix Algebra over Semirings [5])**.** We define the *tropical semiring* as $\mathbb{R}_{\max} = (\mathbb{R} \cup \{-\infty\}, \oplus, \otimes)$, and the *max-min semiring* as $\mathbb{R}_{\max,\min} = (\mathbb{R} \cup \{-\infty\} \cup \{\infty\}, \oplus, \otimes)$, where the arithmetical operations are defined by $x \oplus y = \max\{x, y\}$ and $x \otimes y = x + y$ for all $x, y \in \mathbb{R}_{\max}$ in the *tropical* case, and by $x \oplus y := \max(x, y)$ and $x \otimes y = \min(x, y)$ for all $x, y \in \mathbb{R}_{\max,\min}$ for the *max-min* case. When addressing both semirings at the same time or any semiring more generally, we will use the symbol $\mathbb{R}_T$ (also reminiscent of max-T semirings,

[1] https://github.com/suliman1n/Attacking-Tropical-Stickel-Protocol-by-MILP-and-Heuristic-Optimization-Techniques

of which the max-min semiring and the non-positive part of the tropical semiring are special cases).
The arithmetic operations over any semiring are naturally extended to include matrices and vectors. In particular, the operation $A \otimes \alpha = \alpha \otimes A$, where $\alpha \in \mathbb{R}_T, A \in \mathbb{R}_T^{m\times n}$ 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 $A \in \mathbb{R}_T^{\mathrm{m}\times\mathrm{n}}$ and $B \in \mathbb{R}_T^{m\times n}$, 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 $A \in \mathbb{R}_T^{m\times p}$ and $B \in \mathbb{R}_T^{p\times n}$, as follows:

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

Note that, despite introducing this arithmetic, we will also quite often utilize the usual arithmetical operations to introduce concepts and explain arguments, mostly since the optimization methods that we are going to exploit are based on the usual arithmetic.

Definition 2.2 (Matrix Powers)**.** For $M \in \mathbb{R}_T^{n\times n}$, 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 2.3. (Identity Matrix). The identity matrix $I \in \mathbb{R}_T^{n\times n}$ is of the form $(I)_{ij} = \delta_{ij}$ where

$$\delta_{ij} = \begin{cases} 0 \text{ for tropical case, or } \infty \text{ for max-min case} & \text{if } i = j \\ -\infty & \text{otherwise} \end{cases}$$

Note that the identity matrix can be defined also for a general semiring: one sets the diagonal entries equal to the semiring unity and the off-diagonal entries to the semiring zero [5].

Subsequently, we define the matrix polynomials.

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

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

where $a_k \in \mathbb{R}_T$ for $k = 0, 1, \ldots, d$. Here $A \in \mathbb{R}_T^{n\times n}$ 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 [5], and this fact was utilized by Grigoriev and Shpilrain [6] to construct a tropical implementation of the Stickel protocol (Protocol 1). Quite obviously, this protocol can be implemented over any semiring (and in particular, over the max-min semiring).

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

1. Alice and Bob agree on public matrices $A, B, W \in \mathbb{R}_T^{n\times n}$.
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 $K_b = q_1(A) \otimes U \otimes q_2(B)$.

The two parties end up with an identical key in both protocols 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 attack against Protocol 1 over the tropical semiring was published by Kotov and Ushakov [9], and an analogue of this attack against Protocol 1 over max-min semiring (and, more generally, max-T semiring with continuous T-norm) was discussed in [2]. In the next section, we will compare their performance with the optimization methods proposed in the present paper.

The objectives of the attacks is to find the polynomial coefficients $x_\alpha, y_\beta \quad \forall \alpha, \beta \in \{0, \dots D\}$ where D is the maximum polynomial degree used in the protocols, and hence construct $X = \bigoplus_{\alpha=0}^{D} (x_\alpha \otimes A^{\otimes\alpha})$ and $Y = \bigoplus_{\beta=0}^{D} \left(y_\beta \otimes B^{\otimes\beta}\right)$ that satisfy $X \otimes W \otimes Y = U$. Thus, the attacks aim to recover the shared secret key, by turning $X \otimes W \otimes Y = U$ into the form of a system of linear equations of the shape $A \otimes x = b$ and search for a solution that satisfies a special structure among all possible solutions. Thus, these attacks encounter the problem of finding all minimal solutions of a linear system of the shape $A \otimes x = b$, which is easy to solve when Alice and Bob use low-degree polynomials, as demonstrated numerically in [1, 9, 11] for the tropical case, or in [2] for the max-min case. However, it becomes significantly more challenging for higher-degree polynomials due to the exponential increase in minimal solutions of the system. The full details of the Kotov-Ushakov attack are described below.

We are aiming 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, we substitute these expressions into $X \otimes W \otimes Y = U$ to obtain

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

Combining the summations, we obtain

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

Rearranging those using the distributivity law will give

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

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

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

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

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

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

We now need to scan all solutions to this system, and get the solution that satisfies $z_{\alpha\beta} = x_\alpha \otimes y_\beta$ for some $x_\alpha, y_\beta \in \mathbb{N} \quad \forall\alpha,\beta \in \{0, 1, \ldots, D\}$. Thus, using the theory of $A \otimes x = b$ solvability, we need to find the greatest solution, and all minimal solutions. For each minimal solution, we need to search for a vector $(z_{\alpha\beta})$ in the range [minimal solution,maximum solution] that solves $z_{\alpha\beta} = x_\alpha \otimes y_\beta$ for some x_α, y_β.

Note that, for the tropical case, a minimal solution can be found by finding a minimal cover (i.e. the minimal number of variables that satisfies all the equation in the system), and the other variables are set to $-\infty$. The following algorithm captures this process.

