On implementation of Stickel's key exchange protocol over max-min and max-T semirings

Sulaiman Alhussaini and Sergeĭ Sergeev

Abstract

Given that the tropical Stickel protocol and its variants are all vulnerable to the generalized Kotov-Ushakov attack, we suggest employing the max-min semiring and, more generally, max-T semiring where the multiplication is based on a $T-$norm, as a framework to implement the Stickel protocol. While the Stickel protocol over max-min semiring or max-T semiring remains susceptible to a form of Kotov-Ushakov attack, we demonstrate that it exhibits significantly increased resistance against this attack when compared to the tropical (max-plus) implementation.

Keywords: public key cryptography; cryptographic attack; Stickel protocol; fuzzy algebra; fuzzy relation equations
Classification: 94A60, 08A72, 15A80

1 Introduction

A key exchange protocol is the process, in which two parties (commonly called Alice and Bob) exchange messages in order to jointly compute a shared secret key that cannot be directly intercepted by an eavesdropper (Eve). In public key cryptography, it is common to use various structures in algebra and geometry (such as elliptic curves) to implement such key exchange protocols. The most popular protocol is due to Diffie and Hellman [7], and Stickel's protocol [22] whose unusual implementation is discussed in our paper is, essentially a two-sided variety of Diffie-Hellman.

Tropical cryptography was firstly proposed by Grigoriev and Shpilrain [10] as an alternative framework for cryptographic protocols such as Stickel's since it enjoys several advantages such as efficiency and resistance to some general attacks. In particular, Grigoriev and Shpilrain developed a tropical version of the original Stickel key exchange protocol, the original version of which was vulnerable to common linear algebraic attacks. Their motivation came from the non-invertible nature of matrices in tropical algebra, making the tropical implementation resistant to attacks resembling the ones faced by the original Stickel protocol. It can be also observed that the tropical implementation of cryptographic protocols is faster to execute (since the arithmetical operations can be executed faster). The tropical Stickel protocol was then attacked by Kotov and Ushakov [16]. The Kotov-Ushakov attack was generalized in [17] where it was shown how to apply the same idea to other implementations of Stickel protocol based on matrix commutativity. Also, Grigoriev and Shpilrain [11] proposed two protocols based on tropical semi-direct product, but one of them was shown to be invalid by Isaac and Kahrobaei [14] and the other was successfully attacked by the same authors as well as in [18] and [21]. This highlights the challenges in implementing a secure protocol in the tropical framework.

The main idea of the present paper is to consider implementations of Stickel protocol over max-T semirings where $T\colon [0,1]^2 \mapsto [0,1]$ is an arbitrary $T-$norm and to evaluate its resistance against the Kotov-Ushakov attack comparing it to the tropical version. Although the Kotov-Ushakov attack can be formulated over a general enough class of max-T semirings, we will present the numerical experiments only over the max-min semiring, leaving experimentation with other max-T semiring to the future research.

We are using the term "max-T semiring" here following, e.g., [19] Section 7 and [9]. However, max-T semirings can be considered as a rather old concept as, in particular, the systems $A \otimes x = b$ over such semirings have been studied for many decades as (systems of) *fuzzy relation equations*: see [6, 12, 15] (among many other works). The theory and practice of solving these systems will be useful to us when implementing the Kotov-Ushakov attack. Note that max-T semirings can be also considered as closely related (or part of) BL-algebras and MV-algebras [5].

This paper is organized as follows: Section 2 begins with preliminaries and basic definitions, particularly concerning the max-min semiring and, more generally, max-T semirings. In Section 3, we introduce two implemetations of the Stickel protocol over arbitrary semiring, assessing their applicability, validity, and the behavior of the shared key for the case of max-min semiring. In Section 4, we analyze the security of this new implementation and its resilience compared to tropical counterparts. Finally, in Section 5, we evaluate the resistance of the proposed protocols through a series of numerical experiments. Our codes have been uploaded to GitHub [1].

2 Preliminaries

In this section, we present the standard definitions for the matrix algebra over the max-min semiring. We will use $[n]$ and $[m]$ to denote $\{1,\ldots,n\}$ and $\{1,\ldots,m\}$ respectively.

Definition 2.1 (Max-Min Semiring and Associated Matrix Algebra)**.** The *max-min (fuzzy) semiring* is defined as $\mathbb{R}_{\max,\min} = (\mathbb{R}\cup\{-\infty\}\cup\{\infty\},\oplus,\otimes)$, with these two operations defined by $a \oplus b := \max\{x,y\}$ and $a \otimes b := \min\{x,y\}$. These operations can also be also extended to vectors and matrices to form matrix algebra over the max-min semiring. In particular, the operation $A\otimes\alpha = \alpha\otimes A, \quad$ where $\alpha \in \mathbb{R}_{\max,\min}, A \in \mathbb{R}^{m\times n}_{\max,\min}$ 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 *max-min addition* $A \oplus B$ of two matrices $A \in \mathbb{R}^{\mathrm{m}\times\mathrm{n}}_{\max,\min}$ and $B \in \mathbb{R}^{m\times n}_{\max,\min}$, where $(A)_{ij} =$

[1] https://github.com/suliman1n/On-implementation-of-Stickel-key-exchange-protocol-over-max-min-and-max-T-semirings

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

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

Definition 2.2 (*Max-min Matrix Powers)***.** For $A \in \mathbb{R}^{nxn}_{\text{max,min}}$, the n-th *max-min power* of A is denoted by $A^{\otimes n}$, and is equal to

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

By definition, any *max-min* square matrix to the power 0 equals the *max-min* identity.

Definition 2.3 (*Max-min Identity)***.** The *max-min* identity matrix $I \in \mathbb{R}^{n\times n}_{\text{max,min}}$ is of the form $(I)_{ij} = \delta_{ij}$ where

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

We subsequently define the matrix polynomials over the max-min semiring.

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

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

Here A is a square matrix of any dimension.

Notice that any two matrix polynomials of the same matrix commute in the max-min algebra, as in the classical and tropical cases. Consequently, max-min polynomials can be utilized to create a version of Stickel protocol, exploiting this commutativity property to form a shared secret key.

We also present the modified s-circulants which also could be used as a commutativity tool to construct another implementation of Stickel protocol.

Definition 2.5. (Upper s-Circulants [13], see also [2]). Let $A \in \mathbb{R}^{n\times n}_{\text{max,min}}$. We say that A is an upper-s-circulant, or $A \in C^s_n$, 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 $c_0, c_1, c_2 \ldots, c_{n-1}, s \in \mathbb{R}_{\text{max,min}}$.

