IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 15 December 2022, accepted 23 January 2023, date of publication 27 January 2023, date of current version 1 February 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3240304

RESEARCH ARTICLE

LMIBE: Lattice-Based Matchmaking Identity-Based Encryption for Internet of Things

XUFENG TAO[1], YAN QIANG[1], PENG WANG[2], AND YINGSEN WANG[1], (Graduate Student Member, IEEE)

[1]College of Information and Computer, Taiyuan University of Technology, Taiyuan 030600, China
[2]School of Intelligent Technology and Engineering, Chongqing University of Science and Technology, Chongqing 401331, China

Corresponding author: Peng Wang (pwang@cqust.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61872261, and in part by the Science and Technology Research Program of Chongqing Municipal Education Commission under Grant KJQN202201520.

ABSTRACT Under the usage of new technologies, Internet of Things (IoT) develops rapidly and provides a great convenience for our lives. It is critical for ensuring security to IoT systems as the tremendous growth of IoT applications. Although many cryptography tools (such as identity-based encryption) have been given to provide appropriate security in IoT covering various application fields such as smart home, how to guarantee data confidentiality, provide reasonable data source identification, and resist quantum attacks simultaneously has been a challenging problem. To address this problem, we propose a matchmaking encryption scheme named lattice-based matchmaking identity-based encryption (LMIBE) which can provide bilateral access control for both sender and receiver in IoT systems, and resist quantum attacks. Moreover, we give a formal definition and a security definition for our scheme. Security proof shows that our scheme is secure under the proposed security definition. Finally, by comparing the performance of our scheme with existing works, our proposed scheme has a broad application prospect in IoT environment.

INDEX TERMS Identity-based encryption, matchmaking encryption, post-quantum security, Internet of Things.

I. INTRODUCTION

The Internet of Things (IoT) is a complex and extensive network taking charge of establishing communication among billions of devices. With the continuous development of various types of devices and technologies, IoT technology may be involved in all aspects of our daily life, such as smart home, healthcare, vehicle networks, etc. [1], [2]. In recent years, the primary concern still concentrates on ensuring security and privacy of data communication among IoT devices.

Identity-based encryption (IBE) [3], [4], [5], [6] is an efficient and important measure of protecting data privacy and ensuring secure data communication in IoT. IBE eliminates the barrier raised by the exquisite certificate management needed by other public key encryption schemes, and in which the sender (e.g., sensors) only needs little overhead in encrypting data. For example, IoT devices (senders) can use the identity of other IoT devices (receivers) to encrypt selected data. However, IBE only executes receiver (e.g., servers) access control and does not hold sender access control. Therefore, it is essential to provide a cryptographic mechanism satisfying receiver access control for data confidentiality and sender access control for data source identification.

To solve this problem, a matchmaking IBE (MIBE) scheme is constructed in CRYPTO'19 [7] to realize the access control of the sender and the receiver. The MIBE scheme allows the sender to specify the identity of the receiver for data confidentiality, the receiver could decide whether the data are from the intended sender. That is, MIBE scheme can achieve data confidentiality, receiver access control

The associate editor coordinating the review of this manuscript and approving it for publication was Theofanis P. Raptis.

and data source identification in the IoT environment by checking the matchmaking of the identity for sender and receiver. However, the current existing MIBE scheme can not resist quantum attacks in the circumstances of the rapid development of quantum computers.

In this paper, we construct a lattice-based MIBE (LMIBE) scheme based on IBE and the hardness of the learning with errors (LWE) problem and short integer solution (SIS) problem. LMIBE not only has the advantages of lattice-based cryptography and MIBE scheme, but also has a certain practical value and a broad application prospect in IoT environment. This paper has the following contributions:

1. We present the LMIBE scheme that guarantees three security properties simultaneously: (i) message confidentiality, (ii) data source identification, (iii) post-quantum security.
2. We put forward the secure definition formally of the LMIBE scheme, and provide the process of concrete construction of LMIBE and the formal security proof based on the LWE problem and SIS problem.
3. LMIBE provides a bilateral access control for both sender and receiver, and it allows the receiver to undertake the work of data identification by outsourcing an access structure to a semi-trusted third party (sanitizer) which helps receivers to verify whether ciphertexts satisfy the access structure.
4. To evaluate the theoretical performance of LMIBE, we make comparisons between LMIBE and other lattice-based IBE schemes. The comparison results show that LMIBE possesses better functions and performances than others.

