International Journal for Housing Science and Its Applications
Publish August 6, 2025. Volume 46, Issue 3 Pages 6327-6338

https://doi.org/10.70517/ijhsa463543

Security Analysis and Algorithm Design of Chameleon Signature Scheme Based on Lattice Cryptography under Quantum Attacks

Guoren Xiong[1] and Daofeng Li[1,*]
[1] Computer and Electronics Information School of Guangxi University, Nanning, Guangxi, 530004, China
Corresponding authors: (e-mail: xgren0717@163.com).

Abstract With the rapid development of quantum computers, traditional cryptographic algorithms face serious threats from quantum attacks. In this paper, we design a chameleon signature scheme that can resist quantum computer attacks and analyze its security in detail. The study adopts the idea of lattice-based cryptography to construct a novel chameleon signature scheme and proves the security of the scheme under the random predicate machine model. The innovation of the scheme is that by constructing identity-based chameleon signatures, it is able to withstand quantum computing attacks while maintaining its efficiency. Experimental results show that the scheme is computationally efficient when performing key generation, signature generation and verification. Specifically, under the simulation platform, the new chameleon signature scheme improves the computational efficiency in the handshake process by about 25% compared to the traditional RSA signature scheme. In addition, the scheme in this paper provides stronger authentication security and is able to realize encryption, signature and signing functions at the same time, which has the potential for a wider range of applications. Ultimately, the experiments show that the scheme achieves the desired goals in terms of performance and security, and provides new ideas for digital signature research in the post-quantum era.

Index Terms Quantum Attack, Chameleon Signature, Lattice Cryptography, Security Analysis, Random Predicate Machine, Post-Quantum Era

I. Introduction

In recent years, with the development of quantum computers, difficult problems in traditional cryptographic regimes such as large integer factorization and discrete logarithm problems can be solved in polynomial time using quantum computers [1], [2]. Once the hardness problem, which is the cornerstone of traditional cryptographic regimes, is cracked, the security of various encryption algorithms and digital signature algorithms constructed on it will be fatally threatened by quantum attacks [3]-[5]. Quantum attack is a type of attack based on quantum computing, which utilizes the special properties of quantum computers to crack traditional encryption algorithms [6], [7]. There are two main ways of quantum attack, namely quantum key distribution attack and quantum computing attack [8], [9].

Quantum key distribution attack is when an attacker utilizes a quantum computer to attack the key distribution protocol in order to obtain the key information [10]-[12]. Quantum computing attack is that an attacker utilizes a quantum computer to crack the encryption algorithm so as to obtain the encryption information [13], [14]. The principle of quantum attack is based on the superposition and entanglement properties of quantum bits, which can break traditional encryption algorithms in a very short time through the parallel computing capability of quantum computers [15]-[17]. Therefore, designing a chameleon signature scheme that can resist quantum attacks is essential in the research of digital signatures in the post-quantum era [18], [19].

Distinguished from ordinary digital signatures, the chameleon hash function is used in chameleon signatures to hash the message [20], [21]. When there is no trapdoor information, the chameleon hash function has the same properties as the ordinary hash function [22]. When in possession of trapdoor information, it is easy to find another input with the same hash value [23]. A signature verifier is specified in a chameleon signature and that verifier is able to forge messages for known signatures such that the verification equation still holds [24], [25]. Thus, chameleon signatures are similar to non-repudiation signatures in that they are also non-transmissible, but they have the advantage that they do not require an interaction protocol [26], [27]. Due to these characteristics, chameleon signatures are able to withstand quantum attacks to some extent [28].

In recent years, the emergence of quantum computers has driven challenges to traditional cryptographic algorithms. Especially for cryptographic algorithms based on large integer factorization and discrete logarithm

problems, the high-speed parallel computing capability of quantum computers is able to solve these problems in polynomial time, thus exposing these traditional algorithms to unprecedented security threats. To cope with this challenge, post-quantum cryptography has become a hotspot of current research, and lattice cryptography has gained widespread attention as a cryptographic method that naturally resists attacks from quantum computation.

Chameleon signature is a digital signature scheme with non-repudiation and non-transferability. Unlike traditional digital signatures, chameleon signatures make it possible to forge valid signatures even for those who have the signer's public key by introducing a chameleon hash function, and this feature gives it an advantage against quantum attacks. Since the construction of chameleon signatures relies on the special properties of hash functions and requires the involvement of trapdoor information, it is fundamentally different from traditional digital signature schemes.

In this paper, we focus on chameleon signature schemes based on lattice cryptography, aiming to improve their security in quantum computing environments. Specifically, we propose a new chameleon signature construction that utilizes difficult problems in lattice cryptography to ensure its resistance to quantum attacks. In the scheme design, not only the traditional security requirements are considered, but also the defense mechanism against quantum attacks is specifically incorporated. Through accurate mathematical modeling and experimental verification, the security of the scheme under quantum computing attack is further proved, and the computational efficiency is higher than that of the traditional scheme.

In terms of research ideas, firstly, through a review of the existing literature, the threat of quantum attacks on traditional cryptographic algorithms is clarified, and the potential of chameleon signatures in defending against these attacks is further analyzed. Then, an identity-based chameleon signature scheme is designed by combining the basic theories of lattice cryptography. By introducing reasonable parameters and security assumptions, the theoretical security of the scheme is ensured. In addition, in order to evaluate the performance of the scheme in practical applications, a detailed performance analysis and experimental comparison are conducted to verify its superiority.

II. Preparatory knowledge

II. A. Grid cryptography

Definition 1 (lattice): given a set of linearly independent vectors $b_1, b_2, \cdots, b_n \in \square^m$, the lattice Λ can be generated by a linear combination of the integer coefficients of the vectors $b_1, b_2, \cdots, b_n$, defined as follows:

$$\Lambda(b_1, b_2, \cdots, b_n) = \left\{ \sum_{i=1}^{n} x_i b_i \,|\, x_i \in \square, 1 \le i \le n \right\} \tag{1}$$

Here the vectors $b_1, b_2, \cdots, b_n$ are said to be a set of lattice bases of the lattice Λ, denoted $B = [b_1, b_2, \cdots, b_n] \in \square^{m \times n}$.

There exists a matrix U which is the youngest modulus matrix if all elements in U are integers and U satisfies the determinant ± 1. It is easy to prove that $\Lambda(B) = \Lambda(B')$ if and only if $B' = BU$ [29].

