International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(10s) 2026 pp. 689-703
https://doi.org/10.70917/ijcisim-2026-3644
Article

Polynomial Tropical Key Exchange (PTKE): A Hybrid Post-Quantum Protocol

Sopan J. Chavhan [1*], Shrikant R. Chaudhari [2]

[1]Department of Mathematics, Shri Vyankatesh Arts, Commerce and Science College, Deulgaon Raja, Buldhana, Maharashtra, India
sjchavhanmath17@gmail.com
[2]School of Mathematical Sciences, K.B.C. North Maharashtra University, Umavi Nagar, Jalgaon, Maharashtra, India
drsrchaudhari@nmu.ac.in
*Corresponding author: sjchavhanmath17@gmail.com

Abstract: The emergence of large-scale quantum computers threatens classical public-key cryptosystems based on integer Factorization and discrete logarithms. This paper introduces the Polynomial Tropical Key Exchange (PTKE), a novel hybrid key-exchange protocol that combines tropical algebra with standard symmetric cryptographic primitives. Unlike previous tropical schemes that rely on a single matrix power $M^{\otimes l}$, PTKE uses a secret tropical polynomial $f(x) = \oplus_{k=0}^{d} c_k \otimes x^{\otimes k}$ evaluated at a public matrix M, followed by multiplication with a secret commuting matrix A drawn from a prescribed commuting family. The security analysis introduces the Tropical Polynomial Factorization Problem (TPFP), a new structured decomposition problem associated with recovering private decompositions of PTKE public keys. While related tropical problems are known to be NP-hard, the precise computational complexity of TPFP remains open. Security is based on the working assumption that no efficient algorithm exists for solving protocol-generated instances of TPFP. We prove the correctness of the protocol and analyze its resistance to currently known tropical cryptanalytic attacks. No efficient quantum algorithm for solving PTKE instances is currently known. The protocol is integrated with SHA-256 and AES-256-GCM to derive standard symmetric session keys. Experimental results demonstrate that PTKE is practical for the proposed parameter ranges, making PTKE a promising direction for further research in post-quantum cryptography.
Keywords*:* Post-quantum cryptography; Tropical algebra; Tropical Polynomial Factorization Problem (TPFP); Tropical matrices; Key exchange protocol; Hybrid cryptography.

1. INTRODUCTION

The rapid advancement of quantum computing poses a fundamental threat to contemporary public-key cryptography. Algorithms such as RSA, DSA, and Diffie-Hellman rely on the conjectured hardness of integer Factorization and the discrete logarithm problem. However, Shor's seminal result [1] demonstrated that both problems can be solved in polynomial time on a sufficiently large fault-tolerant quantum computer. Although such quantum computers are not yet available, the possibility of future cryptographically relevant quantum machines has motivated an intensive search for alternative mathematical foundations that resist both classical and quantum attacks, leading to the development of post-quantum cryptography.

In response to the quantum threat, considerable international effort has been devoted to the development of post-quantum cryptography (PQC), which aims to construct public-key primitives that remain secure against both classical and quantum adversaries. This effort has culminated in the standardization of several lattice-based algorithms through the National Institute of Standards and Technology (NIST) Post-Quantum Cryptography Standardization Project, while other approaches continue to be actively investigated for their security, efficiency, and deployment characteristics [2]. Comprehensive surveys of post-quantum cryptography classify these approaches according to their underlying mathematical assumptions and discuss the challenges involved in designing secure quantum-resistant cryptographic systems [3].

Among the most prominent post-quantum approaches are lattice-based, code-based, multivariate, and hash-based cryptosystems. Each of these families offers different trade-offs in terms of key size, computational efficiency,

and security assumptions. In parallel, researchers have investigated more exotic algebraic structures, including non-commutative groups, braid groups, and semirings, as potential foundations for cryptographic protocols. In particular, tropical (idempotent) semirings have attracted considerable attention because of their non-linear algebraic structure, the absence of an underlying group operation, and the NP-hardness of several tropical computational problems [4].

The first systematic application of tropical algebra to public-key cryptography was introduced by Grigoriev and Shpilrain [5], who proposed a key-exchange protocol based on tropical matrix exponentiation. Their construction employed the max-plus (or min-plus) tropical semiring, where addition is replaced by the maximum (or minimum) operation and multiplication corresponds to ordinary addition. This arithmetic is computationally efficient because multiplication reduces to integer addition and addition reduces to a comparison. However, Kotov and Ushakov [6] later showed that the scheme was vulnerable to an attack that recovers the secret exponent by exploiting the structure of the tropical powers. Subsequently, Grigoriev and Shpilrain proposed a modified construction based on tropical semidirect products with extensions by homomorphisms [7], but this variant was broken by the binary-search attack of Rudy and Monico [8] a more efficient attack due to Isaac and Kahrobaei [9].

To address these weaknesses, Muanalifah and Sergeev [10] introduced protocols based on commuting tropical matrices, including Jones matrices and Linde-de la Puente matrices. Although these constructions resist the original Kotov-Ushakov attack, the authors later demonstrated a generalized attack capable of recovering the secret key by expressing the secret matrix as a linear combination of powers of a known public matrix [11]. Consequently, the development of secure and efficient tropical key-exchange protocols remains an open problem.

A practical direction for post-quantum cryptography is the use of hybrid protocols, which combine a post-quantum key-establishment mechanism with well-established symmetric primitives. In such constructions, the post-quantum component generates a shared secret, while standard primitives such as SHA-256 and AES-256-GCM provide key derivation and authenticated encryption.

