# Another Cryptanalysis of a Tropical Key Exchange Protocol

Jackson J and Perumal R*

***Abstract*—In this paper, we undertake a comprehensive analysis of the Two-party public key exchange protocol proposed by Grigoriev & Shpilrain in 2019 which is intriguingly based on the homomorphism of tropical matrix algebras. The protocol was first hailed as a potential improvement in tropical cryptographic approaches. Subsequent cryptanalysis, however, has raised concerns regarding its vulnerability to attacks aiming at getting the secret parameters. The cryptanalytic efforts directed towards this key exchange protocol have not been in vain, as they have unequivocally declared its lack of robustness, ultimately classifying it as an insecure method for secure information exchange. Recognizing the critical importance of addressing such security weaknesses in modern cryptographic systems, our research focuses on uncovering novel and efficient approaches to circumvent the protocol's security. As part of our contribution to the field, we propose an ingenious attack on this specific key exchange protocol. Remarkably, our attack is unique in that it does not necessitate the extraction of any private parameters. Rather, it capitalizes on leveraging the knowledge of public parameters and exploiting certain algebraic properties inherent to the protocol. This innovative strategy represents a significant departure from conventional attacks, which often rely on the extraction of private keys or exhaustive computations.**

***Index Terms*—Cryptography, Cryptanalysis, Key exchange, Tropical algebra, Tropical semirings.**

## I. Introduction

CRYPTOGRAPHY is the art of establishing a secure communication between the sender and the receiver of an information. In 1976, Diffie and Hellman [8] proposed a significant two party key exchange system which paved the way for today's modern cryptography. Subsequently, numerous researchers embraced the Diffie and Hellman protocol as a basis to develop more robust and secure key exchange schemes [2], [3], [4], [5], [7], [14], [23], [27]. Despite the widespread adoption, these protocols did not remain impervious to scrutiny, and various attacks were proposed to expose their vulnerabilities [12], [13], [17], [30]. Such analyses served as essential contributions to the ongoing efforts in cryptographic research, aiming to fortify the security of key exchange methods and ensure the confidentiality of sensitive information in digital communication. In 2005, Stickel introduced a novel key exchange protocol aiming to securely exchange secret keys over a public channel [31]. However, in 2008, this protocol came under cryptanalysis by Sphilrain [29]. In response to the challenges faced by Stickel's protocol, Grigoriev and Sphilrain proposed another key exchange protocol in 2014 [15]. This innovative approach leveraged the principles of tropical algebra as a foundation for generating secure secret keys. Their research demonstrated that this newly proposed protocol effectively withstands attacks based on linear algebra techniques.

In the pursuit of secure key exchange methods, Durcheva & Trendafilov, Durcheva, and Durcheva & Rachev have also contributed to the field by proposing key exchange protocols rooted in tropical matrices. These protocols offer promising avenues for enhancing security in the exchange of secret keys. Durcheva & Trendafilov's work was presented in [9], Durcheva's individual contribution in [10], and Durcheva & Rachev's collaborative effort in [11]. Despite the advancements made by Grigoriev and Sphilrain's protocol, it faced challenges when Kotov and Ushakov [22] carried out an attack in 2018. Their attack harnessed the properties of tropical matrices and tropical polynomials to undermine the security of the protocol. Kotov et. al. found out that the tropical matrices displays pattern in increasing powers of the matrices [19], [32]. By using this property the private parameters were obtained easily.

These collective research efforts underscore the ongoing pursuit of robust and secure key exchange protocols in the face of ever-evolving cryptanalytic techniques. As researchers continue to explore the potential of tropical algebra and related mathematical concepts, the cryptographic community remains committed to ensuring the confidentiality and integrity of secret key exchanges in modern communication systems. To avoid pattern in the powers of matrix, in 2019 Grigoriev & Shpilrain [16] proposed another key exchange protocol which is based on the extension of tropical matrix algebras by homomorphisms. This protocol was cryptanalysed by Rudy & Monico [28] in 2020. They attacked the protocol by recovering the private parameters with a simple binary search. In 2021, Isaac & Kahrobaei [18] proposed an attack on the same protocol which uses the almost linear periodicity property [26] of the matrices defined in Grigoriev's protocol which has a success rate of 100%. They also showed that the second protocol proposed by Grigoriev & Shpilrain cannot be implemented. Another cryptanalysis on the same protocol was given by Muanalifah and Sergeev [25] in 2021 based on the solution of discrete logarithm problem in tropical algebra and they proposed a new key exchange scheme [24]. All the attacks [18], [22], [25] shows that the key exchange scheme proposed by Grigoriev & Shpilrain is insecure. The tropical key exchange schemes were furthered studied in [6], [20], [21]. For a more detailed analysis of tropical key exchange schemes and its attacks, one can refer the paper

Manuscript received February 09, 2023; revised September 04, 2023.

Jackson J is a Research Scholar in the Department of Mathematics, College of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur-603203, Tamilnadu, India. (e-mail: jj3375@srmist.edu.in)

Perumal R is an Assistant Professor in the Department of Mathematics, College of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur-603203, Tamilnadu, India. (Corresponding author to provide e-mail: perumalr@srmist.edu.in)

by Ahmed et. al. [1].

