Computers, Materials & Continua
DOI: 10.32604/cmc.2023.035337
Article

Tech Science Press

Attribute-Based Authentication Scheme from Partial Encryption for Lattice with Short Key

Wangke Yu and Shuhua Wang*

School of Information Engineering, Jingdezhen Ceramic University, Jingdezhen, 333403, China
*Corresponding Author: Shuhua Wang. Email: w614sh@126.com
Received: 17 August 2022; Accepted: 13 October 2022

Abstract: Wireless network is the basis of the Internet of things and the intelligent vehicle Internet. Due to the complexity of the Internet of things and intelligent vehicle Internet environment, the nodes of the Internet of things and the intelligent vehicle Internet are more vulnerable to malicious destruction and attacks. Most of the proposed authentication and key agreement protocols for wireless networks are based on traditional cryptosystems such as large integer decomposition and elliptic curves. With the rapid development of quantum computing, these authentication protocols based on traditional cryptography will be more and more threatened, so it is necessary to design some authentication and key agreement protocols that can resist quantum attacks. In this paper, an anti-quantum authentication scheme for wireless networks based on lattice cryptosystem is constructed. In the attribute-based authentication scheme, the length of the authenticated public-private key pair depends on the maximum order and complexity of the formula in the algorithm. In the attribute-based authentication scheme, there is a certain correlation between the authenticated data and the attribute value of the user in the scheme. We show that the attribute-based authentication scheme gives an attribute-based with smaller public-private key pairs. The security of the attribute-based authentication scheme is based on the sub-exponential hard problem of the LWE (Learning With Errors). The *Q-poly* made by the adversary in the scheme, and our attribute-based authentication scheme guarantees that private data about user attributes and ciphertext cannot be obtained by malicious attackers.

Keywords: Authentication; learning with errors; partial encryption; security

1 Introduction

There are many attributes-based authentication schemes proposed in protocols related to wireless networks and information security, such as references [1–4]. However, most of the proposed authentication and key agreement protocols for wireless networks are based on traditional cryptosystems such as large integer decomposition and elliptic curves. With the rapid development of quantum computing, these authentication protocols based on traditional cryptography will be more and more

threatened. These attribute-based authentication schemes will not be secure in the post-quantum era. At present, the widely used anti-quantum cryptosystem is an anti-quantum algorithm based on lattice cryptosystem and coding-related problems. With the rapid development of quantum computer, the anti-quantum algorithm based on lattice cryptosystem will attract more researchers. For the related security protocols based on lattice cryptosystem [5–7], the anti-quantum performance of the protocols is based on the related difficult problems such as the shortest vector and learning with errors in a lattice-based cryptosystem. The authentication and key agreement protocol based on lattice cryptosystem can also resist various threats brought by quantum computers in the post-quantum era, and can ensure the security of wireless networks, which is a hot issue in anti-quantum algorithms [8–15]. The difficult problem of a lattice-based cryptosystem is that it plays a key role in information security in wireless networks in the future quantum era [16–18]. Based on the difficult problems of lattice-based cryptosystem, many fully homomorphic encryption schemes [19–24] and public-key encryption schemes [25–27] are presented.

In the past decade, many schemes of anti-quantum authentication and security protocols based on the difficult problems of lattice cryptosystem have been proposed [28–34]. In 2016, Bansarkhani et al. [5]. Based on lattice cryptosystem, a new anti-quantum authentication signature protocol is proposed, and the authentication protocol is applied to block chain security. In 2018, Behina et al. [35]. From the difficult problem of lattice-based cryptosystem, an effective key searchable security authentication scheme is proposed, the key searchable security authentication scheme uses a new strategy to search keywords such as keys. In 2019, Fukumitsu et al. [7]. Based on the difficulty of lattice cryptosystem, a secure and efficient authentication signature protocol is proposed, which is proved to be secure in the random model, which is a three-round scheme with the public key aggregation with the security proof, A group signatures scheme without NIZK (Non-Interactive Zero Knowledge) base on lattice was designed [36], but this group signatures scheme requires a combination of attribute-based encryption and signatures. Ma et al. [10]. Based on lattice cipher, an effective anti-quantum authentication signature protocol for blockchains is proposed, which is a four-round scheme with the key aggregation and Tso et al. [12]. An effective anti-quantum blind signature protocol based on attributes from lattices is proposed, which is the attribute-based signature. In 2020, Kansal et al. [9]. Based on the difficulty of lattice cryptosystem, an effective anti-quantum authentication signature scheme is proposed, which is a round optimal secure authentication scheme. In 2020, Sun et al. [37]. Proposed an effective anti-quantum lattice cipher group signature authentication protocol based on zero knowledge proofs. Canard et al. [38]. Proposed an anti-quantum group signature authentication protocol with secure data fixed length based on lattice cryptosystem. The protocol is proved to be secure under the standard model. In 2020, Doss et al. [39]. Proposed a secure and effective meme optimization method based on lattice public key cryptosystem, which is used to transmit important medical privacy information in block chain and the internet of things that can resist the key exchange. The application of the attribute-based authentication scheme also includes hierarchical electronic voting for multiple regions, robust reversible audio watermarking for telemedicine and privacy protection, and much more [40]. At present, many scholars are studying anti-quantum secure signature and authentication protocols based on lattice cryptosystem, such as the quantum-resistant batch verifiable data privacy security authentication protocol of VANETs (Vehicular Ad Hoc Networks) using lattice [8].

Hence, it is of great significance to construct a secure authentication protocol based on the difficult problem of lattice cryptosystem. In this paper, an effective attribute-based authentication protocol is proposed, which supports full homomorphic encryption of information. The length of the public-private key pair in this protocol is short, and the corresponding computational overhead is reduced.

2 Preliminaries

2.1 Lattice

The general definition in these lattices can be expressed as: randomly select a prime number $q_s \geq 2$ and a matrix $B \in \mathbb{Z}_q^{n\times m}$. The specific definition is as follows:

$$\Lambda_{qs}^{\perp}(B) = \{e \in \mathbb{Z}^m : B \cdot e = 0 \bmod q_s\}$$

$$\Lambda_{qs}^{u}(B) = \{e \in \mathbb{Z}^m : B \cdot e = u \bmod q_s\}$$

2.2 The LWE Problem

Definition 1 (LWE Problem [17]). Enter a random integer $q_s = q(n) \geq 2$ and a random Gaussian distribution $\sigma_s = \sigma(n)$ in the $\mathbb{Z}_{q_s}$, the LWE problem is possible to distinguish the following different distributions:

$$(B, Bu + y) \quad and \quad (B, x)$$

where $B \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$, $u \xleftarrow{\$} \mathbb{Z}_q^n$, $y \xleftarrow{\$} \chi^m, x \xleftarrow{\$} \mathbb{Z}_q^m$.