If there exists $m = n$, then the lattice $\Lambda(b_1, b_2, \cdots, b_n)$ is said to be full-dimensional; and if A is a matrix of $n \times m$, then the column vectors are $b_1, b_2, \cdots, b_m$, and the lattice basis B generates the lattice, denoted:

$$\Lambda(B) = \Lambda(b_1, b_2, \cdots, b_m) = \{ Bx \,|\, x \in \square^m \} \tag{2}$$

The shortest distance $\lambda_1(\Lambda)$ of the lattice Λ is known as the shortest nonzero vector length in Λ and is defined as follows:

$$\lambda_1(\Lambda) = \min_{0 \ne x \in \Lambda} \|x\| \tag{3}$$

The symbol $\|\cdot\|$ denotes a Euclidean paradigm. The $\lambda_i(\Lambda)$ of the ith successive shortest length in Λ is defined to be the minimum radius r, and contains at most i linearly independent vectors of length r in the lattice Λ. Similarly to above, $\lambda_i^{\infty}(\Lambda)$ is defined as the shortest distance for which an infinite number of paradigms is the metric. G Given Λ, denote the Gram-Schmidt minimum as: $\tilde{bl}(\Lambda) = \min_B \|\tilde{B}\|$ The minimum here takes all of the lattice bases B in Λ.

Definition 2 (q metrical lattice): if any $q,n,m\in\square$, $A\in\square_q^{n}$, and $u\in\square_q^{n}$ satisfy $Ax=u \bmod q$, then Definition:

$$\Lambda^{\perp}(A)=\left\{y\in\square^{m}:Ay=0 \bmod q\right\} \tag{4}$$

$$\Lambda_u^{\perp}(A)=\left\{y\in\square^{m}:Ay=u \bmod q\right\}=\Lambda^{\perp}(A)+x \tag{5}$$

Observe here that if the vector $v\in\Lambda^{\perp}(A)$, then we get $\Lambda_u^{\perp}(A)=\Lambda^{\perp}(A)+v$, which is defined here as $\Lambda_u^{\perp}(A)$ is the companion set of $\Lambda^{\perp}(A)$.

II. A. 1) Difficulties of character

Definition 3 (Approximate Shortest Vector Problem) (SVP): take as input any lattice basis . Λ . and find a shortest nonzero vector $v\in\Lambda$ that satisfies $\|v\|<\|u\|$ for any nonzero vector $u\in\Lambda$.

Definition 4 (Determining the Approximate Shortest Vector Problem) (Gap SVP): for the lattice bases $\Lambda\in\square^{n\times n}$ and $d\in\square$.

If there is $\lambda_1(\Lambda)\le d$ then $\Lambda\in\square^{n\times n}$ is said to be a YES instance; if there is $\lambda_1(\Lambda)>\gamma(n)\cdot d$ then a NO instance.

Definition 5 (Approximate Nearest Vector Problem) (CVP): taking as input any lattice basis Λ and a target vector $t\in\square^{m}$ in the lattice basis Λ, and outputting a vector in the output lattice Λ that is closest to t to the nonzero vector v such that $\|v-t\|\le\|u-t\|$ is satisfied for any nonzero vector $u\in\Lambda$.

Definition 6 (Approximate Shortest Independent Vector Problem) (SIVP): with any lattice basis $\Lambda\in\square^{n\times n}$ as input, the output n linearly independent vectors $v_1,v_2,\ldots v_n\in\Lambda$, and also satisfy $\|v_i\|\le\lambda_n\Lambda$.

The approximate shortest vector problem and the approximate nearest vector problem are two of the most fundamentally difficult problems in designing lattice cipher schemes. In simple terms, the approximate shortest vector problem is to find the shortest nonzero vector belonging to a given lattice that has been given. The approximate nearest vector problem, on the other hand, is given a point belonging to a lattice to find another point that is nearest to that point. The constructed one-way trapdoor function is based on the SIS hard problem, and in polynomial time the average-case SIS problem can be generalized to the worst-case SIVP hard problem.

Definition 7 (SIS problem): input integer q, system parameter $\beta(n)$ and matrix $A\in\square_q^{n\times m}$. The $SIS_{q,\beta}$ problem is to find a nonzero vector $v\in\square^{m}$ that can satisfy the equation $Av=0 \bmod q$ and the nonzero vector v has a size satisfies $\|v\|\le\beta$.

Definition 8 (ISIS) problem: Input integer q, system parameters $\beta(n)$ and matrix $A\in\square_q^{n\times m}$. By arbitrarily choosing a vector $y\in\square_q^{n}$, the problem of $ISIS_{q,\beta}$ is to find an up to a non-zero vector $v\in\square^{m}$ that can satisfy the equation $Av=y \bmod q$ and the magnitude of the nonzero vector v satisfies $\|v\|\le\beta$.

II. A. 2) Discrete Gaussian distribution

Gaussian distribution has important applications in lattice-based cryptographic schemes and is an important tool for complexity analysis of schemes [30].

Definition 9 (Discrete Gaussian Distribution): a continuous Gaussian distribution on a n-dimensional lattice Λ is defined for any real number $s>0$ as well as on $\square^{n}$ centered on a vector c and parameterized by s :

$$\forall x\in\square^{n},\rho_{s,c}(x)=\exp\left(-\pi\left(\|x-c\|/s^{2}\right)\right) \tag{6}$$

These two values can be ignored if $s=1$ and $c=0$. For any vector $c\in\square^{n}$ centered and any $s>0$, the discrete Gaussian distribution on the lattice Λ is defined as:

$$\forall x\in\Lambda,D_{\Lambda_{s,c}}(x)=\frac{\rho_{s,c}(x)}{\rho_{s,c}(\Lambda)} \tag{7}$$

As with the discrete Gaussian distribution, these two values can be ignored if $s=1$ and $c=0$. The role of the denominator in the above definition is simply to carry out the normalization factor, so $\mathrm{D}_{\Lambda,s,c}(x)$ and $\rho_{s,c}(x)$ are proportional.

Definition 10 (Smoothing parameter): Micciancio and the notion of a smoothing parameter, as follows: in any n-dimensional lattice Λ, for any real number $\varepsilon>0$, the lattice Λ smoothing parameter is denoted by $\eta_\varepsilon = \min\left\{\sigma \in \mathbb{R}^+ \middle| \rho_{1/\sigma}\left(\Lambda^* \setminus \{0\}\right) \le \varepsilon\right\}$, here, Λ^* and Λ are mutually exclusive and Λ^* can be expressed as: $\Lambda^* = \left\{x \in \mathbb{R}^m \mid \forall v \in \Lambda, < x, v > \in \mathbb{R}\right\}$.

Definition 11 (Definition of the smoothing parameter): for any n-dimensional lattice Λ, and real numbers $\varepsilon>0$, B is the lattice base, satisfied:

$$\eta_\varepsilon(\Lambda) \le \|B\| \cdot \sqrt{In(2n(1+1/\varepsilon))/\pi} \tag{8}$$

So, for all functions $\omega\left(\sqrt{\log n}\right)$ with negligible ε, then $\eta_\varepsilon(\Lambda) \le \left\|\tilde{B}\right\| \cdot \omega\left(\sqrt{\log n}\right)$.