Definition 2.6 (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, e.g., [15] for definition). These arithmetics are then naturally extended to matrices and vectors as in Definition 2.1.

Remark 2.1 (On max-T semirings)**.** The max-min semiring introduced earlier is isomorphic to the max-T semiring with $T = \min$, but it is more natural for computations since one can choose to work with integer numbers only. The identity matrix for any max-T semiring is the same as the usual identity matrix (with all 1's on the diagonal and all 0's off the diagonal). The definitions of matrix powers, matrix polynomials and modified circulants all naturally extend to the matrix algebra over max-T semiring.

3 Stickel protocol over max-min and other semirings

In this section, we introduce the Stickel key exchange protocol over the max-min semiring using polynomials (Protocol 1) and modified circulants (Protocol 2), and examine their applicability.

Protocol 1 (Max-min Stickel protocol)**.**

1. Alice and Bob agree on public matrices $A, B, W \in \mathbb{R}^{n\times n}_{\text{max,min}}$.
2. Alice chooses two random max-min 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 max-min 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 Bob's message V, and she has $K_a = p_1(A) \otimes V \otimes p_2(B)$.
5. Bob also computes his secret key using Alice's message U, and he obtains $K_b = q_1(A) \otimes U \otimes q_2(B)$.

Note that $K_a = p_1(A) \otimes V \otimes p_2(B) = p_1(A) \otimes q_1(A) \otimes W \otimes q_2(B) \otimes p_2(B) = q_1(A) \otimes p_1(A) \otimes W \otimes p_2(B) \otimes q_2(B) = q_1(A) \otimes U \otimes q_2(B) = K_b$, which means the two parties end up with the same key due to the commutativity of polynomials of the same matrix in the max-min semiring, resembling classical algebra.

Initially, one might assume that this protocol is vulnerable to exhaustive search attacks because max-min operations do not generate new numbers, making the shared key seemingly easy to guess. However, we argue otherwise. By considering a wide range for both matrix entries and polynomial coefficients, along with a sufficiently large polynomial degree, the protocol yields an extensive array of possibilities, thereby mitigating susceptibility to brute-force attacks.

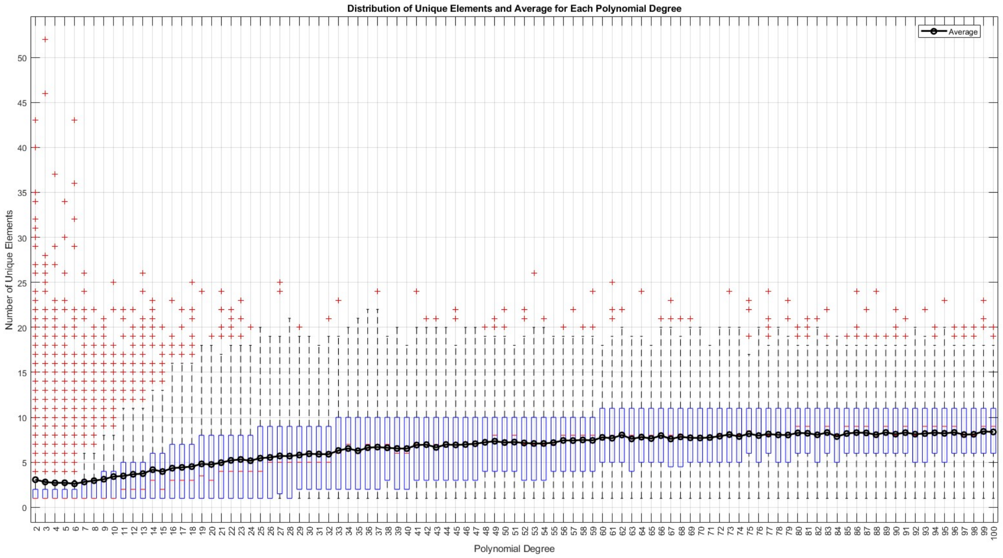

Figure 1: Key randomness for Protocol 1

The following experiment (Figure 1) shows the average number of unique elements in the shared key. The dimension of the matrices is 10 with entries and polynomial coefficients chosen randomly from $[-10000, 10000]$ and 100 trials were performed for each polynomial degree. Note that for high polynomial degrees, there are on average 8 distinct elements in the shared key. Considering the size of the matrix, there exists a large number of arrangements for these elements within the matrix. Hence, exhaustive search for the key would not be feasible.

Protocol 2 (Max-min Stickel protocol based on modified circulants)**.**

1. Alice and Bob agree on $s, t \in \mathbb{R}_{\max,\min}$ and a publicly known matrix $M \in \mathbb{R}^{n\times n}_{\max,\min} \setminus (C^s_n \cup C^t_n)$.
2. Alice generates two matrices $A_1 \in C^s_n$ and $B_1 \in C^t_n$ and sends $U = A_1 \otimes M \otimes B_1$ to Bob .
3. Bob generates two matrices $A_2 \in C^s_n$ and $B_2 \in C^t_n$ and sends $V = A_2 \otimes M \otimes B_2$ to Alice.
4. Alice calculates $K_a = A_1 \otimes V \otimes B_1$.
5. Bob calculates $K_b = A_2 \otimes U \otimes B_2$.

Similarly, note that $K_a = A_1 \otimes V \otimes B_1 = A_1 \otimes A_2 \otimes M \otimes B_2 \otimes B_1 = A_2 \otimes A_1 \otimes M \otimes B_1 \otimes B_2 = A_2 \otimes U \otimes B_2 = K_b$, which means the two parties end up with the same key due the commutative nature of modified circulants.

We also demonstrate the behavior of the shared key as the matrix dimension increases (Figure 2), assessing whether there's adequate variability to prevent brute-force attacks.