In this paper, we propose a new attack on this key exchange scheme which do not require to recover any private parameters to get the shared secret key. With only the known public parameters and some algebraic properties of tropical matrices we can obtain the shared secret key. With our approach, we demonstrate the ability to obtain the shared secret key with impressive efficiency. Our findings reveal that our attack outperforms all other known attacks on this particular key exchange scheme. The speed and efficacy of our method underscore the urgent need for revisiting the security considerations of cryptographic protocols, especially when deploying them in critical applications where information confidentiality is paramount. By shedding light on the vulnerabilities of this public key exchange protocol and proposing a powerful attack strategy, we aim to enhance the overall understanding of cryptographic algorithm design and foster more secure communication systems in the digital age. The insights gained from this research contribute significantly to the ongoing efforts to fortify the foundations of modern cryptography and safeguard sensitive data against potential threats posed by adversaries in an ever-evolving digital era. In Section 2, we have given some preliminaries of tropical algebra. In Section 3, we have given the protocol described in [16]. The proposed attack with an example and algorithm is described in Section 4. Finally, we have concluded with some results of the attack.

## II. Preliminaries

Tropical algebra, also known as max-plus algebra, is a fascinating and relatively young branch of mathematics that emerged in the 1980s as a specialized area of semiring theory. Tropical algebra finds applications in diverse fields such as optimization, control theory, graph theory, and, interestingly, cryptography. The utilization of tropical algebra in cryptographic protocols offers an innovative perspective to tackle the challenges of secure key exchange.

### A. Tropical matrix algebra

In tropical algebra, the usual addition (+) and multiplication ($\cdot$) is replaced with tropical addition (denoted by $\oplus$) and tropical multiplication (denoted by $\odot$) respectively. The following are the two tropical binary operations.

- $x \oplus y = \max(x, y)$ (or) $x \oplus y = \min(x, y)$
- $x \odot y = x + y$.

This seemingly unconventional approach brings about intriguing properties, such as idempotence, where repeated operations yield the same result.

A tropical semiring is a semiring with tropical binary operations. $(\mathbb{R} \cup \{\infty\}, \oplus, \odot)$ is called min-plus semiring, where $x \oplus y = \min(x, y)\ \forall\ x, y \in (\mathbb{R} \cup \{\infty\})$ and $x \odot y = x + y\ \forall\ x, y \in (\mathbb{R} \cup \{\infty\})$. Matrix operations in tropical algebra are similar to traditional matrix operations, except that the operations have been replaced by tropical addition and multiplication.

Let $A = [a_{ij}] \in \mathbb{R}^{m\times n}$ and $B = [b_{ij}] \in \mathbb{R}^{m\times n}$, then $A \oplus B$ is obtained by evaluating the tropical sum of the corresponding elements of $A$ and $B$. Let $A \oplus B = C = [c_{ij}]$ then,

$$c_{ij} = a_{ij} \oplus b_{ij} = \min\{a_{ij}, b_{ij}\}$$

where, $i \in [1, m]\ and\ j \in [1, n]$.

Let $A = [a_{ij}] \in \mathbb{R}^{m\times n}$ and $B = [b_{ij}] \in \mathbb{R}^{n\times p}$. Then, the tropical matrix multiplication, $A \odot B \in \mathbb{R}^{m\times p}$, is given by the matrix $C = [c_{ij}]$ where the entries are,

$$c_{ij} = \bigoplus_{k=1}^{n} a_{ik} \odot b_{kj} = \min\{a_{ik} + b_{kj}\}$$

where, $k \in [1, n], i \in [1, m]\ \&\ j \in [1, p]$.

*Definition 1:* The adjoint multiplication (denoted as "$\circ$") of two elements $x, y$ is defined as

$$x \circ y = x + y + x \cdot y$$

where, '$+$' denotes addition and '$\cdot$' denotes multiplication.

The extension of $\mathbb{Z}$ forms a semigroup under the operation

$$(a, b)(c, d) = ((a \circ d) \oplus c, b \circ d)$$

## III. The protocol

In modern cryptography, key exchange protocols play a vital role in facilitating secure communication between parties over insecure channels. The fundamental challenge in secure key exchange lies in establishing a shared secret key between two entities while safeguarding it from potential eavesdroppers or attackers. Traditional key exchange protocols, such as Diffie-Hellman, rely on the hardness of certain mathematical problems, like discrete logarithms, to ensure the confidentiality of the exchanged keys. However, with the advent of quantum computing and advancements in cryptanalysis, some of these protocols are becoming susceptible to attacks, warranting the exploration of novel and robust alternatives.

In the subsequent section, we delve into a detailed exploration of the protocol presented by Grigoriev & Shpilrain in their seminal work [16]. This particular protocol holds significant importance in the realm of tropical cryptographic research, and we thoroughly examine its fundamental principles, design, and underlying mechanisms. Through this in-depth analysis, we aim to provide a comprehensive understanding of the protocol's strengths and weaknesses.