The rest of this paper is organized as follows. In Section II, we review the existing works related to IBE. In Section III, we recall some theoretical background for lattice-based cryptography. Section IV provides the security definition and system model of our proposed scheme. In Section V, we show the process of concrete construction of our scheme and the security proof. In Section VI, we make a comparison between our scheme and other related schemes in theory evaluation. In Section VII, we present a conclusion.

II. RELATED WORK

As a logical and physical extension of the current internet, IoT [8] is made up of billions of smart connected devices or things [9]. Because these devices in IoT are physically fragile and are usually left unsupervised, IoT applications are often subject to security attacks. Thus, securely transferring data is a significant issue in IoT.

IBE is seen as an efficient encryption tool for secure data communication in IoT because of no requirement of complicated certificate. IBE was first introduced by Shamir [10], while actual implementation was only provided recently. Cocks [11] constructs an IBE scheme by applying quadratic residues modulo a composite (also refer to [12]). IBE schemes [13], [14], [15], [16], [17] have been introduced in the last few decades. Authors [18] introduced the notion of Hierarchical IBE and a pseudo-RSA digital certificate technology that can store an IBE key in the RSA key structure of a certificate is presented in the work [19]. In addition, named fuzzy IBE (FIBE) schemes [20], [21], [22], [23] are proposed in order to ensure the property of error-tolerance. Especially, Mao et al. [23] presented a FIBE scheme for confidential communications in IoT. Furthermore, a study based on IBE provides an authorized equivalence test for a cloud-assisted IoT [5].

Although above mentioned IBE schemes solve some issues in terms of public safety sharing requirements, they can not provide bilateral access control services for users with some particular needs. Ateniese et al. [7] tackled this problem by constructing a matchmaking IBE (MIBE) scheme. MIBE scheme gives stronger privacy protection because it enables the sender to specify the identity of the receiver and ensures the receiver verifies the identity of the sender. However, the MIBE scheme fails to provide quantum security when facing quantum computers.

With the confront of the quantum age, post-quantum cryptography systems have been introduced and a standardization process [24] has been initiated by the National Institute of Standards and Technology (NIST) so as to confront the new computational means. For the aspect of post-quantum cryptography, a great choice is the lattice-based cryptography since its security proofs are based on the worst-case hardness of lattice issues. Additionally, lattice-based IBE schemes have been established for the purpose of resisting quantum attacks, the interested readers can refer to the papers [25], [26], [27], [28], [29]. However, the lattice-based MIBE scheme still does not been constructed at present. In our LMIBE, the verifying algorithm can prevent the unauthorized sender, such that only the identity of the sender matches successfully with the identity specified by a receiver, the receiver with valid decryption keys can recover the message.

III. PRELIMINARIES

A. NOTATIONS

Denote $\mathbb{R}$, $\mathbb{Z}$ as the set of real and integer numbers respectively. We denote $\mathbb{Z}_q$ as $\{0, 1, ..., q-1\}$ with addition modulo q. Denote $\mathbb{Z}^m$ as the set of integer vectors. If vectors belonged to $\mathbb{Z}^m$ are linearly independent when reduced modulo q, then we say these vectors are $\mathbb{Z}_q$ independent. Let m be a positive integer, $[m]$ is denoted by $\{1, 2, ..., m\}$, and $\lceil m \rceil$ and $\lfloor m \rfloor$ denote the minimum integer larger than m and the maximum integer smaller than m respectively. Furthermore, we use lower-case letters (for example b) and capital letters (for example B) to present vectors assumed in column form and matrices, and b_i denotes the i-th component of vector b and B_i denotes the i-th column vector of a matrix B respectively. In addition, $\widetilde{B}$ denotes the Gram-Scahmidt orthogonalization of B. $\|B\|$ and $\|b\|$ denote the norm of B and b in Euclidean norm. A probabilistic polynomial-time

(PPT) algorithm is a randomized algorithm that works in strict polynomial time.