Attack 1 (Tropical Kotov-Ushakov attack [9])**.**

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

2. Among all minimal covers of $[n] \times [n]$ by $S_{\alpha\beta}$, that is, all minimal subsets $\mathcal{C} \subseteq \{0,\dots,D\} \times \{0,\dots,D\}$ such that
$$\bigcup_{(\alpha,\beta)\in\mathcal{C}} S_{\alpha\beta} = [n] \times [n],$$
find a cover for which the system
$$\begin{aligned} x_\alpha + y_\beta &= c_{\alpha\beta}, \quad \text{if } (\alpha,\beta) \in \mathcal{C}, \\ x_\alpha + y_\beta &\leqslant c_{\alpha\beta}, \quad \text{if otherwise.} \end{aligned} \tag{3}$$
is solvable.

For the max-min case, we similarly need to compute the greatest solution c (using Lemma 3.2 in [4]) and all minimal solutions $d^{(i)}$'s (using Section 3.3 in [15] or Chapter 3 in [12]), and search for the required solution. The following algorithm captures this process.

Attack 2 (Max-min Kotov-Ushakov attack [2])**.**

1. Compute the maximum solution c of Equation (2) as:
$$c_{\alpha\beta} = \min_{\gamma,\delta\in[n]} \left(U_{\gamma\delta} : R^{\alpha\beta}_{\gamma\delta} > U_{\gamma\delta}\right) \quad \forall\alpha,\beta \in \{0,\dots,D\}$$

2. Compute all minimal solutions $d^{(i)}$ of Equation (2).

3. Find a minimal solution $d^{(i)}$ with components $d^{(i)}_{\alpha\beta}$ for which the system
$$d^{(i)}_{\alpha\beta} \leq x_\alpha \otimes y_\beta \leq c_{\alpha\beta} \quad \forall\alpha,\beta \in \{0,\dots,D\} \tag{4}$$
is solvable.

Note that system (4) can be transformed into a problem of mixed-integer linear programming as shown in [2].

These attack always succeeds due to it producing X and Y that satisfy $X \otimes W \otimes Y = U$. The proof can be found in [2, 11]. Numerical experiments showing the time taken by these attacks to compromise the tropical implementation of Protocol 1 can be found in [1, 9, 11], and for the max-min implementation see [2].

3 Attacks using Optimization

In this section, we explore more efficient approaches to attacking the tropical and max-min implementations of Protocol 1 that avoid the minimal covering problem and the associated exponential complexity, which are evident in Attack 1 and Attack 2. For all experiments, we use a matrix dimension of 10, which is the default parameter suggested in [6, 9]. This choice allows us to compare the performance of the optimization methods discussed in this paper with the performance of Attack 1 and Attack 2. Also, the coefficients of the polynomials as well as the public matrix entries are random integers in $[-1000, 1000]$.

3.1 Simulated Annealing

Both Attack 1 and Attack 2 aim to find all minimal solutions that satisfy all equations in system (2). In this approach, we aim to find a solution that minimizes the Euclidean distance between the left hand side and the right hand side of the system. Formally, we solve:

$$\min_{x_\alpha, y_\beta} \sum_{(\gamma,\delta)\in[n]\times[n]} f_{\gamma\delta}^2$$

where

$$f_{\gamma\delta} = \max_{\substack{\alpha\in\{0,1,\ldots,D\}\\ \beta\in\{0,1,\ldots,D\}}} (x_\alpha \otimes y_\beta \otimes R_{\gamma\delta}^{\alpha\beta}) - U_{\gamma\delta} \tag{5}$$

This objective function is complex with numerous local minima. However, the simulated annealing algorithm (see, e.g., [10]), when initialized with a sufficiently high temperature parameter, effectively navigates these local minima and converges to the global minimum, where the objective function equals zero.

We now formally outline how the tropical Stickel protocol (Protocol 1 with $\mathbb{R}_T = \mathbb{R}_{\max}$) is attacked using the simulated annealing method.

Attack 3 (Attacking tropical Stickel by simulated annealing)**.**

1. Compute

$$T^{\alpha\beta} = A^{\otimes\alpha} \otimes W \otimes B^{\otimes\beta} - U \quad \forall(\alpha,\beta) \in \{0,1,\ldots,D\}\times\{0,1,\ldots,D\}.$$

2. Let

$$f_{\gamma\delta} = \max_{\substack{\alpha\in\{0,1,\ldots,D\}\\ \beta\in\{0,1,\ldots,D\}}} (x_\alpha + y_\beta + T_{\gamma\delta}^{\alpha\beta}) \quad \forall(\gamma,\delta) \in [n]\times[n].$$

   and

$$F(x,y) = \sum_{(\gamma,\delta)\in[n]\times[n]} f_{\gamma\delta}^2$$

3. Select an initial temperature T, and a random point (x^c, y^c).

4. Repeat until $F(x^c, y^c) = 0$:

(a) Update the temperature with $T_k = T \times 0.95^k$, where k is the trial number.

(b) Select a new candidate point (x^{test}, y^{test}) from the neighbors of (x^c, y^c), and evaluate $F(x^{test}, y^{test})$.

(c) If $e^{\frac{F(x^{test},y^{test})-F(x^c,y^c)}{T_k}} > \text{Random}[0,1)$, then $(x^c, y^c) = (x^{test}, y^{test})$.

5. Let $(\bar{x}, \bar{y}) = (x^c, y^c)$, and construct $X = \bigoplus_{\alpha=0}^{D} (\bar{x}_\alpha \otimes A^{\otimes\alpha})$ and $Y = \bigoplus_{\beta=0}^{D} (\bar{y}_\beta \otimes B^{\otimes\beta})$, and hence the recovered key is $X \otimes V \otimes Y$.