Connection with lattices. Suppose $C = C(m) \in \mathbb{N}$. Some Gaussian distributions $\sigma = \sigma(m)_{m\in\mathbb{N}}$ is called C-bounded as follow:

$$\Pr[\sigma \in \{-C, \cdots, C-1, C\}] = 1.$$

There is a C-bounded Gaussian distribution σ such that solving the LWE problem is as same hard as under the worst-case lattice problems to the factor in $\widetilde{O}(m \cdot q_s/C)$ [17,18].

2.3 Lattice Algorithms

Lemma 1 ([31]) SampleLeft:

Randomly select the matrixes C in $\mathbb{Z}_q^{n\times m}$ and D in $\mathbb{Z}_q^{n\times m_1}$, select a grid base T_C of $\Lambda_q^{\perp}(C)$, a short vector $v \in \mathbb{Z}_q^n$, and the parameter β.

Suppose $G := (C||D)$. The algorithm SampleLeft(C, D, T_D, v, β) outputs the short vector $u \in \mathbb{Z}^{m+m_1}$ over Λ_{G+v}.

Lemma 2 ([31]) SampleRight:

Randomly select the matrixes C in $\mathbb{Z}_q^{n\times k}$, H in $\mathbb{Z}_q^{k\times m}$ and D in $\mathbb{Z}_q^{n\times m}$, select a grid base T_D of $\Lambda_q^{\perp}(D)$, a short vector $v \in \mathbb{Z}_q^n$, and the parameter β.

Suppose $G := (C||D)$. The algorithm SampleRight (C, D, T_D, v, β) the short vector $u \in \mathbb{Z}^{m+k}$ over Λ_{G+v}.

Lemma 3 [29] $Eval_{PK}$ and $Eval_{CT}$:

1. $Eval_{PK}$: Randomly select the matrixes $A_1, A_2, \cdots, A_l, B_1, B_2, \cdots, B_t \in \mathbb{Z}_q^{n\times m}$, and select a formula $f_\gamma : \{0,1\}^l \times \mathbb{Z}_q^t \to \mathbb{Z}_q$, the algorithm $Eval_{PK}$ calculates matrix $A_{f_\gamma} \in \mathbb{Z}_q^{n\times m}$.
2. Eval_{ct}: Randomly select the matrixes $A_1, A_2, \cdots, A_l, B_1, B_2, \cdots, B_t \in \mathbb{Z}_q^{n\times m}$, and select a formula $f_\gamma : \{0,1\}^l \times \mathbb{Z}_q^t \to \mathbb{Z}_q$, due to the $ID \in \{0,1\}^l$ and some vectors $u_1, u_2, \cdots, u_l, v_1, v_2, \cdots, v_t \in \mathbb{Z}_q^m$, the algorithm Eval_{ct} calculates the vector $u_{f_\gamma} \in \mathbb{Z}_q^m$.

3 Attribute-Based Authentication Scheme

Based on the partial hidden predicate encryption protocol based on the difficult problem of lattice cryptosystem, a new attribute-based anti-quantum authentication protocol (*ABAS*) is proposed. The partial implicit predicate encryption protocol based on lattice cryptosystem used in this paper is effective and anti-quantum secure, the detailed process of the scheme is shown in [28,29]. An algorithm for generating two user communication keys is added to our attribute-based anti-quantum authentication protocol, which is based on a symmetric key of a symmetric cryptosystem, and the key length can be controlled by selecting different parameters through the generation algorithm. The attribute-based authentication scheme for a predicate universe C, a symmetric cryptosystem communication key space k_{sc}, and there are five other algorithms (*ABAS*.**Setup,** *ABAS*.**Enc,** *ABAS*.**Keygen,** *ABAS*.**Dec**).

In the section, it is proposed that the public key, common parameter, and master key of all users are generated by the algorithm *ABAS*.**Setup**. Where A_i^j, B_i^j, P_i^j, i represent the i component, j represents the common parameter of the j user, and ID^j represents the identity of the j user. The specific process is as follows:

ABAS.**Setup**$(1^\lambda, 1^t, 1^l, 1^d, 1^Q)$: Given as input the important parameters λ, t, d, the length l and private attributes t respectively. The algorithm *ABAS*.**Setup** outputs some parameters and the most important core key of our attribute-based anti-quantum authentication protocol, the specific process of the *ABAS*.**Setup** is as follows:

1. Randomly select some important parameters (q, m, n, s, u, ρ, N):

   $n \geq d'(k)^{1/\varepsilon}$

   $q = \widetilde{O}(tnd)^{O(d)}$

   $m = O(n \log q)$

   $s = (tn \log q)^{O(d)}$

2. Choose some important random matrices:

   $ID^j \in \{0,1\}^l,\ j = 1, 2, \cdots, z$

   $A_i^j \in \mathbb{Z}_q^{n \times m}$ for $i = 1, 2, \cdots, l,\ j = 1, 2, \cdots, z$

   $B_i^j \in \mathbb{Z}_q^{n \times m}$ for $i = 1, 2, \cdots, t,\ j = 1, 2, \cdots, z$

   $P_i^j \in \mathbb{Z}_q^{n \times m}$ for $i = 1, 2, \cdots, N,\ j = 1, 2, \cdots, z$

3. Sampling matrix with algorithm *TrapGen* [30]: randomly select some important parameters $(1^m, 1^n, q)$, the algorithm *TrapGen* outputs the (A, T_A).
4. The algorithm outputs some parameters and the most important core key of the scheme:

   $ABAS.mpk = (\{A_i^j\}_{i\in[l],j\in[z]}, \{B_i^j\}_{i\in[t],j\in[z]}, A, \{P_i^j\}_{i\in[N],j\in[z]}, \{ID^j\}_{j\in[z]})$,

   $ABAS.msk = (T_A)$

The private key of the scheme for the user is generated using those public parameters generated above, where SK_j represents the private key of the j user.

