A Hybrid Encryption Scheme Based on The Tropical Jones Matrix Multiple Exponentiation Problem

Weisha Kong, Huawei Huang, Changwen Peng, and Ting Xu.

ABSTRACT—At present, the public key cryptosystem is seriously threatened by the quantum computer. Therefore, in the post-quantum cryptography era, it is of great significance to study secure public key cryptography under quantum computing. This study introduces an Oracle-based assumption concerning multiple exponentiation, which is derived from the tropical Jones matrix problem. According to the assumption, a hybrid encryption scheme including symmetric encryption, message authentication code, and hash function is designed. In the standard model, the security of the scheme is proved; that is, the scheme has the indistinguishability under the chosen-ciphertext attack (IND-CCA). Unlike existing tropical cryptographic schemes, the scheme explicitly resists linear algebraic attacks, KU attacks, generalized KU attacks, and quantum attacks, making it a potential candidate for post-quantum cryptographic applications.

Index Terms—hybrid encryption; Jones matrix; public key cryptography; tropical algebra

I. INTRODUCTION

Diffie and Hellman first introduced the notion of public-key cryptography in their seminal work [1], marking a major advancement in its subsequent applications to securing networked systems. Public key cryptosystems, especially elliptic curve cryptography (ECC)[2], are widely used in Internet communication[3], digital signatures[4], cryptocurrency, and other fields due to their efficiency and security. The security of most schemes mainly depends on three kinds of mathematical problems: (1) integer factorization problem (IFP) [4]; (2) Discrete logarithm problem (DLP) [5]; (3) Elliptic curve discrete logarithm problem (ECDLP) [6]. However, the above problems are threatened by quantum computers. Shor proposed a quantum algorithm [7] to solve IFP and DLP in polynomial time. In addition, Proos and Zalka proposed a quantum algorithm [8] to solve ECDLP on F_q.

In 2014, Grigoriev and Shpilrain pioneered the application of tropical semirings in constructing key exchange protocols [9], demonstrating that solving systems of multivariate quadratic polynomial equations over such algebraic structures is NP-hard. Nevertheless, subsequent analysis revealed an inherent limitation: if the tropical matrix entries include negative values, each component rapidly converges to negative infinity as the exponentiation power grows. Due to this vulnerability, the protocol was compromised by a heuristic cryptanalysis method developed by Kotov and Ushakov in 2018 [10]. In order to resist KU-attack, In 2019, Grigoriev and Shpilrain developed an innovative key exchange mechanism [11] utilizing tropical matrix semidirect products. Nevertheless, Rudy and Monico [12] discovered that the exponentiation operation in tropical matrix semidirect products exhibits partial order-preserving properties, which enabled them to successfully compromise the scheme through an efficient binary search approach. Subsequent cryptanalysis by Isaac and Kahrobaei [13], followed by Muanalifah and Sergeev [14], demonstrated additional vulnerabilities in the protocol's construction, leading to successful security breaches. In 2020, Muanalifah and Sergeev introduced two kinds of new tropical exchange matrices (LP matrix and Jones matrix) and proposed three key exchange protocols [15] by using the bilateral action of matrices. In 2022, Huang and Li introduced a novel public-key cryptosystem [16] utilizing the algebraic action of two-side tropical circulant matrices. Also in 2022, Huang and Li developed a new key exchange mechanism [17] by leveraging the matrix multiple exponentiation problem, with security analysis demonstrating its resistance against existing cryptanalytic methods. In 2023, Ahmed et al. [18] proposed a new tropical structure and designed a new key exchange protocol based on this new tropical semiring. However, this protocol was successfully attacked by [19] and [20]. In 2024, Huang and Kong proposed a key exchange protocol [21] based on the Jones matrix multiple exponentiation problem and proved its security, indicating that it has the characteristics of anti-quantum computing.

In 2001, Abdalla et al. [22] proposed a hybrid encryption

Manuscript received November 24, 2024; revised June 12, 2025.

This work was supported in part by the National Natural Science Foundation of China (No.61462016), the Guizhou Provincial Basic Research Program (Natural Science) (No.QIANKEHEJICHU-MS[2025]281), the Natural Science Research Project of Guizhou Provincial Department of Education (No.[2023]010) and the Doctoral Research Start-up Project of Guiyang University (No. GYU-KY-[2025]).

Weisha Kong is a postgraduate student at School of Mathematical Sciences, Guizhou Normal University, Guiyang 550025, China (e-mail: 222100060199@gznu.edu.cn).

Huawei Huang is an associate professor of School of Mathematical Sciences, Guizhou Normal University and the Guizhou Provincial Specialized Key Laboratory of Information Security Technology in Higher Education Institutions, Guiyang 550025, China (Corresponding author, e-mail: 201307045@gznu.edu.cn).

Changwen Peng is a professor of School of Science, Guiyang University, Guiyang 550005, China (Corresponding author, e-mail: pengcw716@126.com).