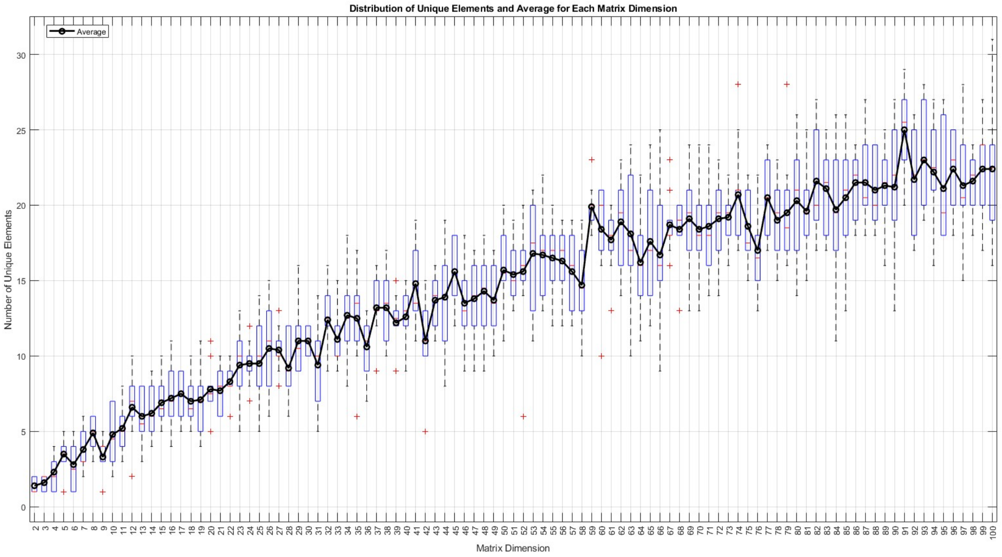

Figure 2: Key randomness for Protocol 2

The average number of unique elements within the matrix increases with matrix dimension. This similarly results in a vast array of possible arrangements for these elements, making simple exhaustive search attacks unfeasible.

Remark 3.1. Both matrix polynomials and upper s-circulants (for a fixed element s) form a commutative semiring with (obvious) identity and zero. For lower s-circulants over the tropical semiring a proof of this fact can be found in [2] and it can be modified to apply to upper s-circulants over any semiring. For the reader's convenience we include a self-contained proof in Appendix. We acknowledge that this proof is based on the arguments from Collett's M.Sci. dissertation [3].

Due to the commutativity of matrix polynomials and modified circulants, both Protocol 1 and Protocol 2 can be implemented using matrix algebra over any semiring, including any max-T semiring.

4 Security analysis of the proposed protocols

In this section, we introduce a max-min/max-T analogue of the Kotov-Ushakov attack over the max-min semiring and its heuristic version (in the max-min case only), and demonstrate the substantially greater difficulty in compromising the max-min protocols relative to their tropical equivalents.

Similar to the original tropical Kotov-Ushakov attack [16] (or the tropical generalized Kotov-Ushakov attack [17]),in order to attack Protocol 1 or Protocol 2, our objective is to find the polynomial coefficients or the circulant parameters $x_\alpha, y_\beta \quad \forall \alpha, \beta \in \{0, \ldots D\}$ where D is the maximum polynomial degree for the case of Protocol 1, or the matrix dimension

$(D = n - 1)$ for the case of Protocol 2. In particular, we define

$$X = \bigoplus_{\alpha \in \{0,\dots D\}} (x_\alpha \otimes A_\alpha)\,, \quad Y = \bigoplus_{\beta \in \{0,\dots D\}} (y_\beta \otimes B_\beta)\,, \tag{1}$$

where A_α and B_β represent the powers of the public matrices A and B respectively in the context of Protocol 1, or serve as generators of modified circulants for Protocol 2 which takes the following form for A_α in the max-min case, and B_β follows similarly

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

Note that for max-T semiring we need to define

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

We know from the protocols that $X \otimes M \otimes Y = U$, and if we substitute (1) for X and Y we get

$$U = \bigoplus_{\alpha \in \{0,\dots D\}} (x_\alpha \otimes A_\alpha) \otimes M \otimes \bigoplus_{\beta \in \{0,\dots D\}} (y_\beta \otimes B_\beta)\,.$$

Then combining the two summations and rearranging the coefficients, we get

$$U = \bigoplus_{\alpha,\beta \in \{0,\dots D\}} x_\alpha \otimes y_\beta \otimes (A_\alpha \otimes M \otimes B_\beta) \tag{2}$$

We then denote $x_\alpha \otimes y_\beta = z_{\alpha\beta}$ and $R^{\alpha\beta} = (A_\alpha \otimes M \otimes B_\beta)$ to rewrite Equation (2) as follows:

$$U = \bigoplus_{\alpha,\beta \in \{0,\dots D\}} z_{\alpha\beta} \otimes R^{\alpha\beta} \tag{3}$$

This is of the form of max-min/max-T linear system "$A \otimes x = b$" where the entries of $R^{\alpha\beta}$ are the coefficients of the system, and $z_{\alpha\beta}$ are the unknowns.

Thus, we need to scan all solutions to Equation (3) and pick a solution that satisfies $z_{\alpha\beta} = x_\alpha \otimes y_\beta$ for some $x_\alpha, y_\beta \quad \forall \alpha, \beta \in \{0, 1, \dots, D\}$. The next proposition for the complete set of solutions of Equation (3) where we "forget" about this important constraint on variables $z_{\alpha\beta}$ is very well-known in fuzzy relations theory.

Proposition 4.1 (e.g. [12],[15])**.** Over the max-min semiring, system (3) has a finite set of minimal solutions and just one maximal solution, which is the greatest solution. With the number of minimal solutions denoted by r, the whole solution set is represented as

$$S = \bigcup_{i=1}^{r} \{x \colon d^{(i)} \leq x \leq c\},$$

where $d^{(i)}$ denotes the *ith* minimal solution and c is the greatest solution of (3).

According to Di Nola et al. [6], this Proposition also extends to max-T semirings where T is a continuous T-norm. Note that, as shown by Di Nola et al. [6], the lower semi-continuity of T-norm guarantees the existence of the greatest solution while in the case of upper semi-continuity of T the set of minimal solutions can be fully described and it can be shown that any solution is lower-bounded by a minimal solution. In particular, Proposition 4.1 holds also for the tropical case where the T-norm is defined as the usual product, and in this case the minimal solutions can be found by zeroing out some components of the greatest solution.

In order to break Stickel's protocol over max-T semiring, assuming that Proposition 4.1 holds we need to compute the greatest solution c (for the max-min case using Lemma 3.2 in [8]) and all minimal solutions $d^{(i)}$'s (for the max-min case using Section 3.3 in [23] or Chapter 3 in [20]), and test the boxes $\{x\colon d^{(i)} \leq x \leq c\}$ for all i until we find a vector z that satisfies $z_{\alpha\beta} = x_\alpha \otimes y_\beta$ for some $x_\alpha, y_\beta \in \mathbb{N} \quad \forall \alpha, \beta \in \{0, 1, \dots, D\}$. The following algorithm captures these processes.

