Journal of Algebra and Related Topics
Vol. , No. -, 2026, pp. -. Research Article

Tropical matrix-based cryptosystems: a post-quantum approach to public key security

Azadeh Ramezanpour Naseri[†], **Ahmad Abbasi**[†,‡], **Reza Ebrahimi Atani**[§*]

[†]*Department of Pure Mathematics, Faculty of mathematical sciences, University of Guilan, Rasht, Iran*
[‡]*Center of Excellence for Mathematical Modeling Optimization and Combinatorial computing (MMOCC) University of Guilan, Rasht, Iran*
[§]*Department of Computer Engineering, University of Guilan, Rasht, Iran*
Emails: azadehramezanpoor@gmail.com, aabbasi@guilan.ac.ir, rebrahimi@guilan.ac.ir

Abstract. In recent years, cryptographic constructions based on alternative algebraic structures have been explored as candidates for post-quantum security. Tropical algebra, with its unique min-plus operations and NP-hard associated computational problems, provides a promising foundation for such schemes. In this work, we introduce a new public key cryptosystem built upon tropical block matrices. Specifically, we design (i) a key exchange protocol and (ii) an encryption scheme analogous to the ElGamal cryptosystem. The security of our protocols relies on the hardness of solving nonlinear systems over tropical semirings. We analyze the resistance of the proposed constructions against brute force and algebraic attacks and discuss their computational efficiency. Our results suggest that tropical block matrix–based schemes offer a novel direction for post-quantum cryptography and extend the scope of tropical algebra applications in secure communication.

Keywords: Cryptosystem, Key Exchange Protocol, Tropical Algebra, Tropical Block Matrices.
AMS Subject Classification 2010: 14G50, 81P94, 94A60

1 Introduction

The rapid expansion of communication networks and digital information exchange has made cryptographic security a fundamental requirement in modern computing. Ensuring confidentiality, integrity, and authentication in data transmission depends critically on the design of robust cryptographic algorithms. Classical public key cryptography, introduced by Diffie and Hellman

*Corresponding author
Received: 04 October 2025/ Revised: 28 January 2026/ Accepted: 02 February 2026
DOI: 10.22124/JART.2026.31859.1858

© 2026 University of Guilan

in 1976 [10], relies on number-theoretic problems such as integer factorization and discrete logarithms. While these schemes have long provided practical security, the advent of quantum algorithms notably Shor's algorithm [24] poses a serious threat to their long-term viability. This challenge has driven an intensive search for post-quantum cryptographic (PQC) constructions built on alternative algebraic foundations [8].

Several approaches have been proposed as PQC candidates, including lattice based schemes [2–5, 15–17], matrix-based systems [21–23, 29], and even protocols leveraging blockchain and voting applications [20]. While many of these frameworks offer promising hardness assumptions, they often involve complex structures and large parameter sizes, motivating the exploration of simpler yet intractable algebraic settings.

One such direction is the use of semirings [12] and tropical algebra in cryptography. Semirings, introduced by Vandiver [28], generalize rings by relaxing additive inverses, and tropical algebra, which was introduced by the Brazilian mathematician Imre Simon [25,26] in the 1970s, also known as min-plus or max-plus algebra provides a semiring structure where addition corresponds to the minimum operation and multiplication corresponds to standard addition [9]. Tropical algebra is computationally efficient, eliminating multiplication in the classical sense, and several of its core problems, such as solving nonlinear tropical systems, are NP-hard [11]. These properties make tropical algebra an attractive platform for cryptographic constructions.

Previous research has demonstrated this potential. Maze, Monico, and Rosenthal [18, 19] introduced early semiring-based cryptosystems, though they were later broken by Steinwandt et al. [27]. Atani and co-authors proposed constructions over semimodules [6, 7] and later extended the study of non-commutative lattice-based cryptography [2,3,5,17]. Grigoriev and Shpilrain [11] formalized the hardness of tropical equations, while more recent works have proposed tropical transformations and matrix-based protocols [1, 13, 14]. Despite these efforts, existing tropical cryptosystems either remain vulnerable to specialized attacks or lack formal analogues to well-established cryptographic primitives.

In this paper, we build on these ideas by introducing a new framework for public key cryptography based on tropical block matrices. By exploiting the structural properties of block matrix operations in the tropical setting, we design a key exchange protocol and an encryption scheme analogous to the ElGamal cryptosystem. Our approach leverages the computational intractability of solving nonlinear tropical systems while retaining the efficiency advantages of tropical algebra.

The main contributions of this work are summarized as follows:

- New Cryptographic Framework: We introduce a novel use of tropical block matrices in the design of public key protocols, extending the algebraic tools available for tropical cryptography.

- Key Exchange Protocol: We propose a key exchange scheme whose security is grounded in the NP-hardness of solving nonlinear tropical systems.

- Encryption Scheme: We design an ElGamal-like public key encryption scheme based on tropical block matrices, providing a new alternative to classical number-theoretic constructions. We analyze resistance of the proposed protocols to well known cryptographic

attacks and we discuss computational aspects of our protocols, highlighting the absence of multiplication operations and potential efficiency advantages in implementation.