Ting Xu is a postgraduate student at School of Mathematical Sciences, Guizhou Normal University, Guiyang 550025, China (e-mail: 222100060215@gznu.edu.cn).

scheme based on the Diffie-Hellman problem and proved that it achieves indistinguishability under chosen-ciphertext attack in the standard model. In 2010, Chen et al. proposed an identity-based encryption scheme [23] based on DHIES. The scheme employed a bilinear pairing of the secondary key combination structure. It only needed to perform a pair of calculations during the public key generation process and did not require a special hash function. The researchers formally established the scheme's security under selective identity-based chosen-ciphertext attacks (IND-sID-CCA) within the random oracle framework. Nevertheless, Susilo et al. [24] successfully employed the XL algorithm to cryptanalyze multivariate quadratic (MQ) problems under specific parameter configurations, thereby proving the vulnerability of Chen's construction against chosen-ciphertext attacks. In 2010, Pei et al. [25] introduced a novel public-key cryptosystem leveraging the properties of ergodic matrices. However, Gu et al. [26] employed the ergodic matrix property and the linearization method to prove that the security reduction of the public key encryption scheme is incorrect. In 2015, Huang [27] proved that the computational TEME problem is polynomial-time solvable and cracked the ciphertext of the cryptosystem based on the ergodic matrix. In 2024, based on the two-sided action problem of the tropical LP matrix, Pan et al. [28] proposed an Oracle two-sided tropical matrix action hypothesis designed a hybrid encryption scheme based on the hypothesis, and proved that the scheme has indistinguishability under the chosen-ciphertext attack in the standard model. Muanalifah and Sergeev [15] pointed out that there exists a generalized KU attack in the two-sided action problem of tropical matrices.

Our contribution: This work presents a novel public-key cryptosystem constructed from the Jones matrix multiple exponentiation problem. The proposed framework combines symmetric encryption primitives, message authentication codes, and cryptographic hash functions, with a formal security proof demonstrating IND-CCA2 security in the standard model. Compared to previous schemes, the scheme proposed in this paper can resist linear algebraic attacks, KU attacks, generalized KU attacks, and quantum attacks.

The structure of this paper is organized as follows. Section 2 provides the necessary mathematical preliminaries and background concepts. Section 3 details our proposed public-key encryption scheme based on the Jones matrix multiple exponentiation (ME) problem. The security analysis and formal proofs are presented in Section 4. Finally, Section 5 concludes the paper with a summary of our contributions and findings.

II. Preliminaries

We represent the set $\{1,2,\cdots,n\}$ as $[n]$.

To facilitate understanding of the subsequent content, we have provided some foundational concepts.

Definition 2.1 ([29] (Semiring))**.** A semiring is a triple $(\Re,+,\cdot)$ where $\Re$ is a non-empty set equipped with two binary operations $+$ (addition) and $\cdot$ (multiplication) satisfying the following axioms:

(1) It forms a commutative monoid concerning addition, having a zero-element denoted as 0;

(2) It forms a monoid concerning multiplication, having an identity element 1 and $1\neq 0$;

(3) $(\forall a,b,c\in\Re)a\cdot(b+c)=a\cdot b+a\cdot c;(a+b)\cdot c=a\cdot c+b\cdot c$.

Definition 2.2 ([30] (Tropical Semiring))**.** Let $S=\mathbb{Z}\cup\{-\infty\}$. Define two operations $\oplus$ and $\otimes$ as follows:

$$x\oplus y=\max\{x,y\},x\otimes y=x+y$$

$-\infty$ and 0 satisfied the following equations:

$$x\oplus(-\infty)=x,x\otimes 0=x,\forall x\in\mathbb{Z}$$

The algebraic structure $(S,\oplus,\otimes)$ forms a commutative semiring where the additive neutral element is $-\infty$ and the multiplicative neutral element is 0. This structure is referred to as the integer tropical semiring.

Definition 2.3 ([31] Tropical Matrix)**.** Denote by $\mathbb{M}_k(S)$ the collection of all square matrices of dimension $k\times k$ with entries from the set S. We define binary operation $\oplus$ and $\otimes$ on $\mathbb{M}_k(S)$:

Denote $A=[a_{ij}],B=[b_{ij}]$, then

$$A\oplus B=[a_{ij}]\oplus[b_{ij}]=[a_{ij}\oplus b_{ij}]$$

$$A\otimes B=[a_{ij}]\otimes[b_{ij}]=[a_{i1}\otimes b_{1j}\oplus a_{i2}\otimes b_{2j}\oplus\cdots\oplus a_{ik}\otimes b_{kj}]$$

Example 2.1. Let $A=\begin{bmatrix}1&2\\2&3\end{bmatrix},B=\begin{bmatrix}2&5\\4&6\end{bmatrix}$, we have

$$A\oplus B=\begin{bmatrix}1&2\\2&3\end{bmatrix}\oplus\begin{bmatrix}2&5\\4&6\end{bmatrix}=\begin{bmatrix}2&5\\4&6\end{bmatrix},$$

$$A\otimes B=\begin{bmatrix}1&2\\2&3\end{bmatrix}\otimes\begin{bmatrix}2&5\\4&6\end{bmatrix}=\begin{bmatrix}6&8\\7&9\end{bmatrix}.$$

A. Jones Matrix

To facilitate understanding of the encryption scheme we propose in the future, we examine a particular class of matrices originally introduced by Jones [32] in his foundational work.

Definition 2.4 ([15] (Jones Matrix))**.** Consider an $n\times n$ tropical matrix $A=[a_{ij}]$. If A satisfies the inequality:

$$a_{ij}\otimes a_{jk}\leq a_{ik}\otimes a_{jj},\forall i,j,k\in[n],$$

then A is termed a Jones matrix.

Definition 2.5 ([15] (Deformation)**.** Given a Jones matrix $A=[a_{ij}]$ and a real number $\alpha\in\mathbb{R}$, we define the α-deformation of A as the matrix $A^{(\alpha)}=\left(a_{ij}^{(\alpha)}\right)$, where each entry is given by

$$a_{ij}^{(\alpha)}=a_{ij}\otimes\left(a_{ii}\oplus a_{jj}\right)^{\otimes(\alpha-1)}.$$

The deformation of the Jones matrix satisfies the commutative law of multiplication under specific conditions, and we have the following theorem:

Theorem 2.1 ([15])**.** For any Jones matrix A and real parameter $\alpha\leq 1$, the α-deformation $A^{(\alpha)}$ preserves the Jones matrix property.