The following properties of the discrete Gaussian distribution are given by Gentry et al:

Lemma 1 For any n-dimensional lattice Λ, there exists $c \in \mathbb{R}^n$ and a real number $\varepsilon\left(1^\lambda\right)$, and given any parameter $\eta_\varepsilon(\Lambda)$, there are:

$$\Pr\left[\|x-c\| > s\sqrt{n}\right] \le \frac{1+\varepsilon}{1-\varepsilon} \cdot 2^{-n} \tag{9}$$

Lemma 2 For any n-dimensional lattice Λ and parameters $c \in \mathbb{R}^n$, and a lattice basis B of the lattice Λ such that $s \ge \left\|\tilde{B}\right\| \cdot \omega\left(\sqrt{\log n}\right)$, can be introduced:

$$\Pr\left[\|x-c\| > s\sqrt{n}\right] \le negl(n) \tag{10}$$

II. A. 3) Trap Derivation Algorithms

The trapdoor derivation algorithm presents a very simple and efficient mechanism to safely derive the trapdoor of matrix $A \in \mathbb{R}_q^{n \times m}$ from the trapdoor of extension $A' \in \mathbb{R}_q^{n \times m'}$ of A. There are several advantages over the Gerky delegation technique: first, and most importantly, the size of the derived trapdoor grows only linearly, not quadratically, with the dimension m' of $\Lambda^\perp(A')$. Second, the algorithm is relatively efficient because the algorithm does not need to test the linear independence of the Gaussian samples or compute the expensive ToBasis operation. Third, the obtained trapdoor T' has a good Gaussian distribution, is easy to analyze, and is useful in applications.

Definition 12 (Trap Derivative Algorithm) (DelTrap): input matrix A, parity check matrix $A' = [A|A_1] \in \mathbb{R}_q^{n \times (m+m')}$ and originally matrix G-trap T, invertible matrix $H' \in \mathbb{R}_q^{n \times n}$, new trap T' is obtained by Gaussian sampling over $\Lambda^\perp(A)$ using T, which satisfies $AT' = H'G - A_1$. The distribution of column vectors of T' satisfies a discrete Gaussian distribution with the following properties:

Lemma 3 Trapdoor Derivation Algorithm For the input G matrix $G \in \mathbb{R}_q^{n \times m}$, one can make the dimensionality of the column vectors of the G matrix generated as $\mathbb{R}_q^n$.

Lemma 4 The statistical distance between the distribution of the new trap T' generated using the trap derivation algorithm and the discrete Gaussian distribution is negligible.

Lemma 5 Arbitrarily transforming the column vectors of the parity check matrix A' does not affect the use of the algorithm.

II. A. 4) Ideal grid

The concept of ideal lattice was proposed in 2006. Simply put, an ideal lattice is a lattice with a special ring structure, and its advantage over the general lattice is that an ideal lattice can represent a vector as an n-dimensional lattice, which reduces the spatial size and spatial complexity of the lattice representation. And the representation of the ideal lattice is relatively simple, only a number of generating elements to represent, especially the main ideal lattice can be represented by only one generating element. Therefore, it greatly improves the speed of operation and thus reduces the time complexity [31].

II. B.Chameleon Signature

Let the message space be M, the random number space be R and the signature value space be S. A standard CS scheme consists of three main participants: the signer S, the designated verifier V and the arbiter:

(1) Setup: input security parameters λ and output public parameters pp.

(2) Key Gen: input pp, output public-private key pairs (pk_S, sk_S) and (pk_V, sk_V) for S and V.

(3) Sign: A probabilistic algorithm run by S. Input pp, public key pk_V, public-private key pair (pk_S, sk_S) and message $\mu \in \mathrm{M}$, output random number $r \in \mathrm{R}$ and signature value $\sigma \in \mathrm{S}$.

(4) Verify: a deterministic algorithm run by V. Inputs pp, public keys pk_s and pk_V, $\mu \in \mathrm{M}$, $r \in \mathrm{R}$ and $\sigma \in \mathrm{S}$. Output 1 or 0.

(5) Forge: probabilistic algorithm run by V. Input pp, public key pk_s, public-private key pair (pk_V, sk_V), algorithm Sign generated by S running on $\mu \in \mathrm{M}$, $r \in \mathrm{R}$ and $\sigma \in \mathrm{S}$, output a new message $\mu' \in \mathrm{M}$ and a random number $r' \in \mathrm{R}$ that satisfies $Verify(pp, pk_s, pk_v, \mu', r', \sigma) \to 1$.

A safe CS scheme needs to satisfy the following properties:

Definition 13 A CS scheme is said to be strongly unforgeable under an adaptive choice message attack if for any PPT the adversary A wins the following game with the advantage $ADV_{CS\_A}^{Non-transferability}$ is negligible.

Definition 14 A CS scheme is said to be nontransmissible if the advantage $ADV_{CS\_A}^{Non-transferability}$ for an adversary A winning the following game for any PPT is negligible.

Definition 15 A CS scheme is said to satisfy signer rejectability if $(\mu, r, \sigma) \in \mathrm{M} \times \mathrm{R} \times \mathrm{S}$ is forged by the designated verifier V and the signer S has the ability to convince the arbiter J to reject the signature. Conversely, a CS scheme is said to satisfy signer non-repudiation if (μ, r, σ) is genuinely generated by S and it cannot be denied [32].

III. Quantum-attack-resistant chameleon signature scheme on grids

This section introduces the new identity-based chameleon signature scheme on the lattice and rigorously proves the security of the scheme under the stochastic predicate machine model. In particular, the message space $M = \{0,1\}^m$, the identity space $ID = \{0,1\}^*$, the random number space $R = D_{z^m,s}$, and the signature value space $S = D_{z^m,s}$, and $id_S, id_V \in ID$ correspond to the identities of the signer and the designated verifier, respectively.

III. A. Program structure

$Setup(1^n) \to (pp, msk)$: enter the security parameter n such that the prime $q = poly(n)$, the integer $m = 2n\lceil \log_2 q \rceil$, Gaussian parameter $s = O\%(n^2)$. KGC performs the following operations:

1) Run $Trap\ Gen(q, n, m)$ to generate the trapdoor $A \in Z_q^{n \times m}$ and the trapdoor $\Lambda_q^{\perp}(A)$ of T_A.

2) Randomly select $B \xleftarrow{\$} Z_q^{n \times m}$ as the common matrix for constructing the chameleon hash function CH.

3) The collision-resistant hash functions $H_1 : \{0,1\}^* \to D_{m \times m}$ and $H_2 : \{0,1\}^* \to Z_q^n$, where $Dm_{m \times m}$ is the distribution of $\bmod q$ invertible and column vectors on $Z^{m \times m}$ obeying the distribution D_{z^m, s_R}, see Lemma 1.