By developing cryptographic protocols over tropical block matrices, this work contributes to the growing body of research in post-quantum cryptography and opens a new line of inquiry into the role of semiring-based structures in secure communication. The remainder of this paper is organized as follow: Section 2 provides preliminary information on tropical matrix algebra. In section 3, we define the block matrix $M_P(A, B)$. Then, in section 4, we present our protocols based on the tropical block matrix. Finally, we analyze the security and performance of the protocols in section 5. Finally the paper will be concluded in section 6.

2 Preliminaries

In this section, tropical algebra, tropical polynomial and tropical matrix are defined.

2.1 Tropical Semiring Over Integer

Tropical algebra are semiring, which their structure similar is to a ring, but without the requirement that each element must have an additive inverse. Tropical algebra is one of example of semiring.

Let $\mathcal{Z} = \mathbb{Z} \cup \{\infty\}$, equipped with two binary operations, tropical addition and tropical multiplication defined as follows:

$$\forall\ \mathrm{x}, \mathrm{y} \in \mathcal{Z}, \quad \mathrm{x} \oplus \mathrm{y} := \min(\mathrm{x}, \mathrm{y}), \quad (\mathrm{x} \otimes \mathrm{y}) := \mathrm{x} + \mathrm{y},$$

The element ∞ satisfies the following properties:

$$\forall\ \mathrm{x} \in \mathcal{Z}, \quad \infty \oplus \mathrm{x} = \mathrm{x}, \quad \text{and} \quad \infty \otimes \mathrm{x} = \infty.$$

It follows that $(\mathcal{Z}, \oplus, \otimes)$ is a commutative semiring, with the zero element as ∞ and the multiplicative identity as o. It is called tropical semiring of integer [9].

2.2 Tropical Polynomial Semiring

Definition 1. *A tropical polynomial over $\mathcal{Z}$ in the indeterminat x is any function of the form:*

$$p(x) = a_n \otimes x^{\otimes n} \oplus a_{n-1} \otimes x^{\otimes n-1} \oplus \cdots \oplus a_1 \otimes x \oplus a_0,$$

where each a_i is an integer number and n is a natural number.

$$x^{\otimes n} = \underbrace{x \otimes \cdots \otimes x}_{n-times}.$$

Because it dose not be amboguous in practice, we will write x^n instead of $x^{\otimes n}$.

2.3 Tropical Matrix Semiring

Let $\mathbb{M}_n(\mathcal{Z})$ be the set of all $n \times n$ matrices over $\mathcal{Z}$, then $A \in \mathbb{M}_n(\mathcal{Z})$ is called a tropical matrix. Also, we can define the addition, multiplication and scalar multiplication for tropical matrices. For all $A = (a_{ij})_{n\times n}$, $B = (b_{ij})_{n\times n} \in \mathbb{M}_n(\mathcal{Z})$ and any scalar $k \in \mathcal{Z}$, we have:

- $A \oplus B = (a_{ij} \oplus b_{ij})_{n\times n}, \quad \forall\ i, j = 1, \ldots, n$
- $A \otimes B = (\bigoplus_{k=1}^{n}\{a_{ik} \otimes b_{kj}\})_{n\times n}, \quad \forall\ i, j = 1, \ldots, n$
- $k \otimes A = \mathrm{diag}(k, \ldots, k) \otimes \mathrm{A}$

A scalar matrices are the matrices with an element $\lambda \in \mathcal{Z}$ on the diagonal and ∞ elsewhere denoted by $\begin{pmatrix} \lambda & \infty \\ \infty & \lambda \end{pmatrix}$. Multiplying a square matrix by a scalar amounts to multiplying it by the corresponding matrix.

Example 1.

$$\begin{pmatrix} 2 & 5 \\ 3 & 4 \end{pmatrix} \oplus \begin{pmatrix} 7 & 3 \\ 6 & -1 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 3 & -1 \end{pmatrix}.$$

$$\begin{pmatrix} 2 & 5 \\ 3 & 4 \end{pmatrix} \otimes \begin{pmatrix} 7 & 3 \\ 6 & -1 \end{pmatrix} = \begin{pmatrix} 9 & 4 \\ 10 & 3 \end{pmatrix}.$$

$$3 \otimes \begin{pmatrix} 2 & 5 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 3 & \infty \\ \infty & 3 \end{pmatrix} \begin{pmatrix} 2 & 5 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 5 & 8 \\ 6 & 7 \end{pmatrix}.$$

For a matrix $A \in \mathbb{M}_n(\mathcal{Z})$, Then we define the nth tropical matrix power of A as

$$A^{\otimes n} = A \otimes A \otimes A \otimes \cdots \otimes A.$$

We have $A^{\otimes 0} = I$.