Theorem 2.2 ([15])**.** For any Jones matrix $A\in\mathbb{M}_k(S)$ and parameters $\alpha,\beta\in[0,1]$, the deformed matrices satisfy the commutativity relation:

$$A^{(\alpha)}\otimes A^{(\beta)}=A^{(\beta)}\otimes A^{(\alpha)}.$$

Building upon the preceding results, we now introduce the

notion of a quasi-polynomial as follows.

Definition 2.6 ([15] (Quasi-polynomial))**.** Let $N \in \mathbb{M}_k(S)$ be a Jones matrix. We say a matrix B is a quasi-polynomial of N if it can be expressed as

$$B = \bigoplus_{\alpha \in M} a_\alpha \otimes N^{(\alpha)}$$

where M is a finite set of rational numbers in the interval [0,1] and each $a_\alpha \in S$. The collection of all such quasi-polynomials of N forms the set denoted by $S\left[N^{(\alpha)}\right]$.

B. Multiple Exponentiation Problem of Tropical Jones Matrices

Before defining the ME problem, let's first introduce a new semigroup action.

Consider a non-negative integer circulant matrix A, a Jones matrix $N \in \mathbb{M}_k(S)$, and a vector

$$\vec{H} = (H_1, H_2, \cdots, H_n) \in \left(S\left[N^{(\alpha)}\right]\right)^n .$$

We now examine the action of the multiplicative semigroup $C_n(\mathbb{Z}^+)$ on the Cartesian product $\left(S\left[N^{(\alpha)}\right]\right)^n$, defined component-wise as follows:

$$\vec{H}^A = \left(\bigotimes_{i=1}^{n} H_i^{a_{1i}}, \bigotimes_{i=1}^{n} H_i^{a_{2i}}, \cdots, \bigotimes_{i=1}^{n} H_i^{a_{ni}}\right),$$

where each component H $H_i^{a_{ji}}$ represents the a_{ji} -fold tropical product $H_i \otimes H_i \otimes \cdots \otimes H_i$. This construction yields a well-defined semigroup action of $C_n(\mathbb{Z}^+)$ on $\left(S\left[N^{(\alpha)}\right]\right)^n$.

Definition 2.7 ([17] (ME problem))**.** Given a Jones matrix $N \in \mathbb{M}_k(S)$ and a vector

$$\vec{H} = (H_1, H_2, \cdots, H_n) \in \left(S\left[N^{(\alpha)}\right]\right)^n$$

where $\vec{U} = \vec{H}^A$ for some unknown circulant matrix $A \in C_n(\mathbb{Z}^+)$, the "Multiple Exponentiation Problem" (ME Problem) consists of finding such a matrix A given only $\vec{H}$ and $\vec{U}$. Here, the underlying Jones matrix N is not known a priori.

Proposition 2.1 ([17])**.** When there exists a component H_i in the vector $\vec{H}$ such that all other components satisfy $H_j \in \langle H_i \rangle$ for $j \neq i$ (where $i, j \in [n]$), the Multiple Exponentiation Problem reduces to the Discrete Logarithm Problem in polynomial time.

Based on the ME problem, we can construct a one-way function $f(A)$ of the Jones matrix.

Definition 2.8 (One-way Function)**.** Let $A \in C_n(\mathbb{Z}^+)$ be a circulant matrix, $\vec{H} = (H_1, H_2, \cdots, H_n) \in \left(S\left[N^{(\alpha)}\right]\right)^n$, define the one-way function $f(A)$ as follows:

$$f(A) = \vec{H}^A .$$

C. Hybrid Encryption Scheme and Its Security Definition

We define the following cryptographic spaces:

Message space: $Message = \{0,1\}^*$,

Ciphertext space: $Ciphertext = \{0,1\}^*$,

Randomness space: $\{0,1\}^\infty$ (denoting infinite binary strings),

Public key space: $PK \subseteq \{0,1\}^*$,

Secret key space: $SK \subseteq \{0,1\}^*$.

The hybrid encryption algorithm consists of three algorithms, $ASYM = (\overline{E}, \overline{D}, \overline{K})$, where $\overline{K}$ is the key generation algorithm, which takes a coins $r \in Coins$ as input and outputs a key pair $(pk, sk) \in PK \times SK$; Algorithm $\overline{E}$ is the encryption algorithm, which takes a public key $pk \in PK$, plaintext x , a coins $r \in Coins$ as input, and outputs ciphertext $y = \overline{E}(pk, x, r)$; Algorithm $\overline{D}$ is the decryption that takes in the private key $sk \in SK$, ciphertext $y \in Ciphertext$, and outputs plaintext $\overline{D}(sk, y) \cup \{BAD\}$. The BAD indicates that the ciphertext is invalid, that is, it is not the encryption result of any plaintext.

The public key encryption schemes adhere to the IND-CCA security criterion, which ensures ciphertext indistinguishability during chosen-ciphertext attacks in the find-then-predict experimental framework.