$ABAS.\mathbf{Keygen}(ABAS.msk, f^j_{\gamma_j})$: Randomly select the circuit of the j user $f^j_{\gamma_j}$ and the most important core key of our attribute-based anti-quantum authentication protocol, output the private key $sk^j_{f^j_{\gamma_j}}$ of the j-th user. The specific process of the algorithm $ABAS.\mathbf{Keygen}$ is as follows:

1. Compute the parameter $(A^j_{f^j_{\gamma_j}})_{j\in[z]}$ with algorithm $\mathrm{Eval}_{\mathrm{PK}}$.

   $(A^j_{f^j_{\gamma_j}})_{j\in[z]} = \mathrm{Eval}_{\mathrm{PK}}(\{A^j_i\}_{i\in[l],j\in[z]}, \{B^j_i\}_{i\in[t],j\in[z]}, f^j_{\gamma_j})$

2. Sample a random subset $\Delta \subset [N]$ with $|\Delta| = u$, and respectively compute the sum of subset Δ $P^j_\Delta = \sum_{i\in\Delta} P^j_i, j = 1, 2, \cdots, z$.
3. Sampling the key with algorithm SampleLeft: $\begin{bmatrix} K^j_1 \\ K^j_2 \end{bmatrix} \leftarrow \mathrm{SampleLeft}\left(A, A^j_{f^j_{\gamma_j}} + \gamma_j G, T_A, P^j_\Delta, s\right)$ where s is a Gaussian parameter, and

   $\left[A \middle| A^j_{f^j_{\gamma_j}} + \gamma_j G\right]\begin{bmatrix} K^j_1 \\ K^j_2 \end{bmatrix} = P^j_\Delta.$

4. Let $SK_j = \begin{bmatrix} K^j_1 \\ K^j_2 \end{bmatrix}, j = 1, 2, \cdots, z$, and output the private key $sk^j_{f^j_{\gamma_j}}$ of the j-th user $sk^j_{f^j_{\gamma_j}} = (\Delta, SK_j)$, $j = 1, 2, \cdots, z$.

Take Alice and Bob as an example, Alice and Bob are necessary to authenticate each other before finally generating a symmetric key for communication, which is jointly generated by the Alice private attributes x^a and Bob private attributes x^b. The symmetric key authentication for communication is as follows: if Alice and the first user communicate for the first time, the partial communication key associated with Alice should be negotiated first. The partial communication key associated with the Alice negotiation process is as follows: assuming that Alice is the initiator of the communication, Alice first uses the hash algorithm H_1 to generate the message m_a associated with private attributes x^a, and then encrypts the message m_a using the public key of Bob, then sends the ciphertext c_{ID^a} to Bob. The specific negotiation process is as follows:

$ABAS.\mathbf{Enc}(ABAS.mpk, (x^a, ID^a), H_1)$. The $ABAS.\mathbf{Enc}$ algorithm gets as input $ABAS.mpk$, $x^a \in \{0,1\}^t$, the identification $ID^a \in \{0,1\}^l$ and the hash function H_1, out the ciphertext c_{ID^a}. The specific process of the algorithm $ABAS.\mathbf{Enc}$ is as follows:

1. Sample a Gaussian parameter $s \leftarrow D_{\mathbb{Z}^n, s_B}$, two Gaussian parameters $e \leftarrow D_{\mathbb{Z}^m, s_B}$, $e'_k \leftarrow D_{\mathbb{Z}^m, s_D}$ and $k \in [N]$.
2. Choose a security hash function $H_1 : \{0,1\}^* \rightarrow \{v_1 : v_1 \in \{0,1\}^{\tau_1}\}$.
3. Compute the message m_a associated with x^a: $m_a = H_1(x^a)$
4. Select a parameter b, and set $b = [0, 0, \cdots, 0, \lceil q/2 \rceil m_a]^{\mathrm{T}} \in \mathbb{Z}^m_q$. Compute

   $\beta_0 = A^{\mathrm{T}} s + e$

   $\beta_{1,k} = P^{\mathrm{T}}_k s + e'_k + b, k \in [N]$

5. Random sampling t matrices $R'_i \xleftarrow{\$} \{-1, 1\}^{m\times m}$, Where $i = 1, 2, \cdots, t$, compute:

   $v_i = (B_i + x^a_i G)^{\mathrm{T}} s + (R'_i)^{\mathrm{T}} e$

6. Random sampling l matrices $R_i \xleftarrow{\$} \{-1,1\}^{m\times m}$, where $i = 1, 2, \cdots, l$, compute:

   $u_i = (A_i + ID_i^a G)^{\mathrm{T}} s + (R_i)^{\mathrm{T}} e$

7. Finally, out the encrypted ciphertext c_{ID^a}:

   $c_{ID^a} = (H_1, ID^a, \beta_0, \{\beta_{1,k}\}_{k\in[N]}, \{u_i\}_{i\in[l]}, \{v_i\}_{i\in[l]})$

After receiving the ciphertext c_{ID^a}, which is sent by Alice, Bob decrypts the data c_{ID^a} using private key SK_b, the specific process is as follows:

$ABAS.\mathbf{Dec}(sk_{f_{\gamma_b}^b}, c_{ID^a})$. The $ABAS.\mathbf{Dec}$ algorithm inputs ciphertext c_{ID^a}, the public part of the attribute ID^a and own secret key $sk_{f_{\gamma_b}^b}$, output the partial communication key associated with Alice. The specific process is:

1. Based on these parameters $(ID^a, \{u_i\}, \{v_i\})$, use $\mathrm{Eval}_{\mathrm{ct}}$ to compute $u_{f_{\gamma_b}^b}$:

   $u_{f_{\gamma_b}^b} = \mathrm{Eval}_{\mathrm{ct}}(\{A_i^j, u_i\}_{i\in[l],j\in[z]}, \{B_i^j, v_i\}_{i\in[l],j\in[z]}, f_{\gamma_b}^b, ID^a)$.

2. Compute:

   $$\eta = \sum\nolimits_{k\in[N]} \beta_{1,k} - SK_b \begin{pmatrix} \beta_0 \\ u_{f_{\gamma_b}^b} \end{pmatrix}.$$

3. If

   $[\mathrm{Rd}(\eta[1]), \mathrm{Rd}(\eta[2]), \cdots, \mathrm{Rd}(\eta[m-1])] = 0,$

   Then set $\mu = \mathrm{Rd}(\eta[m])$ and output μ. Otherwise, termination $\perp$.