Hybrid integration has already been explored for protocols such as TLS and SSH [12], and the IETF has investigated design issues for hybrid key exchange in TLS 1.3 [13]. Following this approach, Durcheva [14] recently proposed a hybrid tropical key-exchange scheme based on the Tropical Factorization Discrete Logarithm Problem (TFDLP), combined with SHA-256 and AES-GCM. Although the construction avoids some earlier attacks, its security remains tied to the Factorization of a single tropical matrix power, which may exhibit periodic algebraic behaviour that could potentially be exploited in future cryptanalysis.

In this work, we propose a new hybrid key-exchange protocol called the Polynomial Tropical Key Exchange (PTKE). The central idea is to replace the matrix exponentiation $M^{\otimes l}$ used in earlier schemes by a tropical polynomial evaluation

$$f(M),$$

Where,

$$f(x) = \bigoplus_{k=0}^{d} c_k \otimes x^{\otimes k}$$

is a secret tropical polynomial of degree at most d. The public key of a user is then constructed as

$$K_A = f(M) \otimes A,$$

where A is a secret matrix chosen from a prescribed commuting family, such as the Linde-de la Puente matrices.

The security analysis of PTKE is motivated by the Tropical Polynomial Factorization Problem (TPFP): given the public matrix M and a public key K_A, recover a valid decomposition into a tropical polynomial evaluation and a commuting matrix factor.

This construction offers several advantages over previous tropical designs:

- ***Larger key space:*** Instead of a single secret exponent, the private key contains $d + 1$ polynomial coefficients together with a secret commuting matrix, resulting in a substantially larger parameter space.

- ***Reduced periodic structure:*** The polynomial evaluation combines many powers of the public matrix, making the periodic patterns exploited in known attacks substantially less apparent than in matrix exponentiation-based constructions.
- ***Structured Factorization problem:*** Recovering the private information requires solving a structured decomposition problem of the form

$$K_A = f(M) \otimes A,$$

where one factor must be a tropical polynomial evaluation of the public matrix and the second factor must belong to a prescribed commuting family. This leads naturally to the Tropical Polynomial Factorization Problem (TPFP). While tropical polynomial Factorization over restricted coefficient sets is known to be NP-hard [4] and tropical matrix Factorization is also hard [15], the precise complexity of TPFP remains open, providing a fresh basis for security.

The PTKE protocol is implemented as a hybrid construction; the shared secret is hashed to derive a symmetric key that is subsequently used with AES-256-GCM. This approach combines the conjectured post-quantum hardness of the tropical component with the standardization and practical efficiency of widely deployed symmetric primitives.

The remainder of this paper is organized as follows. Section 2 recalls the necessary preliminaries on tropical semirings, matrices, polynomials, and commuting families. Section 3 presents the PTKE protocol. Section 4 introduces the Tropical Polynomial Factorization Problem and the associated hardness assumption. Section 5 presents experimental results and performance analysis. Section 6 analyses security against currently known attacks. Finally, Section 7 concludes the paper.

2. Preliminaries

This section reviews the basic concepts from tropical algebra that are required for the proposed Polynomial Tropical Key Exchange (PTKE) protocol.

Definition 1 *(Tropical Semiring).* The max-plus tropical semiring is the algebraic structure

$$\mathcal{T} = (\mathbb{Z} \cup \{-\infty\}, \oplus, \otimes),$$

where the operations are defined by

$$a \oplus b = \max(a, b), a \otimes b = a + b.$$

The additive identity is $\varepsilon = -\infty$, and the multiplicative identity is $e = 0$.

The tropical semiring is additively idempotent since $a \oplus a = a$ for every $a \in \mathcal{T}$. The min-plus tropical semiring $(\mathbb{Z} \cup \{+\infty\}, \min, +)$ is equivalent to the max-plus semiring under negation.

2.1 Tropical Matrices

Let $M_n(\mathcal{T})$ denote the set of all $n \times n$ matrices over the tropical semiring. For matrices $X, Y \in M_n(\mathcal{T})$ and scalar $\alpha \in \mathcal{T}$, tropical matrix operations are defined entrywise by

$$(X \oplus Y)_{ij} = x_{ij} \oplus y_{ij} = \max_{1 \le i,j \le n} (x_{ij}, y_{ij}),$$

$$(X \otimes Y)_{ij} = \bigoplus_{k=1}^{n} (x_{ik} \otimes y_{kj}) = \max_{1 \le k \le n} (x_{ik} + y_{kj}),$$

and

$$(\alpha \otimes X)_{ij} = \alpha + x_{ij}.$$

The tropical identity matrix I has entries

$$I_{ij} = \begin{cases} 0, & i = j \\ -\infty, & i \neq j \end{cases}$$

while the tropical zero matrix has all entries equal to $-\infty$.

2.2 Tropical Matrix Powers

For a matrix $M \in M_n(\mathcal{T})$, tropical powers are defined recursively by

$$M^{\otimes 0} = I,$$
$$M^{\otimes k} = M^{\otimes (k-1)} \otimes M, k \geq 1.$$

Thus,

$$M^{\otimes k} = \underbrace{M \otimes M \otimes \cdots \otimes M}_{k \text{ times}}.$$

Tropical matrix powers play the same role as ordinary matrix powers in classical algebra and form the basis of many tropical cryptographic constructions.

2.3 Tropical Polynomials

Definition 2 *(Tropical Polynomial).* A tropical polynomial of degree at most d is an expression of the form

$$f(x) = \bigoplus_{k=0}^{d} c_k \otimes x^{\otimes k},$$

where $c_k \in \mathcal{T}$.