Definition 2.9 ([33])**.** Let $ASYM = (\overline{E}, \overline{D}, \overline{K})$ be a public key encryption scheme and A be an adversary. Consider the following experimental process:

Experiment		$Exp^{ind-cca-fg}_{ASYM,A}$
(pk, sk)	$\leftarrow$	$\overline{K}$
(x_0, x_1, s)	$\leftarrow$	$A^{\overline{D}_{sk}}(find, pk)$
b	$\overset{R}{\leftarrow}$	$\{0,1\}$
y	$\leftarrow$	$\overline{E}_{pk}(x_b)$
$\tilde{b}$	$\leftarrow$	$A^{\overline{D}_{sk}}(guess, pk, y, s)$
if $\tilde{b} = b$		
then return 1		
else		
return 0		

Now define the $ind-cca-advantage$ of A in the find-and-guess notion as follows:

$$Adv^{ind-cca-fg}_{ASYM,A} = 2\Pr[Exp^{ind-cca-fg}_{ASYM,A} = 1] - 1$$

For any t, c , we define the $ind-cpa-advantage$ of $ASYM$ as

$$Adv^{ind-cpa-fg}_{ASYM,A}(t, c) = \max_A \left\{Adv^{ind-cpa-fg}_{ASYM,A}\right\},$$

where the maximum is over all A with time-complexity t , making to the decryption oracle at most q queries the sum of whose lengths is at most c bits

III. Hybrid Key Encryption Scheme for Jones Matrix ME Problem

In this section, based on the ME problem of Jones matrix, we construct a new hybrid key encryption scheme using message authentication code and hash function.

A. Encryption Component

(1) *Message Authentication Code*

Consider a message space denoted as $Message=\{0,1\}^*$, a key space $mKey=\{0,1\}^{mLen}$, and a tag space $Tag=\{0,1\}^{tLen}$. A message authentication code consists of two polynomial-time algorithms $MAC=(\tau,\nu)$, where:

The tagging algorithm τ takes as input a secret key $k\in mKey$ and a message $x\in Message$, producing an authentication tag $\tau(k,x)$.

The verification algorithm ν accepts a key $k\in mKey$, a message $x\in Message$, and a tag $\iota\in Tag$, then outputs a bit $b=\upsilon(k,x,t)\in\{0,1\}$, where b = 1 indicates acceptance and b = 0 denotes rejection.

For correctness, it is required that for all $k\in mKey$ and $x\in Message$, $\nu(k,x,\tau(k,x))=1$ must hold. We now formalize the security notion for message authentication codes.

The security of MAC means that it has strong existential unforgeability under chosen message attack (*suf-cma*). Now we consider an experiment. First, a random key $k\in mKey$ is determined, which is confidential to the adversary, but the adversary can access the verification code to generate a random oracle $\tau_k(\cdot)$ and an authentication oracle $v_k(\cdot)$. Finally, adversary A can output a valid message-tag pair (x^*,ι^*), and does not use the algorithm $\tau_k(\cdot)$ to get x^*, then the message can be said to be successfully forged by the adversary.

Definition 3.1 ([22])**.** Let A be an adversary and MAC be a message authentication scheme. Consider the following experiment:

Experiment $Exp^{suf-cma}_{MAC,A}$

$k \xleftarrow{R} mKey$

$(x^*,t^*) \leftarrow A^{\tau_k(\cdot),\upsilon_k(\cdot,\cdot)}$

if $\upsilon_k(x^*,t^*)=1$, *and* ι^* *was never return by* t^* *in response to query* x^*
  return 1
else
  return 0

Now define the advantage of the adversary's unforgeability under chosen message attack ($suf-cma-advantage$) is defined as

$$Adv^{suf-cma}_{MAC,A}=\Pr\left[Exp^{suf-cma}_{MAC,A}=1\right],$$

for any $t,q_t,\mu_t,q_\upsilon,\mu_\upsilon$, we can define the $suf-cma-advantage$ of MAC as

$$Adv^{suf-cma}_{MAC}(t,q_t,\mu_t,q_\upsilon,\mu_\upsilon)=\max_A\left\{Adv^{suf-cma}_{MAC,A}\right\},$$

here the maximum refers to the maximum of the advantage of such adversary A, t represents the time-complexity of this attack. Adversary A performs up to q_t queries on the verification code generation oracle, and the sum of the length of the query result is up to μ_t bits. Adversary A performs up to q_υ queries on the verification oracle, and the sum of the length of the query result is up to μ_υ bits.

(2) *Symmetric Encryption*

A symmetric encryption scheme consists of two algorithms, denoted as $SYM=(\overline{E},\overline{D})$. The encryption algorithm $\overline{E}$ takes as input a secret key $k\in eKey$, a plaintext $x\in Message$, and randomness $r\in Coins$, producing a ciphertext $\overline{E}(k,x,r)$. The decryption algorithm $\overline{D}$ accepts a key $k\in eKey$ and a ciphertext $y\in Ciphertext$, and outputs either a plaintext $x'\in Message$ or a special symbol BAD, indicating that the ciphertext is invalid.

The security of symmetric encryption can be characterized by indistinguishability against chosen-plaintext attacks in a find-then-guess framework ($ind-cpa-fg$). To formally define this security notion, we model the adversary's capabilities through a two-phase challenge experiment consisting of a query stage followed by a guessing stage.

Definition 3.2 ([22])**.** Consider a symmetric encryption scheme $SYM=(\overline{E},\overline{D})$ and a probabilistic polynomial-time adversary A. The security experiment proceeds as follows:

Experiment $Exp^{ind-cpa-fg}_{SYM,A}$

$k \xleftarrow{R} eKey$

$(x_0,x_1,s) \leftarrow A^{\overline{E}(k,\cdot)}(find)$

$b \xleftarrow{R} \{0,1\}$

$y \leftarrow \overline{E}(k,x_b)$

$\tilde{b} \leftarrow A^{\overline{E}(k,\cdot)}(guess,y,s)$

if $\tilde{b}=b$
  then return 1
else
  return 0

The $ind-cpa-advantage$ of an adversary A against the symmetric encryption scheme SYMSYM is formally defined as:

$$Adv^{ind-cpa-fg}_{SYM,A}=2\Pr\left[Exp^{ind-cpa-fg}_{SYM,A}=1\right]-1.$$

The $ind-cpa-advantage$ of the symmetric encryption scheme SYM is defined for any adversarial constraints t,q and μ as:

$$Adv^{ind-cpa-fg}_{SYM}(t,q,\mu)=\max_A\left\{Adv^{ind-cpa-fg}_{SYM,A}\right\},$$

where the maximum is over all A with time-complexity of t, making to the encryption oracle at most q queries the sum of whose lengths is at most μ bits.