4. Compute the partial communication key associated with Alice: $m_a = \mu$.

The partial communication key associated with the Bob negotiation process is as follows: Alice uses the hash function H_1 to generate the data m_b associated with private attributes x^b, and then encrypts the message m_b with Bob's public key, and then sends the ciphertext c_{ID^b} to Bob. Then, Bob can use the hash algorithm H_2 to generate the symmetric key for communication k_{sc}^{ab}.The specific process is as follows:

$ABAS.\mathbf{Enc}(ABAS.mpk, (x^b, ID^b), H_1, H_2)$. The $ABAS.\mathbf{Enc}$ algorithm gets as input $ABAS.mpk$, the attributes $x^b \in \{0,1\}^t$, $ID^b \in \{0,1\}^l$ and the hash function H_1 and H_2, output the ciphertext c_{ID^b}. The specific process is as follows:

1. Sample a Gaussian parameter $s \leftarrow D_{\mathbb{Z}^n, s_B}$, two Gaussian parameters $e \leftarrow D_{\mathbb{Z}^m, s_B}$ and $e_k^{'} \leftarrow D_{\mathbb{Z}^m, s_D}$, where $k = 1, 2, \cdots, N$.
2. Compute the message m_b associated with x^b: $m_b = H_1(x^b)$
3. Select a parameter b', and set $b' = [0, 0, \cdots, 0, \lceil q/2 \rceil m_b]^{\mathrm{T}} \in \mathbb{Z}_q^m$. Compute:

   $\beta_0 = A^{\mathrm{T}} s + e$

   $\beta_{1,k} = P_k^{\mathrm{T}} s + e_k^{'} + b', k \in [N]$

4. Random sampling t matrices $R_i^{'} \xleftarrow{\$} \{-1,1\}^{m\times m}$, where $i = 1, 2, \cdots, t$, compute:

   $v_i = (B_i + x_i^b G)^{\mathrm{T}} s + (R_i^{'})^{\mathrm{T}} e$

5. Random sampling l matrices $R_i \xleftarrow{\$} \{-1,1\}^{m\times m}$, where $i = 1, 2, \cdots, l$, compute:

$$u_i = (A_i + ID_i^b G)^{\mathrm{T}} s + (R_i)^{\mathrm{T}} e$$

6. Choose a hash algorithm $H_2 : \{0,1\}^* \to \{v_2 : v_2 \in \{0,1\}^{\tau_2}\}$.
7. Compute the symmetric communication key with Bob: $k_{sc}^{ab} = H_2(m_a, m_b)$
8. Out the ciphertext

$$c_{ID^b} = (H_2, ID^b, \beta_0, \{\beta_{1,k}\}_{k\in[N]}, \{u_i\}_{i\in[l]}, \{v_i\}_{i\in[l]})$$

After receiving the ciphertext c_{ID^b}, which is sent by Bob, Alice decrypts the data c_{ID^b} with private key SK_a, and compute the symmetric communication key with Bob, the specific process is as follows:

ABAS.**Dec** $(sk_{f_{\gamma_a}^a}, c_{ID^b})$. The *ABAS*.**Dec** algorithm gets as input the ciphertext c_{ID^b}, the attribute ID^b, the secret key $sk_{f_{\gamma_a}^a}$, and the hash function H_2, output the authentication symmetric key. The specific process is as follows:

1. Using $(ID^b, \{u_i\}, \{v_i\})$, apply the $\mathrm{Eval}_{\mathrm{ct}}$ algorithm to compute:

$$u_{f_{\gamma_a}^a} = \mathrm{Eval}_{\mathrm{ct}}(\{A_i^j, u_i\}_{i\in[l],j\in[z]}, \{B_i^j, v_i\}_{i\in[l],j\in[z]}, f_{\gamma_a}^a, ID^b)$$

2. Compute

$$\eta = \sum\nolimits_{k\in[N]} \beta_{1,k} - SK_a \begin{pmatrix} \beta_0 \\ u_{f_{\gamma_a}^a} \end{pmatrix}$$

3. Round computes each datum of η. If

$$[\mathrm{Rd}(\eta[1]), \mathrm{Rd}(\eta[2]), \cdots, \mathrm{Rd}(\eta[m-1])] = 0$$

Then set $\mu' = \mathrm{Rd}(\eta[m])$ and output μ'. Otherwise, termination $\perp$.

4. Compute the partial communication key associated with Bob: $m_b = \mu'$.
5. Compute the symmetric communication key with Bob: $(k_{sc}^{ab})' = H_2(m_a, m_b)$.

Finally, the whole attribute-based authentication Scheme is over, and Alice and Bob can communicate securely with the authentication symmetric key $(k_{sc}^{ab})' = k_{sc}^{ab}$.

4 Analysis

4.1 Correctness

The correctness of Alice to Bob's partial authentication in the *ABAS* follows from our choice of parameters. The specific process is as follows:

$$\begin{aligned} u_{f_{\gamma_b}^b} &= \mathrm{Eval}_{\mathrm{ct}}(\{A_i^j, u_i\}_{i\in[l],j\in[z]}, \{B_i^j, v_i\}_{i\in[l],j\in[z]}, f_{\gamma_b}^b, ID^a) \\ &= (A_{f_{\gamma_b}^b}^b + f_{\gamma_b}^b(x, ID^a) \cdot G)^{\mathrm{T}} \cdot s + e_{\mathrm{Eval}}. \end{aligned}$$

If $f_{\gamma_b}^b(x, ID^a) = \gamma_b \bmod q$, then

$$\begin{pmatrix} \beta_0 \\ u_{f_{\gamma_b}^b} \end{pmatrix} = \begin{pmatrix} A^{\mathrm{T}} \\ (A_{f_{\gamma_b}^b}^b + \gamma_b \cdot G)^{\mathrm{T}} \end{pmatrix} \cdot s + \begin{pmatrix} e \\ e_{\mathrm{Eval}} \end{pmatrix}.$$

Compute

$$(SK_b)^{\mathrm{T}} \cdot \begin{pmatrix} \beta_0 \\ u_{f^b_{\gamma_b}} \end{pmatrix} = P^b_{\Delta} \cdot s + (SK_b)^{\mathrm{T}} \cdot \begin{pmatrix} e \\ e_{\mathrm{Eval}} \end{pmatrix},$$

$$\sum\nolimits_{k\in[N]} \beta_{1,k} - (SK_b)^{\mathrm{T}} \cdot \begin{pmatrix} \beta_0 \\ u_{f^b_{\gamma_b}} \end{pmatrix} = b + \sum\nolimits_{k\in[N]} e'_k - (SK_b)^{\mathrm{T}} \cdot \begin{pmatrix} e \\ e_{\mathrm{Eval}} \end{pmatrix}.$$

If the first $m-1$ coordinates of $\sum_{k\in[N]} e'_k - (SK_b)^{\mathrm{T}} \cdot \begin{pmatrix} e \\ e_{\mathrm{Eval}} \end{pmatrix}$ are less than $q/4$, which means that the correctness of Alice to Bob's partial authentication.