Given a matrix $M \in M_n(\mathcal{T})$, the polynomial is evaluated as

$$f(M) = \bigoplus_{k=0}^{d} c_k \otimes M^{\otimes k}.$$

Remark 1. For a fixed matrix M, the collection

$$\{f(M) \mid f \text{ a tropical polynomial } \}$$

forms a commutative subsemiring of $M_n(\mathcal{T})$. This follows from the commutativity of tropical polynomial multiplication and evaluation at the same matrix argument.

2.4 Commuting Matrix Families

A family of matrices $\mathcal{C} \subseteq M_n(\mathcal{T})$ is called a commuting family if

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

for all $A, B \in \mathcal{C}$.

Commuting matrix families play a central role in tropical cryptography because they allow two parties to combine secret matrices while ensuring that the resulting products agree.

The PTKE protocol uses a particular commuting family introduced by Linde and de la Puente.

2.5 Linde-de la Puente Matrices

Definition 3 *(Linde-de la Puente Matrices [10]).* Let $\alpha \geq 0$ and $\beta \leq 0$. An $n \times n$ matrix $L = (\ell_{ij}) \in M_n(\mathcal{T})$ is called a Linde-de la Puente matrix if

$$\ell_{ii} = \alpha$$

for every diagonal entry and

$$\ell_{ij} \in [2\beta, \beta]$$

for every off-diagonal entry $i \neq j$.

A fundamental property of this family is that any two such matrices commute under tropical multiplication.

Theorem 1 *(Linde-de la Puente [10]).* If A and B are Linde-de la Puente matrices with the same parameters α and β, then

$$A \otimes B = B \otimes A.$$

In the proposed PTKE implementation, we use $\alpha = 0, \beta = -1000$, and select each off-diagonal entry independently and uniformly from $[2\beta, \beta] = [-2000, -1000]$.

3. Polynomial Tropical Key Exchange Protocol

The proposed Polynomial Tropical Key Exchange (PTKE) protocol combines tropical polynomial evaluation with commuting tropical matrices to establish a shared secret between two parties.

3.1 Protocol Description

Public parameters consist of the tropical semiring

$$\mathcal{T} = (\mathbb{Z} \cup \{-\infty\}, \max, +),$$

a matrix dimension $n \geq 64$, a public matrix

$$M \in M_n(\mathcal{T}),$$

whose entries are chosen uniformly from $[0, 2^{256}]$, a polynomial degree bound $d \geq 20$, and a commuting family of tropical matrices $\mathcal{C}$, instantiated by the Linde-de la Puente family.

1. Alice chooses a private tropical polynomial

$$f(x) = \bigoplus_{k=0}^{d} c_k \otimes x^{\otimes k},$$

with coefficients $c_k \in [0, 2^{256}]$, together with a secret matrix $A \in \mathcal{C}$.

2. Similarly, Bob chooses

$$g(x) = \bigoplus_{k=0}^{d} b_k \otimes x^{\otimes k},$$

with coefficients $b_k \in [0, 2^{256}]$, and a secret matrix $B \in \mathcal{C}$.

3. The corresponding public keys are

$$K_A = f(M) \otimes A, K_B = g(M) \otimes B.$$

4. After exchanging public keys, Alice computes

$$K_{AB} = f(M) \otimes K_B \otimes A,$$

while Bob computes

$$K_{BA} = g(M) \otimes K_A \otimes B.$$

Theorem 2 *(Correctness of PTKE).* In the Polynomial Tropical Key Exchange protocol,

$$K_{AB} = K_{BA}.$$

Proof. Substituting the public keys yields

$$K_{AB} = f(M) \otimes g(M) \otimes B \otimes A$$

and

$$K_{BA} = g(M) \otimes f(M) \otimes A \otimes B.$$

Since the polynomial evaluations can be written as $f(M) = \oplus_i \ c_i \otimes M^{\otimes i}$ and $g(M) = \oplus_j \ b_j \otimes M^{\otimes j}$, their tropical product computes terms of the form $c_i + b_j + M^{\otimes(i+j)}$. Tropical addition is commutative, therefore

$$f(M) \otimes g(M) = \bigoplus_{i,j} \left(c_i + b_j\right) \otimes M^{\otimes(i+j)} = g(M) \otimes f(M).$$

Moreover, matrices in the commuting family $\mathcal{C}$ satisfy

$$A \otimes B = B \otimes A,$$

So, it follows that

$$K_{AB} = K_{BA}.$$

Hence both parties obtain the common shared secret

$$K := K_{AB} = K_{BA}. \ \square$$

Proposition 1 *(Computational Complexity).* Assume that the tropical matrix powers

$$M^{\otimes 0}, M^{\otimes 1}, \dots, M^{\otimes d}$$

have been pre-computed. For matrix dimension n and polynomial degree bound d, the PTKE protocol has the following asymptotic costs:

- Computing the tropical polynomial evaluation $f(M)$ requires $O(dn^2)$ tropical operations.
- Key generation, consisting of the computation of $K_A = f(M) \otimes A$, requires $O(dn^2 + n^3)$ tropical operations.
- Shared-secret computation (using the already computed (M)) requires two tropical matrix multiplications and therefore costs $O(n^3)$ tropical operations.