(3) *Hash Function*

Let $H:M^S_{n\times n}\to\{0,1\}^{hLen}$ (that $hLen$ is a natural number) be a Hash function that can transform a tropical matrix vector into a binary bit string.

In order to ensure that the public key encryption scheme based on Jones matrix is indistinguishability under chosen-ciphertext attack, H should satisfy the following assumption of Oracle multiple exponentiation based on Jones matrix.

Definition 3.3 ([22])**.** Let A be an adversary, S is a tropical matrix semiring, $hLen$ be a number, and

$H:\{0,1\}^{*}\to\{0,1\}^{hLen}$. Now consider the following two experiments:

Experiment $Exp_{S,H,A}^{odh-real}$

$V \leftarrow f(A)=\overline{H}^{A}$

$U \leftarrow f(B)=\overline{H}^{B}$

$w \leftarrow H(f(BA))=H\left(\left(\overline{H}^{B}\right)^{A}\right)$

$\mathrm{H}_{V}(Z)=H\left(f_{Z}(V)\right)$ $(oracle)$

$b \leftarrow A^{H_{V}(\cdot)}(U,V,W)$

return b

Experiment $Exp_{S,H,A}^{odh-rand}$

$V \leftarrow f(A)=\overline{H}^{A}$

$U \leftarrow f(B)=\overline{H}^{B}$

$w \xleftarrow{R} (0,1)^{hLen}$

$\mathrm{H}_{V}(Z)=H\left(f_{Z}(V)\right)$ $(oracle)$

$b \leftarrow A^{H_{V}(\cdot)}(U,V,W)$

return b

In the above experiments, if the index of W is the product of the index of U and V, then the final return value of b is 1, otherwise it returns 0. Please note that here, the adversary can access the oracle but cannot directly query the value of $\overline{H}^{A}$ or $\overline{H}^{B}$ in the oracle.

Now, define the advantage of the adversary A for the Jones matrix of the Oracle multiple exponentiation problem as follows:

$$Adv_{S,H,A}^{odh}=\Pr\left[Exp_{S,H,A}^{odh-real}=1\right]-\Pr\left[Exp_{S,H,A}^{odh-rand}=1\right].$$

B. Hybrid Encryption Scheme Based on Jones Matrix Multiple exponentiation Problem

Consider a symmetric encryption scheme denoted as $SYM=(\overline{E},\overline{D})$, where the key length is $eLen$. Additionally, let $MAC=(\tau,\nu)$ represent a message authentication code with a key length of $mLen$. Furthermore, suppose there exists a hash function $H:M_{n\times n}^{S}\to\{0,1\}^{mLen+eLen}$ capable of converting a tropical matrix vector into a binary string of fixed length.

Consider a Jones matrix-based hybrid encryption scheme denoted as $JMPES=(\overline{E},\overline{D},\overline{K})$. This scheme comprises three components: a key generation algorithm $\overline{K}$, an encryption procedure $\overline{E}$, and a decryption mechanism $\overline{D}$.

Key generation algorithm $\overline{K}$:

Algorithm $\overline{K}$
Begin
$A \leftarrow C_{n}(\mathbb{Z}^{+})$
$pk \leftarrow \overline{H}^{A}$
$sk \leftarrow A$
return (pk,sk)
End

Encryption algorithm $\overline{E}$:

Algorithm $\overline{E}$:
Begin
$B \leftarrow C_{n}(\mathbb{Z}^{+})$
$Z \leftarrow f_{pk}(B)=\overline{H}^{AB}$
$U \leftarrow \overline{H}^{B}$
$h \leftarrow H(Z)$
$mKey \leftarrow h\{1,\cdots,mLen\}$
$eKey \leftarrow h\{mLen+1,\cdots,mLen+eLen\}$
$eM \leftarrow \overline{E}(eKey,x)$
$t \leftarrow \tau(mKey,eM)$
$y \leftarrow U\|eM\|t$
return y
End

Decryption algorithm $\overline{D}$:

Algorithm $\overline{D}(sk=A,y)$
Begin
$U\|eM\|t \leftarrow y$
$Z \leftarrow f_{U}(sk)=\overline{H}^{BA}$
$h \leftarrow H(Z)$
$mKey \leftarrow h\{1,\cdots,mLen\}$
$eKey \leftarrow h\{mLen+1,\cdots,mLen+eLen\}$
if $\upsilon(mKey,eM,t)=0$
then return *BAD*
$x \leftarrow \overline{D}(eKey,eM)$
return x
End

The algorithm flowchart of the hybrid encryption scheme is described in Figure 1.

IV. Security Analysis and Efficiency Analysis

A. Security analysis

This section presents a security analysis of the aforementioned hybrid encryption scheme against chosen-ciphertext attacks. Following the demonstration approach outlined in [22], we establish the subsequent theorem.