Otherwise, if $f^b_{\gamma_b}(x, ID^a) = \gamma^*_b \neq \gamma_b \bmod q$, then setting $\gamma'_b = \gamma^*_b + \gamma_b$ for γ^*_b, so

$$\eta = \sum\nolimits_{k\in[N]} \beta_{1,k} - (SK_b)^{\mathrm{T}} \cdot \begin{pmatrix} \beta_0 \\ u_{f^b_{\gamma_b}} \end{pmatrix} = b + \gamma^*_b \cdot (SK_b)^{\mathrm{T}} \cdot G + e^*.$$

Therefore, with overwhelming probability from the No.1 to No.$m-1$ parameters of η are less than $q/4$.

The security of Bob to Alice's other partial authentication in the $ABAS$ is the same as above.

So, the symmetric communication key of Bob and Alice is:

$$k^{ab}_{sc} = H_2(m_a, m_b) = (k^{ab}_{sc})'.$$

4.2 Security

The specific process of the security of Alice to Bob's partial authentication in the $ABAS$ is as follows:

Proof. First, we describe the auxiliary evaluation algorithms of the proof.

$ABAS.\mathrm{Setup}^*_1$: The specific process is as follows:

1. Sampling matrix with algorithm *TrapGen* [30]: randomly select some important parameters $(1^m, 1^n, q)$, the algorithm *TrapGen* outputs the (A, T_A).
2. Random sample l parameters $R_i \xleftarrow{\$} \{-1, 1\}^{m\times m}$, compute $A_i = AR_i - ID^b_i G \in \mathbb{Z}^{n\times m}_q$, where $i = 1, 2, \cdots, l$.
3. Random sample t parameters $R'_i \xleftarrow{\$} \{-1, 1\}^{m\times m}$, compute $B_i = AR'_i - x_i G \in \mathbb{Z}^{n\times m}_q$, where $i = 1, 2, \cdots, t$.
4. Random choose some subsets $\Delta^*_1, \Delta^*_2, \cdots \Delta^*_{i'}, \cdots, \Delta^*_{Q'}$ the size of each subset is v, which has the unique index, where $i' = 1, 2, \cdots, Q'$.
5. Sample some random matrices $P^b_k \in \mathbb{Z}^{n\times m}_q$ make them satisfied with $P^b_{\Delta^*_i} = \sum_{k\in\Delta^*_i} P^b_k$, where $i' = 1, 2, \cdots, Q'$ and $k = 1, 2, \cdots, N$.
6. Sample the private key $SK^*_i \leftarrow (D_{\mathbb{Z}^{2m},s})^m$ and compute:

$$P^{b,*}_k = \left[A \left| A^{b,*}_{f^{b,*}_{\gamma^{b,*}_i}} + \gamma^{b,*}_i G \right. \right] \begin{bmatrix} K^{b,*}_{1,i} \\ K^{b,*}_{2,i} \end{bmatrix} = \left[A \left| AR^{b,*}_{f^{b,*}_{\gamma^{b,*}_i}} \right. \right] \begin{bmatrix} K^{b,*}_{1,i} \\ K^{b,*}_{2,i} \end{bmatrix} \forall i \in [Q']$$

where $SK^{b,*}_i = \begin{bmatrix} K^{b,*}_{1,i} \\ K^{b,*}_{2,i} \end{bmatrix}$.

7. Output necessary public key of our scheme as

$$ABAS.mpk = (\{A^b_i\}_{i\in[l]}, \{B^b_i\}_{i\in[t]}, A, \{P^b_i\}_{i\in[N]})$$

And the most important core key of our scheme as

$$ABAS.msk = (T_A, \{R_i^b\}_{i\in[l]}, \{R_i^{b,'}\}_{i\in[l]}, \{SK_i^{b,*}\}_{i\in[N]})$$

$ABAS.\text{Enc}_1^*$: The specific process is as follows:

1. Sample a Gaussian parameter $s \leftarrow D_{\mathbb{Z}^n,s_B}$, two Gaussian parameters $e \leftarrow D_{\mathbb{Z}^m,s_B}$ and $e_k'' \leftarrow D_{\mathbb{Z}^m,s_D}$, where $k = 1, 2, \cdots, N$.
2. Select a parameter b', and set $b = [0, 0, \cdots, 0, \lceil q/2 \rceil k_{ab}]^{\mathrm{T}} \in \mathbb{Z}_q^m$. Compute:

   $\beta_0 = A^{\mathrm{T}}s + e$

   $\beta_{1,k} = (SK_k^b)^{\mathrm{T}}\beta_0 + e_k'' + b, k \in [N]$.
3. Compute the u_i:

   $u_i = (R_i)^{\mathrm{T}}\beta_0$, where, $i = 1, 2, \cdots, l$.
4. Random sampling t matrices $R_i \xleftarrow{\$} \{-1, 1\}^{m\times m}$, compute the v_i:

   $v_i = (R_i^{'})^{\mathrm{T}}\beta_0$, Where, $i = 1, 2, \cdots, t$.
5. Final output the encrypted ciphertext

   $(H, ID^a, \beta_0, \{\beta_{1,k}\}_{k\in[N]}, \{u_i\}_{i\in[l]}, \{v_i\}_{i\in[t]})$.