Proof. Evaluating the tropical polynomial consists of $d + 1$ scalar-matrix multiplications followed by entrywise tropical additions, each requiring $O(n^2)$ operations; hence polynomial evaluation costs $O(dn^2)$. Multiplication of two $n \times n$ tropical matrices requires $O(n^3)$ operations. Key generation performs one such multiplication, while shared-secret computation performs two. The stated bounds follow. $\square$

3.2 Key Derivation and Encryption

The shared matrix K is serialized into a canonical byte representation and processed using SHA-256:

$$k_{\text{sym}} = \text{SHA} - 256(\text{Encode}(K)).$$

The resulting 256-bit value is used as the symmetric key for AES-256-GCM encryption and authentication. Given a plaintext message m and a nonce N, encryption produces

$$(c, t) = \text{AES} - 256 - \text{GCM}\left(k_{\text{sym}}, N, m\right),$$

where c denotes the ciphertext and t the authentication tag. The recipient verifies the authentication tag and decrypts the ciphertext using the same derived key k_{sym} .

Algorithm 1. Polynomial Tropical Key Exchange (PTKE)

Require: *Public matrix M, matrix dimension n, polynomial degree bound d, commuting family $\mathcal{C}$*

1. *Alice randomly samples a tropical polynomial f of degree at most d.*
2. *Alice randomly selects $A \in \mathcal{C}$.*
3. *Alice computes $K_A \leftarrow f(M) \otimes A$.*
4. *Bob randomly samples a tropical polynomial g of degree at most d.*
5. *Bob randomly selects $B \in \mathcal{C}$.*
6. *Bob computes $K_B \leftarrow g(M) \otimes B$.*
7. *Alice and Bob exchange the public keys K_{a} and K_{β}.*

8. $Alice\ computes\ K_{AB} \leftarrow f(M) \otimes K_B \otimes A.$
9. $Bob\ computes\ K_{BA} \leftarrow g(M) \otimes K_A \otimes B.$
10. $Set\ K \leftarrow K_{AB} = K_{BA}.$
11. $Derive\ the\ symmetric\ key\ k_{\text{sym}} \leftarrow SHA-256(Encode(K)).$
12. $Encrypt/decrypt\ messages\ using\ AES-256-GCM\ with\ k_{\text{sym}}.$

Ensure: $Both\ parties\ share\ the\ identical\ session\ key.$

4. The Tropical Polynomial Factorization Problem (TPFP)

We now formally define the Tropical Polynomial Factorization Problem (TPFP), which underlies the security assumptions used throughout the remainder of the paper.

Definition 4 *(Tropical Polynomial Factorization Problem (TPFP)).* Let $M \in M_n(\mathcal{T})$ be a public tropical matrix and let $P = f(M) \otimes A$, where f is a tropical polynomial of degree at most d and $A \in \mathcal{C}$ belongs to a prescribed commuting family.

The search version of TPFP is the problem of recovering a pair $(\tilde{f}, \tilde{A})$ such that

$$P = \tilde{f}(M) \otimes \tilde{A}, \qquad \tilde{A} \in \mathcal{C}.$$

Definition 5 *(Decision TPFP).* Given (M, P, d, r), determine whether there exist a tropical polynomial f with $\deg(f) \leq d$ and a matrix $A \in \mathcal{C}$ such that

$$P = f(M) \otimes A,$$

where

$$A \neq I,$$

and the total bit length of the finite coefficients of f does not exceed r. The restriction $A \neq I$ excludes the trivial decomposition $P = f(M) \otimes I$, which would otherwise make every instance of Decision TPFP automatically positive.

4.1 Relation to PTKE and Existing Factorization Problems

Every PTKE public key has the form

$$K_A = f(M) \otimes A,$$

where f and A are secret. Consequently, recovering a valid private decomposition of a public key is precisely an instance of the search version of TPFP.

TPFP may be viewed as a structured tropical Factorization problem. Classical tropical polynomial Factorization asks whether a tropical polynomial h can be written as

$$h = f \otimes g,$$

while tropical matrix Factorization asks whether a matrix P can be decomposed as

$$P = X \otimes Y.$$

In contrast, TPFP seeks a decomposition

$$P = f(M) \otimes A,$$

where one factor is restricted to the polynomial subsemiring

$$\{f(M) \mid f \text{ is a tropical polynomial }\},$$

and the other belongs to a prescribed commuting family $\mathcal{C}$.

Thus TPFP combines features of both tropical polynomial Factorization [4] and tropical matrix Factorization [15], while imposing additional algebraic structure. To the best of our knowledge, this particular structured Factorization problem has not previously been proposed as the basis of a tropical key-exchange protocol.

4.2 TPFP Hardness Assumption

While a formal reduction from an NP-hard problem to TPFP is not currently known, the problem is inspired by two well-studied hard tropical problems. Tropical polynomial Factorization over restricted coefficient sets is NP-hard [4], and tropical matrix Factorization is also known to be computationally difficult [15]. The absence of an efficient attack on PTKE instances leads us to adopt the following working hardness assumption.

Assumption 1 *(TPFP Hardness Assumption)*. For the parameter ranges

$$n \geq 64, \qquad d \geq 20,$$

with polynomial coefficients chosen uniformly from $[0,2^{256}]$ and commuting matrices sampled from the Linde-de la Puente family $\mathcal{C}$, no probabilistic polynomial-time algorithm is currently known that solves the search version of TPFP with non-negligible probability over the distribution of instances generated by the PTKE protocol.

The assumption concerns recovery of a valid decomposition (f, A) from a PTKE public key $= f(M) \otimes A$; it is a computational assumption on random protocol instances, not a consequence of any worst-case complexity result.