Theorem 4.1. Consider three cryptographic components: *SYM* as a symmetric encryption mechanism, *MAC* as an authentication protocol, and *JMPES* as a Jones matrix-derived public key cryptosystem. For any t,q,μ,c, the advantage of adversary A in the chosen-ciphertext attack is

$$Adv_{JMPES}^{ind-cca-fg}(t,q,\mu,c)\le Adv_{SYM}^{ind-cpa-fg}(t,0,0)+2Adv_{S,H}^{odh}(t,q)+2Adv_{MAC}^{suf-cma}(t,1,c,q,\mu),$$

where t denotes the running time of the adversary, c is an infinite string, and the oracle algorithm performs at most q decryption queries, and the sum of the lengths of the query results is at most μ bits.

Proof Sketch. We begin by assuming the security of both the

symmetric encryption scheme SYM and the message authentication scheme MAC. Furthermore, the function is postulated to satisfy the Jones matrix-based Oracle multiple exponentiation hypothesis. Let $y = U \| eM \| t$ be the challenge ciphertext. The ciphertext of the adversary A 's guessing phase can be divided into the two following forms. We call a *Type*1 query a ciphertext of the form $U \| eM \| t$. A *Type*2 query has the form $\tilde{y} = \bar{U} \| eM \| t$ with $\bar{U} \neq U$.

Suppose that *SOMEVALID* denotes the event that adversary A performs a *Type*1 query $\tilde{y}$ in Experiment $Exp_{JMPES,A}^{ind-cca-fg}$ such that $\tilde{D}_{sk}(\tilde{y}) \neq BAD$. Let $\overline{SOMEVALID}$ denote the event where there is no *Type*1 query $\tilde{y}$ such that $\tilde{D}_{sk}(\tilde{y}) \neq BAD$ in the experiment $Exp_{JMPES,A}^{ind-cca-fg}$. According to reference [22], we have the following three claims.

Claim 1. $\Pr\left[Exp_{S,H,A}^{odh-real} = 1\right] = \frac{1}{2} + \frac{Adv_{JMPES,A}^{ind-cca-fg}}{2}$.

Claim 2.

$$\Pr\left[Exp_{S,H,A}^{odh-rand} = 1 \wedge \overline{SOMEVALID}\right] \leq \frac{1}{2} + \frac{Adv_{SYM}^{ind-cpa-fg}(t,0,0)}{2}.$$

Claim 3.

$$\Pr\left[Exp_{S,H,A}^{odh-rand} = 1 \wedge \overline{SOMEVALID}\right] \leq Adv_{MAC}^{suf-cma}(t,1,c,q,\mu).$$

From definition 8 and claims 1, 2, and 3, we have

$$\begin{aligned} Adv_{S,H,A}^{odh} &\geq \frac{1}{2} + \frac{Adv_{JMPES,A}^{ind-cca-fg}}{2} - \frac{1}{2} - \frac{Adv_{SYM}^{ind-cpa-fg}(t,0,0)}{2} \\ &\quad - Adv_{MAC}^{suf-cma}(t,1,c,q,\mu) \\ &= \frac{Adv_{JMPES,A}^{ind-cca-fg}}{2} - \frac{Adv_{SYM}^{ind-cpa-fg}(t,0,0)}{2} - Adv_{MAC}^{suf-cma}(t,1,c,q,\mu) \end{aligned},$$

whence

$$\begin{aligned} Adv_{JMPES,A}^{ind-cca-fg} &\leq Adv_{SYM}^{ind-cpa-fg}(t,0,0) + 2Adv_{S,H,A}^{odh} \\ &\quad + 2\,Adv_{MAC}^{suf-cma}(t,1,c,q,\mu). \end{aligned}$$

Since the time-complexity of the adversary A is at most t , and most q queries to its oracle H_{υ} , we have the inequality: $Adv_{S,H,A}^{odh} \leq Adv_{S,H}^{odh}(t,q)$. Thus, we rewrite the above conclusion:

$$\begin{aligned} Adv_{JMPES,A}^{ind-cca-fg} &\leq Adv_{SYM}^{ind-cpa-fg}(t,0,0) + 2Adv_{S,H}^{odh}(t,q) \\ &\quad + 2\,Adv_{MAC}^{suf-cma}(t,1,c,q,\mu). \end{aligned}$$

This is the advantage of the Jones matrix multiple exponentiation problem public key encryption scheme under a chosen-ciphertext attack.

By definition 2.9, the above process proves that our proposed scheme has indistinguishability under chosen-ciphertext attack (IND-CCA).

Breaking the private key problem of the above proposed public key encryption scheme is actually to solve the tropical Jones matrix multiple exponentiation problem. References [17] and [21] have proved the difficulty of solving this problem. Therefore, it is not feasible to solve for the private key in the scheme given the public key in our proposed scheme. Compared with the general Jones matrix encryption scheme, this scheme adds a secure message authentication code *MAC* and a hash function H that satisfies the Oracle multiple exponentiation assumption. Therefore, the security of this scheme is due to other general encryption schemes.

Table 1 provides a comparison of our scheme with other relevant schemes in terms of resisting chosen-ciphertext attack.

B. Efficiency analysis

We next examine the computational complexity of the proposed hybrid encryption system. Let $A \in C_n(\mathbb{Z}^+)$ represent a circulant matrix with entries $a_0, a_1, \cdots, a_{n-1}$ bounded within [0, *s*-1]. The protocol's dominant computational cost arises from the matrix power computation $\overline{H}^A$. Execution times for $\overline{H}^A$ under different parameter configurations are presented in Table 2, while Table 3 evaluates the scheme's efficiency when processing messages of varying lengths.