### A. Protocol description

Let $S = (M_n(\mathbb{Z}), \oplus, \odot)$ be a tropical semiring of matrices over $\mathbb{Z}$ of order $n$.

- Alice and Bob agree on public matrices $M$ and $H$, where $M, H \in S$.
- Alice selects a private $m \in \mathbb{N}$. She then calculates $(M, H)^m = (A, H^m)$ and sends $A$ to Bob.
- Bob selects a private $n \in \mathbb{N}$. She then calculates $(M, H)^n = (B, H^n)$ and sends $B$ to Bob.
- Alice computes $K_a = (B \circ H^m) \oplus A$.
- Bob computes $K_b = (A \circ H^n) \oplus B$.

Now, $K_a = K_b$ is the shared secret key of Alice and Bob.

In this tropical key exchange scheme, the parties involved employ a unique mathematical approach inspired by the tropical algebraic structure. Unlike traditional cryptographic methods, this scheme employs max-plus algebra to perform computations that ensure security in an unconventional yet efficient manner. The authors claim that, since the first component incorporates products of matrices M and H, which differ in length and order, discerning any discernible pattern within the resulting matrix's entries becomes challenging. Yet, we deploy an attack on this protocol.

### B. Example

The following is a simplified illustration of a key exchange protocol in the form of a toy example. This example aims to provide a basic understanding of how the key exchange protocol functions.

- Let $M = \begin{bmatrix} -128 & -325 \\ 145 & -164 \end{bmatrix}$, $H = \begin{bmatrix} 535 & 165 \\ 255 & -134 \end{bmatrix}$ be the two public matrices chosen by Alice and Bob.
- Alice selects her private parameter, $m = 12$.
- Now, she calculates,

$$(M,H)^{12} = \left(\begin{bmatrix} -128 & -325 \\ 145 & -164 \end{bmatrix}, \begin{bmatrix} 535 & 165 \\ 255 & -134 \end{bmatrix}\right)^{12} = \left(\begin{bmatrix} -1410 & -1799 \\ -1249 & -1638 \end{bmatrix}, \begin{bmatrix} 535 & 165 \\ 255 & -134 \end{bmatrix}^{12}\right)$$

  and sends the matrix $A = \begin{bmatrix} -1410 & -1799 \\ -1249 & -1638 \end{bmatrix}$ to Bob.
- Similarly, Bob selects his private parameter, $n = 7$.
- Bob then calculates,

$$(M,H)^{7} = \left(\begin{bmatrix} -128 & -325 \\ 145 & -164 \end{bmatrix}, \begin{bmatrix} 535 & 165 \\ 255 & -134 \end{bmatrix}\right)^{7} = \left(\begin{bmatrix} -740 & -1129 \\ -579 & -968 \end{bmatrix}, \begin{bmatrix} 535 & 165 \\ 255 & -134 \end{bmatrix}^{7}\right)$$

  and sends the matrix $B = \begin{bmatrix} -740 & -1129 \\ -579 & -968 \end{bmatrix}$ to Alice.
- Alice now computes,

$$\begin{aligned} K_a &= (B \circ H^m) \oplus A \\ &= \left(\begin{bmatrix} -740 & -1129 \\ -579 & -968 \end{bmatrix} \circ \begin{bmatrix} 535 & 165 \\ 255 & -134 \end{bmatrix}^{12}\right) \oplus \begin{bmatrix} -1410 & -1799 \\ -1249 & -1638 \end{bmatrix} \\ &= \left(\begin{bmatrix} -740 & -1129 \\ -579 & -968 \end{bmatrix} \odot \begin{bmatrix} 535 & 165 \\ 255 & -134 \end{bmatrix}^{12}\right) \oplus \begin{bmatrix} -740 & -1129 \\ -579 & -968 \end{bmatrix} \oplus \begin{bmatrix} 535 & 165 \\ 255 & -134 \end{bmatrix}^{12} \oplus \begin{bmatrix} -1410 & -1799 \\ -1249 & -1638 \end{bmatrix} \\ &= \begin{bmatrix} -2348 & -2737 \\ -2187 & -2576 \end{bmatrix} \oplus \begin{bmatrix} -740 & -1129 \\ -579 & -968 \end{bmatrix} \oplus \begin{bmatrix} -920 & -1309 \\ -1219 & -1608 \end{bmatrix} \oplus \begin{bmatrix} -1410 & -1799 \\ -1249 & -1638 \end{bmatrix} \\ K_a &= \begin{bmatrix} -2348 & -2737 \\ -2187 & -2576 \end{bmatrix} \end{aligned}$$