5. Experimental Evaluation

The proposed Polynomial Tropical Key Exchange (PTKE) protocol was implemented in Python 3.11 using native integer arithmetic together with optimized tropical matrix operations. All experiments were performed in the Google Colab cloud environment using a Linux-based runtime on a virtual machine equipped with an Intel ® Xeon ® CPU @ 2.20 GHz (2 vCPUs) and 12 GB RAM. Execution time was measured using Python's $time.perf\_counter()$ high-resolution timer, while peak memory consumption was obtained using Python's $tracemalloc$ module. To improve the reliability of the reported measurements, each benchmark was repeated 100 times, and the reported execution times correspond to the arithmetic mean of all executions. Before each execution, Python's garbage collector was explicitly invoked to reduce runtime fluctuations.

All experiments used randomly generated public tropical matrices together with randomly generated tropical polynomial coefficients and commuting Linde-de la Puente matrices. Unless otherwise stated, the default parameter set consisted of polynomial degree $d = 20$, coefficient bit length of 256 bits, and matrix dimensions ranging from 16 × 16 to 128 × 128.

5.1 Runtime Performance

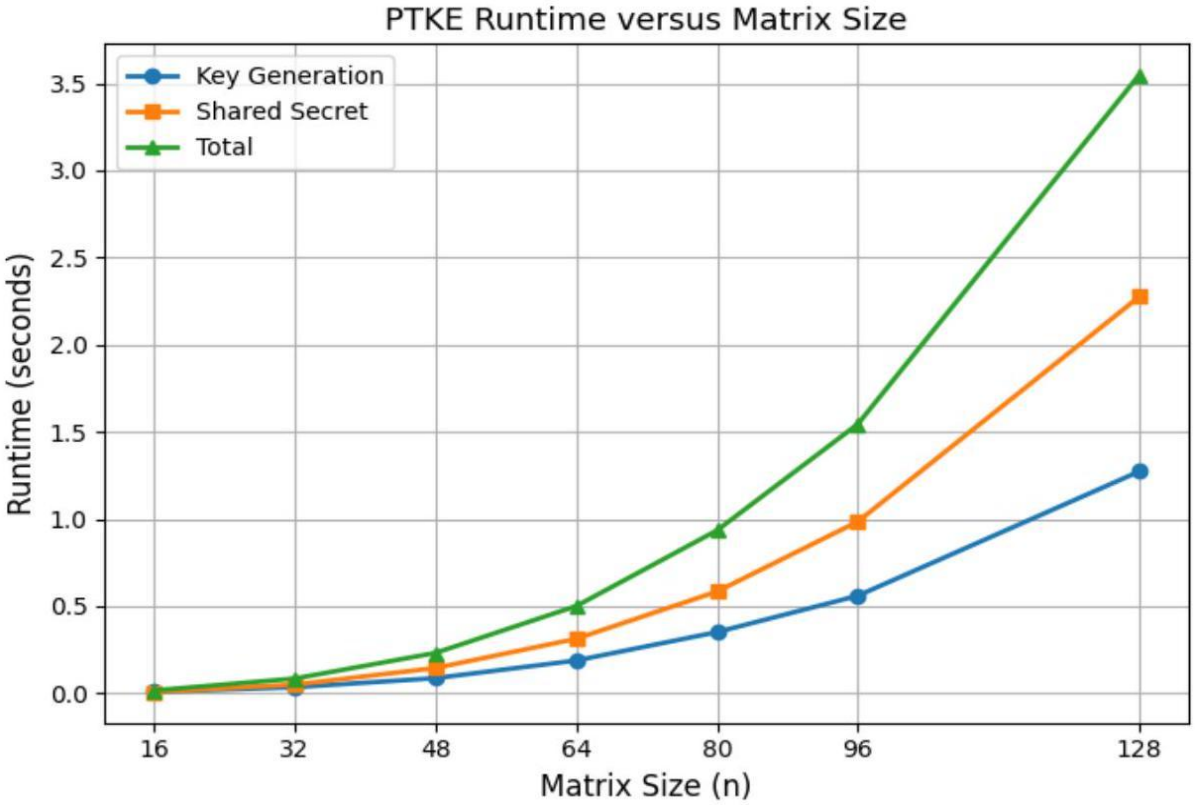
We first evaluate the computational cost of PTKE as the matrix dimension increases while fixing the polynomial degree at $d = 20$. Subsequently, we investigate the influence of the polynomial degree while keeping the matrix dimension fixed at 64×64.

Table 1: Runtime performance versus matrix size

n	Key Generation (s)	Shared Secret (s)	Total (s)
16	0.008352	0.007764	0.016115
32	0.034587	0.049685	0.084271
48	0.086674	0.144814	0.231489
64	0.187981	0.312465	0.500446
80	0.350880	0.583864	0.934744
96	0.559519	0.985091	1.544610
128	1.273164	2.275765	3.548929

Table 1 Summarizes the average execution time required for key generation, shared-secret computation, and the complete key exchange for different matrix sizes. *Figure 1* illustrates the corresponding scalability trend.

Figure 1: Average runtime of PTKE as a function of matrix dimension.



The execution time grows smoothly with the dimension. A complete key exchange requires only 0.016 s for 16 × 16 matrices and approximately 3.55 s for 128 × 128 matrices. This behaviour reflects the cubic complexity of tropical matrix multiplication, which dominates polynomial evaluation. Matrices of order 64 complete in roughly half a second, while larger dimensions increase the cost of known attack strategies and enlarge the search space of PTKE instances.

Table 2: Runtime performance versus polynomial degree

d	Key Generation (s)	Shared Secret (s)	Total (s)
5	0.068769	0.138655	0.207424
10	0.075197	0.139569	0.214765
15	0.085989	0.146138	0.232127
20	0.099023	0.157744	0.256767
25	0.100001	0.165057	0.265059
30	0.113466	0.172292	0.285758

Figure 2: Average runtime of PTKE as a function of polynomial degree.