4) Output the public parameters $pp = (A, B, H_1, H_2)$ and the system master private key $msk = T_A$.

$Key\ Gen(msk, id) \to (sk_{id})$: Enter the master private key msk and the identity $id \in ID$, and the KGC performs the following:

1) Let $R_{id} = H_1(id) \in D_{m \times m}$, compute $F_{id} = A \cdot R_{id}^{-1} \bmod q$ (hereafter, we will refer to F_{id_S} and F_{id_V} as F_S and F_V).

2) Run $Basis\ Del(A, R_{id}, T_A, s)$ to generate the trapdoor $\Lambda_q^{\perp}(F_{id})$ for $T_{F_{id}}$.

3) Output private key $sk_{id} = T_{F_{id}}$.

$Sign\left(id_S, id_V, sk_{id_s}, \mu\right) \to \left(\mu, r, \sigma\right)$: Input the signer's identity $id_S \in ID$, the identity of the specified verifier $id_V \in ID$, the signer's private key $sk_{id} = T_{F_{id}}$, and the message $\mu \in \{0,1\}^m$ and the signer performs the the following operation:

1) First find out if the local signature list stores (id_V, μ, r, σ), if it exists, perform 6), otherwise perform 2).

2) Let $R_{id_s} = H_1\left(id_S\right)$ and $R_{id_V} = H_1\left(id_V\right)$, calculate $F_S = A \cdot R_{id_S}^{-1} \bmod q$ and $F_V = A \cdot R_{id_V}^{-1} \bmod q$.

3) Randomly select $r \xleftarrow{\$} R$ and compute the hash $y = CH(\mu, r) = B \cdot \mu + F_V \cdot r \bmod q$.

4) Let $h = H_2\left(id_s, id_V, bin(y)\right)$, where $bin(y) \in \{0,1\}^{n\lceil \log_2 q \rceil}$ is the binary of $y = CH(\mu, r)$.

5) Run $Sample\,\mathrm{Pre}\left(F_S, T_{F_s}, s, h\right)$ to generate the signature value $\sigma \in Z^m$.

6) Output (μ, r, σ) and store (id_V, μ, r, σ) in the local signature list.

$Verify\left(id_S, id_V, \mu, r, \sigma\right) \to \left(Acc\ or\ \mathrm{Rej}\right)$: enter signer identity $id_S \in ID =$, specify verifier identity $id_V \in \mathrm{ID}$, the message $\mu \in \{0,1\}^m$, the random number $r \in R$, and the signature value $\sigma \in S$, the verifier performs the following operations:

1) Verify that $0 < \|r\|$, and $\|\sigma\| \le s \cdot \sqrt{m}$, holds.

2) Let $R_{id_S} = H_1\left(id_S\right)$ and $R_{id_V} = H_1\left(id_V\right)$, calculate $F_S = A \cdot R_{id_S}^{-1} \bmod q$ and $F_V = A \cdot R_{idv}^{-1} \bmod q$.

3) Calculate $y = B \cdot \mu + F_V \cdot r \bmod q$ to verify that $F_S \cdot \sigma = H_2\left(id_S, id_V, bin(y)\right) \bmod q$ Whether or not it holds.

4) If all the above conditions hold, output Acc, otherwise output Rej.

$Simulate\left(id_V, sk_{idv}, \mu, r, \sigma\right) \to \left(\mu', r', \sigma\right)$: Enter the identity of the specified verifier id_V, the private key $sk_{idv} = T_{Fv}$, and the $(\mu, r, \sigma) \in M \times R \times S$ generated by the signer, and the specified verifier performs the following operations:

1) Make $R_{id_V} = H_1\left(id_V\right)$ and compute $F_V = A \cdot R_{id_V}^{-1} \bmod q$.

2) Calculate $y = CH(\mu, r) = B \cdot \mu + F_V \cdot r \bmod q$.

3) Pick $\mu' \in M$ and $\mu' \ne \mu$ and compute $v = y - B \cdot \mu' \bmod q$.

4) Run $Sample\,\mathrm{Pre}\left(F_V, T_F, s, v\right)$ to generate random numbers $r' \in \mathrm{R}$.

5) Output the chameleon signature triad (μ', r', σ).

III. B. Security analysis

Theorem 1: Assuming that the problem $SIS_{q,m,2s\sqrt{m}}$ is hard, the schemes in this section are SUF-SID-CMA secure.

PROOF: Assuming that the PPT adversary A launches a selective identity and adaptive selective messaging attack on the above IBCS scheme, and is able to forge signatures by a non-negligible margin $Adv_{IBCS,A}^{SUF-SID-CMA} = \varepsilon$, then the challenger C is able to solve the $\mathrm{SIS}_{q,m,2s\sqrt{m}}$ puzzle instance $A^* \cdot e^* = 0 \bmod q$ where $\mathbf{A}^* \in \mathrm{Z}_q^{n \times m}$. The interaction game between C and A is as follows:

Initial: A announces the target identities $id_S \in ID$ and $id_V \in ID$ for its attack.

Setup: C randomly select $R^* \xleftarrow{\$} D_{m \times m}$ and $B \xleftarrow{\$} Z_q^{n \times m}$ such that $A = A^* \cdot R^* \bmod q$, send $pp = (A, B)$ as to A.

H_1 queries: given $id_i \in \mathrm{ID}$, if $id_i \ne id_S$, C find out if the list of keys stores $\left(id_i, R_i, F_i, T_{F_i}\right)$. If it exists, return $H_1\left(id_i\right) = R_i$ directly; otherwise, run $Sample\ Rwith\ Basis\left(A\right)$ to generate $R_i \in Dm_{m \times m}$, $F_i \in \mathscr{L}_q^{m \times m}$ and $\Lambda_q^{\perp}\left(F_i\right)$ trapdoor T_{F_i}, where $F_i = A \cdot R_i^{-1} \bmod q$, saves $\left(id_i, R_i, F_i, T_{F_i}\right)$ to the key list and returns $H_1\left(id_i\right) = R_i$. If $id_i = id_s$, save $\left(id_s, R^*, A^*, \perp\right)$ to the key list and return $H_1\left(id_s\right) = R^*$.