This attack experimentally achieved a perfect success rate. The time taken in seconds to compromise Protocol 1 using this approach is presented in Figure 1.

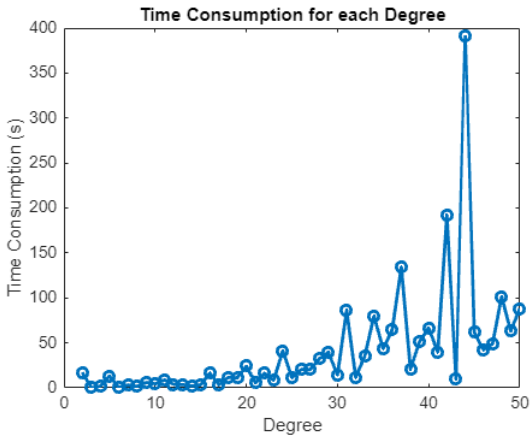

Figure 1: Attacking the tropical version of Protocol 1 using Algorithm 3

Note that this attack is significantly faster than Attack 1, averaging about 30 times the speed for a polynomial degree of 50. (Refer to [1] for detailed experimental results of Attack 1). We also observe that the attack might take significantly longer in some trials. This is probably caused by how optimal the probabilistic selection of the next neighboring point in the simulated annealing algorithm is, as well as the number of iterations performed until convergence.

For the max-min implementation of Protocol 1, the simulated annealing algorithm often struggles to reach the zero of the objective function, frequently getting stuck in local minima. Therefore, we have to utilizes the lowest local minimum obtained to attempt to recover the secret key: see Step 4 in Attack 4.

Attack 4 (Attacking max-min Stickel by simulated annealing)**.**

1. Compute

$$R^{\alpha\beta} = A^{\otimes\alpha} \otimes W \otimes B^{\otimes\beta} \quad \forall(\alpha, \beta) \in \{0, 1, \ldots, D\} \times \{0, 1, \ldots, D\}.$$

2. Let

$$f_{\gamma\delta} = \max_{\substack{\alpha\in\{0,1,\ldots,D\} \\ \beta\in\{0,1,\ldots,D\}}} (x_\alpha \otimes y_\beta \otimes R^{\alpha\beta}_{\gamma\delta}) - U_{\gamma\delta} \quad \forall(\gamma, \delta) \in [n] \times [n].$$

and

$$F(x,y) = \sum_{(\gamma,\delta)\in[n]\times[n]} f_{\gamma\delta}^2$$

3. Select an initial temperature T, and a random point (x^c, y^c).

4. Repeat until $F(x^c, y^c)$ does not change after N loops:

   (a) Update the temperature with $T_k = T \times 0.95^k$, where k is the trial number.

   (b) Select a new candidate point (x^{test}, y^{test}) from the neighbors of (x^c, y^c), and evaluate $F(x^{test}, y^{test})$.

   (c) If $e^{\frac{F(x^{test},y^{test})-F(x^c,y^c)}{T_k}} > \text{Random}[0,1)$, then $(x^c, y^c) = (x^{test}, y^{test})$.

5. Let $(\bar{x}, \bar{y}) = (x^c, y^c)$, and construct $X = \bigoplus_{\alpha=0}^{D} (\bar{x}_\alpha \otimes A^{\otimes\alpha})$ and $Y = \bigoplus_{\beta=0}^{D} (\bar{y}_\beta \otimes B^{\otimes\beta})$, and hence the recovered key is $X \otimes V \otimes Y$.

In the experiments we set $N = 300$. Although this attack does not achieve a perfect success rate, it frequently recovers the majority of the entries of the secret key. The average number of recovered entries and the average execution time are illustrated in Figure 2.

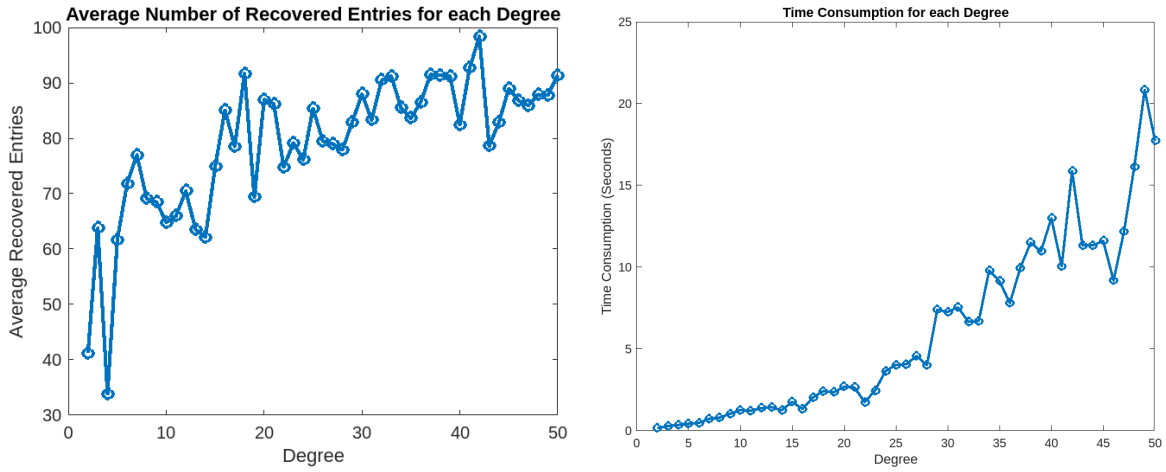

Figure 2: Attacking the max-min version of Protocol 1 using Algorithm 4

Note that this attack is significantly faster than Attack 2 (for detailed experimental results of Attack 2, refer to [2]). However, as shown experimentally, it does not guarantee the successful recovery of the entire secret key.