Attack 1 (Max-min/max-T generalized Kotov-Ushakov attack)**.**

1. Compute the maximum solution c of Equation (3). In the max-min case:

$$c_{\alpha\beta} = \min_{\gamma,\delta\in[n]} \Big(U_{\gamma\delta} : R^{\alpha\beta}_{\gamma\delta} > U_{\gamma\delta} \Big) \quad \forall \alpha, \beta \in \{0, \dots, D\}$$

2. Compute all minimal solutions $d^{(i)}$ of Equation (3).

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.

In the max-min case system (4) can be transformed into a problem of mixed-integer linear programming, following an observation by [4]. In particular, $\min(x_\alpha, y_\beta) \leq c_{\alpha\beta}$ means either x_α, y_β or both are less than or equal to $c_{\alpha\beta}$, which can be expressed as $x_\alpha - (1 - w_{\alpha\beta})M \leq c_{\alpha\beta}$ and $y_\beta - (1 - k_{\alpha\beta})M \leq c_{\alpha\beta}$ with M being a sufficiently large number, and $w_{\alpha\beta} + k_{\alpha\beta} = 1$ such that $w_{\alpha\beta}, k_{\alpha\beta} \in \{0, 1\}$. Obviously, $\min(x_\alpha, y_\beta) \geq d^{(i)}_{\alpha\beta}$ can be equivalently written as $x_\alpha \geq d^{(i)}_{\alpha\beta}$, $y_\beta \geq d^{(i)}_{\alpha\beta}$.
Thus, the system (4) can equivalently be written as

$$\begin{aligned} & x_\alpha \geq d^{(i)}_{\alpha\beta}, y_\beta \geq d^{(i)}_{\alpha\beta} \\ & \\ & x_\alpha - (1 - w_{\alpha\beta})M \leq c_{\alpha\beta}, \quad y_\beta - (1 - k_{\alpha\beta})M \leq c_{\alpha\beta}, \\ & w_{\alpha\beta} + k_{\alpha\beta} = 1, \\ & w_{\alpha\beta}, k_{\alpha\beta} \in \{0, 1\} \end{aligned} \tag{5}$$

We now prove that Attack 1 works, due to it producing X and Y that satisfy $X \otimes M \otimes Y = U$.

Proposition 4.2. Let U be the message that Alice sent to Bob in Protocol 1 or Protocol 2. Then Attack 1 yields

$$X = \bigoplus_{\alpha \in \{0,\ldots D\}} (x_\alpha \otimes A_\alpha), \quad Y = \bigoplus_{\beta \in \{0,\ldots D\}} (y_\beta \otimes B_\beta),$$

such that X and Y satisfy $X \otimes M \otimes Y = U$.

Proof. Since $U = X \otimes M \otimes Y$, then there is a vector z that solves Equation (3) with $z_{\alpha\beta} = x_\alpha \otimes y_\beta$ for some x_α and y_β such that $X = \bigoplus_{\alpha \in \{0,\ldots D\}} (x_\alpha \otimes A_\alpha)$ and $Y = \bigoplus_{\beta \in \{0,\ldots D\}} (y_\beta \otimes B_\beta)$. We now need to show that the method described in Attack 1 does find such vector. Since the attack, due to Proposition 4.1, searches for all possible solutions of Equation (3), it is guaranteed that it finds a solution that solves system (4) (or equivalently system (5)) because we know that there exist coefficients x_α and y_β such that $\bigoplus_{\alpha,\beta} x_\alpha \otimes y_\beta \otimes R^{\alpha\beta} = U$, and these coefficients can be used to construct X and Y. □

Since Attack 1 is very computationally heavy, it might not be practical, especially when Alice and Bob use very high polynomial degrees or matrix dimensions (see in the numerical experiments below). An attacker then would consider a heuristic version of the attack. One possible heuristic, which we are presenting only for the max-min case, would be as shown in Attack 2, where the attacker checks for a vector that solves system (4) (or equivalently system (5)) in just one box, where the lowest corner of the box is the lower bound r suggested by Gavalec in [8] Lemma 5.2. (i.e., $r \leq z$ for any solution z of Equation (3)) , and similarly the highest corner of the box is the greatest solution of Equation (3). The attack succeeds if a solution is found, and fails if otherwise.

Attack 2 (Heuristic version of Attack 1 in the max-min case)**.**

1. Compute the greatest solution c of Equation (3).

2. Compute the lower bound r for solutions of Equation (3) suggested in [8] Lemma 5.2.

3. Solve the system

$$r_{\alpha\beta} \leq \min(x_\alpha, y_\beta) \leq c_{\alpha\beta} \quad \forall \alpha, \beta \in \{0, \ldots, D\}$$

5 Implementations and Numerical Experiments

We now implement the attacks on Protocol 1 and Protocol 2, analyzing their behaviour and execution time. We also compare the resistance of the two proposed max-min protocols with their tropical counterparts.

In our series of experiments we investigate the behavior of Attack 1 in which we count the number of enumerated minimal solutions, and how many of them were tested to recover the shared key. We also measure the time taken by this attack to break the protocol. It appears that the numbers of enumerated and tested minimal solutions are much higher than the tropical case (as reported by Kotov and Ushakov experiment in [16]). Furthermore, as the degree of polynomial or the matirx dimension grows, the number of minimal solutions skyrockets, leading to significantly prolonged attack times, often spanning several hours already for low dimensions. Such instances tend to occur more frequently as the degree increases, likely attributed to the high number of minimal solutions driven by the increase in key randomness. We expect that the max-min protocols require significantly more time to compromise compared to their tropical counterparts, primarily due to the increased number of enumerated and tested minimal solutions, in addition to having to solve a harder optimization problem (we have to solve a linear programming problem in the case of tropical Stickel protocol, compared with mixed-integer linear programming for the max-min case).

We used a 10 dimensional matrix and a polynomial degree from 2 to 10 for the case of Protocol 1, and a matrix dimension from 2 to 10 for the case of Protocol 2, and both matrix entries and polynomial coefficients are in $[-10000, 10000]$. The results of this experiment (the number of minimal solutions and the execution time are shown in Tables 1 and 2). The code was executed on MATLAB R2023b running on Windows 11 64-bit, equipped with an Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz and 16.0 GB RAM.

Degree	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Number of Minimal Solutions	5	11	54	664	439	3198	12493	20834	27342
Number of Tested Minimal Solutions	1	1	54	1	43	1261	1	199	373
Time Taken (seconds)	0.01	0.04	0.34	2.9	52.4	986	1545	12204	14924

Table 1: The performance of Attack 1 on the protocol based on polynomials

Dimension	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Number of Minimal Solutions	4	6	16	3125	5040	6480	22400	32256	40000
Number of Tested Minimal Solutions	1	4	12	31	1	1	709	5351	6321
Time Taken (seconds)	0.01	0.03	0.1	11.4	32.5	47.1	1121	10362	14073

Table 2: The performance of Attack 1 on the protocol based on circulants

To compare these results with the efficiency of Kotov-Ushakov attack in the tropical case, we demonstrate here the results of our numerical experiments (Figure 3) presented previously in [1].