$ABAS.\text{KeyGen}_1^*$: The $ABAS.\text{KeyGen}_1^*$ has a special function that will be marked if some public and private key pairs have been questioned before. The specific process is as follows:

1. Compute the key corresponding to $f_{\gamma_b}^b$ as:

   $A_{f_{\gamma_b}^b} \leftarrow \text{Eval}_{\text{PK}}(\{A_i^b\}, \{B_i^b\}, f_{\gamma_b}^b)$
2. We know that $A_{f_{\gamma_b}^b} = AR_{f_{\gamma_b}^b} - \left\langle x, \hat{f}\left(ID^b\right)\right\rangle G$. For different key query, the specific process is as follows:

1) A $f_{\gamma_b}^b$ such that $f_{\gamma_b}^b\left(x, \hat{f}\left(ID^b\right)\right) = 0$. Then:

$$\left[A \left| A_{f_{\gamma_b}^b} + \rho G\right.\right] = \left[A \left| AR_{f_{\gamma_b}^b} + \left(\rho - \left\langle x, \hat{f}\left(ID^b\right)\right\rangle\right) G\right.\right].$$

Let

$$SK \leftarrow \text{SampleRight}\left(A, \left(\rho - \left\langle x, \hat{f}\left(ID^b\right)\right\rangle\right).G, R_{f_{\gamma_b}^b}, T_G, \sum_{k\in[N]} \Delta_k P_{\Delta}^k, s\right).$$

Therefore that:

$$\left[A \left| A_{f_{\gamma_b}^b} + \rho G\right.\right]\begin{bmatrix} K_1^b \\ K_2^b \end{bmatrix} = \sum_{k\in[N]} \Delta_k P_{\Delta}^k$$

Return $\begin{bmatrix} K_1^b \\ K_2^b \end{bmatrix}$.

2) The $f^{b,*}_{\gamma_i^{b,*}}$, such that $\left\langle x, \hat{f}^* \left(ID^{b,*}\right)\right\rangle = \gamma_i^{b,*}$, in which case, return $\begin{bmatrix} K_{1,i}^{b,*} \\ K_{2,i}^{b,*} \end{bmatrix}$.

$ABAS.\text{KeyGen}_2^*$: In the realistic simulation, the algorithm $ABAS.\text{KeyGen}_2^*$ will select the No.0 public-private key pair, while in algorithm $ABAS.\text{KeyGen}_1^*$, the No.1 public-private key pair will be selected.

$ABAS.\text{Enc}_2^*$: The game simulation $ABAS.\text{Enc}_2^*$ random switch the ciphertext data β_0. The algorithm $ABAS.\text{Enc}_1^*$ will generate all the elements and data that need to be encrypted by itself.

$ABAS.\text{Enc}_3^*$: The simulation $ABAS.\text{Enc}_3^*$ random change these ciphertext data $\{u_i\}, \{v_i\}$.

$ABAS.\text{Setup}_2^*$: The real simulation $ABAS.\text{Setup}_2^*$ random chose the public data $\{B_j\}$, A. The game simulation random chose the data A_i^b, P_i^b.

Now, we describe a sim algorithm, which claims that the result of the real algorithm is indistinguishable from game simulation through the following hybrids.

(1). The first case that satisfies indistinguishable situation is the following two simulation algorithm:

Algorithm 0: The realistic simulation.

Algorithm 1: The simulation $ABAS.\text{Setup}_1^*$ replaces the game simulation $ABAS.\text{Setup}$. The simulation $ABAS.\text{Setup}_1^*$ outputs some parameters and the most important core key of our attribute-based anti-quantum authentication protocol using (x, ID^a) and $\{f^b_{\gamma_{b,i}}\}_{i\in[Q']}$.

(2). The second case that satisfies indistinguishable situation is the following two simulation algorithm:

Algorithm 1: This algorithm is the same as algorithm 1 in the first case.

Algorithm 2: The game simulation $ABAS.\text{Enc}_1^*$ replaces the $ABAS.\text{Enc}$. The $ABAS.\text{Enc}_1^*$ compute the data β_0, and the $ABAS.\text{Enc}$ compute the public-private key pair of the scheme.

(3). The third case that satisfies indistinguishable situation is the following two simulation algorithm:

Algorithm 2: This algorithm is the same as algorithm 2 in the second case.

Algorithm 3: The game simulation $ABAS.\text{KeyGen}_1^*$ replaces the $ABAS.\text{KeyGen}$, and using the lattice basis T of other matrices instead of A.

(4). The fourth case that satisfies indistinguishable situation is the following two simulation algorithm:

Algorithm 3: This algorithm is the same as algorithm 3 in the third case.

Algorithm 4: The algorithm $ABAS.\text{Enc}_2^*$ replaces the $ABAS.\text{Enc}_1^*$. The algorithm $ABAS.\text{Enc}_2^*$ random switches the data β_0, which is encrypted.

(5). The fifth case that satisfy indistinguishable situation is the following two simulation algorithm:

Algorithm 4: This algorithm is the same as algorithm 4 in the fourth case.

Algorithm 5: The game simulation $ABAS.\text{KeyGen}_2^*$ replaces the $ABAS.\text{KeyGen}_1^*$. The $ABAS$ .KeyGen_2^* is mostly the same as the algorithm $ABAS$.KeyGen, except for the $\{f_{\gamma_{b,i}}^{b,*}\}_{i\in[Q']}$ corresponding to the public-private key pair.

(6). The sixth case that satisfy indistinguishable situation is the following two ism algorithm:

Algorithm 5: This algorithm is the same as algorithm 5 in the fifth case.

Algorithm 6: The game simulation $ABAS.\text{Enc}_3^*$ replaces the $ABAS.\text{Enc}_2^*$. The $ABAS.\text{Enc}_3^*$ random change these ciphertext data $\{u_i\}, \{v_i\}$.

(7). The seventh case that satisfy indistinguishable situation is the following two ism algorithm:

Algorithm 6: This algorithm is the same as algorithm 6 in the sixth case.

Algorithm 7: The game simulation $ABAS.\text{Setup}_2^*$ replaces the $ABAS.\text{Setup}_1^*$.

A detailed proof of indistinguishability (1) –(7) is provided in the references [23,29]. The security of Bob with Alice's other partial authentication in the $ABAS$ is the same as above, this completes the security proof.

4.3 Performance Analysis

Next, we compare our attribute-based authentication scheme with other related secret key schemes [6,13,14,22]. We mainly focus on the computational costs, storage overhead, and several security properties.

As depicted in Table 1, we compare the storage overhead and other related secret key schemes. The public key parameter' size is $m^2 \log q$ in [6], is $4n \log q$ in [13], is $(2l+9)m^2 \log q$ in [14], is $2lm^2 \log q$ in [22], and is $2n(t+l+k) \log q$ in our attribute-based authentication scheme. For the length of public-private key pair, our attribute-based authentication scheme based on the concealable partial predicate encryption, that is gates thereby further reducing the complexity of the formula. The length of public-private key pair in the attribute-based authentication scheme only related to the complexity of the formula, which helps to reduce the secret key length.