3.2 Kotov-Ushakov Attack Using MILP Solver

We now propose an attack that recovers the secret key by solving a mixed integer linear program (MILP), following an observation by [3]. Specifically, we start by transforming system (1) in the Kotov-Ushakov attack into a linear system by converting the disjunctive constraints into linear constraints by using Boolean variables and a big parameter. This

approach allows us to avoid dealing with system (2) and the associated challenge of enumerating all minimal solutions. Then we solve this system of inequalities using the Gurobi solver [7] (but we could use any other available MILP solver instead). See Attack 5 for a detailed description.

Attack 5 (Kotov-Ushakov attack on tropical Stickel protocol using MILP solver)**.**

1. Compute

$$T^{\alpha\beta} = A^{\otimes\alpha} \otimes W \otimes B^{\otimes\beta} - U \quad \forall(\alpha,\beta) \in \{0,1,\dots,D\} \times \{0,1,\dots,D\}.$$

2. Find x, y and z that satisfy the following system where M is a big enough number, α and β range from 0 to D, and γ and δ range from 1 to n:

$$\begin{aligned} &x_\alpha + y_\beta + T^{\alpha\beta}_{\gamma\delta} \le 0 \quad \forall\alpha,\beta,\gamma,\delta, \\ &x_\alpha + y_\beta + T^{\alpha\beta}_{\gamma\delta} + (1 - z_{\alpha\beta\gamma\delta})M \ge 0 \quad \forall\alpha,\beta,\gamma,\delta, \\ &z_{\alpha\beta\gamma\delta} \in \{0,1\} \quad \forall\alpha,\beta,\gamma,\delta, \\ &\sum_{(\alpha,\beta)} z_{\alpha\beta\gamma\delta} = 1 \quad \forall\gamma,\delta. \end{aligned} \tag{6}$$

Note that the number of variables in system (6) increases both with the matrix dimension and the polynomial degree used in the protocol. Specifically, the number of variables would be $2(D+1) + n^2(D+1)^2$. Also, the number of equations in this system is $2n^2(D+1)^2 + n^2$. Figure 3 illustrates the time taken by Attack 5 when applied to the tropical Stickel protocol.

The attack on the max-min version of Protocol 1 can be similarly described: see Attack 6.

Attack 6 (Kotov-Ushakov attack on max-min Stickel protocol using MILP solver)**.**

1. Compute

$$R^{\alpha\beta} = A^{\otimes\alpha} \otimes W \otimes B^{\otimes\beta} \quad \forall(\alpha,\beta) \in \{0,1,\dots,D\} \times \{0,1,\dots,D\}.$$

2. Solve the following system for all $(\alpha,\beta) \in \{0,1,\dots,D\} \times \{0,1,\dots,D\}$ and $(\gamma,\delta) \in [n] \times [n]$.

$$x_\alpha - (1 - z^{(1)}_{\alpha\beta\gamma\delta})M \le U_{\gamma\delta}$$

$$y_\beta - (1 - z^{(2)}_{\alpha\beta\gamma\delta})M \le U_{\gamma\delta}$$

$$R^{\alpha\beta}_{\gamma\delta} - (1 - z^{(3)}_{\alpha\beta\gamma\delta})M \le U_{\gamma\delta}$$

$$z^{(i)}_{\alpha\beta\gamma\delta} \in \{0,1\} \quad \text{and} \quad \sum_{i=1}^{3} z^{(i)}_{\alpha\beta\gamma\delta} = 1$$

$$x_\alpha + (1 - z_{\alpha\beta\gamma\delta})M \ge U_{\gamma\delta}$$

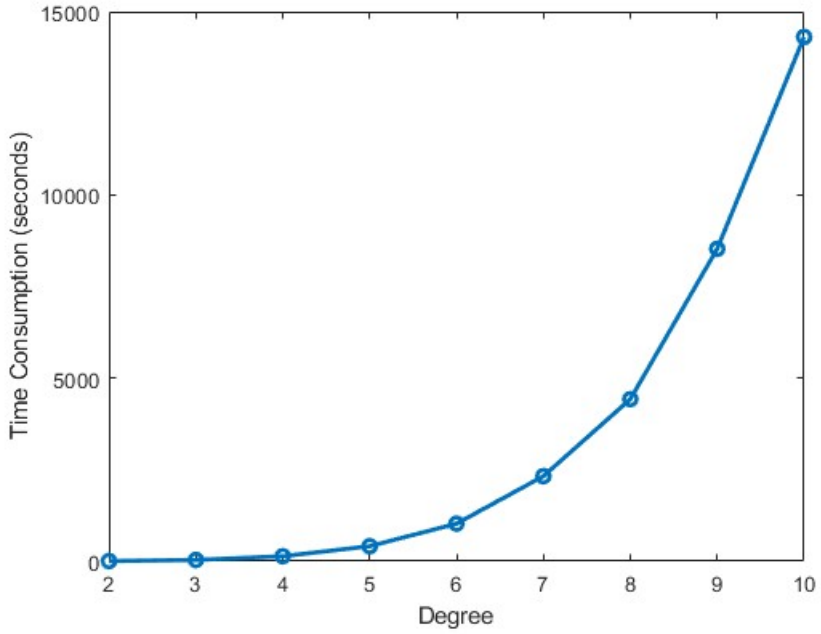

Figure 3: Attacking tropical version of Protocol 1 using Algorithm 5

$$y_\beta + (1 - z_{\alpha\beta\gamma\delta})M \geq U_{\gamma\delta}$$
$$R_{\gamma\delta}^{\alpha\beta} + (1 - z_{\alpha\beta\gamma\delta})M \geq U_{\gamma\delta}$$
$$z_{\alpha\beta\gamma\delta} \in \{0, 1\} \quad \text{and} \quad \sum_{(\alpha,\beta)} z_{\alpha\beta\gamma\delta} = 1$$

Note that the number of variables in this system similarly increases with both the matrix dimension and the polynomial degree used in the protocol. Specifically, the number of variables is $2(D+1) + n^2(D+1)^2 + 3n^2(D+1)^2$. Also, the number of equations in this system is $7n^2(D+1)^2 + n^2$. The time taken by Attack 6 when applied to the max-min Stickel protocol is illustrated in Figure 4. We observe that the computational time required for this approach is worse than that of the tropical case (Figure 3).