Figures 4 show the success rate and time spent by Attack 2 on Protocol 1 (which is a heuristic versio of the Kotov-Ushakov attack). Unfortunately, this attack performs very poorly against Protocol 2, with success rate dropping to 0% already for very low dimensions. Obviously, this heuristic is much faster that Attack 1 since it avoids enumerating all minimal solutions.

Another advantage for max-min protocols over the tropical ones is that the max-min protocols demonstrate greater resilience against the two-sided discrete logarithm attacks. This is attributed to the rarity of a single monomial dominating in the polynomial, unlike

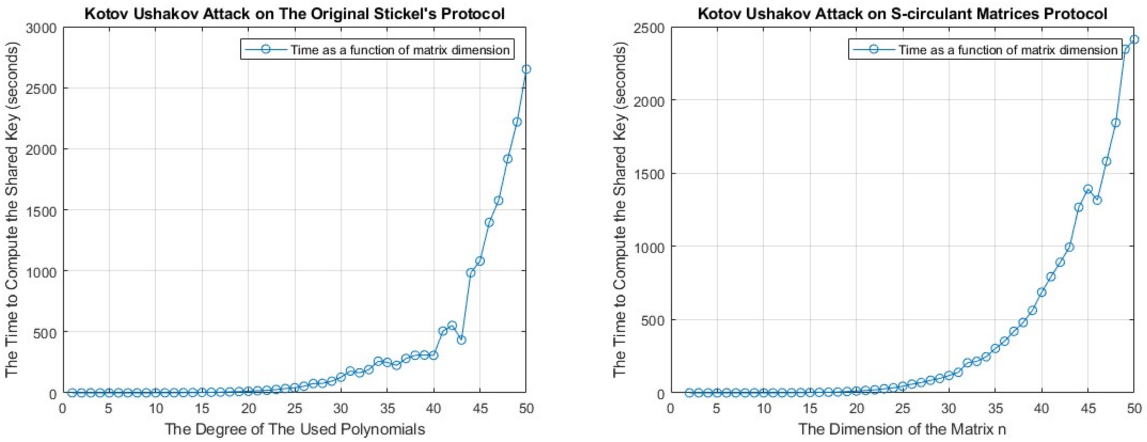

Figure 3: Time taken for Kotov-Ushakov attack to break Tropical Stickel Protocol based on polynomials (left) and modified circulants (right) [1].

the tropical version where such dominance is much more common. To assess the frequency of single monomial dominance in both max-min and tropical cases, we conducted a simple numerical experiment where we sampled the matrix entries and polynomial coefficients from $[-1000, 1000]$ and noticed that a single monomial represents a 10-th degree polynomial 83% of the times, compared with 0% for the max-min case.

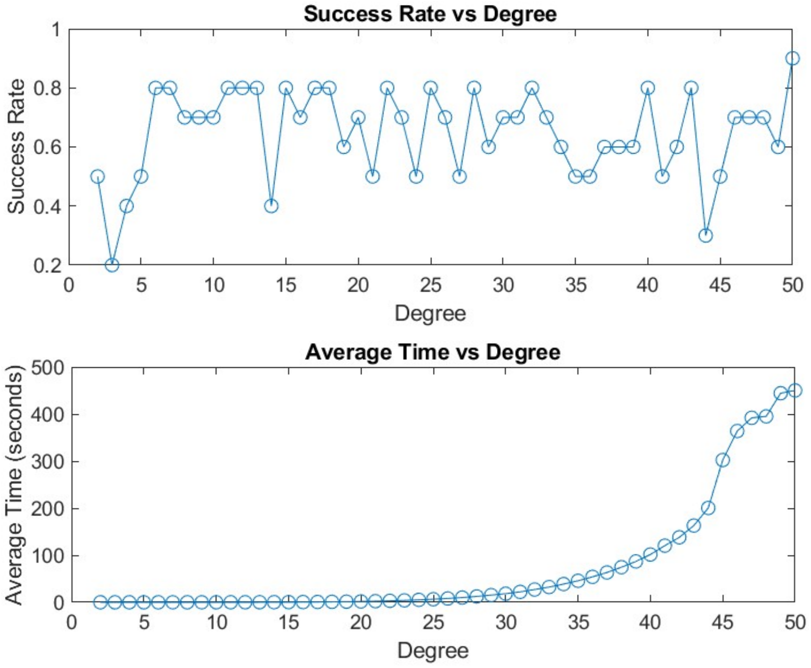

Figure 4: Success rate and time of Attack 2 on Protocol 1

6 Conclusions

In this work we have suggested to implement Stickel protocol over max-T semirings, starting with the most familiar max-min (fuzzy) semiring and considering two versions of it: based on polynomials and based on modified circulants. We also formulated a max-min/max-T analogue of Kotov-Ushakov attack which, like in the case of the original Kotov-Ushakov attack, enumerates all minimal solutions and, among the solution set that a minimal solution defines, tries to find a solution that has the required structure.

It may be concerning that the max-min semiring does not produce new numbers and therefore the keys generated by Alice and Bob have only a small number of different entries. While this tends to be the case (especially when compared with the tropical versions of the same protocols), the number of different entries is significant and in general does not allow for a quick brute force attack. Potentially, an implementation using a different T-norm can improve it further.

The max-min implementation seems more resistant to the existing attacking techniques such as the Kotov-Ushakov attack mostly because of the much bigger number of minimal solutions, which skyrockets as the degree of polynomial or the dimension of the circulant increases.

Our attempt to implement the Kotov-Ushakov attack heuristically is not very successful, especially in the case of modified circulants. Even in the case of polynomials the success rate is not overwhelming and the time taken is higher compared to the heuristic techniques in the tropical case (see [1]).

The future research could focus on picking some interesting classes of T-norms to provide more secure platforms for the Stickel (and possibly other) protocols or on further improvement of the Kotov-Ushakov attack on this protocol over various semirings.

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] B. Amutha and R. Perumal. Key exchange protocols based on tropical circulant and anti-circulant matrices. *AIMS Mathematics*, 8(7):17304–17334, 2023.

[3] C. Collett. Public key cryptography in max-plus algebra. Master's thesis, University of Birmingham, School of Mathematics, Birmingham, UK, June 2023.