B. LATTICE

Assume $B = \big[b_1|\cdots|b_m\big]$ belongs to $\mathbb{R}^{m\times m}$, whose columns vectors $b_1, \cdots, b_m \in \mathbb{R}^m$ are linearly independent. The following set [30] is a lattice Λ generated by B,

$$\Lambda = \left\{y \in \mathbb{R}^m \text{ such that } \exists s \in \mathbb{Z}^m,\ y = Bs = \sum_{i=1}^{m} s_i b_i\right\}.$$

Definition 1 [31]: Let q be a prime number, $A_0 \in \mathbb{Z}_q^{n\times m}$ and $\varsigma \in \mathbb{Z}_q^n$, we have

$$\Lambda_q(A_0) := \big\{\vartheta \in \mathbb{Z}^m \text{ such that } \exists\zeta \in \mathbb{Z}_q^n \text{ where } A_0^\top \zeta = \vartheta\ (mod\ q)\big\},$$
$$\Lambda_q^\perp(A_0) := \big\{\vartheta \in \mathbb{Z}^m \text{ such that } A_0\vartheta = 0\ (mod\ q)\big\},$$
$$\Lambda_q^\varsigma(A_0) := \big\{\vartheta \in \mathbb{Z}^m \text{ such that } A_0\vartheta = \varsigma\ (mod\ q)\big\}.$$

Theorem 1 [32]: For $m = \lceil 6n\log q\rceil$ with an odd integer number $q \geq 3$, there exists a PPT algorithm TrapGen(q, n) that returns matrixes $(A_0 \in \mathbb{Z}_q^{n\times m},\ T_{A_0} \in \mathbb{Z}^{m\times m})$ such that the matrix A_0 is statistically close to a uniform distribution over $\mathbb{Z}_q^{n\times m}$ and the matrix T_{A_0} is a basis for lattice $\Lambda_q^\perp(A_0)$ satisfying

$$\big\|\widetilde{T_{A_0}}\big\| \leq \mathcal{O}\big(\sqrt{n\log q}\big),\ \|T_{A_0}\| \leq \mathcal{O}(n\log q)$$

with all but negligible probability in n.

Assume $\mathcal{L} \subseteq \mathbb{Z}^m$, $\sigma \in \mathbb{R}_{>0}$ is an arbitrary positive parameter and $c \in \mathbb{R}^m$ is an arbitrary vector. We denote a Gaussian-shaped function on $\mathbb{R}^m$ as $\rho_{\sigma,c}(\iota) = \exp\big(-\pi\frac{\|\iota-c\|^2}{\sigma^2}\big)$ by using center c and Gaussian parameter σ. Let the sum of $\rho_{\sigma,c}$ over $\mathcal{L}$ be $\rho_{\sigma,c}(\mathcal{L}) = \sum_{\iota\in\mathcal{L}}\rho_{\sigma,c}(\iota)$. And define the discrete Gaussian distribution [33] over $\mathcal{L}$ with Gaussian parameters σ and center c as $\mathcal{D}_{\mathcal{L},\sigma,c}$ satisfying

$$\forall \jmath \in \mathcal{L},\ \mathcal{D}_{\mathcal{L},\sigma,c}(\jmath) = \frac{\rho_{\sigma,c}(\jmath)}{\rho_{\sigma,c}(\mathcal{L})}.$$

We will often define the Gaussian distribution $\mathcal{D}_{\mathcal{L},\sigma,c}$ over $\mathcal{L} = \Lambda_q^\perp(A_0)$ with $A_0 \in \mathbb{Z}_q^{n\times m}$.

Let $A \in \mathbb{Z}_q^{n\times tm}$ where $A = [A_1, \ldots, A_t]$ with every matrix $A_j \in \mathbb{Z}_q^{n\times m}$. For $\Gamma = \{j_1, \ldots, j_l\} \subseteq [t]$, denote $A_\Gamma = [A_{j_1}, \ldots, A_{j_l}]$. We can apply a short basis of $\Lambda_q^\perp(A_\Gamma)$ with some $\Gamma \subseteq [t]$ to generate a short basis of $\Lambda_q^\perp(A)$.