Therefore, both Attack 5 and Attack 6 require significantly more time even for lower polynomial degrees compared to the tropical and max-min Kotov-Ushakov attacks (Attack 1 and Attack 2). This is likely due to the high number of variables involved in the linear system. Consequently, these attacks does not provide any significant advantage over the previously described Kotov-Ushakov attacks.

3.3 Shpilrain Attack Using MILP Solver

We now propose an alternative method to formulate the MILP to attack the tropical and max-min implementations of Protocol 1. Specifically, we introduce the tropical and max-min

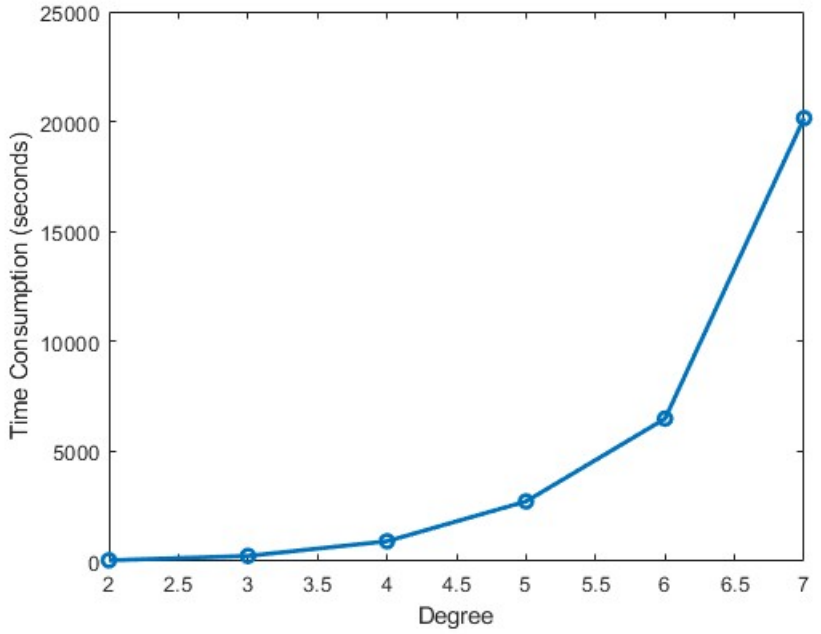

Figure 4: Attacking max-min version of Protocol 1 using Algorithm 6

versions of the Shpilrain attack [13], where our objective is to find X and Y such that

$$\begin{cases} X \otimes A = T \\ A \otimes X = T \\ Y \otimes B = R \\ B \otimes Y = R \\ X \otimes W \otimes Y = U \end{cases} \tag{7}$$

where T and R contain newly introduced auxiliary variables t_{ij}, r_{ij} for $(i,j) \in [n] \times [n]$. Then, the MILP can similarly be formulated by converting the disjunctive constraints into linear constraints with Boolean variables. In particular, for the first equation of (7), with a_{ij} being the entries of A, we have

$$\max_{k \in [n]} (x_{ik} \otimes a_{kj}) = t_{ij} \quad \forall (i,j) \in [n] \times [n],$$

which can be represented as the following set of inequalities

$$x_{ik} \otimes a_{kj} \leq t_{ij} \quad \forall i,j,k \in [n],$$

and with M being a sufficiently large number

$$x_{ik} \otimes a_{kj} + (1 - z_{kij})M \geq t_{ij} \quad \forall i,j,k \in [n],$$

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

The rest of inequalities can similarly be formulated using the other equations in (7), and then we solve the system using MILP solver. The tropical and max-min versions of the attack are described below in Attack 7 and Attack 8. We observe that the number of variables in the system increases only with the matrix dimension, but not the polynomial degree used in the protocol. Specifically, for the tropical case, the number of variables in this system is $4n^2 + 4n^3 + n^4$, and the number of equations is $5n^2 + 8n^3 + 2n^4$. For the max-min case, the number of variables is $4n^2 + 12n^3 + 4n^4$, and the number of equations is $5n^2 + 20n^3 + 7n^4$.

Attack 7 (Attacking tropical Stickel protocol using (7) and MILP solver)**.**

1. Represent (7) (over the tropical semiring) by the following system:

$$
\begin{aligned}
&x_{ik} + a_{kj} \leq t_{ij} \quad \forall i,j,k \in [n],\\
&x_{ik} + a_{kj} + (1 - z_{1kij})M \geq t_{ij} \quad \forall i,j,k \in [n],\\
&z_{1kij} \in \{0,1\}, \quad \forall i,j,k \in [n],\\
&\sum_k z_{1kij} = 1 \quad \forall i,j \in [n],
\end{aligned}
$$

$$
\begin{aligned}
&a_{ik} + x_{kj} \leq t_{ij} \quad \forall i,j,k \in [n],\\
&a_{ik} + x_{kj} + (1 - z_{2kij})M \geq t_{ij} \quad \forall i,j,k \in [n],\\
&z_{2kij} \in \{0,1\}, \quad \forall i,j,k \in [n],\\
&\sum_k z_{2kij} = 1 \quad \forall i,j \in [n],
\end{aligned}
$$