Compared with other encryption schemes based on tropical algebra or traditional mathematical problems, our scheme performs well in terms of efficiency while resisting various attacks (such as linear algebra attack, KU attack, generalized KU attack, and quantum attack). Although the computational complexity is affected by the matrix size and message length, in practical applications, appropriate parameters can be selected according to specific requirements to balance security and efficiency. For example, in scenarios with extremely high security requirements and sufficient computing resources, a larger matrix order can be adopted; in scenarios with higher efficiency requirements and relatively lower security requirements, the matrix order can be appropriately reduced.

V. CONCLUSION

In this paper, we introduce a novel hybrid encryption scheme based on the tropical Jones matrix multiple exponentiation problem, leveraging the security of this problem to construct a post-quantum cryptographic primitive. Our scheme integrates symmetric encryption, message authentication codes (MAC), and cryptographic hash functions, ensuring security in the standard model. We rigorously prove that the proposed scheme achieves indistinguishability under chosen-ciphertext attack (IND-CCA), a fundamental security requirement for modern encryption. Compared with previous tropical algebra-based cryptographic schemes, our work makes the following key contributions:

(1) Novel Hard Problem Construction: We introduce and formalize the tropical Jones matrix multiple exponentiation problem, demonstrating its computational hardness and its applicability to public key encryption.

(2) Enhanced Security Properties: Unlike existing tropical cryptographic schemes, our construction explicitly resists linear algebraic attacks, KU attacks, generalized KU attacks, and quantum attacks, making it a potential candidate for post-quantum cryptographic applications.

(3) Enhanced Security Properties: Unlike existing tropical cryptographic schemes, our construction explicitly resists linear algebraic attacks, KU attacks, generalized KU attacks, and quantum attacks, making it a potential candidate for post-quantum cryptographic applications.

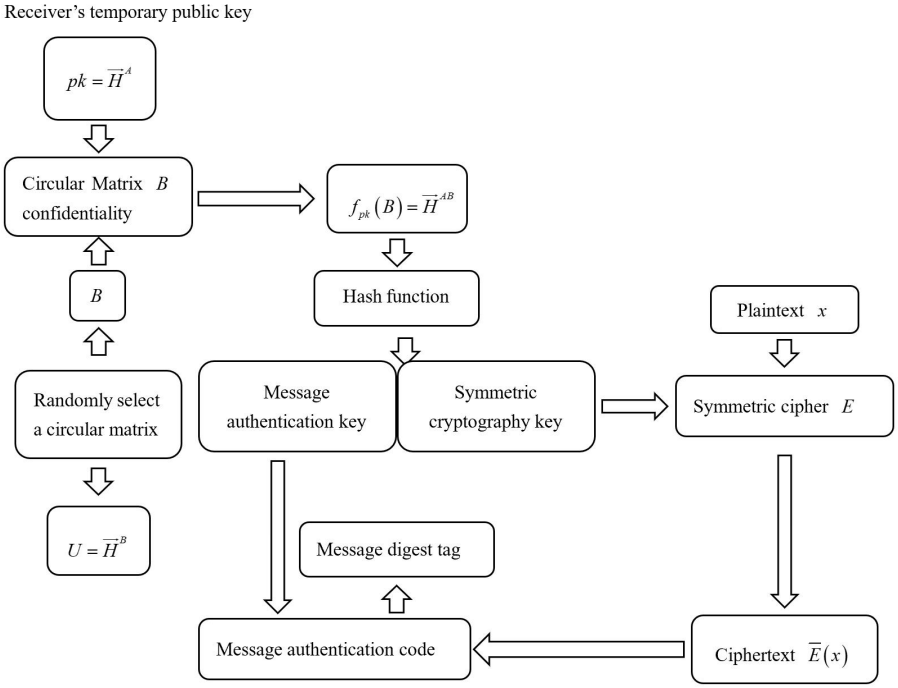

Fig 1. Scheme Flowchart.

TABLE I
COMPARISON AMONG RELEVANT ENCRYPTION SCHEMES

Scheme	Mathematical Problems	Chosen-Ciphertext Attack	Linear Algebraic Attack	KU Attack	Generalized KU Attack	Quantum Attack
Abdalla[22]	Diffie-Hellman problem	√	√	√	√	×
Chen[23]	Diffie-Hellman problem	√	√	√	√	×
Pei[25]	Two-side Ergodic Matrices Exponentiation problem	√	×	√	√	×
Pan[28]	Two-sided matrix action problem	√	√	√	×	×
Our scheme	Jones matrix multiple exponentiation problem	√	√	√	√	√

√ means that the scheme can resist the corresponding attack, while × does not.

TABLE 2
PERFORMANCE COMPARISON UNDER SOME PARAMETERS

k	n	s	Timing of $\overrightarrow{H}^A$ (s)
10	80	2	1.085
15	50	3	1.930
20	40	4	2.379
25	40	5	5.609
28	35	6	5.690

TABLE 3
PERFORMANCE COMPARISON UNDER DIFFERENT MESSAGE LENGTHS

Message lengths (bit)	Average encryption time (s)	Average decryption time (s)	Average key generation time (s)	Size of the key space (bit)	Size of the ciphertext space (bit)
128	1.350	1.283	1.243	128	256
256	1.520	1.427	1.243	128	384
512	1.987	1.756	1.243	128	640
1024	2.165	2.142	1.243	128	1152

(4) Rigorous Security Proofs: We establish the IND-CCA security of our scheme in the standard model, relying on the Oracle multiple exponentiation assumption rather than heuristic security arguments.

Future work could focus on optimizing the proposed scheme and exploring its integration into broader cryptographic frameworks, such as digital signatures or secure multi-party computation. Additionally, further investigation into the computational hardness of the tropical Jones matrix multiple exponentiation problem could strengthen its theoretical foundation and practical applicability.