- Similarly, Bob computes,

$$\begin{aligned} K_b &= (A \circ H^n) \oplus B \\ &= \left(\begin{bmatrix} -1410 & -1799 \\ -1249 & -1638 \end{bmatrix} \circ \begin{bmatrix} 535 & 165 \\ 255 & -134 \end{bmatrix}^{7}\right) \oplus \begin{bmatrix} -740 & -1129 \\ -579 & -968 \end{bmatrix} \\ &= \left(\begin{bmatrix} -1410 & -1799 \\ -1249 & -1638 \end{bmatrix} \odot \begin{bmatrix} 535 & 165 \\ 255 & -134 \end{bmatrix}^{7}\right) \oplus \begin{bmatrix} -1410 & -1799 \\ -1249 & -1638 \end{bmatrix} \oplus \begin{bmatrix} 535 & 165 \\ 255 & -134 \end{bmatrix}^{7} \oplus \begin{bmatrix} -740 & -1129 \\ -579 & -968 \end{bmatrix} \\ &= \begin{bmatrix} -2348 & -2737 \\ -2187 & -2576 \end{bmatrix} \oplus \begin{bmatrix} -1410 & -1799 \\ -1249 & -1638 \end{bmatrix} \oplus \begin{bmatrix} -250 & -639 \\ -549 & -938 \end{bmatrix} \oplus \begin{bmatrix} -740 & -1129 \\ -579 & -968 \end{bmatrix} \\ K_b &= \begin{bmatrix} -2348 & -2737 \\ -2187 & -2576 \end{bmatrix} \end{aligned}$$

- Hence, Alice and Bob gets the same key , $K_a = K_b = \begin{bmatrix} -2348 & -2737 \\ -2187 & -2576 \end{bmatrix}$ which can be used as the shared secret key.

### C. The suggested parameters

The recommended parameters for the protocol are as follows,

- The order of the matrices is 30.
- The entries of the public matrices $M$ and $H$ are chosen uniformly randomly in [-1000,1000].
- The private exponents $m$ and $n$ are on the order $2^{200}$.

## IV. The attack

In this section, we present our novel and sophisticated attack on the public key exchange protocol proposed by Grigoriev & Shpilrain, which is founded on the intriguing principles of tropical matrix algebras. The primary goal of this attack is to demonstrate the vulnerability of the protocol and unveil potential security weaknesses that may have been overlooked in previous analyses.

The motivation behind conducting this attack stems from the critical importance of ensuring the robustness and confidentiality of cryptographic protocols, especially when they are applied in sensitive and mission-critical applications. As the digital landscape becomes increasingly dynamic and adversaries continuously evolve their tactics, the need for more resilient and secure cryptographic schemes is very important.

### A. Description of the attack

Let us consider two public matrices, $M$ and $H$, which have been independently chosen by Alice and Bob. Now, Alice selects her private parameter, denoted as $m$, and utilizes it to compute a new matrix, $A$. Subsequently, Alice shares this matrix $A$ with Bob. Likewise, Bob chooses his private parameter, represented as $n$, and employs it to calculate another matrix, referred to as $B$. Bob then communicates this matrix $B$ back to Alice.

*Theorem 1:* Let M,H be any two matrix of same dimension. Then,

$$(M,H)^n = (M \oplus H \oplus H^2 \oplus H^3 \oplus \cdots \oplus H^{n-1} \oplus (M \odot (H \oplus H^2 \oplus H^3 \oplus \cdots \oplus H^{n-1})), H^n)$$

*Proof:* We will prove this by induction on '$n$'

$$\begin{aligned}(M,H)^2 &= (M,H)(M,H)\\ &= ((M \circ H) \oplus M, H^2)\\ &= (M \oplus H \oplus MH, H^2)\end{aligned}$$

$$\begin{aligned}(M,H)^3 &= (M,H)^2(M,H)\\ &= (M \oplus H \oplus MH, H^2)(M,H)\\ &= (((M \oplus H \oplus MH) \circ H) \oplus M, H^3)\\ &= (M \oplus H \oplus MH \oplus H \oplus MH \oplus H^2 \oplus MH^2 \oplus M, H^3)\\ &= (M \oplus H \oplus H^2 \oplus MH \oplus MH^2, H^3)\end{aligned}$$

$$\begin{aligned}(M,H)^4 &= (M,H)^3(M,H)\\ &= (M \oplus H \oplus H^2 \oplus MH \oplus MH^2, H^3)(M,H)\\ &= (((M \oplus H \oplus H^2 \oplus MH \oplus MH^2) \circ H) \oplus M, H^4)\\ &= (M \oplus H \oplus H^2 \oplus MH \oplus MH^2 \oplus H \oplus MH \oplus H^2 \oplus H^3 \oplus MH^2 \oplus MH^3 \oplus M, H^4)\\ &= (M \oplus H \oplus H^2 \oplus H^3 \oplus MH \oplus MH^2 \oplus MH^3 , H^4)\end{aligned}$$