$$
\begin{aligned}
&y_{ik} + b_{kj} \leq r_{ij} \quad \forall i,j,k \in [n],\\
&y_{ik} + b_{kj} + (1 - z_{3kij})M \geq r_{ij} \quad \forall i,j,k \in [n],\\
&z_{3kij} \in \{0,1\} \quad \forall i,j,k \in [n],\\
&\sum_k z_{3kij} = 1 \quad \forall i,j \in [n],
\end{aligned}
$$

$$
\begin{aligned}
&b_{ik} + y_{kj} \leq r_{ij} \quad \forall i,j,k \in [n],\\
&b_{ik} + y_{kj} + (1 - z_{4kij})M \geq r_{ij} \quad \forall i,j,k \in [n],\\
&z_{4kij} \in \{0,1\}, i,j,k \in [n]\\
&\sum_k z_{4kij} = 1 \quad \forall i,j \in [n],
\end{aligned}
$$

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

   where a_{ij}, b_{ij}, w_{ij} are respectively the entries of the public matrices A, B, W.

2. Solve the system using a MILP solver.

Attack 8 (Attacking max-min Stickel protocol using (7) and MILP solver)**.**

1. Represent (7) (over the max-min semiring) by the following system

$$
\begin{aligned}
&x_{ik} - (1 - z^{(1)}_{1kij})M \leq t_{ij} \quad \forall i,j,k \in [n],\\
&a_{kj} - (1 - z^{(2)}_{1kij})M \leq t_{ij} \quad \forall i,j,k \in [n],\\
&z^{(1)}_{1kij} + z^{(2)}_{1kij} = 1 \quad \forall i,j,k \in [n],\\
&x_{ik} + (1 - z^{(3)}_{1kij})M \geq t_{ij} \quad \forall i,j,k \in [n],\\
&a_{kj} + (1 - z^{(3)}_{1kij})M \geq t_{ij} \quad \forall i,j,k \in [n],\\
&z^{(1)}_{1kij}, z^{(2)}_{1kij}, z^{(3)}_{1kij} \in \{0,1\} \quad \forall i,j,k \in [n]\\
&\sum_k z^{(3)}_{1kij} = 1 \quad \forall i,j \in [n],
\end{aligned}
$$

$$
\begin{aligned}
&a_{ik} - (1 - z^{(1)}_{2kij})M \leq t_{ij} \quad \forall i,j,k \in [n],\\
&x_{kj} - (1 - z^{(2)}_{2kij})M \leq t_{ij} \quad \forall i,j,k \in [n],\\
&z^{(1)}_{2kij} + z^{(2)}_{2kij} = 1 \quad \forall i,j,k \in [n],\\
&a_{ik} + (1 - z^{(3)}_{2kij})M \geq t_{ij} \quad \forall i,j,k \in [n],\\
&x_{kj} + (1 - z^{(3)}_{2kij})M \geq t_{ij} \quad \forall i,j,k \in [n],\\
&z^{(1)}_{2kij}, z^{(2)}_{2kij}, z^{(3)}_{2kij} \in \{0,1\} \quad \forall i,j,k \in [n]\\
&\sum_k z^{(3)}_{2kij} = 1 \quad \forall i,j \in [n],
\end{aligned}
$$

$$
\begin{aligned}
&y_{ik} - (1 - z^{(1)}_{3kij})M \leq r_{ij} \quad \forall i,j,k \in [n],\\
&b_{kj} - (1 - z^{(2)}_{3kij})M \leq r_{ij} \quad \forall i,j,k \in [n],\\
&z^{(1)}_{3kij} + z^{(2)}_{3kij} = 1 \quad \forall i,j,k \in [n],\\
&y_{ik} + (1 - z^{(3)}_{3kij})M \geq r_{ij} \quad \forall i,j,k \in [n],\\
&b_{kj} + (1 - z^{(3)}_{3kij})M \geq r_{ij} \quad \forall i,j,k \in [n],\\
&z^{(1)}_{3kij}, z^{(2)}_{3kij}, z^{(3)}_{3kij} \in \{0,1\} \quad \forall i,j,k \in [n]\\
&\sum_k z^{(3)}_{3kij} = 1 \quad \forall i,j \in [n],
\end{aligned}
$$

$$
\begin{aligned}
&b_{ik} - (1 - z^{(1)}_{4kij})M \leq r_{ij} \quad \forall i,j,k \in [n],\\
&y_{kj} - (1 - z^{(2)}_{4kij})M \leq r_{ij} \quad \forall i,j,k \in [n],\\
&z^{(1)}_{4kij} + z^{(2)}_{4kij} = 1 \quad \forall i,j,k \in [n],\\
&b_{ik} + (1 - z^{(3)}_{4kij})M \geq r_{ij} \quad \forall i,j,k \in [n],\\
&y_{kj} + (1 - z^{(3)}_{4kij})M \geq r_{ij} \quad \forall i,j,k \in [n],\\
&z^{(1)}_{4kij}, z^{(2)}_{4kij}, z^{(3)}_{4kij} \in \{0,1\} \quad \forall i,j,k \in [n]\\
&\sum_{k} z^{(3)}_{4kij} = 1 \quad \forall i,j \in [n],
\end{aligned}
$$