H_2 queries: given $id_i, id_j \in ID$ and $\mu \in M$, C find out if the key list has $\left(id_i, R_i, F_i, T_{F_i}\ or \perp\right)$ and the signature list has $\left(id_i, id_j, \mu, r, \sigma\right)$. If it exists, return $H_2\left(id_i, id_j, bin(y)\right) = F_i \cdot \sigma \bmod q$; otherwise, use the method in

H_1 queries to generate $\left(id_i, R_i, F_i, T_{F_i} \text{ or } \perp\right)$, pick a random number $r \xleftarrow{\$} R$, compute $y = CH(\mu, r) = B \cdot \mu + F_j \cdot r \bmod q$, randomly pick $e \xleftarrow{\$} D_{\varphi^m, s}$, save $\left(id_i, id_j, \mu, r, \sigma\right)$ to the local signature list, and return $H_2\left(id_i, id_j, bin(y)\right) = F_i \cdot \sigma \bmod q$. From Lemma 2, the output of $Sample\ Rwith\ Basis(A)$ is $R_i \in Dm_{m\times m}$. From Lemma 4, the statistics of $F_i \cdot \sigma \bmod q$ are close to uniformly distributed. In summary, the return values of H_1 queries and H_2 queries are indistinguishable from the output statistics of H_1 and H_2 in the real program.

Key queries: A Enter $id_i \in \mathrm{ID}$, and $id_i \notin \{id_s, id_V\}, \mathrm{C}$, C to find the local key vault $\left(id_i, R_i, F_i, T_{F_i}\right)$, returning $sk_{id_i} = T_{F_i}$.

Sign queries: A inputs $id_i, id_j \in \mathrm{ID}$ (id_i and id_j correspond to the signer and the designated verifier respectively) and $\mu \in M$, C looks up the local signature repository $\left(id_i, id_j, \mu, r, \sigma\right)$, returning (μ, r, σ).

Outputs: A Output id_S for id_V generated by forging $\left(\mu^*, r^*, \sigma^*\right) \in M \times R \times S$, is satisfied:

1) $Verify\left(id_s, id_V, \mu^*, r^*, \sigma^*\right) \to Acc$.

2) A has not performed Key queries for id_S and id_V.

3) $\left(id_s, id_V, \mu^*\right)$ and $\left(r^*, \sigma^*\right)$ are not the inputs to a particular Signquery and return.

Without loss of generality, assume that A has initiated a H_2 query with input $\left(id_s, id_V, \mu^*\right)$ to C before the output forges $\left(\mu^*, r^*, \sigma^*\right)$, and that C stores $\left(id_V, R_V, F_V, T_{F_V}\right)$ and $\left(id_s, id_V, \mu^*, r_{\mu^*}, \sigma_{\mu^*}\right)$ locally. After A outputs the forgery $\left(id_S, id_V, \mu^*, r^*, \sigma^*\right)$, C looks up the local signature repository $\left(id_S, id_V, \mu^*, r_{\mu^*}, \sigma_{\mu^*}\right)$ and gets $\left(\mu^*, r_{\mu^*}, \sigma_{\mu^*}\right)$. Since $\left(\mu^*, r^*, \sigma^*\right) \in M \times R \times S$ is a successful forgery:

$$\begin{aligned} F_S \cdot \sigma^* &= F_S \cdot \sigma_{\mu^*} \\ &\Rightarrow A \cdot \left(H_1\left(id_S\right)\right)^{-1} \cdot \sigma^* = A^* \cdot R^* \cdot \left(R^*\right)^{-1} \cdot \sigma^* \\ &= A^* \cdot \sigma^* = A^* \cdot \sigma_{\mu^*} \bmod q \end{aligned} \tag{11}$$

The forgery $\left(\mu^*, r^*, \sigma^*\right)$ of A is illustrated by the following two scenarios, as opposed to the local signature base of C $\left(\mu^*, r_{\mu^*}, \sigma_{\mu^*}\right)$ is different:

1) If A has initiated a Sign query with inputs $\left(id_s, id_V, \mu^*\right)$ and C returns $\left(\mu^*, r_{\mu^*}, \sigma_{\mu^*}\right)$. Since A wins the game by outputting a valid strongly forged signature, i.e., $\left(id_s, id_V, \mu^*\right)$ and $\left(r^*, \sigma^*\right)$ is not the input and return of a particular Signquery, therefore, $\sigma^* \neq \sigma_{\mu^*}$

2) If A has not initiated a Signquery with input $\left(id_s, id_V, \mu^*\right)$, since A has initiated an input $\left(id_S, id_V, \mu^*\right)$ query with H_2, C has stored $\left(\mu^*, r_{\mu^*}, \sigma_{\mu^*}\right)$ and returns $H_2\left(id_S, id_V, bin(y)\right) = A^* \cdot \sigma_{\mu^*}$. By the original image minimum entropy property, there is a great probability $1 - 2^{-\omega(\log_2 n)}$ such that $\sigma^* \neq \sigma_{\mu^*}$. Obviously, C is able to find ε with probability close to $\varepsilon' = \varepsilon \cdot \left(1 - 2^{-\omega(\log_2 n)}\right)$ with a probability $SIS_{q,m,2s\sqrt{m}}$ problem example $A^* \cdot e^* = 0 \bmod q$ solution $e^* = \left(\sigma^* - \sigma_{\mu^*}\right)^T \in Z^m$, satisfies $A^* \cdot e^* = 0 \bmod q$, and $0 < \left\|e^*\right\| \le 2s\sqrt{m}$. Thus, $Adv_{IBCS,\mathrm{A}}^{SUF-SID-CMA} = \varepsilon \approx \varepsilon' = negl(n)$, which otherwise contradicts the difficulty assumption of the SIS problem.

Theorem 2: The schemes in this section are nontransmissible.

Proof: the adversary A chooses the target identities $id_s \in ID$ and $id_V \in ID$. The challenger C runs the algorithm Key Gen to generate (F_S, T_{F_S}) and (F_V, T_{F_V}); picks the message $\mu_0 \in M$, and runs $Sign(id_s, id_V, F_S, \mu_0)$ generate random number $r_0 \in R$ and signature value $\sigma \in S$; run $Simulate(id_V, T_{F_V}, \mu_0, r_0, \sigma)$ Generate a new message $\mu_1 \in M$ and a random number $r_1 \in R$. The C randomly selects $b \in \{0,1\}$ and finally returns $(\mu_b, r_b, \sigma) \in M \times R \times S$.

From the above procedure, $r_0 \in D_{Z^m,s}$, r_1 is generated for running the algorithm SamplePre. By Lemma 3, the short vectors r_0 and r_1 are statistically not divisible. For (μ_0, r_0, σ) and (μ_1, r_1, σ), there is $\mathrm{CH}(\mu_0, r_0) = \mathrm{CH}(\mu_1, r_1)$, i.e., $B \cdot \mu_0 + F_V \cdot r_0 = B \cdot \mu_1 + F_V \cdot r_1 \bmod q$. Therefore, condition 3) in Algorithm Verify holds, i.e.

$$\begin{aligned} F_S \cdot \sigma &= H_2\left(id_s, id_V, bin\left(B \cdot \mu_0 + F_V \cdot r_0\right)\right) \\ &= H_2\left(id_s, id_V, bin\left(B \cdot \mu_1 + F_V \cdot r_1\right)\right) \bmod q \end{aligned} \tag{12}$$

Clearly, the chameleon signatures (r_0, σ) and (r_1, σ) returned by the challenger C with respect to $\mu_0 \in M$ and $\mu_1 \in M$ are statistically indistinguishable for the adversary A. Therefore, the dominance of A is negligible, i.e., $Adv_{IBDCS,A}^{IBCS-NT} = negl(n)$.