$$\vdots$$

$$\begin{aligned}(M,H)^n &= (M,H)^{n-1}(M,H)\\ &= (M \oplus H \oplus H^2 \oplus H^3 \oplus \cdots \oplus H^{n-2} \oplus MH \oplus MH^2 \oplus MH^3 \oplus \cdots \oplus MH^{n-2}, H^{n-1})(M ,H)\\ &= (((M \oplus H \oplus H^2 \oplus H^3 \oplus \cdots \oplus H^{n-2} \oplus MH \oplus MH^2 \oplus MH^3 \oplus \cdots \oplus MH^{n-2}) \circ H) \oplus M ,H^n)\\ &= ((M \oplus H \oplus H^2 \oplus H^3 \oplus \cdots \oplus H^{n-2} \oplus MH \oplus MH^2 \oplus MH^3 \oplus \cdots \oplus MH^{n-2} \oplus H \oplus MH \oplus H^2 \oplus H^3 \oplus H^4 \oplus \cdots \oplus H^{n-1} \oplus MH^2 \oplus MH^3 \oplus MH^4 \oplus \cdots \oplus MH^{n-1}, H^n)\\ &= (M \oplus H \oplus H^2 \oplus H^3 \oplus \cdots \oplus H^{n-1} \oplus (M \odot (H \oplus H^2 \oplus H^3 \oplus \cdots \oplus H^{n-1})), H^n)\end{aligned}$$

■

Consider the difference between the Secret key ($KEY$) and the result of the operation ($A \odot B$) denoted as $DIF$, which can be expressed as $DIF = KEY - [A \odot B]$. Our findings reveal a noteworthy pattern: regardless of the chosen values of $m$ and $n$, the matrix $DIF$ remains constant for fixed $M$ and $H$. This intriguing property emerges due to the fact that the term $KEY - [A \odot B]$ becomes entirely independent of the private parameters $m$ and $n$, emphasizing the stability and invariance of this difference matrix within the context of the given protocol.

$$\begin{aligned}DIF &= M_{m+n} - (M_m \odot M_n)\\ &= M \oplus H \oplus H^2 \oplus H^3 \oplus \cdots \oplus H^{m+n-1} \oplus (M \odot (H \oplus H^2 \oplus H^3 \oplus \cdots \oplus H^{m+n-1})) -\\ &\quad [M \oplus H \oplus H^2 \oplus H^3 \oplus \cdots \oplus H^{m-1} \oplus (M \odot (H \oplus H^2 \oplus H^3 \oplus \cdots \oplus H^{m-1})) \odot (M \oplus H \oplus H^2 \oplus H^3 \oplus \cdots \oplus H^{n-1} \oplus (M \odot (H \oplus H^2 \oplus H^3 \oplus \cdots \oplus H^{n-1})))]\end{aligned}$$

In the above equation, the higher powers of $H$ gets cancelled out because in tropical algebra $H \oplus H = H, H^2 \oplus H^2 = H^2, H^3 \oplus H^3 = H^3, \cdots, H^n \oplus H^n = H^n$.

As a consequence, $DIF$ becomes independent of higher powers of $H$, leaving behind only specific constant terms determined by the defect and period of $M$ and $H$. Consequently, the process of recovering the secret key is substantially simplified, as it suffices to identify this independent $DIF$ and perform the calculation of $A \odot B$, where $A$ and $B$ represent public parameters. Leveraging the relationship $KEY = DIF + [A \odot B]$, we can effortlessly obtain the shared secret key, thanks to the reduced complexity and clarity of the steps involved in the protocol. This insight marks a significant advancement in the efficiency and effectiveness of extracting the secret key and reinforces the practicality of the proposed key exchange scheme.

### B. An example

The following is a toy example of the proposed attack of the key exchange protocol.

Let $M = \begin{bmatrix} -128 & -325 \\ 145 & -164 \end{bmatrix}$, $H = \begin{bmatrix} 535 & 165 \\ 255 & -134 \end{bmatrix}$ be the two public matrices chosen by Alice and Bob.

Now, we have given the obtained secret key for different sets of $(m,n)$ and also the matrix $A \odot B$ for the corresponding $(m,n)$'s.

- For $(m,n) = (2,2)$

$$\implies K_a = K_b = \begin{bmatrix} -338 & -727 \\ -177 & -566 \end{bmatrix}$$

$$(A \odot B)_{(2,2)} = \begin{bmatrix} -368 & -757 \\ -207 & -596 \end{bmatrix}$$

- For $(m,n) = (2,3)$

$$\implies K_a = K_b = \begin{bmatrix} -472 & -861 \\ -311 & -700 \end{bmatrix}$$

$$(A \odot B)_{(2,3)} = \begin{bmatrix} -502 & -891 \\ -341 & -730 \end{bmatrix}$$