2.4 Inverse Tropical Matrix

The invertible matrices in the tropical algebra are tropical diagonal matrices. $A_{n\times n}$ matrix is called diagonal, denoted by $\mathrm{diag}(d_1, \ldots, d_{\mathrm{n}})$, if all its diagonal entries are $d_1, \ldots, d_n \in \mathbb{Z}$ and off-diagonal entries are ∞.

Definition 2. *The matrix* $\mathrm{diag}(0)$ *is called the unit matrix and denoted by* I*, or by* I_n *if indicating its size is required.*

The additive inverse of tropical matrix do not exit. Multiplicative inverse of a matrix A is a matrix denoted by A^{-1} such that $A \otimes A^{-1} = I$. In $\mathbb{M}_{2\times 2}$, if $A = \begin{pmatrix} a & \infty \\ \infty & a \end{pmatrix}$ then $A^{-1} = \begin{pmatrix} -a & \infty \\ \infty & -a \end{pmatrix}$ such that $\begin{pmatrix} a & \infty \\ \infty & a \end{pmatrix} \otimes \begin{pmatrix} -a & \infty \\ \infty & -a \end{pmatrix} = \begin{pmatrix} 0 & \infty \\ \infty & 0 \end{pmatrix}$.

Clearly, if an inverse matrix to A exists then it is unique. If $A = \mathrm{diag}(a_1, \ldots, a_{\mathrm{n}})$, $a_1, \ldots, a_n \in \mathbb{Z}$ then $A^{-1} = \mathrm{diag}({a_1}^{-1}, \ldots, {a_{\mathrm{n}}}^{-1})$.

3 The Tropical Matrices $M_P(A, B)$

In this section, we introduce the notion of the tropical matrix product $M_P(A, B)$, which will be used in the design of our cryptographic schemes. We first recall the basic operations of tropical algebra and then extend them to block matrices.

Definition 3. *Let A, B, P be any three square tropical matrices of the same order, then the tropical block matrices $M_p(A, B)$ is defined as:*

$$M_p(A, B) = \begin{pmatrix} A & P \\ 0 & B \end{pmatrix}.$$

The following theorem deals with the powers of $M_p(A, B)$.

Theorem 1. *For $l \in \mathbb{N}^*$, we have*

$$(M_p(A, B))^{\otimes l} = \begin{pmatrix} A^{\otimes l} & P_l \\ 0 & B^{\otimes l} \end{pmatrix},$$

where $P_l = \bigoplus_{k=0}^{l-1} A^{\otimes(l-1-k)} \otimes P \otimes B^k$.

Proof. We prove it by inductive hypothesis on l. For $l = 1$, we have $(M_p(A, B))^{\otimes 1} = \begin{pmatrix} A^{\otimes 1} & P_1 \\ 0 & B^{\otimes 1} \end{pmatrix} = M_p(A, B)$ and $P_1 = P$, satisfied. Now assuming the statement is true for l, we prove it for $(l+1)$. Here, we have

$$\begin{aligned}(M_p(A, B))^{\otimes(l+1)} &= (M_p(A, B))^{\otimes l} \otimes M_p(A, B) \\ &= \begin{pmatrix} A^{\otimes l} & P_l \\ 0 & B^{\otimes l} \end{pmatrix} \otimes \begin{pmatrix} A & P \\ 0 & B \end{pmatrix} \\ &= \begin{pmatrix} A^{\otimes l} \otimes A & A^{\otimes l} \otimes P \oplus P_l \otimes B \\ o & B^{\otimes l} \otimes B \end{pmatrix}.\end{aligned}$$

Since,

$$\begin{aligned}A^{\otimes l} \otimes P \oplus P_l \otimes B &= A^{\otimes l} \otimes P \oplus (\bigoplus_{k=0}^{l-1} A^{\otimes(l-1-k)} \otimes P \otimes B^k) \otimes B \\ &= A^{\otimes l} \otimes P \oplus [(A^{\otimes(l-1)} \otimes P \otimes B) \oplus (A^{\otimes(l-2)} \otimes P \otimes B^2) \oplus \cdots \oplus P \otimes B \\ &= \bigoplus_{k=0}^{l} A^{\otimes(l-k)} \otimes P \otimes B^k = P_{l+1},\end{aligned}$$

we have

$$(M_p(A, B))^{l+1} = \begin{pmatrix} A^{\otimes(l+1)} & P_{l+1} \\ 0 & B^{\otimes(l+1)} \end{pmatrix},$$

where $P_{l+1} = \bigoplus_{k=0}^{l} A^{\otimes(l-k)} \otimes P \otimes B^k$. □

4 Public Key Cryptosystems Based on Tropical Matrices

In this section, we introduce two cryptographic protocols based on tropical block matrices $M_P(A,B)$: (i) a key exchange protocol, and (ii) a public key encryption scheme analogous to the ElGamal cryptosystem. Both constructions rely on the hardness of the Tropical Matrix Diffie–Hellman (TMDH) problem defined in Section 5.