Table 1: Storage overheads of all schemes

Scheme	Private key size	Public key size
[6]	$(n + nt) \log q$	$m^2 \log q$
[13]	$n \log q$	$4n \log q$
[14]	$3m^2 \log q$	$(2l + 9)m^2 \log q$
[22]	$2m^2 \log q$	$2lm^2 \log q$
$ABAS$(Our)	$2m \log q$	$2n(t + l + k) \log q$

In Table 2, the SM represents the standard model, and the SCPA represents the selective chosen plaintext attack, the NTRU represents the number theory research unit, and the CVP represents the closest vector problem. We compare the security properties and other related secret key schemes, according to the Table 1, Li et al. [13] is more effectivie than our attribute-based authentication scheme over lattice in terms of computational storage, which is based on NTRU lattice, so it lacks provable security. Gentry et al. [22], Wang et al. [14] and Brakerski et al. [6] Schemes are slightly weaker than our attribute-based authentication scheme over lattice in terms of computational complexity and storage.

Moreover, our scheme is based on partially hiding predicate encryption, so the key size is also efficient, and our scheme is provably security of $(Q, poly)$ based on the LWE problem. Therefore, our attribute-based authentication scheme is more secure resistance to quantum computers than over schemes.

Table 2: Security properties of all schemes

Scheme	Assumption	Provable security	Postquantum
[6]	SM SCPA	YWS	YWS
[13]	NTRU CVP	NO	YWS
[14]	SM SCPA	YWS	YWS
[22]	SM SCPA	YWS	YWS
ABAS(our)	LWE	YWS	YWS

5 Citations

Based on the LWE hard problem over lattice cryptosystem, an anti-quantum authentication scheme for wireless networks is proposed in this paper. In the attribute-based authentication scheme, there is a certain correlation between the authenticated data and the attribute values of the users in the scheme. For the length of public-private key pair, in our attribute-based authentication scheme based on the concealable partial predicate encryption, that is gates thereby further reducing the complexity of the formula. The length of public-private key pair only related to the complexity of the formula in the scheme, which helps to reduce the secret key length. Future work, we will continue to explore and design anti-quantum authentication protocols based on lattice cryptosystem, which is an anti-quantum sublattice cipher security protocol that will run more efficiently and have less storage space.

Funding Statement: This work was supported by the Special Project for Scientific and Technological Cooperation of Jiangxi Province [no. 20212BDH80021].

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. Azees, P. Vijayakumar and L. J. Deboarh, "EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467–2476, 2017.

[2] J. Zhang, J. Cui, H. Zhong, Z. Chen and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 722–735, 2021.

[3] H. Li, F. Guo, L. Wang, J. Wang, B. Wang *et al.,* "A blockchain-based public auditing protocol with self-certified public keys for cloud data," *Security and Communication Networks*, vol. 2021, no. 1, pp. 6623639–6623649, 2021.

[4] A. Yang, X. Tan, J. Baek and D. S. Wong, "A new ADS-B authentication framework based on efficient hierarchical identity-based signature with batch verification," *IEEE Transactions on Services Computing*, vol. 10, no. 2, pp. 165–175, 2017.

[5] R. El Bansarkhani and J. Sturm, "An efficient lattice-based multi signature scheme with applications to bitcoins," in *Proc. of the Int. Conf. on Cryptology and Network Security (CANS 2016)*, vol. 10052 of LNCS, Milan, Italy, pp. 140–155, 2016.
[6] Z. Brakerski, D. Cash D, R. Tsabary and H. wee, "Targeted homomorphic attribute-based encryption," in *Proc. of Theory of Cryptography (TCC 2016)*, Beijing, China, pp. 330–360, 2016.
[7] M. Fukumitsu and S. Hasegawa, "A lattice-based provably secure multi signature scheme in quantum random oracle model," in *Proc. of the 14th Int. Conf. on Provable and Practical Security (ProvSec 2020)*, Singapore, Singapore, pp. 45–64, 2020.
[8] S. Mukherjee, D. S. Gupta and G. Biswas, "An efficient and batch verifiable conditional privacy-preserving authentication scheme for VANETs using lattice," *Computing*, vol. 101, no. 12, pp. 1763–1788, 2019.
[9] M. Kansal and R. Dutta, "Round optimal secure multi signature schemes from lattice with public key aggregation and signature compression," in *Proc. of the 12th Int. Conf. on Cryptology in Africa (AFRICACRYPT 2020)*, Cairo, Egypt, pp. 281–300, 2020.
[10] C. Ma and M. Jiang, "Practical lattice-based multi signature schemes for blockchains," *IEEE Access*, vol. 7, pp. 179765–179778, 2019.
[11] P. Dupont, J. Hesse, D. Pointcheval, L. Reyzin and S. Yakoubov, "Fuzzy password-authenticated key exchange," in *Proc. of the 37th Annual Int. Conf. on the Theory & Applications of Cryptographic Techniques (EUROCRYPT 2018)*, Tel Aviv, Israel, pp. 393–424, 2018.
[12] R. Tso, Z. Liu and Y. Tseng, "Identity-based blind multi signature from lattices," *IEEE Access*, vol. 7, pp. 182916–182923, 2019.
[13] D. Li, H. Chen, C. Zhong, T. Li and F. Wang, "A new self-certified signature scheme based on ntrusing for smart mobile communications," *Wireless Personal Communications*, vol. 96, no. 3, pp. 4263–4278, 2017.
[14] G. Wang, Z. Liu Z and D. Gu, "Ciphertext policy attribute-based encryption for circuits from LWE assumption," in *Proc. of the 21st Int. Conf. on Information and Communications Security (ICICS 2019)*, Beijing, China, pp. 278–396, 2019.
[15] N. Tahat, A. K. Alomari, O. M. Al-Hazaimeh and M. F. Al-Jamal, "An efficient self-certified multi-proxy signature scheme based on elliptic curve discrete logarithm problem," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 23, no. 4, pp. 935–948, 2020.
[16] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proc. of the 37th Annual ACM Symp. on Theory of Computing, Association for Computing Machinery (STOC 2005)*, New York, NY, USA, pp. 84–93, 2005.
[17] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM*, vol. 56, no. 6, pp. 1–122, 2009.
[18] C. Peikert, "Public-key cryptosystems from the worst-case shortest vector problem," in *Proc. of the 41th Annual ACM Symp. on Theory of Computing, Association for Computing Machinery (STOC 2009)*, Bethesda, MD, USA, pp. 333–342, 2009.
[19] Z. Brakerski, A. Langlois, C. Peikert, O. Regev and D. Stehlé, "Classical hardness of learning with errors," in *Proc. of the 45th Annual ACM Symp. on Theory of Computing, Association for Computing Machinery (STOC 2013)*, New York, NY, USA, pp. 575–584, 2013.
[20] Z. Brakerski, C. Gentry and V. Vaikuntanathan, "(Leveled) fully homomorphic encryption without bootstrapping," in *Proc. of the 3rd Innovations in Theoretical Computer Science Conf. (ITCS 2012)*, Cambridge, MA, USA, pp. 309–325, 2012.
[21] L. Ducas and D. M. Fhew, "Bootstrapping homomorphic encryption in less than a second," in *Proc. of the 34th Annual Int. Conf. on the Theory & Applications of Cryptographic Techniques (EUROCRYPT 2015)*, Sofia, Bulgaria, pp. 617–640, 2015.
[22] C. Gentry, A. Sahai and B. Waters, "Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based," in *Proc. of the 33th Annual Int. Conf. on Cryptology (CRYPTO 2013)*, Santa Barbara, California, USA, pp. 75–92, 2013.
[23] S. Agrawal, "Stronger security for reusable garbled circuits, general definitions and attacks," in *Proc. of the 37th Annual Int. Conf. on Cryptology (CRYPTO 2017)*, Santa Barbara, CA, USA, pp. 3–35, 2017.