Theorem 3: The schemes in this section satisfy signer rejectability and non-repudiation.

Proof: the signer id_s generates the triple $(\mu, r, \sigma) \in M \times R \times S$ and sends it to the designated verifier $id_V \in ID$, and it may be assumed that id_s tries to deny it, i.e., id_s denies that he or she is the true signer of (μ, r, σ). According to the protocol DenPro, id_s needs to produce $(\mu', r', \sigma) \in M \times R \times S$ to persuade the arbiter J and be able to pass the verification, then:

$$CH(\mu, r) = CH(\mu', r') = (B \mid F_V) \cdot \begin{pmatrix} \mu \\ r \end{pmatrix} = (B \mid F_V) \cdot \begin{pmatrix} \mu' \\ r' \end{pmatrix} \bmod q \tag{13}$$

Further, there are $(B \mid F_V) \cdot \begin{pmatrix} \mu - \mu' \\ r - r' \end{pmatrix} = 0 \bmod q$, and furthermore, $(\mu', r') \neq (\mu, r)$, otherwise the presentation of id_s is invalid. Obviously, this will yield an efficient solution $e^* = \begin{pmatrix} \mu - \mu' \\ r - r' \end{pmatrix}$ for $SIS_{q,2m,2s\sqrt{m}}$ problem instance $A^* \cdot e^* = 0 \bmod q$, which contradicts the difficulty assumption of the SIS problem. Therefore, the solutions in this section satisfy signer nonrepudiation.

Conversely, since id_s is not repudiation-eligible, if id_s produces (μ', r', σ) against the disputed triple (μ, r, σ), which can be verified and satisfies $(\mu', r') \neq (\mu, r)$, the arbiter can fully conclude that (μ, r, σ) is generated truthfully by id_s. Further, it is sufficient to prove that (m', r', s) is forged by id_V, i.e., the present scheme satisfies signer rejectability.

IV. Programmatic analysis

IV. A. Operational Performance

In order to analyze the computing performance of this paper's scheme, C++ is used to simulate the process of handshaking between a pair of client and server nodes using the TLS1.3 protocol of this paper and the original protocol, respectively, with the transmission, reception and processing time of a single packet between the two nodes set to satisfy the exponential distribution with a mean value of 500ms. The protocol in this paper uses NTRU signature scheme and SWIFFT hash algorithm instead of the RSA signature scheme and sha256 hash algorithm in the original protocol, respectively, in which the NTRU signature scheme and SWIFFT hash algorithm are implemented using existing open source software packages. The hardware and software configuration of the simulation platform is shown in Table 1.

Table 1: Configuration of experimental platform

Configuring	Parameter value
CPU	Intel i5-10700,4.0GHz
Memory capacity	16GB
Operating system	Windows 10
Development tool	Visual Studio 2019

Comparing the time required to complete the handshake protocols of the original and improved schemes under different session concurrency scenarios as shown in Fig. 1, it can be seen that the time required for TLS handshake of the improved protocol is lower than that required for handshake of the original protocol at 10~10^5 concurrencies. The reason for improving the computational efficiency of the protocol is that the NTRU algorithm and the SWIFFT algorithm use matrix multiplication, the RSA algorithm uses the modulo power algorithm, and the sha256 uses the Merkle-Damgard iterative structure, the matrix multiplication operation has the characteristic of faster operation speed compared to the latter two, so the handshake process cryptographic operations take less time, and the whole handshake protocol takes less time, and the efficiency is higher. The whole handshake protocol takes less time and is more efficient.

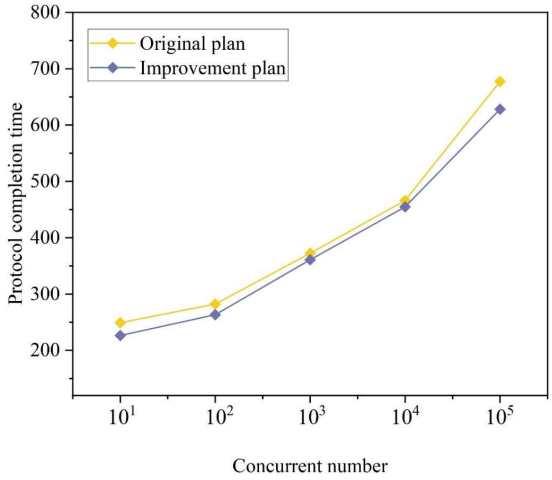


Figure 1: Scheme performance comparison

IV. B. Comparative analysis

Existing generalized signature cipher schemes are all based on discrete logarithm and bilinear pair implementation, while the scheme in this paper is constructed based on the lattice hard problem, compared with the schemes based on discrete logarithm and bilinear pairs, the lattice cipher is extended in ciphertext size under the same security strength, although there is a certain extension of the ciphertext size. However, its operations are all very efficient linear operations, and the computational efficiency is generally much higher than the former, and the lattice cipher is also one of the most important candidates for quantum attack-resistant ciphers. Therefore, we do not compare the efficiency of this scheme with similar existing discrete logarithm-based schemes in detail, but only compare the related lattice-based signature cipher schemes. According to the requirements of practical application environment, the generalized signature can realize three functions of encryption, signature and signature at the same time, but compared with the traditional signature scheme, the construction of the generalized signature scheme should not be at the cost of significant sacrifice of efficiency. From the perspective of quantum attack resistance, combined with the above design principles and the characteristics of trapdoor-free construction, we compare the ciphertext size of this scheme with that of the existing trapdoor-free lattice-based encryption, signature and sign-secret schemes in the following, and the specific results of the comparison are shown in Table 2, where $|\mathrm{M}|$ denotes the bit-length of the plaintext, S_D denotes the Gaussian sampling operation, S_T denotes the original image sampling with trapdoor, M_v denotes the matrix-vector multiplication operation, M_R denotes the polynomial ring multiplication operation, and $n=2^k, n, q$ defines the ring R_q.