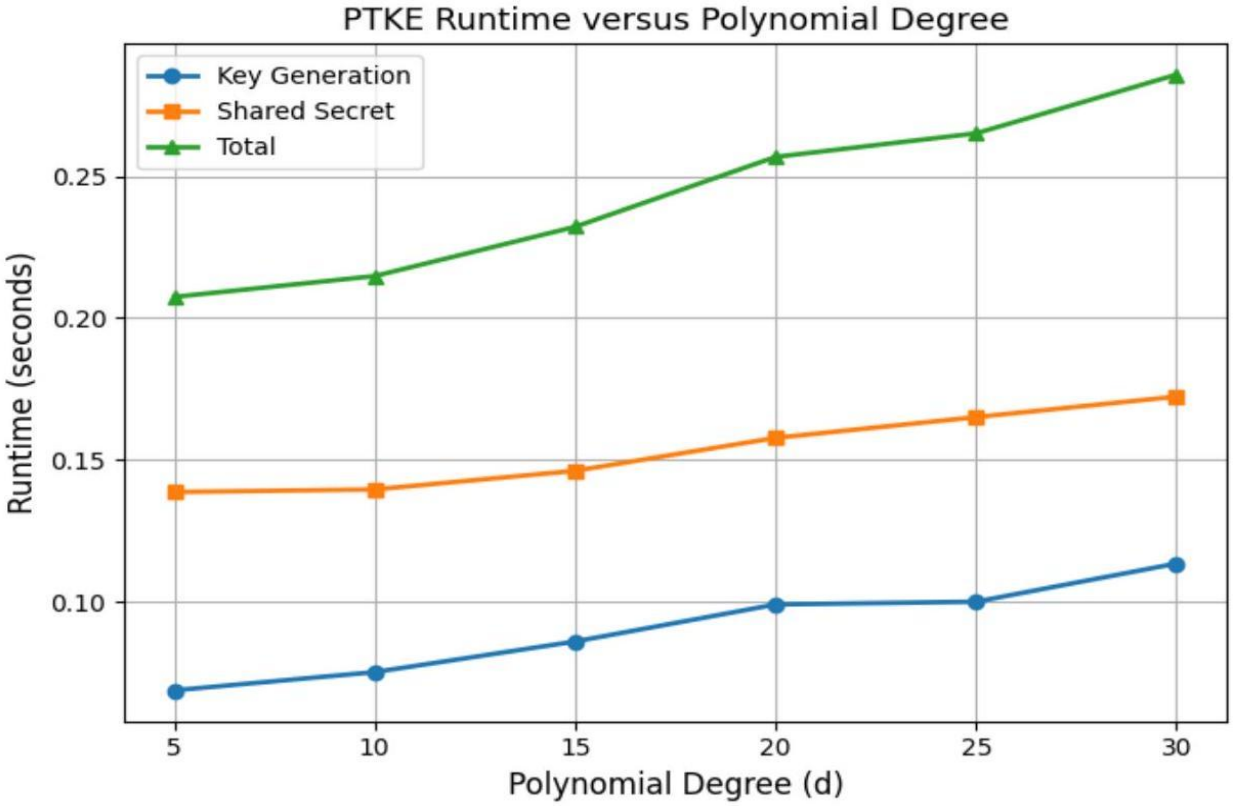


Table 2 and *Figure 2* show the effect of varying the polynomial degree while fixing $n = 64$.

Increasing the polynomial degree from 5 to 30 raises the total execution time from 0.207 s to 0.286 s, an increase of approximately 38%. This modest growth confirms that tropical matrix multiplication dominates the cost.

5.2 Memory and Communication Cost

Besides computational efficiency, practical deployment also depends on the memory requirements during protocol execution and the communication overhead introduced by public-key transmission.

Table 3 shows that both the peak memory usage and the public-key size increase approximately quadratically with the matrix dimension, as expected for $n \times n$ tropical matrices. Even for the largest evaluated instance (128×128), the implementation requires only 2.40 MB of peak memory. The reported public-key sizes correspond to the in-memory Python representation; a compact fixed-length encoding would further reduce the communication overhead.

Table 3: Memory and communication cost versus matrix size

n	Peak Memory (MB)	Public Key Size (KB)
16	0.0558	8.16
32	0.1551	32.63
48	0.3478	73.41
64	0.6086	130.50

80	0.9651	203.91
96	1.3826	293.63
128	2.3998	522.00

Table 4 compares representative tropical key-exchange protocols according to their underlying mathematical problems, private-key representations, and support for hybrid deployment. Unlike previous constructions, PTKE employs a tropical polynomial together with a commuting matrix, leading naturally to the Tropical Polynomial Factorization Problem (TPFP), while remaining compatible with standard hybrid key-establishment techniques.

Table 4: Comparison of representative tropical key-exchange protocols.

Protocol	Underlying Hard Problem	Secret Representation	Hybrid
Grigoriev-Shpilrain [5]	Two-sided matrix action	Single exponent	No
Grigoriev-Shpilrain [7]	Semidirect product	Single exponent	No
Muanalifah-Sergeev [10]	Commuting matrix decomposition	Commuting matrix	No
Huang-Li [16]	Multiple exponentiation	Multiple exponents	No
Durcheva [14]	TFDLP	Exponent + commuting matrix	Yes
PTKE (This work)	TPFP	Polynomial + commuting matrix	Yes

6. Security Analysis and Parameter Selection

We analyze PTKE under the TPFP hardness assumption introduced in Section 4. Given a public matrix M and a public key

$$K_A = f(M) \otimes A,$$

where f is a tropical polynomial and $A \in \mathcal{C}$ belongs to the prescribed commuting family, an adversary must solve the structured decomposition problem underlying TPFP.