Theorem 2 [34]: Assume positive integers n, q, m, t satisfy $q \geq 2$ and $m \geq 2n\lg q$. There is a PPT algorithm SampleBasis, when inputting $A \in \mathbb{Z}^{n\times tm}$, a set $\Gamma \subseteq [t]$, a basis B_Γ for $\Lambda_q^\perp(A_\Gamma)$, and an integer $\Upsilon \geq \|\widetilde{B}_\Gamma\| \cdot \sqrt{tm} \cdot \omega(\sqrt{\log tm})$, it will output $T_B \leftarrow$ SampleBasis$(A, B_\Gamma, \Gamma, \Upsilon)$ such that, for an non-negligible fraction of $A \in \mathbb{Z}_q^{n\times tm}$, T_B is a basis of $\Lambda_q^\perp(A)$ with $\|\widetilde{T}_B\| \leq \Upsilon$ (with non-negligible probability). Additionally, the distribution of T_B only relies on A and Υ (but does not rely on B_Γ and Γ) up to a statistical distance.

Theorem 3 [28]: Assume $q \geq 2$, $A_0 \in \mathbb{Z}_q^{n\times m}$ with $m > n$, T_{A_0} is a basis for $\Lambda_q^\perp(A_0)$ and $\sigma \geq \|\widetilde{T_{A_0}}\|\omega(\sqrt{\log m})$. Then for a vector $\nu \in \mathbb{Z}_q^n$, there exists a PPT algorithm SamplePre $(A_0, T_{A_0}, \nu, \sigma)$ which outputs $\hbar \in \Lambda_q^\nu(A_0)$ sampled from a distribution statistically close to $\mathcal{D}_{\Lambda_q^\nu(A_0),\sigma}$.

C. COMPLEXITY ASSUMPTIONS

The security of our construction for LMIBE scheme is based on the LWE problem and SIS problem, the definition of LWE problem and SIS problem as follows.

Definition 2: [35] Assume q is a prime, n is a positive integer, and χ is a distribution over $\mathbb{Z}_q$. An $(\mathbb{Z}_q, n, \chi)$-LWE problem instance contains access to an unauthorized challenge oracle $\mathcal{O}$, which is either a noisy pseudo-random sampler $\mathcal{O}_s$ associated with a secret key $s \in \mathbb{Z}_q^n$ or a truly random sampler $\mathcal{O}_\Phi$, they have the following behaviors respectively:
$\mathcal{O}_s$: returns samples with the form $(\varrho_i, \tau_i) = (\varrho_i, \varrho_i^\top s + \varphi_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, here $\varrho_i \in \mathbb{Z}_q^n$ is random, $\varphi_i \in \mathbb{Z}_q$ is a noise sample from χ, and $s \in \mathbb{Z}_q^n$ is a random secret key.
$\mathcal{O}_\Phi$: returns truly random samples from $\mathbb{Z}_q^n \times \mathbb{Z}_q$.
Note that we can query the oracle $\mathcal{O}$ many times for the $(\mathbb{Z}_q, n, \chi)$-LWE problem. When $\big|Pr[\mathcal{A}^{\mathcal{O}_s} = 1] - Pr[\mathcal{A}^{\mathcal{O}_\Phi} = 1]\big|$ is non-negligible for $s \in \mathbb{Z}_q^n$, $\mathcal{A}$ determines the $(\mathbb{Z}_q, n, \chi)$-LWE problem.

Definition 3 (SIS problem): Given the parameters n, m, q, η and a random matrix $A_0 \in \mathbb{Z}_q^{n\times m}$, the SIS problem is to find a nonzero vector $e \in \mathbb{Z}_q^m$ such that $\|e\| \leqslant \eta$ and $A_0 e = 0\ (\mod q)$.

IV. PROBLEM FORMULATION

LMIBE allows to verify the ciphertext and prevents unauthorized senders, such that only valid decryption keys can be used to obtain the message. This section gives the security definition and system model of LMIBE.