- For $(m,n) = (2,4)$
$\implies K_a = K_b = \begin{bmatrix} -606 & -995 \\ -445 & -834 \end{bmatrix}$
$(A \odot B)_{(2,4)} = \begin{bmatrix} -636 & -1025 \\ -475 & -863 \end{bmatrix}$
- For $(m,n) = (2,10)$
$\implies K_a = K_b = \begin{bmatrix} -1410 & -1799 \\ -1249 & -1638 \end{bmatrix}$
$(A \odot B)_{(2,10)} = \begin{bmatrix} -1440 & -1829 \\ -1279 & -1668 \end{bmatrix}$
- For $(m,n) = (2,156)$
$\implies K_a = K_b = \begin{bmatrix} -20974 & -21363 \\ -20813 & -21202 \end{bmatrix}$
$(A \odot B)_{(2,156)} = \begin{bmatrix} -21004 & -21393 \\ -20843 & -21232 \end{bmatrix}$
- For $(m,n) = (7,13)$
$\implies K_a = K_b = \begin{bmatrix} -2482 & -2871 \\ -2321 & -2710 \end{bmatrix}$
$(A \odot B)_{(7,13)} = \begin{bmatrix} -2512 & -2901 \\ -2351 & -2740 \end{bmatrix}$
- For $(m,n) = (43,74)$
$\implies K_a = K_b = \begin{bmatrix} -15480 & -15869 \\ -15319 & -15708 \end{bmatrix}$
$(A \odot B)_{(43,74)} = \begin{bmatrix} -15510 & -15899 \\ -15349 & -15738 \end{bmatrix}$
- For $(m,n) = (420,897)$
$\implies K_a = K_b = \begin{bmatrix} -176280 & -176669 \\ -176119 & -176508 \end{bmatrix}$
$(A \odot B)_{(420,897)} = \begin{bmatrix} -176310 & -176699 \\ -176149 & -176538 \end{bmatrix}$
- For $(m,n) = (1265,3564)$
$\implies K_a = K_b = \begin{bmatrix} -646888 & -647277 \\ -646727 & -647116 \end{bmatrix}$
$(A \odot B)_{(1265,3564)} = \begin{bmatrix} -646918 & -647307 \\ -646757 & -647146 \end{bmatrix}$

From these matrices we can clearly observe that, for $M = \begin{bmatrix} -128 & -325 \\ 145 & -164 \end{bmatrix}$ & $H = \begin{bmatrix} 535 & 165 \\ 255 & -134 \end{bmatrix}$ we have $K_a(or\ K_b) - [A \odot B] = \begin{bmatrix} 30 & 30 \\ 30 & 30 \end{bmatrix}$ irrespective of the private parameters $m$ & $n$ chosen by Alice and Bob.

Thus, to attack this key exchange scheme we only have to know $M, H, A$ & $B$. Since $M, H, A$ & $B$ are public matrices we can easily recover the secret key without the knowledge of any private parameters.

### C. Time Complexity

In our attack, we do not extract the private parameter, instead we directly attack the shared secret key. So, the number of operations required to attack the secret key is independent of the size of the private parameter. Instead, the complexity of our attack depends on the size of the matrices $M$ and $H$. Thus the time complexity of our proposed attack is $O(1)$.

### D. Algorithm of the attack

**Algorithm 1:** To extract the secret key

**Input :** Matrices $M, H, A, B$
**Output:** Shared secret key

$a \circ b := a + b + (a \cdot b)$
$(a,b)(c,d) := ((a \circ d) \oplus c, b \circ d)$
**for** $i \leftarrow 1$ **to** $4n$ **do**
  $(M,H)^{i+1} = (M,H)^i(M,H) = (M_{i+1}, H_{i+1})$
**end**
**for** $i \leftarrow 1$ **to** $4n$ **do**
  **for** $j \leftarrow 1$ **to** $4n$ **do**
    $T_{(i,j)} = M_{(i+j)}$
    $AB_{(i,j)} = M_i \odot M_j$
    $DIF_{(i,j)} = T_{(i,j)} - AB_{(i,j)}$
  **end**
**end**
**for** $k \leftarrow 1$ **to** $n^2$ **do**
  **if** $DIF_{(i,j)} = DIF_{(i,j+k)}$ **then**
    **return**
  **end**
  $DIF_{(i,j)}$ is the required difference
**end**
$KEY = DIF_{(i,j)} + AB_{(i,j)}$
**return** $KEY$ *is the secret key*

### E. Experimental analysis

The attack, as proposed, was implemented using Python 3.10 programming language and executed on a computer equipped with an 11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz processor and 16 GB of RAM. To ensure reliable and consistent results, the experiment was repeated 10000 times for each value of n, where n represents the dimension of the public matrices. The collected data regarding the time taken to successfully extract the secret key through the attack has been meticulously tabulated and is presented in Table I for further analysis and evaluation.

TABLE I
TIME TAKEN TO EXTRACT THE SHARED SECRET KEY

| Size of the matrix (n) | Time taken in seconds (s) |
|---|---|
| 2 | 0.0001 |
| 4 | 0.0103 |
| 8 | 0.062 |
| 10 | 0.213 |
| 12 | 0.812 |
| 15 | 2.003 |
| 20 | 5.071 |
| 25 | 9.326 |
| 30 | 18.921 |

The data in the Table I is plotted in Figure 1.