[24] R. Steinfeld, A. Sakzad and R. K. Zhao, "Practical MP-LWE-based encryption balancing security-risk versus efficiency," *Designs Codes and Cryptography*, vol. 87, pp. 2847–2884, 2019.
[25] A. Lombardi, V. Vaikuntanathan and T. D. Vuong, "Lattice trapdoors and IBE from middle-product LWE," in *Proc. of the Theory of Cryptography Conf. (TCC 2019)*, Nuremberg, Germany, pp. 24–54, 2019.
[26] A. Pellet-Mary, G. Hanrot and D. Stehlé, "Approx-SVP in ideal lattices with pre-processing," in *Proc. of the 38th Annual Int. Conf. on the Theory & Applications of Cryptographic Techniques (EUROCRYPT 2019)*, Darmstadt, Germany, pp. 685–716, 2019.
[27] S. Gorbunov, V. Vaikuntanathan and H. Wee, "Functional encryption with bounded collusions via multi-party computation," in *Proc. of the 32nd Annual Int. Conf. on Cryptology (CRYPTO 2012)*, Santa Barbara, CA, USA, pp. 162–179, 2012.
[28] Y. Ishai and H. Wee, "Partial garbling schemes and their applications," in *Proc. of the Int. Colloquium on Automata, Languages, and Programming (ICALP 2014)*, Copenhagen, Denmark, pp. 650–662, 2014.
[29] S. Gorbunov, V. Vaikuntanathan and H. Wee, "Predicate encryption for circuits from lwe," in *Proc. of the 35th Annual Int. Conf. on Cryptology (CRYPTO 2015)*, Santa Barbara, CA, USA, pp. 503–523, 2015.
[30] C. Gentry, C. Peikert and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. of the 40th Annual ACM Symp. on Theory of Computing, Association for Computing Machinery (STOC 2008)*, Victoria (BC), Canada, pp. 197–206, 2008.
[31] S. Agrawal, D. Boneh and X. Boyen, "Efficient lattice (H)IBE in the standard model," in *Proc. of the 29th Annual Int. Conf. on the Theory & Applications of Cryptographic Techniques (EUROCRYPT 2010)*, French Riviera, pp. 553–572, 2010.
[32] D. Cash, D. Hofheinz, E. Kiltz and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," *Journal of Cryptology*, vol. 25, no. 4, pp. 601–639, 2012.
[33] C. Baum, I. Damgård, V. Lyubashevsky, S. Oechsner and C. Peikert, "More efficient commitments from structured lattice assumptions," in *Proc. of the 11th Conf. on Security and Cryptography for Networks (SCN 2018)*, Amalfi, Italy, pp. 614–629, 2018.
[34] V. Lyubashevsky and G. Neven, "One-shot verifiable encryption from lattices," in *Proc. of the 36th Annual Int. Conf. on the Theory & Applications of Cryptographic Techniques (EUROCRYPT 2017)*, Paris, France, pp. 293–323, 2017.
[35] R. Behnia, M. O. Ozmen and A. A. Yavuz, "Lattice-based public key searchable encryption from experimental perspectives," *IEEE Transactions on Dependable Secure Compute*, vol. 17, no. 6, pp. 1269–1282, 2018.
[36] S. Katsumata and S. Y amada, "Group signatures without NIZK: From lattices," in *Proc. of the 38th Annual Int. Conf. on the Theory & Applications of Cryptographic Techniques (EUROCRYPT 2019)*, Darmstadt, Germany, pp. 312–344, 2019.
[37] Y. Sun and Y. Liu, "A lattice-based fully dynamic group signature scheme without NIZK," in *Proc. of the Information Security and Cryptology (INSCYPT 2020)*, Guangzhou, China, pp. 359–367, 2020.
[38] S. Canard, A. Georgescu, G. Kaim, A. R. Langlois and J. Traoré, "Constant-size lattice-based group signature with forward security in the standard model," in *Proc. of the 14th Int. Conf. on Provable and Practical Security (ProvSec 2020)*, Singapore, Singapore, pp. 24–44, 2020.
[39] S. Doss, J. Paranthaman, S. Gopalakrishnan, A. Duraisamy, S. Pal *et al.,* "Memetic optimization with cryptographic encryption for secure medical data transmission in IoT-based distributed systems," *Computers, Materials & Continua*, vol. 64, no. 2, pp. 1577–1594, 2021.
[40] X. Zhang, X. Sun, X. Sun, W. Sun and S. K. Jha, "Robust reversible audio watermarking scheme for telemedicine and privacy protection," *Computers, Materials & Continua*, vol. 71, no. 2, pp. 3035–3050, 2022.