4.1 Key Exchange Protocol Based on Tropical Block Matrices

The first protocol is a tropical analogue of the Diffie–Hellman key exchange. Consider the set of matrices $\mathbb{M}_n(\mathcal{Z})$ of order $n \times n$ with entries from tropical semiring $\mathcal{Z}$. It is clear that $(\mathbb{M}_n(\mathcal{Z}), \oplus, \otimes)$ is a matrix algebra, which called the tropical matrix algebra.

The public parameters of the protocol is $P \in \mathbb{M}_n(\mathcal{Z})$. Key exchange protocol based on tropical block matrix is the following.

(1) Alice chooses a private exponent as her secret key $l \in \mathbb{N}$ and matrix $A \in \mathbb{M}_n(\mathcal{Z})$ then publishes the set $E_A = \{X | A \otimes X = X \otimes A, X \neq I, 0\}$.

(2) Bob chooses a private exponent as his secret key $k \in \mathbb{N}$ and matrix $B \in \mathbb{M}_n(\mathcal{Z})$ then publishes the set $E_B = \{X | B \otimes X = X \otimes B, X \neq I, 0\}$.

(3) Alice selects another private key $C \in E_B$ such that $C \otimes B = B \otimes C$ and computes a matrix $(M_P(A,C))^{\otimes l}$, where

$$(M_P(A,C))^{\otimes l} = \begin{pmatrix} A^{\otimes l} & M_l(A,C) \\ o & C^{\otimes l} \end{pmatrix},$$

where,

$$M_l(A,C) = \bigoplus_{n=0}^{l-1} A^{\otimes(l-1-n)} \otimes P \otimes C^{\otimes n},$$

and she sends $M_l(A,C)$ to Bob.

(4) Bob selects another private key $D \in E_A$ such that $A \otimes D = D \otimes A$ and computes a matrix $(M_P(D,B))^{\otimes k}$, where

$$(M_P(D,B))^{\otimes k} = \begin{pmatrix} D^{\otimes k} & M_k(D,B) \\ o & B^{\otimes k} \end{pmatrix},$$

where,

$$M_k(D,B) = \bigoplus_{m=0}^{k-1} D^{\otimes(k-1-m)} \otimes P \otimes B^{\otimes m},$$

and he sends $M_k(D,B)$ to Alice.

(5) Alice computes shared secret key $M_{k,l}$ by using her private key l.

$$K_{\text{Alice}} = M_{k,l} = \bigoplus_{n=0}^{l-1} A^{\otimes(l-1-n)} \otimes M_k(D,B) \otimes C^{\otimes n}.$$

(6) Bob computes shared secret key $M_{l,k}$ by using his private key k.

$$K_{\text{Bob}} = M_{l,k} = \bigoplus_{m=0}^{k-1} D^{\otimes(k-1-m)} \otimes M_l(A,C) \otimes B^{\otimes m}.$$

Since $A \otimes D = D \otimes A$ and $C \otimes B = B \otimes C$, we have $M_{k,l} = M_{l,k}$. So, Alice and Bob share a common secret key $K = M_{k,l} = M_{l,k}$.

The following theorem shows that $K_{\text{Alice}} = K_{\text{Bob}}$.

Theorem 2. *If* $K_{\text{Alice}} = M_{k,l} = \bigoplus_{n=0}^{l-1} A^{\otimes(l-1-n)} \otimes M_k(D,B) \otimes C^{\otimes n}$ *and* $K_{\text{Bob}} = M_{l,k} = \bigoplus_{m=0}^{k-1} D^{\otimes(k-1-m)} \otimes M_l(A,C) \otimes B^{\otimes m}$, *then* $K_{\text{Alice}} = K_{\text{Bob}}$, *where* $M_k(D,B) = \bigoplus_{m=0}^{k-1} D^{\otimes(k-1-m)} \otimes P \otimes B^{\otimes m}$ *and* $M_l(A,C) = \bigoplus_{n=0}^{l-1} A^{\otimes(l-1-n)} \otimes P \otimes C^{\otimes n}$

Proof. We have

$$\begin{aligned} K_{\text{Alice}} = M_{k,l} &= \bigoplus_{n=0}^{l-1} A^{\otimes(l-1-n)} \otimes M_k(D,B) \otimes C^{\otimes n} \\ &= \bigoplus_{n=0}^{l-1} A^{\otimes(l-1-n)} \otimes (\bigoplus_{m=0}^{k-1} D^{\otimes(k-1-m)} \otimes P \otimes B^{\otimes m}) \otimes C^{\otimes n} \\ &= \bigoplus_{n=0}^{l-1} \bigoplus_{m=0}^{k-1} A^{\otimes(l-1-n)} \otimes D^{\otimes(k-1-m)} \otimes P \otimes B^{\otimes m} \otimes C^{\otimes n}, \end{aligned}$$

$$\begin{aligned} K_{\text{Bob}} = M_{l,k} &= \bigoplus_{m=0}^{k-1} D^{\otimes(k-1-m)} \otimes M_l(A,C) \otimes B^{\otimes m} \\ &= \bigoplus_{m=0}^{k-1} D^{\otimes(k-1-m)} \otimes (\bigoplus_{n=0}^{n-1} A^{\otimes(l-1-n)} \otimes P \otimes C^{\otimes n}) \otimes B^{\otimes m} \\ &= \bigoplus_{m=0}^{k-1} \bigoplus_{n=0}^{l-1} D^{\otimes(k-1-m)} \otimes A^{\otimes(l-1-n)} \otimes P \otimes C^{\otimes n} \otimes B^{\otimes m}. \end{aligned}$$