6.1 Security Model and Relation to TPFP

We consider a passive adversary that observes all public parameters and the exchanged public keys. The adversary receives

$$(M, K_A, \mathcal{C})$$

and attempts to compute a pair

$$(\tilde{f}, \tilde{A})$$

such that

$$\tilde{f}(M) \otimes \tilde{A} = K_A, \qquad \tilde{A} \in \mathcal{C}.$$

Finding such a decomposition is precisely the search version of TPFP. Consequently, any algorithm capable of solving TPFP on PTKE instances can recover a valid decomposition of PTKE public keys.

Under the TPFP hardness assumption, no probabilistic polynomial-time algorithm is known that solves this decomposition problem with non-negligible probability on protocol-generated instances. This is a computational

assumption on the distribution of instances generated by PTKE and should not be interpreted as a consequence of any worst-case complexity result.

6.2 Resistance to Known Attacks

Several attacks have been proposed against earlier tropical cryptographic constructions. Their effectiveness relies on algebraic structures that are absent from PTKE.

Kotov-Ushakov attacks. The Kotov-Ushakov attack [6] targets protocols whose public keys expose a single tropical matrix power $M^{\otimes \ell}$. In contrast, PTKE public keys have the form $K_A = f(M) \otimes A$, where f is a tropical polynomial and A is an independently chosen commuting matrix. Since PTKE does not expose a single secret exponent, the attack has no known direct adaptation.

Generalized Kotov-Ushakov attacks. Muanalifah and Sergeev [11] extended the Kotov-Ushakov methodology to protocols whose secret matrices admit a low-dimensional representation over a public basis. No comparable representation is known for the Linde-de la Puente family used by PTKE, whose off-diagonal entries are independently sampled within prescribed intervals.

Rudy-Monico and periodicity attacks. The Rudy-Monico attack [8] exploits the semidirect-product construction of Grigoriev and Shpilrain [7]. PTKE does not employ semidirect products and therefore does not expose the required structure. Likewise, periodicity-based attacks exploit sequences of tropical matrix powers [9]. PTKE replaces a single matrix power by a tropical polynomial evaluation together with an independent commuting matrix, and no direct extension of existing periodicity attacks is currently known.

Algebraic attacks. An adversary may attempt to recover the unknown polynomial coefficients and commuting matrix by solving

$$\left(\bigoplus_{k=0}^{d} c_k \otimes M^{\otimes k} \right) \otimes A = K_A.$$

This yields a structured system of tropical polynomial constraints, which is precisely an instance of the search version of TPFP. At present, no efficient algorithm is known for solving TPFP on PTKE instances. Resistance to this class of attacks therefore relies on the TPFP hardness assumption.

Quantum attacks. No reduction of TPFP to the Hidden Subgroup Problem is known, and no efficient quantum algorithm for solving TPFP is currently known. Grover's algorithm provides at most a quadratic speedup over exhaustive search, so appropriately chosen parameters retain a substantial security margin against brute-force attacks. This should be interpreted as the absence of known quantum attacks rather than as a proof of post-quantum security.

The discussion above considers the principal cryptanalytic techniques proposed against tropical key exchange protocols. For convenience, *Table 5* summarizes the applicability of these published attacks to representative tropical constructions.

Table 5: Summary of published cryptanalytic attacks against representative tropical key-exchange protocols.

Protocol	**Kotov-Ushakov Attack**	**Rudy-Monico Attack**	**Generalized KU Attack**
Grigoriev-Shpilrain [5]	✓	-	-
Grigoriev-Shpilrain [7]	-	✓	-
Muanalifah-Sergeev [10]	-	-	✓
Huang-Li [16]	-	-	-

Durcheva [14]	-	-	-
PTKE (This work)	-	-	-

Legend: ✓= published successful attack; "_" = not applicable.

As shown in *Table 5,* the published attacks exploit algebraic properties specific to earlier tropical protocols, including single-exponent representations, semidirect-product constructions, and low-dimensional commuting matrix decompositions. Since PTKE employs a tropical polynomial together with an independent commuting matrix, no direct adaptation of these attacks is currently known for protocol-generated instances.

6.3 Parameter Selection

The security and efficiency of PTKE depend primarily on the matrix dimension n, the polynomial degree d, and the coefficient bit length. Larger values of these parameters increase the search space of the TPFP while also increasing computational cost.

Throughout the experimental evaluation we considered matrix dimensions

$$n \in \{16,32,48,64,80,96,128\},$$

polynomial degrees

$$d \in \{5,10,15,20,25,30\},$$

and uniformly generated 256-bit tropical polynomial coefficients. Unless otherwise stated, the default configuration is

$$n = 64, d = 20.$$

This parameter set provides a good balance between computational efficiency and algebraic complexity. As demonstrated in Section 5, a complete key exchange requires approximately 0.50 s while consuming less than 1 MB of peak memory. Increasing the matrix dimension to $n = 128$ raises the execution time to approximately 3.55 s but also enlarges the algebraic search space available to an adversary.

The polynomial degree controls the complexity of the hidden tropical polynomial. Experimental results show that increasing the degree from 5 to 30 causes only a moderate increase in runtime, suggesting that larger polynomial degrees can be employed without significantly affecting practical performance.

Since no precise security reduction from PTKE to TPFP is currently known, these parameter choices should be regarded as experimentally motivated recommendations rather than security-level guarantees. Establishing conservative parameter sets based on future cryptanalytic advances remains an important direction for future work.