The generalized signing scheme in this paper is $n^* \log q - k$ bits smaller than the signing scheme of LWD16, which is mainly due to the fact that the new scheme is based on the ideal lattice construction, which can improve the efficiency of polynomial ring operation by using the fast Fourier transform, and also provides better

authentication security in terms of security. Compared with the original KEM construction of FK18, the ciphertext size is only increased by k bits, and compared with the original KEX construction of FK18, the ciphertext size is smaller, and the efficiency does not change much, but the scheme in this paper provides a stronger level of confidentiality security.R The new scheme is more efficient in achieving the same CCA2. In addition, both LWD16 and FK18 can only provide the function of signing secret, while this paper's scheme can provide three functions of encryption, signature, and signing secret according to the requirements of the actual application environment, which really realizes the generalized signing secret.

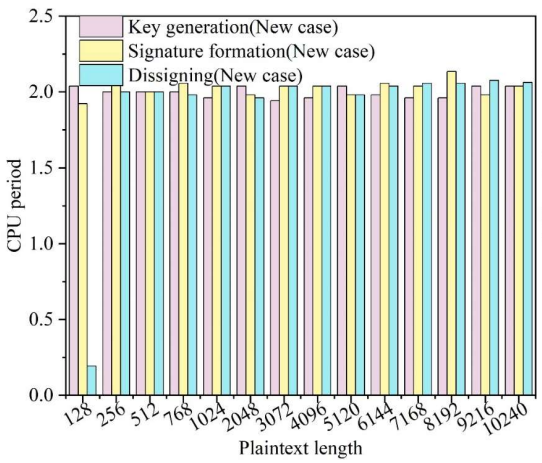
The scheme satisfies the indistinguishable security of selective ciphertext attack (IND-CCA2) and the strong unforgeable security of selective message attack (SUF-CMA), and the scheme does not use the complex original image sampling and inverse operation with trapdoor, which has high computational efficiency. Compared with the existing related trapdoor-less Gergil signature and encryption schemes, the scheme in this paper has similar ciphertext size but higher security, and can provide three functions of encryption, signature and encryption at the same time, which is more practical.

Table 2: Comparison results of the relevant scheme

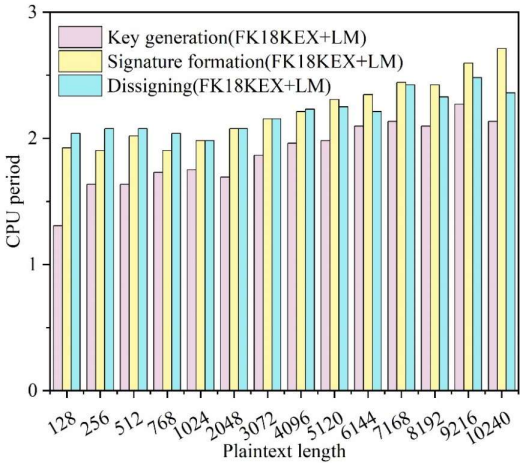
Scheme	Safety	Public key size	Text size	Packing operation	Unpacking operation
LWD16	IND-CCA2 EUF-CMA	$2n^2 \log q$	$4n^* \log q$ $+\lvert M \rvert$	$4\mathrm{S}_D$ $+6M_v$	$3M_R$
FK18	IND-CPA SUF-CMA	$2n \log q$	$4n^* \log q$ $+\lvert M \rvert$	$8M_R$	$5M_R$
		$2n \log q$	$3n^* \log q$ $+\lvert M \rvert$	$8M_R$	$5M_R$
	IND-CCA@ EUF-CMA	$2n \log q$	$2n \log q + l_{NN}$ $+n \log n \log q$ $+2l_n \log n$ $+\lvert M \rvert$	$8M_R + \log nM_R$	$5M_R +$ $\log nM_R$
		$2n \log q$		$8M_R + \log nM_R$	$5M_R +$ $\log nM_R$
	IND-CCA2 SUF-CMA	$2n \log q$	$3n^* \log q$ $+\mathrm{k}+\lvert M \rvert$	$8M_R$	$5M_R$

IV. C. Experiments and Performance Analysis

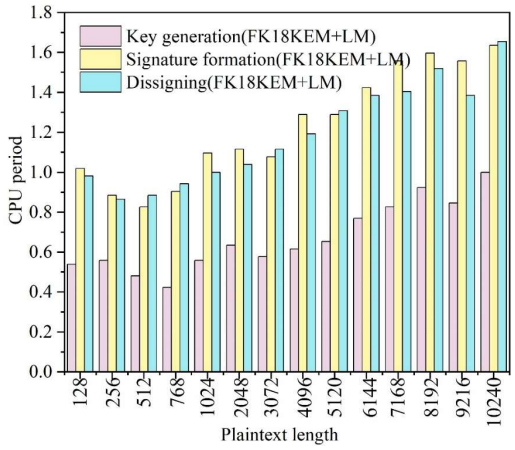
During the experiment, we use CPU clock cycle counting to represent the running time (higher precision), and take the method of running the algorithm 1000 times to take the average value (reduce the error) to obtain the experimental results, which are shown in Figure 2. The experimental data show that the key generation algorithm for generalized signature encryption does not change much with the change of plaintext length. This is mainly due to the fact that the security parameters chosen by the new scheme are fixed, for the sign-and-secret and encryption-only algorithms the time spent starts from an initial value and increases slowly and linearly with the increase of the message length, while the signature-only algorithm does not have a significant response to the change of the plaintext message length. The reason may be because the time-consuming computation of the signature and encryption scheme can be viewed as consisting of two parts, the signature part is to take a fixed length hash value of the message and then sign it, so the signature is rarely affected by the length of the message. The encryption requires grouping and encrypting the message group by group, and the time consumed is directly proportional to the length of the plaintext message. In addition, after converting FK18 to CCA2 security strength, the new scheme has similar key generation time and significantly less signing and unsigning time compared to KEM and KEX constructions of FK18.



(a) New case



(b) FK18KEX+LM



(c) FK18KEM+LM

Figure 2: Similar GSC efficiency comparison

V. Conclusion

The chameleon signature scheme based on lattice cryptography proposed in this paper shows good security and computational efficiency under quantum computing attacks. The scheme's resistance to quantum attacks under the stochastic predicate machine model is demonstrated through accurate security analysis, especially in resisting adaptive choice of message attack (SUF-CMA) and nondeliverability with significant advantages. The experimental results show that the new signature scheme has a significant improvement in computational efficiency compared with the traditional RSA signature scheme in different scenarios. In the experiments simulating the TLS protocol, the improved protocol saves about 25% of time in the handshaking process compared to the original protocol.

In terms of computing performance, the scheme in this paper adopts NTRU signature and SWIFFT hash algorithm, which avoids the more complex operations in RSA signature and sha256 hash algorithm and improves the overall computing efficiency. In addition, the scheme not only provides the signature function, but also can support both encryption and signature and encryption functions, which provides more choices for practical applications. By comparing with other lattice-based encryption and signature schemes, this paper's scheme demonstrates advantages in ciphertext size and security, and has higher practicality.