Since $A \otimes D = D \otimes A$ and $C \otimes B = B \otimes C$. One has $K_{\text{Alice}} = K_{\text{Bob}}$. □

4.2 Public Key Cryptosystem based on Tropical Matrix

- Key generation: Alice and Bob agree on a matrix $P \in \mathbb{M}_n(\mathcal{Z})$. Alice chooses $l \in \mathbb{N}^*$, the matrix $A \in \mathbb{M}_n(\mathcal{Z})$ and publish the set E_A. Then selects $C \in E_A$ and computs $M_l(A,C)$ see, 4.1. The secret key Alice is $l \in \mathbb{N}^*, A \in \mathbb{M}_n(\mathcal{Z}), C \in E_A$. The public key Alice is $U = M_l(A,C)$.

- Encryption: Bob wants to send a plaintext messages $M \in \mathbb{M}_n(\mathcal{Z})$ to Alice.

(1) Bob chooses $k \in \mathbb{N}$, the matrix $B \in \mathbb{M}_n(\mathcal{Z})$ and publishes the set E_B then select $D \in E_A$.

(2) Bob computes $V = M_P(D, B)$ as a part of ciphertext.

(3) Bob computes $Q = M + \bigoplus_{m=0}^{k-1} D^{\otimes(k-1-m)} \otimes U \otimes B^{\otimes m}$ as a rest of the ciphertext, where "+" is the ordinary integer matrix addition.

(4) Bob sends the ciphertext (V, Q) to Alice.

- Decryption: Alice recives the ciphertext (V, Q) and tries to decrypt it.

(1) Using her secret key $l \in \mathbb{N}^*, \mathbb{A} \in \mathbb{M}_n(\mathcal{Z}), C \in E_B$, Alice computes $W = \bigoplus_{n=0}^{l-1} A^{\otimes(l-1-n)} \otimes V \otimes C^{\otimes n}$

(2) Alice computes $Q - W$, where "$-$" is ordinary integer matrix. since

$$Q - W = M + \bigoplus_{m=0}^{k-1} D^{\otimes(k-1-m)} \otimes U \otimes B^{\otimes m} - \bigoplus_{n=0}^{l-1} A^{\otimes(l-1-n)} \otimes V \otimes C^{\otimes n} = M.$$

5 Security Analysis and Performance Analysis

In this section, we analyze the security of the proposed cryptographic protocols. We first introduce the underlying hardness assumption that supports our construction, and then formalize the security model for both the key exchange protocol and the encryption scheme. Finally, we discuss resistance to classical, algebraic, and quantum attacks.

5.1 Hardness Assumptions

The security of the proposed key exchange and encryption schemes is based on the presumed computational hardness of certain problems in tropical linear algebra. We emphasize that, in contrast to classical group-based cryptography, the algebraic setting of tropical semirings lacks a well-established hierarchy of reductions between computational problems. Consequently, our security arguments are based on explicit hardness assumptions rather than proven reductions from known NP-hard problems.

Definition 4 (Tropical Matrix Diffie–Hellman (TMDH) Problem)**.** *Let $B \in \mathbb{Z}_{\min}^{n\times n}$ be a public tropical matrix, and let a, b be secret positive integers. Given the matrices*

$$X = B^{\otimes a}, \qquad Y = B^{\otimes b},$$

the Tropical Matrix Diffie–Hellman (TMDH) problem consists of computing

$$Z = B^{\otimes ab},$$

without knowledge of a or b.

The TMDH problem is inspired by the classical Diffie–Hellman problem but is formulated in the non-group setting of tropical matrix semirings. While the general Tropical System Solving Problem (TSSP) is known to be NP-hard, we do not claim a formal polynomial-time reduction from TSSP to TMDH. Instead, we treat TMDH as an independent hardness assumption, motivated by the following observations: entries of tropical matrix powers correspond to solutions of shortest-path problems over weighted directed graphs, and recovering exponents from such powers appears computationally difficult due to the nonlinear and combinatorial structure of tropical matrix multiplication.

At present, no polynomial-time algorithm is known for solving the TMDH problem for general tropical matrices of cryptographic dimensions. Establishing formal reductions or complexity-theoretic hardness results for TMDH remains an important open problem and is left for future work.

Lemma 1 (Heuristic Indistinguishability of Block Exponentiation)**.** *Let A, B, P be tropical matrices of appropriate dimensions, and let*

$$M = MP(A, B) = \begin{pmatrix} A & P \\ \infty & B \end{pmatrix}.$$

For a randomly chosen exponent ℓ, the matrix $M^{\otimes \ell}$ does not reveal (A, B, P) or ℓ to any known polynomial-time adversary with non-negligible advantage.