[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 and A. Lettieri. Finite BL algebras. *Discrete Mathematics*, 269:93–112, 2003.

[6] 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.

[7] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

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

[9] M. Gavalec, Z. Němcová, and S. Sergeev. Tropical linear algebra with the Łukasiewicz T-norm. *Fuzzy Sets and Systems*, 276:131–148, 2015. Theme: Logic and Algebra.

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

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

[12] M. Higashi and G.J. Klir. Resolution of finite fuzzy relation equations. *Fuzzy Sets and Systems*, 13:65–82, 1984.

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

[14] 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.

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

[16] 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.

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

[18] 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.

[19] V. Nitica and S. Sergeev. Tropical convexity over max-min semiring. In G.L. Litvinov and S.N. Sergeev, editors, *Tropical and Idempotent Mathematics and Applications*, volume 616 of *Contemporary Mathematics*, pages 241–260. American Mathematical Society, 2014.

[20] 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.

[21] D. Rudy and C. Monico. Remarks on a tropical key exchange system. *Journal of Mathematical Cryptology*, 15(1):280–283, 2020.

[22] 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.

[23] 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

A Appendices

A.1 Upper s-circulant matrices commute [3]

Let A be an upper s-circulant matrix with parameters $c_0, c_1, c_2 \ldots, c_{n-1}$ and let B be an upper-s-circulant matrix with parameters $d_0, d_1, d_2 \ldots, d_{n-1}$, then we have

$$A = \begin{pmatrix} c_0 & c_{n-1} \otimes s & c_{n-2} \otimes s & \cdots & c_1 \otimes s \\ c_1 & c_0 & c_{n-1} \otimes s & \cdots & c_2 \otimes s \\ c_2 & c_1 & c_0 & \cdots & c_3 \otimes s \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{n-1} & c_{n-2} & c_{n-3} & \cdots & c_0 \end{pmatrix} \quad B = \begin{pmatrix} d_0 & d_{n-1} \otimes s & d_{n-2} \otimes s & \cdots & d_1 \otimes s \\ d_1 & d_0 & d_{n-1} \otimes s & \cdots & d_2 \otimes s \\ d_2 & d_1 & d_0 & \cdots & d_3 \otimes s \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ d_{n-1} & d_{n-2} & d_{n-3} & \cdots & d_0 \end{pmatrix}$$

$$\text{and} \quad A \otimes B = \begin{pmatrix} e_{11} & e_{12} & e_{13} & \cdots & e_{1n} \\ e_{21} & e_{22} & e_{23} & \cdots & e_{2n} \\ e_{31} & e_{32} & e_{33} & \cdots & e_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ e_{n1} & e_{n2} & e_{n3} & \cdots & e_{nn} \end{pmatrix},$$

where

$$
\begin{aligned}
e_{11} &= (c_0 \otimes d_0) \oplus (c_{n-1} \otimes s \otimes d_1) \oplus (c_{n-2} \otimes s \otimes d_2) \oplus \cdots \oplus (c_1 \otimes s \otimes d_{n-1}) \\
e_{21} &= (c_1 \otimes d_0) \oplus (c_0 \otimes d_1) \oplus (c_{n-1} \otimes s \otimes d_2) \oplus \cdots \oplus (c_2 \otimes s \otimes d_{n-1}) \\
e_{31} &= (c_2 \otimes d_0) \oplus (c_1 \otimes d_1) \oplus (c_0 \otimes d_2) \oplus \cdots \oplus (c_3 \otimes s \otimes d_{n-1}) \\
&\vdots \\
e_{n1} &= (c_{n-1} \otimes d_0) \oplus (c_{n-2} \otimes d_1) \oplus (c_{n-3} \otimes d_2) \oplus \cdots \oplus (c_0 \otimes d_{n-1}) \\
e_{12} &= (c_0 \otimes d_{n-1} \otimes s) \oplus (c_{n-1} \otimes s \otimes d_0) \oplus (c_{n-2} \otimes s \otimes d_1) \oplus \cdots \oplus (c_1 \otimes s \otimes d_{n-2}) \\
e_{22} &= (c_1 \otimes d_{n-1} \otimes s) \oplus (c_0 \otimes d_0) \oplus (c_{n-1} \otimes s \otimes d_1) \oplus \cdots \oplus (c_2 \otimes s \otimes d_{n-2}) \\
e_{32} &= (c_2 \otimes d_{n-1} \otimes s) \oplus (c_1 \otimes d_0) \oplus (c_0 \otimes d_1) \oplus \cdots \oplus (c_3 \otimes s \otimes d_{n-2}) \\
&\vdots \\
e_{n2} &= (c_{n-1} \otimes d_{n-1} \otimes s) \oplus (c_{n-2} \otimes d_0) \oplus (c_{n-3} \otimes d_1) \oplus \cdots \oplus (c_0 \otimes d_{n-2}) \\
e_{13} &= (c_0 \otimes d_{n-2} \otimes s) \oplus (c_{n-1} \otimes s \otimes d_{n-1} \otimes s) \oplus (c_{n-2} \otimes s \otimes d_0) \oplus \cdots \oplus (c_1 \otimes s \otimes d_{n-3}) \\
e_{23} &= (c_1 \otimes d_{n-2} \otimes s) \oplus (c_0 \otimes d_{n-1} \otimes s) \oplus (c_{n-1} \otimes s \otimes d_0) \oplus \cdots \oplus (c_2 \otimes s \otimes d_{n-3}) \\
e_{33} &= (c_2 \otimes d_{n-2} \otimes s) \oplus (c_1 \otimes d_{n-1} \otimes s) \oplus (c_0 \otimes d_0) \oplus \cdots \oplus (c_3 \otimes s \otimes d_{n-3}) \\
\vdots \\
e_{n3} &= (c_{n-1} \otimes d_{n-2} \otimes s) \oplus (c_{n-2} \otimes d_{n-1} \otimes s) \oplus (c_{n-3} \otimes d_0) \oplus \cdots \oplus (c_0 \otimes d_{n-3}) \\
e_{1n} &= (c_0 \otimes d_1 \otimes s) \oplus (c_{n-1} \otimes s \otimes d_2 \otimes s) \oplus (c_{n-2} \otimes s \otimes d_3 \otimes s) \oplus \cdots \oplus (c_1 \otimes s \otimes d_0) \\
e_{2n} &= (c_1 \otimes d_1 \otimes s) \oplus (c_0 \otimes d_2 \otimes s) \oplus (c_{n-1} \otimes s \otimes d_3 \otimes s) \oplus \cdots \oplus (c_2 \otimes s \otimes d_0) \\
e_{3n} &= (c_2 \otimes d_1 \otimes s) \oplus (c_1 \otimes d_2 \otimes s) \oplus (c_0 \otimes d_3 \otimes s) \oplus \cdots \oplus (c_3 \otimes s \otimes d_0) \\
\vdots \\
e_{nn} &= (c_{n-1} \otimes d_1 \otimes s) \oplus (c_{n-2} \otimes d_2 \otimes s) \oplus (c_{n-3} \otimes d_3 \otimes s) \oplus \cdots \oplus (c_0 \otimes d_0)
\end{aligned}
$$