REFERENCES

[1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, 1976.

[2] M. S. Khan and D. S. Sakkari, "Security and performance analysis of elliptic curve crypto system using bitcoin curves," *IAENG International Journal of Computer Science*, vol. 50, no. 2, pp. 745-758, 2023.

[3] Z. Elhadari, H. Zougagh, N. Idboufker et al., "Survey on the adoption of blockchain technology in internet of things environments: Techniques, challenges and future research directions," *IAENG International Journal of Computer Science*, vol. 52, no. 1, pp. 59-89, 2025.

[4] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978.

[5] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions.on Information Theory*, vol. 31, no. 4, pp. 469-472, 1985.

[6] N. Morteza, M. R. Bonyadi, M. Ehsan et al., "A protocol for digital signature based on the elliptic curve discrete logarithm problem," *Journal of Applied Sciences*, vol. 8, no. 10, pp. 1919-1925, 2008.

[7] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 41, pp. 303-332, 1999.

[8] J. Proos and C. Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves," *arXiv preprint quant-ph/0301141*, 2003.

[9] D. Grigoriev and V. Shpilrain, "Tropical cryptography," *Communications in Algebra*, vol. 42, no. 6, pp. 2624-2632, 2014.

[10] M. Kotov and A. Ushakov, " Analysis of a key exchange protocol based on tropical matrix algebra," *Journal of the American College of Surgeons*, vol. 207, no. 3, pp. S56-S57, 2018.

[11] D. Grigoriev and V. Shpilrain, "Tropical cryptography II: Extensions by homomorphisms," *Communications in Algebra*, vol. 47, no. 10, pp. 4224-4229, 2019.

[12] D. Rudy and C. Monico, "Remarks on a tropical key exchange system," *Journal of Mathematical Cryptology*, vol. 15, no. 1, pp. 280-283, 2021.

[13] S. Isaac and D. Kahrobaei, "A closer look at the tropical cryptography," *International Journal of Computer Mathematics*: Computer Systems Theory, vol. 6, no. 2, pp. 137-142, 2021.

[14] 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, 2021.

[15] A. Muanalifah and S. Sergeev, "Modifying the tropical version of Stickel's key exchange protocol," *Applications of Mathematics*, vol. 65, no. 6, pp. 727-753, 2020.

[16] H. Huang, C. Li, and L. Deng, "Public-key cryptography based on tropical circular matrices," *Applied Sciences*, vol. 12, no. 15, p. 7401, 2022.

[17] H. Huang and C. Li, "Tropical cryptography based on multiple exponentiation problem of matrices," *Security and Communication Networks*, pp. 1-9, 2022.

[18] K. Ahmed, S. Pal, and R. Mohan, "Key exchange protocol based upon a modified tropical structure," *Communications in Algebra*, vol. 51, no. 1, pp. 214-223, 202.

[19] H. Huang, C. Peng, and L. Deng, "Cryptanalysis of a key exchange protocol based on a modified tropical structure," *Designs, Codes and Cryptography*, vol. 92, no. 11, pp. 3843-3858, 2024.

[20] S. Alhussaini, C. Collett, and S. Sergeev, "On the tropical two-sided discrete logarithm and a key exchange protocol based on the tropical algebra of pairs," *Communications in Algebra*, vol. 1, no. 24, 2024.

[21] H. Huang, W. Kong, and T. Xu, "Asymmetric cryptography based on the tropical Jones matrix," *Symmetry*, vol. 16, no. 4, p. 456, 2024.

[22] M. Abdalla, M. Bellare, and P. Rogaway, "DHAES: An encryption scheme based on the Diffie-Hellman problem," *IACR Cryptology ePrint Archive*, pp. 143-158, 2001.

[23] Y. Chen, M. Charlemagne, Z. Guan et al., "Identity-based encryption based on DHIES," *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, pp. 82-88, 2010.

[24] W. Susilo and J. Baek, "On the security of the identity-based encryption based on DHIES from ASIACCS 2010," *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, pp. 376-380, 2011.

[25] H. Pei, Y. Zhao, and H. Zhao, "Security of the cryptosystems based on ergodic matrices," *Journal of Electronics*, vol. 38, no. 8, pp. 1908-1913, 2010.

[26] C. Gu, Z. Jing, and Z. Yu, "Security on public key encryption scheme based on ergodic matrices," *Journal of Electronics*, vol. 42, no. 10, pp. 2081-2085, 2014.

[27] H. Huang, C. Peng, and Y. Qu, "Security of the cryptosystems based on ergodic matrices," *Journal on Communications*, vol. 8, 2015.

[28] G. Pan, H. Huang, and X. Jiang, "A hybrid encryption scheme based on the bilateral interaction problem of tropical LP matrix," *Journal of Jiaying*, vol. 42, no. 3, pp. 1-8, 2024.

[29] J. S. Golan, *Semirings and their Applications*. Springer Science & Business Media, 2013.

[30] D. Speyer and B. Sturmfels, "Tropical mathematics," *Mathematics Magazine*, vol. 82, no. 3, pp. 163-173, 2009.

[31] H. Huang, "Cryptosystems based on tropical congruent transformation of symmetric matrices," *Symmetry*, vol. 14, no. 11, p. 2378, 2022.

[32] D. L. Jones, *Special and Structured Matrices in Max-Plus Algebra.* Doctoral dissertation, University of Birmingham, 2017.

[33] S. Micali, C. Rackoff, and B. Sloan, "The notion of security for probabilistic cryptosystems," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 412-426, 1988.