Heuristic Argument. The off-diagonal block of $M^{\otimes \ell}$ is given by a tropical sum of terms of the form

$$\bigoplus_{i=0}^{\ell-1} A^{\otimes(\ell-1-i)} \otimes P \otimes B^{\otimes i},$$

whose entries are nonlinear tropical polynomials in the entries of A, B, and P. Recovering the individual components or the exponent ℓ from this expression requires solving structured systems of tropical equations, a task for which no efficient general algorithm is currently known.

Moreover, while tropical matrix powers admit interpretations via shortest-path problems and may exhibit eventual periodicity, exploiting such properties to recover hidden exponents or matrix factors in this block setting remains an open problem. To the best of our knowledge, no cryptanalytic technique leveraging these properties has been shown to break constructions of this form at cryptographic parameter sizes.

Accordingly, we treat the indistinguishability of $M^{\otimes \ell}$ as a heuristic assumption, analogous to exponent-hiding assumptions in classical Diffie–Hellman–type constructions. □

Proposition 1 (Heuristic Hardness of Centralizer Reconstruction)**.** *Let $A \in \mathbb{Z}_{\min}^{n \times n}$ be a private tropical matrix, and let*

$$E_A = \{X \mid A \otimes X = X \otimes A\}$$

denote its commutant. Given access to one or more nontrivial elements of E_A, reconstructing A is assumed to be computationally hard for polynomial-time adversaries.

Heuristic Argument. Determining a matrix A from commutation relations $A \otimes X = X \otimes A$ amounts to solving systems of tropical polynomial equations with strong structural constraints.

While commutants of tropical matrices have been studied in algebraic contexts, no general polynomial-time algorithm is known for reconstructing a hidden matrix from partial information about its commutant.

In our constructions, the protocol does not require publishing the full set E_A, but only sampled elements derived from it. We therefore assume that recovering A from such information is infeasible, and we explicitly state this as an independent hardness assumption rather than a derived result. □

5.2 Security of the Key Exchange Protocol

The proposed key exchange protocol is analogous to classical Diffie–Hellman. Let B be a public block matrix. Alice selects a private exponent a and publishes $X = B^{\otimes a}$; Bob selects a private exponent b and publishes $Y = B^{\otimes b}$. Both compute the shared secret as:

$$K = (B^{\otimes a})^{\otimes b} = (B^{\otimes b})^{\otimes a} = B^{\otimes ab}.$$

Theorem 3. *Under Assumption 5.1, the shared key in the key exchange protocol is indistinguishable from random to any PPT adversary observing only public values B, X, Y.*

Proof sketch. Suppose an adversary $\mathcal{A}$ can distinguish the shared key from random with non-negligible probability. Then $\mathcal{A}$ can be used to construct an algorithm that solves the TMDH problem by outputting $Z = B^{\otimes ab}$, contradicting Assumption 5.1. □

5.3 Security of the Encryption Scheme

Our encryption scheme is modeled on ElGamal, where semantic security corresponds to *indistinguishability under chosen-plaintext attack (IND-CPA).*

Definition 5 (IND-CPA)**.** *An encryption scheme is IND-CPA secure if no PPT adversary can distinguish between encryptions of two chosen plaintexts with advantage greater than negligible in the security parameter.*

Theorem 4. *The tropical ElGamal-like encryption scheme achieves IND-CPA security under the TMDH assumption.*

Proof sketch. The encryption of a message m consists of a pair $(C_1, C_2) = (B^{\otimes r}, m \oplus (Y^{\otimes r}))$, where Y is the recipient's public key and r is random. Given C_1, recovering the blinding factor requires solving an instance of TMDH. If an adversary could distinguish between encryptions of m_0 and m_1, it would solve the TMDH problem, contradicting Assumption 5.1. Hence, the scheme is IND-CPA secure. □

5.3.1 Brute-force Attacks

Exhaustively searching for exponents a, b requires time exponential in their bit-length. For sufficiently large parameters (e.g., 256-bit exponents), brute force is infeasible.

5.3.2 Quantum Adversaries

Shor's algorithm does not apply, as the scheme does not rely on factorization or discrete logarithms. Grover's algorithm yields only a quadratic speedup for exhaustive search, so parameters should be doubled (e.g., 512-bit exponents) to maintain post-quantum security.

5.3.3 Algebraic Attacks

Solving the public equations reduces to solving systems of nonlinear tropical equations, which is NP-hard in the general case. Block structure does not admit known simplifications that reduce the hardness.

5.3.4 Structural Attacks

Tropical block matrices do not embed efficiently into classical linear algebra, preventing linearization attacks common in matrix-based cryptography.

5.4 Performance and Efficiency Analysis

In addition to security, the practical viability of a public key cryptosystem depends on the size of its public parameters, key lengths, ciphertext expansion, and computational complexity. We briefly analyze these aspects for the proposed tropical block matrix–based protocols.