$$
\begin{aligned}
&x_{ik} - (1 - z^{(1)}_{5klij})M \leq u_{ij} \quad \forall i,j,k,l \in [n],\\
&w_{kl} - (1 - z^{(2)}_{5klij})M \leq u_{ij} \quad \forall i,j,k,l \in [n],\\
&y_{lj} - (1 - z^{(3)}_{5klij})M \leq u_{ij} \quad \forall i,j,k,l \in [n],\\
&z^{(1)}_{5klij} + z^{(2)}_{5klij} + z^{(3)}_{5klij} = 1 \quad \forall i,j,k,l \in [n],\\
&x_{ik} + (1 - z^{(4)}_{5klij})M \geq u_{ij} \quad \forall i,j,k,l \in [n],\\
&w_{kl} + (1 - z^{(4)}_{5klij})M \geq u_{ij} \quad \forall i,j,k,l \in [n],\\
&y_{lj} + (1 - z^{(4)}_{5klij})M \geq u_{ij} \quad \forall i,j,k,l \in [n],\\
&z^{(1)}_{5klij}, z^{(2)}_{5klij}, z^{(3)}_{5klij}, z^{(4)}_{5klij} \in \{0,1\},\\
&\sum_{k,l} z^{(4)}_{5klij} = 1 \quad \forall i,j \in [n].
\end{aligned}
$$

Here a_{ij}, b_{ij}, w_{ij} are, respectively, the entries of the public matrices A, B, W.

2. Solve the system using a MILP solver.

Note that a distinct advantage of these attacks is that they are independent of the polynomial degree used in the protocol. Therefore, Alice and Bob cannot improve the protocol's resistance against these attacks by increasing the polynomial degree, a way that is very effective against Kotov-Ushakov attack and its max-min analogue (Attack 1 and Attack 2). A major drawback, however, is the high number of equations and hence variables involved in the linear program, which demands substantial memory storage. Figure 5 shows the time taken by Attack 7 for different polynomial degrees.

As illustrated in Figure 5, this attack is much faster than Attack 1 and maintains consistent computational efficiency across varying polynomial degrees. It is worth noting that for larger matrix dimensions, such as $n = 10$ or higher, the Gurobi solver may encounter challenges in directly solving the system in some trials. Fine-tuning of the solver parameters is required to solve the system in such cases. The time taken by Attack 8 for different polynomial degrees is shown in Figure 6. Note that due to the higher number of equations and variables in the max-min case compared with the tropical case, the memory required for encoding the linear program for a dimension higher than 8 would exceed the available memory threshold.