We can simplify these equations, remembering that the subscripts are always integers, therefore, if $i, j \in \mathbb{Z}$ and $0 \leq i, j \leq n-1$ we can rewrite these as

$$e_{11} = \bigoplus_{i+j=0} (c_i \otimes d_j) \oplus \bigoplus_{i+j=n} (s \otimes c_i \otimes d_j)$$

$$e_{21} = \bigoplus_{i+j=1} (c_i \otimes d_j) \oplus \bigoplus_{i+j=n+1} (s \otimes c_i \otimes d_j)$$

$$e_{31} = \bigoplus_{i+j=2} (c_i \otimes d_j) \oplus \bigoplus_{i+j=n+2} (s \otimes c_i \otimes d_j)$$

$$\vdots$$

$$e_{n1} = \bigoplus_{i+j=n-1} (c_i \otimes d_j)$$

$$e_{12} = \bigoplus_{i+j=n-1} (s \otimes c_i \otimes d_j)$$

$$e_{22} = \bigoplus_{i+j=0} (c_i \otimes d_j) \oplus \bigoplus_{i+j=n} (s \otimes c_i \otimes d_j)$$

$$e_{32} = \bigoplus_{i+j=1} (c_i \otimes d_j) \oplus \bigoplus_{i+j=n+1} (s \otimes c_i \otimes d_j)$$

$$\vdots$$

$$e_{n2} = \bigoplus_{i+j=n-2} (c_i \otimes d_j) \oplus \bigoplus_{i+j=2n-2} (s \otimes c_i \otimes d_j)$$

$$e_{13} = \bigoplus_{i+j=n-2} (s \otimes c_i \otimes d_j) \oplus \bigoplus_{i+j=2n-2} \left(s^{\otimes 2} \otimes c_i \otimes d_j\right)$$

$$e_{23} = \bigoplus_{i+j=n-1} (s \otimes c_i \otimes d_j)$$

$$e_{33} = \bigoplus_{i+j=0} (c_i \otimes d_j) \oplus \bigoplus_{i+j=n} (s \otimes c_i \otimes d_j)$$

$$e_{n3} = \bigoplus (c_i \otimes d_j) \oplus \bigoplus_{i+j=2n-3} (c_i \otimes d_j)$$

$$e_{1n} = \bigoplus_{i+j=1} (s \otimes c_i \otimes d_j) \oplus \bigoplus_{i+j=n+1} \left(s^{\otimes 2} \otimes c_i \otimes d_j\right)$$

$$e_{2n} = \bigoplus_{i+j=2} (s \otimes c_i \otimes d_j) \oplus \bigoplus_{i+j=n+2} \left(s^{\otimes 2} \otimes c_i \otimes d_j\right)$$

$$e_{3n} = \bigoplus_{i+j=3} (s \otimes c_i \otimes d_j) \oplus \bigoplus_{i+j=n+3} \left(s^{\otimes 2} \otimes c_i \otimes d_j\right)$$

$$\vdots$$

$$e_{nn} = \bigoplus_{i+j=0} (c_i \otimes d_j) \oplus \bigoplus_{i+j=n} (s \otimes c_i \otimes d_j)$$

Therefore, in general we have :

$$e_{pq} = \bigoplus_{i+j=p-q} (c_i \otimes d_j) \oplus \bigoplus_{i+j=n+p-q} (s \otimes c_i \otimes d_j) \oplus \bigoplus_{i+j=2n+p-q} \left(s^{\otimes 2} \otimes c_i \otimes d_j\right), \quad 1 \leq p, q \leq n.$$

Here and below we will assume $0 \leq i, j \leq n-1$. We now consider $B \otimes A$

$$B \otimes A = \begin{pmatrix} f_{11} & f_{12} & f_{13} & \cdots & f_{1n} \\ f_{21} & f_{22} & f_{23} & \cdots & f_{2n} \\ f_{31} & f_{32} & f_{33} & \cdots & f_{3n} \\ \vdots & \vdots & \vdots & \ddots & \cdots \\ f_{n1} & f_{n2} & f_{n3} & \cdots & f_{nn} \end{pmatrix}$$

In a similar manner, we find a general formula for f_{pq} as

$$f_{pq} = \bigoplus_{i+j=p-q} (d_i \otimes c_j) \oplus \bigoplus_{i+j=n+p-q} (s \otimes d_i \otimes c_j) \oplus \bigoplus_{i+j=2n+p-q} \left(s^{\otimes 2} \otimes d_i \otimes c_j\right), \quad 1 \leq p, q \leq n.$$

We notice the solutions to $i + j = r$ for some r, where i, j are integers inclusively between 1 and $n-1$ and r is an integer inclusively between 1 and $2n-2$, are symmetric. For example $i + j = 1$ has solutions $(1, 0)$ and $(0, 1)$. This implies that

$$\begin{aligned} e_{pq} &= \bigoplus_{i+j=p-q} (c_i \otimes d_j) \oplus \bigoplus_{i+j=n+p-q} (s \otimes c_i \otimes d_j) \oplus \bigoplus_{i+j=2n+p-q} \left(s^{\otimes 2} \otimes c_i \otimes d_j\right) \\ &= \bigoplus_{i+j=p-q} (d_i \otimes c_j) \oplus \bigoplus_{i+j=n+p-q} (s \otimes d_i \otimes c_j) \oplus \bigoplus_{i+j=2n+p-q} \left(s^{\otimes 2} \otimes d_i \otimes c_j\right) \\ &= f_{pq} \quad 1 \leq p, q \leq n. \end{aligned}$$

As $e_{pq} = f_{pq}$ for all p and q, we obtain

$$A \otimes B = \begin{pmatrix} e_{11} & e_{12} & e_{13} & \cdots & e_{1n} \\ e_{21} & e_{22} & e_{23} & \cdots & e_{2n} \\ e_{31} & e_{32} & e_{33} & \cdots & e_{3n} \\ \vdots & \vdots & \vdots & \ddots & \cdots \\ e_{n1} & e_{n2} & e_{n3} & \cdots & e_{nn} \end{pmatrix} = \begin{pmatrix} f_{11} & f_{12} & f_{13} & \cdots & f_{1n} \\ f_{21} & f_{22} & f_{23} & \cdots & f_{2n} \\ f_{31} & f_{32} & f_{33} & \cdots & f_{3n} \\ \vdots & \vdots & \vdots & \ddots & \cdots \\ f_{n1} & f_{n2} & f_{n3} & \cdots & f_{nn} \end{pmatrix} = B \otimes A.$$

Thus any two upper s-circulant matrices commute.