5.4.1 Key Sizes

The public key consists of one or more tropical block matrices of dimension $n \times n$, with entries drawn from an integer range $[0, q)$. Each entry requires $\lceil \log_2 q \rceil$ bits. Thus, the size of a single public matrix is

$$|PK| = n^2 \cdot \lceil \log_2 q \rceil \text{ bits.}$$

The private key is an integer exponent $a \in [1, 2^\lambda]$, requiring λ bits, where λ is the security parameter. For $\lambda = 256$, private keys remain compact.

5.4.2 Ciphertext Expansion

An encryption of a message m produces two components:

$$C = (C_1, C_2) = (B^{\otimes r},\ m \oplus (Y^{\otimes r})),$$

where C_1 is a tropical block matrix of the same dimension as the public key, and C_2 is a masked version of the message. Therefore, ciphertext expansion is approximately one additional matrix plus the length of the message, i.e.,

$$|C| \approx |PK| + |m|.$$

This is comparable to ElGamal encryption, which doubles ciphertext size, but with matrices in place of group elements.

5.4.3 Computational Complexity

The dominant operations in both the key exchange and the encryption scheme are tropical matrix multiplications. For block matrices of dimension n, the complexity of one multiplication is $O(n^3)$, although this can be reduced using optimized algorithms for min-plus matrix multiplication. Computing exponentiations $B^{\otimes r}$ via repeated squaring requires $O(\log r)$ multiplications. Hence:

- **Key generation:** $O(\log a \cdot n^3)$ tropical operations.
- **Encryption:** $O(\log r \cdot n^3)$ tropical operations.
- **Decryption:** A single matrix–vector tropical multiplication, $O(n^2)$.

Compared with classical number-theoretic schemes, tropical operations avoid modular exponentiations, relying only on additions and minimizations, which are lightweight and parallelizable.

5.4.4 Parameter Considerations

For $n = 64$ and $q = 2^{16}$, a public key requires about 64 KB, which is larger than RSA or ECC keys but comparable to several lattice-based PQC candidates. Ciphertexts are approximately twice the size of public keys, which is acceptable for secure communication settings but may be heavy for constrained devices. Tropical operations are inherently parallelizable on GPUs and hardware accelerators, suggesting that practical efficiency may improve significantly with optimized implementations.

The proposed protocols rest on TMDH hardness assumption. While this provides a foundation for security, further cryptanalytic study is necessary to validate its robustness. The comparison of key sizes, ciphertext sizes, and main operations between the proposed tropical block matrix scheme and classical/PQC systems is shown in Table 1.

Table 1: Comparison of key sizes, ciphertext sizes, and main operations between the proposed tropical block matrix scheme and classical/PQC systems.

Scheme	**Key Size (Public/Private)**	**Ciphertext Size**	**Main Operations**
RSA-2048	2048 bits / 2048 bits	2048 bits	Modular exponentiation
ECC (P-256)	256 bits / 256 bits	512 bits	Elliptic curve scalar multiplication
Lattice-based (Kyber-768, NIST PQC)	∼1184 bytes / ∼2400 bytes	∼1088 bytes	Polynomial multiplication (NTT)
Proposed Tropical Block Matrix Scheme	$n^2 \cdot \lceil \log_2 q \rceil$ bits / λ bits	$\approx \lvert PK \rvert + \lvert m \rvert$	Tropical matrix multiplication (min-plus)

6 Conclusions

In this paper, we proposed new cryptographic constructions based on tropical block matrices $M_P(A, B)$, including a key exchange protocol and a public key encryption scheme inspired by ElGamal. The security of these protocols is grounded in the NP hardness of solving nonlinear systems over tropical semirings, which makes them resistant to cryptographic attacks. Unlike traditional number theoretic approaches, our framework eliminates the need for multiplication in the classical sense, leveraging the computational simplicity of tropical operations. While the proposed protocols demonstrate conceptual novelty and potential efficiency, further investigation is required to fully assess their robustness against advanced cryptanalytic techniques and quantum adversaries.

Several directions for future research naturally arise from this work. A primary avenue is a deeper cryptanalytic study of the proposed tropical block matrix–based schemes, including the investigation of potential structural, algebraic, and adaptive attacks, as well as tighter security reductions under well-defined hardness assumptions. Another important direction concerns parameter selection and optimization, with the goal of reducing key sizes and ciphertext expansion while maintaining an adequate security margin. In addition, extending the proposed framework to other tropical or semiring-based algebraic structures, as well as designing additional cryptographic primitives such as digital signatures or authenticated key exchange protocols within this setting, represents a promising line of future research.

We believe that this work provides a foundation for future research at the intersection of tropical algebra and cryptography, opening new directions for the design of secure and efficient public key systems.

References

[1] K. Ahmed, S. Pal and R. Mohan, *A review of the tropical approach in cryptography*, Cryptologia, (1) **47** (2021), 63–87.

[2] R. E. Atani, Sh.E. Atani and A. H. Karbasi, *A new ring-based SPHF and PAKE protocol on ideal lattices*, The ISC International Journal of Information Security, (1) **11** (2019), 75-86.