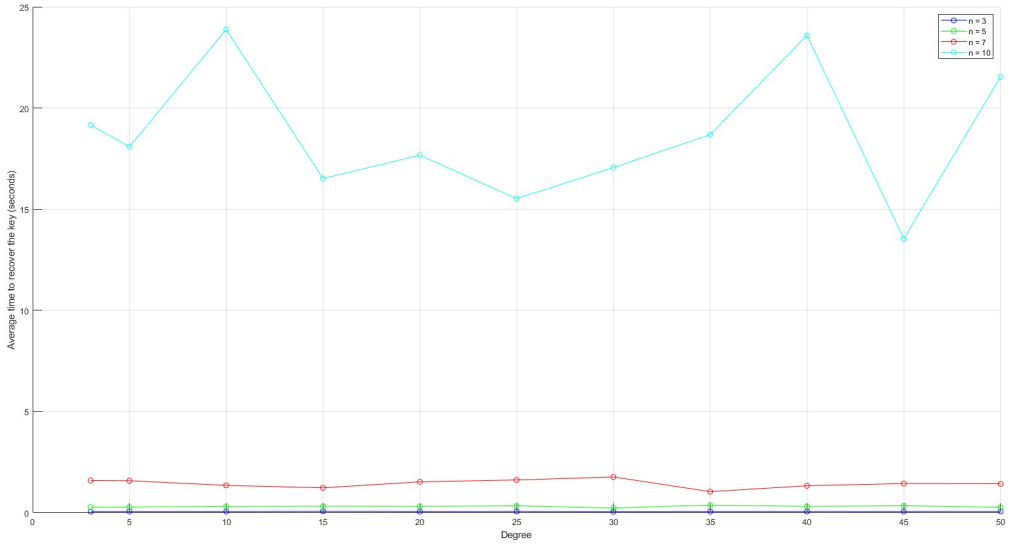

Figure 5: Attacking tropical version of Protocol 1 using Algorithm 7

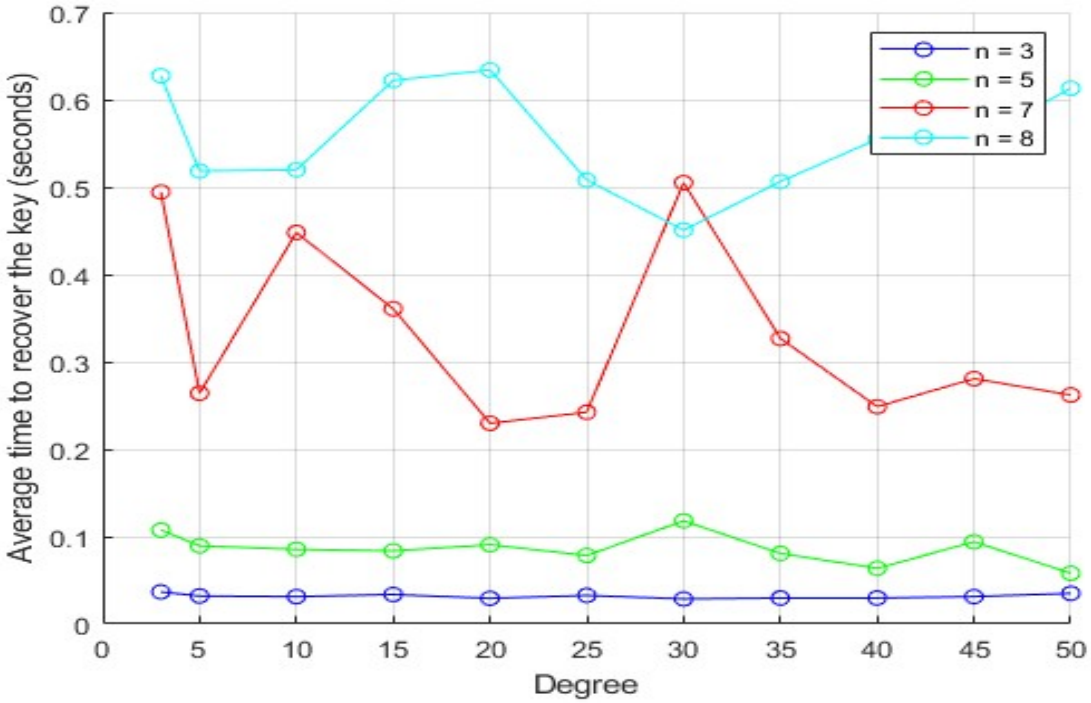

Figure 6: Attacking max-min version of Protocol 1 using Algorithm 8

4 Conclusion

In this paper, we proposed three attacks against the tropical and max-min implementations of Stickel protocol. Our aim was to avoid the hard problem of minimal covers enumeration and the associated exponential complexity encountered in the typical Kotov-Ushakov attack. While we previously proposed an attack against these protocols [1], [2] that avoided enumerating all minimal solutions by carefully selecting a single minimal solution, this method, although very successful for the tropical case, occasionally fails. Consequently, it is plausible that Alice and Bob could design the protocol's public matrices to resist this attack, and this method still shows increasing complexity with the polynomial degree used, though not exponentially. Thus, the goal of the three attacks was to achieve a perfect success rate with the lowest possible execution time and reduced dependence on the polynomial degree, which is commonly the variable parameter controlled by Alice and Bob.

The first proposed attack aims to find a solution x that minimizes an objective function of the shape $\sum_i((A \otimes x)_i - b_i)^2$ instead of finding all solutions of a system of the shape $A \otimes x = b$ as in the typical Kotov-Ushakov attack. This attack achieved a perfect success rate against the tropical Stickel protocol and a high success rate against the max-min Stickel protocol, both with very fast execution times. Additionally, the execution time showed only a minor increase as the polynomial degree increased.

The second proposed attack aims to solve the system of the shape $A \otimes x = b$ by transforming it into a mixed-integer linear system and then solving it using MILP solver. Unfortunately, this attack demonstrated slower execution times compared to the typical Kotov-Ushakov attack, and it remains heavily dependent on the polynomial degree used in the targeted protocols. Consequently, similar to the typical Kotov-Ushakov attack, Alice and Bob can resist this attack by increasing the polynomial degree.

The third proposed attack (which we call Shpilrain's attack) aims to solve equations (7) by formulating them as a mixed-integer linear program. Interestingly, this attack is completely independent from the used polynomial degree in the protocol, which makes it effective even if Alice and Bob use very high polynomial degrees. The attack has also demonstrated remarkably fast execution times. A significant limitation of this attack is its high memory requirement due to the need of encoding a large number of equations. Consequently, Alice and Bob could potentially defend against it by employing large matrix dimensions. However, it is worth noting that the typical Kotov-Ushakov attack would likely encounter similar challenges in such scenarios, specifically those related to the high number of minimal covers.

Let us also observe that Shpilrain's attack also applies to the modifications of Stickel protocol based on Jones matrices and Linde-de la Puente matrices suggested in [11]. Namely, the protocol based on Jones matrices is only replacing the tropical polynomials of A and B with tropical quasi-polynomials of the same matrices, so we can still find X and Y directly from (7) (and its MILP reformulation). As for the Linde-de la Puente matrices, equations $X \otimes A = A \otimes X$ and $Y \otimes B = B \otimes Y$ have to be replaced with linear inequalities and equations that define Linde-de la Puente matrices. We are not including the results here but

the situation is similar to what is reported in Figure 5.

Finally, it is notable that the findings presented in this paper likely indicate that the max-min implementation of the Stickel protocol overall tends to be more resistant than the tropical implementation. This conclusion arises because two of the three proposed attacks in this paper, alongside the single cover heuristic [1], demonstrate much greater effectiveness against the tropical case. Furthermore, the typical Kotov-Ushakov attack is more efficient against the tropical Stickel protocol compared to its analogue against the max-min Stickel protocol. Better implementation of Shpilrain's attack which would allow for breaking protocols with higher dimensional matrix is still to be considered.

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. 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`.

[3] 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.

[4] M. Gavalec. Solvability and unique solvability of max–min fuzzy equations. *Fuzzy Sets and Systems*, 124(3):385–393, 2001. Fuzzy Logic.

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

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

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

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

[9] 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.

[10] Z. Michalewicz and D. Fogel. *How to Solve it: Modern Heuristics*. Springer, 2000.

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

[12] K. Peeva and Y. Kyosev. *Fuzzy Relational Calculus – Theory, Applications and Software (with CD-ROM)*, volume 22 of *Advances in Fuzzy Systems – Applications and Theory*. World Scientific Publishing Company, 2004.

[13] V. Shpilrain. Cryptanalysis of stickel's key exchange scheme. In *Computer Science - Theory and Applications*, pages 283–288, 2008.

[14] 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.

[15] Z. Zahariev. Solving max-min fuzzy linear systems of equations. Algorithm and software. *Annual of "Informatics" section. Union of Scientists in Bulgaria*, 6:1–16, 2013. Available from `http://e-university.tu-sofia.bg/e-publ/files/12485_SUB-Informatics-2013-6-001-016.pdf`.

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