Overall, the research in this paper provides a new way of thinking for secure digital signature schemes in the post-quantum era, especially in the face of quantum attacks, the lattice-based chameleon signature scheme is undoubtedly a potential solution.

References

[1] Rietsche, R., Dremel, C., Bosch, S., Steinacker, L., Meckel, M., & Leimeister, J. M. (2022). Quantum computing. Electronic Markets, 32(4), 2525-2536.

[2] Preskill, J. (2018). Quantum computing in the NISQ era and beyond. Quantum, 2, 79.
[3] Cao, Y., Romero, J., Olson, J. P., Degroote, M., Johnson, P. D., Kieferová, M., ... & Aspuru-Guzik, A. (2019). Quantum chemistry in the age of quantum computing. Chemical reviews, 119(19), 10856-10915.
[4] Bonnetain, X., Hosoyamada, A., Naya-Plasencia, M., Sasaki, Y., & Schrottenloher, A. (2019, November). Quantum attacks without superposition queries: the offline Simon's algorithm. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 552-583). Cham: Springer International Publishing.
[5] Cai, B. B., Wu, Y., Dong, J., Qin, S. J., Gao, F., & Wen, Q. Y. (2023). Quantum Attacks on 1K-AES and PRINCE. The Computer Journal, 66(5), 1102-1110.
[6] Gong, C., Guan, W., Gani, A., & Qi, H. (2022). Network attack detection scheme based on variational quantum neural network. The Journal of Supercomputing, 78(15), 16876-16897.
[7] Satoh, T., Nagayama, S., Suzuki, S., Matsuo, T., Hajdušek, M., & Van Meter, R. (2021). Attacking the quantum internet. IEEE Transactions on Quantum Engineering, 2, 1-17.
[8] Sharma, P., Agrawal, A., Bhatia, V., Prakash, S., & Mishra, A. K. (2021). Quantum key distribution secured optical networks: A survey. IEEE Open Journal of the Communications Society, 2, 2049-2083.
[9] Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE access, 8, 21091-21116.
[10] Jain, N., Stiller, B., Khan, I., Elser, D., Marquardt, C., & Leuchs, G. (2016). Attacks on practical quantum key distribution systems (and how to prevent them). Contemporary Physics, 57(3), 366-387.
[11] Sundar, B., Walschaers, M., Parigi, V., & Carr, L. D. (2021). Response of quantum spin networks to attacks. Journal of Physics: Complexity, 2(3), 035008.
[12] Qin, H., Kumar, R., & Alléaume, R. (2016). Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution. Physical Review A, 94(1), 012325.
[13] Stewart, I., Ilie, D., Zamyatin, A., Werner, S., Torshizi, M. F., & Knottenbelt, W. J. (2018). Committing to quantum resistance: a slow defence for Bitcoin against a fast quantum computing attack. Royal Society open science, 5(6), 180410.
[14] Khalid, Z. M., & Askar, S. (2021). Resistant blockchain cryptography to quantum computing attacks. International Journal of Science and Business, 5(3), 116-125.
[15] Zheng, X. (2024). Research on blockchain smart contract technology based on resistance to quantum computing attacks. Plos one, 19(5), e0302325.
[16] Portmann, C., & Renner, R. (2022). Security in quantum cryptography. Reviews of Modern Physics, 94(2), 025008.
[17] Song, F. (2014, October). A note on quantum security for post-quantum cryptography. In International Workshop on Post-Quantum Cryptography (pp. 246-265). Cham: Springer International Publishing.
[18] Xu, J., Chen, H., Yang, X., Wu, W., & Song, Y. (2021). Verifiable image revision from chameleon hashes. Cybersecurity, 4, 1-13.
[19] Thanalakshmi, P., Anitha, R., Anbazhagan, N., Park, C., Joshi, G. P., & Seo, C. (2022). A hash-based quantum-resistant designated verifier signature scheme. Mathematics, 10(10), 1642.
[20] Wu, C., Ke, L., & Du, Y. (2021). Quantum resistant key-exposure free chameleon hash and applications in redactable blockchain. Information Sciences, 548, 438-449
[21] Chen, X., Zhang, F., Susilo, W., Tian, H., Li, J., & Kim, K. (2014). Identity-based chameleon hashing and signatures without key exposure. Information Sciences, 265, 198-210.
[22] Xie, D., Peng, H., Li, L., & Yang, Y. (2017). Homomorphic signatures from chameleon hash functions. Information Technology and Control, 46(2), 274-286.
[23] Thanalakshmi, P., & Anitha, R. (2022). A quantum resistant chameleon hashing and signature scheme. IETE Journal of Research, 68(3), 2271-2282.
[24] Wang, Y., & Ismail, E. S. (2024). Tightly-Secure Two-Tier Signatures on Code-Based Digital Signatures with Chameleon Hash Functions. Mathematics (2227-7390), 12(15).
[25] Xiong, G., & Li, D. (2025). Security Analysis and Signature Algorithm Design of Gegami's Identity-Based Chameleon Signature Scheme under Quantum Attack Resistance. J. COMBIN. MATH. COMBIN. COMPUT, 127, 6805-6822.
[26] Astrizi, T., Custódio, R., & Moura, L. (2020, October). Post-quantum signature with preimage chameleon hashing. In Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg) (pp. 69-82). SBC.
[27] Thakur, T., & Sharma, B. K. (2016). ID-BASED CHAMELEON HASHING AND CHAMELEON SIGNATURE BASED ON GQ SCHEME. International Journal of Applied Mathematics, 29(2), 227-242.
[28] Thanalakshmi, P., Anitha, R., Anbazhagan, N., Cho, W., Joshi, G. P., & Yang, E. (2021). A hash-based quantum-resistant chameleon signature scheme. Sensors, 21(24), 8417.
[29] Qureshi Imran M Hussain & Vijay Kale. (2025). Mobile node authentication with risk-based modified lattice cryptography enabled adaptive multifactor authentication for secure data transmission. Computers and Electrical Engineering,124(PA),110272-110272.
[30] Ogorodnikov V. A.,Akenteva M. S. & Kargapolova N. A. (2024). An Approximate Algorithm for Simulating Stationary Discrete Random Processes with Bivariate Distributions of Their Consecutive Components in the Form of Mixtures of Gaussian Distributions. Numerical Analysis and Applications,17(2),169-173.
[31] Robson Ricardo de Araujo. (2025). The condition number associated with ideal lattices from odd prime degree cyclic number fields. Journal of Mathematical Cryptology,19(1).
[32] Thanalakshmi P.,Anitha R.,Anbazhagan N.,Cho Woong,Joshi Gyanendra Prasad & Yang Eunmok. (2021). A Hash-Based Quantum-Resistant Chameleon Signature Scheme. Sensors,21(24),8417-8417.