## V. ADVANTAGES OF OUR ATTACK

Our cryptographic attack on the key exchange protocol, which is based on tropical algebra homomorphism, offers numerous significant advantages over previous methods. One particularly interesting benefit is that our approach

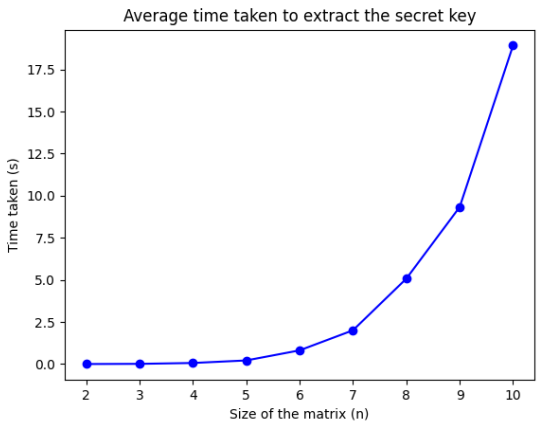


Fig. 1. Average time taken to extract the secret key

allows us to extract the secret key directly, eliminating the need to discover the public parameters.

By focusing on extracting the secret key itself, our attack exposes a fundamental flaw in the architecture of the protocol. This understanding is of great value to cryptographers and protocol designers, as it enables them to identify and rectify the underlying weaknesses. Armed with this knowledge, the cryptography community can forge ahead and construct more robust and secure key exchange protocols for the future, bolstering their resistance against attempts aimed at extracting secret keys.

In essence, the advantages of our cryptographic attack stem from its ability to directly retrieve the secret key without compromising the public parameters. This streamlined method enhances the attack procedure's efficiency and highlights crucial flaws in the protocol's design. Ultimately, these benefits contribute to the advancement of cryptography research and the development of more secure and resilient key exchange systems. As a result, our work plays a pivotal role in fortifying the foundations of cryptographic security.

## VI. Conclusion

We have attacked the key exchange scheme proposed by Grigoriev and Shpilrain which uses an extension on tropical cryptography by homomorphism. Our attack exploits the fact that the difference between the secret key and the product of shared matrices is irrespective of the choice of public parameters of Alice and Bob. The effects of this study go beyond the specific key exchange protocol under consideration. It emphasizes the importance of pattern detection and comprehensive cryptographic analysis in assuring the security and resilience of key exchange schemes. Cryptographers and researchers should be mindful of the potential hazards and vulnerabilities connected with the use of novel mathematical frameworks in cryptographic protocols, such as tropical algebra.

While this protocol has been subjected to prior attacks, our approach stands out as significantly faster than all previous attempts. Unlike other attacks that rely on extracting the private parameter from the available public information, leading to varying attack complexities based on the choices of Alice and Bob's private parameters, our method directly targets the secret key without any dependence on these private parameters. As a result, the complexity of our attack remains consistent and independent of the specific choices made by Alice and Bob for their private parameters. This key advantage streamlines the attack process and enhances its efficiency, making our approach a compelling and robust solution for the protocol's security concerns. Moving forward, it is suggested that future research focus on fixing the highlighted weaknesses and building improved versions of the key exchange protocol based on tropical algebra homomorphism. Furthermore, investigating different mathematical frameworks and cryptographic algorithms may aid in the development of more resilient and secure key exchange protocols.

Finally, the attack described in this research study gives light on the vulnerabilities in the key exchange protocol based on tropical algebra. It is a timely reminder that even the most inventive cryptographic solutions require careful examination and constant enhancement to survive growing security threats in an increasingly interconnected digital landscape.

## References

[1] Ahmed, K., Pal, S., Mohan, R., 2021. A review of the tropical approach in cryptography. Cryptologia, 1-25. DOI: https://doi.org/10.1080/01611194.2021.1994486.

[2] Ahmed K, Pal S, Mohan R. Key exchange protocol based upon a modified tropical structure. Communications in Algebra. 2022 Jun 28:1-0. https://doi.org/10.1080/00927872.2022.2095566.

[3] Alvarez R, Martinez FM, Vicent JF, Zamora A. A new public key cryptosystem based on matrices. WSEAS Information Security and Privacy. 2007 Dec 14;3639. https://dl.acm.org/doi/abs/10.5555/1981242.1981247.

[4] Álvarez R, Tortosa L, Vicent JF, Zamora A. Analysis and design of a secure key exchange scheme. Information Sciences. 2009 May 30;179(12):2014-21. https://doi.org/10.1016/j.ins.2009.02.008.

[5] Amutha, B., and R. Perumal. "Public key exchange protocols based on tropical lower circulant and anti circulant matrices." AIMS Mathematics 8.7 (2023): 17307-17334.

[6] Benardi Widhiara, Yusuf Kurniawan, and Bety Hayat Susanti, RM70 : A Lightweight Hash Function, IAENG International Journal of Applied Mathematics, vol. 53, no.1, pp94-102, 2023.

[7] Climent JJ, Navarro PR, Tortosa L. Key exchange protocols over noncommutative rings. The case of. International Journal of Computer Mathematics. 2012 Sep 1;89(13-14):1753-63. https://doi.org/10.1080/00207160.2012.696105.

[8] Diffie, W., Hellman, M.,E., 1976. New directions in cryptography, IEEE Trans. Inform. Theory.vol IT-22(6):644-654.

[9] Durcheva MI, Trendafilov ID. Public key cryptosystem based on max-semirings. InAIP Conference Proceedings 2012 Nov 1 (Vol. 1497, No. 1, pp. 357-364). American Institute of Physics. https://doi.org/10.1063/1.4766805.