[3] R. E. Atani, Sh. E. Atani and A. H. Karbasi, *A provably secure variant of ETRU based on extended ideal lattices over direct product of dedekind domains*, Journal of Computing and Security, (1) **5** (2018), 13-34.

[4] R. E. Atani, Sh. E. Atani and A. H. Karbasi, *EEH: AGGH-like public key cryptosystem over the eisenstein integers using polynomial representations*, The ISC Int. J. Inform. Security, (2) **7** (2015), 115-126.

[5] R. E. Atani, Sh. E. Atani and A. H. Karbasi, *NETRU: A non-commutative and secure variant of CTRU cryptosystem*, The ISC International Journal of Information Security, (1) **10** (2018), 45-53.

[6] R. E. Atani, Sh. E. Atani and S. Mirzakuchaki, *Public key cryptography based on semimodules over qutient semi-rings*, International Mathematical Forum, (49-52) **2** (2007), 2561-2570.

[7] R. E. Atani, Sh. E. Atani and S. Mirzakuchaki, *Public key cryptography using semigroup actions and semirings*, Journal of Discrete Mathematical Sciences and Cryptography, (4) **11** (2008), 437–445.

[8] D. J. Bernstein, J. Buchmann and E. Dahmen, *Post-quantum Cryptography*, Springer Berlin, Heidelberg, 2009.

[9] S. David and S. Bernd, *Tropical Mathematics*, Math. Mag., **82** (2009), 163-173.

[10] W. Diffie and M. E. Hellman, *New direction in cryptography*, IEEE Trans. Inf. Theory., **22** (1976), 644-654.

[11] D. Grigoriev and V. Shpilrain, *Tropical cryptography*, Communications in Algebra, (6) **42** (2014), 2624-2632.

[12] J. S. Golan, *Semirings and Their Applications*, Springer Science Business Media: Berlin, Germany, 1999. Chapter 21.

[13] H. Huang, *Cryptosystems based on tropical congruent transformaton of symmetric matrices*, Symmetry, **14** (2022), 23-78.

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

[15] A. H. Karbasi and R. E. Atani, *ILTRU: An NTRU-like public key cryptosystem over ideal lattices*, Cryptology ePrint Arxive, paper 2015/549, (2015).

[16] A. H. Karbasi, R. E. Atani, *PSTRU: A provably secure variant of NTRUEncrypt over extended ideal lattices*, The 2nd National Industrial Mathematics Conference, Tabriz, Iran, 2015.

[17] A. H. Karbasi, R. E. Atani and Sh. E. Atani, *PairTRU: pairwise non-commutative extension of the NTRU public key cryptosystem*, IJISS, (1) **7** (2018), 11–19.

[18] G. Maze, Ch. Monico and J. Rosenthal, *A public key cryptosystem based on actions by semi-group*, In Proceedings of the IEEE International Symposium on Information Theory, (2002) 266-289.

[19] G. Maze, Ch. Monico and J. Rosenthal, *Public key cryptography based on semi-group actions*, Advances in Mathematics of Communications, **1** (2007), 489-507.

[20] E. Mehraban, T. A. Gulliver, R. E. Atani and E. Hincal, *A novel electronic voting system using a blind signature scheme and blockchain*, 11th International Symposium on Telecommunications (IST), Tehran, Islamic Republic of Iran, (2024), 790-794.

[21] E. Mehraban, T. A. Gulliver, R. E. Atani and E. Hincal. *Blind RSA signatures from the $t-$generalized Lehmer sequences of some classes of groups*, Mathematical Foundations of Computing, https://doi.org/10.3934/mfc.2025036.

[22] E. Mehraban, T. A. Gulliver, R. E. Atani and E. Hincal, *Diffie-Hellman key exchange on the Heisenberg group*, Journal of Combinatorial Mathematics and Combinatorial Computing, **127**, 301-315.

[23] A. R. Naseri, A. Abbasi and R. E. Atani, *A new public key cryptography using M_q matrix*, Journal of Mathematical Modeling, (4) **11** (2023), 681-693.

[24] P. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAMJ. Comput., **26** (1997), 1484-1509.

[25] I. Simon, *On semigroups of matrices over the tropical semiring*, RAIRO-Theor. Inform. Appl., **28** (1994), 277-294.

[26] I. Simon, *Recognizable sets with multiplicities in the tropical semiring*, Mathemathical Foundations of Computer Science, (1988) 107-120.

[27] R. Steinwandt and A. S. Corona, *Cryptanalysis of a 2-party key establishment based on a semi-group action problem*, Adv. Math. Commun., **5** (2011), 87-92.

[28] H. Vandiver, *Note on a simple type of algebra in which the cancellation law of addition does not hold*, Bull. Am. Math. Soc., **40** (1934), 914-920.

[29] M. Zeriouh, A. Chillali and A. Boua, *Cryptography based on the matrices*, Boletim da Sociedade Paranaense de Matematica, **37** (2019), 75-83.