A.2 Upper s-circulant matrices are a semiring [3]

Recall that

$$e_{pq} = \bigoplus_{i+j=p-q} (c_i \otimes d_j) \oplus \bigoplus_{i+j=n+p-q} (s \otimes c_i \otimes d_j) \oplus \bigoplus_{i+j=2n+p-q} \left(s^{\otimes 2} \otimes c_i \otimes d_j\right), \quad 1 \leq p, q \leq n$$

We observe that $e_{pq} = e_{(p+1)(q+1)}$ as

$$e_{(p+1)(q+1)} = \bigoplus_{i+j=(p+1)-(q+1)} (c_i \otimes d_j) \oplus \bigoplus_{i+j=n+(p+1)-(q+1)} (s \otimes c_i \otimes d_j) \oplus \bigoplus_{i+j=2n+(p+1)-(q+1)} \left(s^{\otimes 2} \otimes c_i \otimes d_j\right)$$

$$= \bigoplus_{i+j=(p-q)} (c_i \otimes d_j) \oplus \bigoplus_{i+j=n+p-q} (s \otimes c_i \otimes d_j) \oplus \bigoplus_{i+j=2n+p-q} \left(s^{\otimes 2} \otimes c_i \otimes d_j\right) = e_{pq}$$

So we have

$$e_{pq} = e_{(p+1)(q+1)} \quad \text{for } 1 \leq p, q \leq n.$$

As we have shown that all entries on the sme diagonal of $A \otimes B$ are equal to each other, in order to show that it is an upper s-circulant matrix, it remains to show that the first column and the first row are as they should be in an upper s-circulant matrix. For example, we need to show that $e_{12} = e_{n1} \otimes s$ and $e_{13} = e_{(n-1)1} \otimes s$. We do not need to consider e_{00}. In general we need to show that

$$e_{1q} = s \otimes e_{(n+2-q)1} \quad \text{for } 2 \leq q \leq n.$$

Using our general formula we see that

$$e_{1q} = \bigoplus_{i+j=1-q} (c_i \otimes d_j) \oplus \bigoplus_{i+j=n+1-q} (s \otimes c_i \otimes d_j) \oplus \bigoplus_{i+j=2n+1-q} \left(s^{\otimes 2} \otimes c_i \otimes d_j\right)$$

$$= \bigoplus_{i+j=n+1-q} (s \otimes c_i \otimes d_j) \oplus \bigoplus_{i+j=2n+1-q} \left(s^{\otimes 2} \otimes c_i \otimes d_j\right)$$

$$= s \otimes \left(\bigoplus_{i+j=n+1-q} (c_i \otimes d_j) \oplus \bigoplus_{i+j=2n+1-q} (s \otimes c_i \otimes d_j) \right), \quad 2 \leq q \leq n.$$

We also have

$$s \otimes e_{(n-q+2)1} = s \otimes \left(\bigoplus_{i+j=(n+2-q)-1} (c_i \otimes d_j) \oplus \bigoplus_{i+j=n+(n+2-q)-1} (s \otimes c_i \otimes d_j) \oplus \bigoplus_{i+j=2n+(n+2-q)-1} \left(s^{\otimes 2} \otimes c_i \otimes d_j\right) \right), \quad 2 \leq q \leq n.$$

$$= s \otimes \left(\bigoplus_{i+j=n+1-q} (c_i \otimes d_j) \oplus \bigoplus_{i+j=2n+1-q} (s \otimes c_i \otimes d_j) \oplus \bigoplus_{i+j=3n-q+1} \left(s^{\otimes 2} c_i \otimes d_j\right) \right)$$

$$= s \otimes \left(\bigoplus_{i+j=n+1-q} (c_i \otimes d_j) \oplus \bigoplus_{i+j=2n-q-1} (s \otimes c_i \otimes d_j) \right) = e_{1q} \quad \text{for } 2 \leq q \leq n$$

Therefore, we have shown that

$$e_{1q} = s \otimes e_{(n+2-q)1} \quad \text{for } 2 \leq q \leq n$$

Using the above equations we can see that $A \otimes B = B \otimes A$ is indeed an upper s-circulant. We are left to show that $A \oplus B \in C_n^s$ to prove that the set of upper s-circulant matrices is indeed a (commutative) semiring. This follows since

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

$$\oplus \begin{pmatrix} d_0 & d_{n-1} \otimes s & d_{n-2} \otimes s & \cdots & d_1 \otimes s \\ d_1 & d_0 & d_{n-1} \otimes s & \cdots & d_2 \otimes s \\ d_2 & d_1 & d_0 & \cdots & d_3 \otimes s \\ \vdots & \vdots & \vdots & \ddots & \cdots \\ d_{n-1} & d_{n-2} & d_{n-3} & \cdots & d_0 \end{pmatrix}$$

$$= \begin{pmatrix} c_0 \oplus d_0 & (c_{n-1} \oplus d_{n-1}) \otimes s & (c_{n-2} \oplus d_{n-2}) \otimes s & \cdots & (c_1 \oplus d_1) \otimes s \\ c_1 \oplus d_1 & c_0 \oplus d_0 & (c_{n-1} \oplus d_{n-1}) \otimes s & \cdots & (c_2 \oplus d_2) \otimes s \\ c_2 \oplus d_2 & c_1 \oplus d_1 & c_0 \oplus d_0 & \cdots & (c_3 \oplus d_3) \otimes s \\ \vdots & \vdots & \vdots & \ddots & \cdots \\ c_{n-1} \oplus d_{n-1} & c_{n-2} \oplus d_{n-2} & c_{n-3} \oplus d_{n-3} & \cdots & c_0 \oplus d_0 \end{pmatrix}$$

This is an upper s-circulant matrix with entries $(c_0 \oplus d_0), (c_1 \oplus d_1), \ldots, (c_{n-1} \oplus d_{n-1})$. Hence $A \oplus B \in C_n^s$ and due to the commutative property of $\oplus$, we also have that $B \oplus A \in C_n^s$. Hence C_n^s is indeed a commutative semiring.