[10] Durcheva MI. Public key cryptography with max-plus matrices and polynomials. InAIP Conference Proceedings 2013 Dec 18 (Vol. 1570, No. 1, pp. 491-498). American Institute of Physics. https://doi.org/10.1063/1.4854794.

[11] Durcheva M, Rachev M. A public key encryption scheme based on idempotent semirings. InAIP Conference Proceedings 2015 Nov 30 (Vol. 1690, No. 1, p. 060008). AIP Publishing LLC. https://doi.org/10.1063/1.4936746.

[12] Eftekhari M. Cryptanalysis of some protocols using matrices over group rings. InInternational conference on cryptology in Africa 2017 May 24 (pp. 223-229). Springer, Cham. https://doi.org/10.1007/978-3-319-57339-7_13.

[13] Gentry C and M. Syzdlo. 2002. Cryptanalysis of the revised NTRU signature scheme. In International conference on the theory and applications of cryptographic techniques, 299–320. Berlin: Springer. https://doi.org/10.1007/3-540-46035-7_20.

[14] Grigoriev D, Ponomarenko I. Constructions in public-key cryptography over matrix groups. arXiv preprint math/0506180. 2005 Jun 10. https://doi.org/10.48550/arXiv.math/0506180.
[15] Grigoriev, D., and V. Shpilrain, Tropical cryptography, Comm. Algebra 42 (2014), no. 6, 2624–2632.
[16] Grigoriev, D., and V. Shpilrain. 2019. Tropical cryptography II: extensions by homomorphisms. Communications in Algebra 47 (10):4224–9. doi:10.1080/00927872.2019.1581213.
[17] Hofheinz D, Steinwandt R. A practical attack on some braid group based cryptographic primitives. InInternational workshop on public key cryptography 2003 Jan 6 (pp. 187-198). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-36288-6_14.
[18] Isaac, S., and D. Kahrobaei. 2021. A closer look at the tropical cryptography. International Journal of Computer Mathematics: Computer Systems Theory 6 (2):137–42.
[19] Izhakian, Z., 2009. Basics of linear algebra over the extended tropical semiring. Contemp. Math. DC: American mathematical society, p.173.
[20] I. Cherkaoui, Diffie-Hellman Multi-Challenge using a New Lossy Trapdoor Function Construction, IAENG International Journal of Applied Mathematics, vol. 51, no.3, pp736-742, 2021.
[21] Jyoti Shetty, Sudhakara G, and Vinay Madhusudanan, Encryption System Involving Matrix Associated With Semigraphs, IAENG International Journal of Applied Mathematics, vol. 52, no.2, pp458-465, 2022.
[22] Kotov, M., and A. Ushakov. 2018. Analysis of a key exchange protocol based on tropical matrix algebra. Journal of Mathematical Cryptology 12 (3):137–41. doi:10.1515/jmc-2016- 0064.
[23] Maze G, Monico C, Rosenthal J. Public key cryptography based on semigroup actions. arXiv preprint cs/0501017. 2005 Jan 10. https://doi.org/10.48550/arXiv.cs/0501017.
[24] Muanalifah, A., Sergeev, S. (2020). Modifying the tropical version of stickel's key exchange protocol. Applications of Mathematics: Dec;65(6):727-53.
[25] Muanalifah, A., and S. Sergeev. 2021. On the tropical discrete logarithm problem and security of a protocol based on tropical semidirect product. Communications in Algebra 49:1–19. arXiv preprint arXiv: 2101.02781. doi:10.1080/00927872.2021.1975125.
[26] Nachtigall K. Powers of matrices over an extremal algebra with applications to periodic graphs. Mathematical Methods of Operations Research. 1997;46(1):87-102. https://doi.org/10.1007/BF01199464.
[27] Odoni RW, Varadharajan V, Sanders PW. Public key distribution in matrix rings. Electronics Letters. 1984 Apr 26;20(9):386-7. https://doi.org/10.1049/el:19840267.
[28] Rudy, D., and C. Monico. 2020. Remarks on a tropical key exchange system. Journal of Mathematical Cryptology 15 (1):280–3. doi:10.1515/jmc-2019-0061.
[29] Shpilrain., Vladimir., 2008. Cryptanalysis of Stickel's key exchange scheme, Int. j. comput. sci. Springer, Berlin, Heidelberg.
[30] Steinwandt R. Loopholes in two public key cryptosystems using the modular group. InInternational workshop on public key cryptography 2001 Feb 13 (pp. 180-189). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-44586-2_14.
[31] Stickel, E. 2005. A new method for exchanging secret keys. In Third International Conference on Information Technology and Applications (ICITA'05), IEEE (2), 426–430.
[32] Suroto, Diah Junia Eksi Palupi, and Ari Suparwanto. 2022 ,The Cholesky Decomposition of Matrices over the Symmetrized Max-Plus Algebra, IAENG International Journal of Applied Mathematics, vol. 52, no.3, pp678-683.