6.4 Limitations and Open Problems

The present security analysis has several limitations.

- No formal reduction from recovering the shared secret (or the private keys) to the search version of TPFP is currently known.
- The average-case hardness of TPFP on protocol-generated instances remains an open question.
- Security against active adversaries has not yet been formally analyzed.
- No formal proof of post-quantum security is currently available.
- Further cryptanalysis is needed to validate the proposed parameter ranges and to investigate the possibility of specialized attacks exploiting the algebraic structure of TPFP.

Existing attacks against tropical key-exchange protocols exploit single-exponent representations, low dimensional commuting families, semidirect-product constructions, or periodic power sequences. These features are absent from PTKE. Nevertheless, average-case hardness, formal security reductions, and quantum complexity remain important open problems for future work.

Under the TPFP hardness assumption, no efficient classical or quantum attack against PTKE is currently known.

7. Conclusion

This paper introduced the Polynomial Tropical Key Exchange (PTKE), a tropical-algebraic key-exchange protocol that replaces matrix exponentiation with tropical polynomial evaluation combined with commuting matrix families. The design leads naturally to the Tropical Polynomial Factorization Problem (TPFP), which serves as the underlying hardness assumption.

The security of PTKE rests on the intractability of TPFP for random protocol instances. While related tropical problems are NP-hard, the precise complexity of TPFP remains open. No currently known tropical cryptanalytic technique extends directly to PTKE, and no efficient quantum attack is known. Experimental results confirm that PTKE is practical: a full key exchange takes under one second for the recommended parameters ($n = 64, d = 20$) and scales predictably to larger sizes.

The protocol integrates standard symmetric primitives, making it suitable for hybrid deployment. Future work includes average-case cryptanalysis of TPFP, the design of authenticated key exchange variants, investigation of alternative commuting families, and the construction of digital signature schemes based on the same Factorization problem.

Acknowledgements

The authors are grateful to the Department of Mathematics, Shri Vyankatesh Arts, Commerce and Science College, Deulgaon Raja, and the School of Mathematical Sciences, K.B.C. North Maharashtra University, Jalgaon, for providing the academic environment and computational facilities that supported this research.

The authors also thank the anonymous reviewers and editors for their valuable comments and suggestions, which helped improve the quality and presentation of this manuscript.

Declarations

Funding

The authors received no specific funding for this work.

Conflicts of Interest

The authors declare that they have no competing interests.

Availability of Data and Materials

No datasets were generated or analyzed during the current study. All experimental data reported in this paper were produced using the implementation developed by the authors.

Code Availability

The implementation used for the experimental evaluation is available from the corresponding author upon reasonable request.

Author Contributions

Sopan J. Chavhan conceived the protocol, carried out the theoretical analysis, implemented the algorithms, performed the experiments, and prepared the initial manuscript. Shrikant R. Chaudhari supervised the research, contributed to the mathematical development and security analysis, and reviewed and revised the manuscript. Both authors read and approved the final manuscript.

References

1. P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.
2. National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography Standardization." Available: https://csrc.nist.gov/projects/post-quantum-cryptography. Accessed: July 2026.
3. D. J. Bernstein, J. Buchmann, and E. Dahmen (Eds.), *Post-Quantum Cryptography*. Berlin, Heidelberg: Springer, 2009.
4. K. H. Kim and F. W. Roush, "Factorization of polynomials in one variable over the tropical semiring," *arXiv preprint* arXiv:math/0501167, 2005.

5. D. Grigoriev and V. Shpilrain, "Tropical cryptography," *Communications in Algebra*, vol. 42, no. 6, pp. 2624–2632, 2014.
6. M. Kotov and A. Ushakov, "Analysis of a key exchange protocol based on tropical matrix algebra," *Journal of Mathematical Cryptology*, vol. 12, no. 3, pp. 137–141, 2018.
7. D. Grigoriev and V. Shpilrain, "Tropical cryptography II: Extensions by homomorphisms," *Communications in Algebra*, vol. 47, no. 10, pp. 4224–4229, 2019.
8. D. Rudy and C. Monico, "Remarks on a tropical key exchange system," *Journal of Mathematical Cryptology*, vol. 15, no. 1, pp. 280–283, 2021.
9. S. Isaac and D. Kahrobaei, "A closer look at tropical cryptography," *International Journal of Computer Mathematics: Computer Systems Theory*, vol. 6, no. 2, pp. 137–142, 2021.
10. A. Muanalifah and S. Sergeev, "Modifying the tropical version of Stickel's key exchange protocol," *Applicable Mathematics*, vol. 65, pp. 727–753, 2020.
11. A. Muanalifah and S. Sergeev, "On the tropical discrete logarithm problem and security of a protocol based on tropical semidirect product," *Communications in Algebra*, vol. 50, no. 2, pp. 861–879, 2022.
12. E. Crockett, C. Paquin, and D. Stebila, "Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH," *IACR Cryptology ePrint Archive*, Report 2019/858, 2019.
13. D. Stebila, S. Fluhrer, and S. Gueron, "Design issues for hybrid key exchange in TLS 1.3," *IETF Internet-Draft*, 2019.
14. M. Durcheva, "Hybrid tropical-based protocol for post-quantum cryptography," *WSEAS Transactions on Mathematics*, vol. 23, pp. 58–68, 2026.
15. Y. Shitov, "The complexity of tropical matrix factorization," *Advances in Mathematics*, vol. 254, pp. 138–156, 2014.
16. H. Huang and C. Li, "Tropical cryptography based on multiple exponentiation problem of matrices," *Security and Communication Networks*, vol. 2022, Article ID 1024161, 2022.