A. SYSTEM MODEL

As illustrated in Fig.1, our proposed LMIBE scheme consists of four types of independent entities: key generation center (KGC), sender S, a semi-trusted third party called sanitizer and receiver R. The KGC is regarded as a trusted entity that initializes the LMIBE scheme. The KGC creates public parameter pk and master secret key msk and use them to generate the encryption key ek_{σ_1} and decryption key dk_{ρ_1} according to the specified individual's identities ρ_1 and σ_1. Then the KGC distributes the encryption key ek_{σ_1} to the sender S and decryption key dk_{ρ_1} to the receiver R (see ① in Fig. 1). In order to send a message M to receiver R, a sender S uses its encryption key ek_{σ_1} and identity rcv of authorized receiver to encrypt the message, and then sends the ciphertext CT to the sanitizer (see ② in Fig. 1), after receiving the ciphertext CT, the sanitizer verifies whether the ciphertext CT matches the identity snd specified by the receiver or not. If matching success i.e. $snd = \sigma_1$, then the ciphertext CT is leaved, otherwise, the sanitizer discards it. Finally, the receiver R can access the sanitizer and decrypts correctly the ciphertext CT if and only if $rcv = \rho_1$ by using the decryption key dk_{ρ_1} (see ③ in Fig. 1).

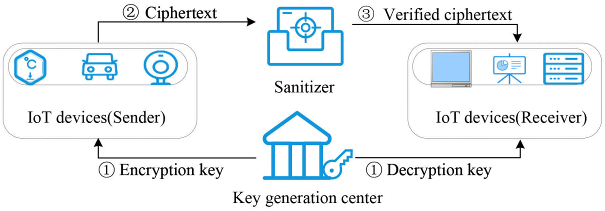

FIGURE 1. System model.

Formally, LMIBE contains six polynomial algorithms Setup, SKGen, RKGen, Enc, Verify, Dec. The formal definition of LMIBE is defined as follows.

- Setup$(1^\lambda) \rightarrow (pk, msk)$: The KGC is regarded as a trusted authority that initializes the LMIBE scheme. It runs the Setup algorithm by taking a security parameter λ as input, and generating public parameter pk and the master secret key msk as outputs. For simplicity, the common input pk is left out in other algorithms.
- SKGen$(msk, \sigma_1) \rightarrow ek_{\sigma_1}$: The KGC runs this SKGen algorithm that inputs a master key msk and a identity $\sigma_1 \in \{0, 1\}^*$ of the sender. Then it returns a encryption key ek_{σ_1}.
- RKGen$(msk, \rho_1) \rightarrow dk_{\rho_1}$: The KGC runs this RKGen algorithm that inputs a master key msk, a identity $\rho_1 \in \{0, 1\}^*$ of the receiver. Then it returns a decryption key dk_{ρ_1}.
- Enc$(ek_{\sigma_1}, M, rcv) \rightarrow CT$: The Enc algorithm is executed by the sender. It encrypts a message $M \in \{0, 1\}$ with the encryption key ek_{σ_1} and a target identity rcv of the receiver, and then outputs a ciphertext CT.
- Verify$(CT, snd) \rightarrow$ 1 or 0: The Verify algorithm is executed by the sanitizer. It inputs ciphertext CT, a target identity snd of the sender. Then it returns a bit 1 if and only if $snd = \sigma_1$; else returns a bit 0.
- Dec$(CT, dk_{\rho_1}) \rightarrow M$ or $\perp$: The Dec algorithm is executed by the receiver. It applies a decryption key dk_{ρ_1} to decrypt the ciphertext CT. Then it outputs a plaintext M if and only if $rcv = \rho_1$; else returns $\perp$.

B. SECURITY DEFINITION

In our LMIBE scheme, two security definitions are presented. They are indistinguishability under a chosen-plaintext attack (IND-CPA) and existential unforgeability under a chosen message attack (EU-CMA) in the random oracle model.

Definition 4: (IND-CPA) The IND-CPA security for a LMIBE scheme means that the advantage

$$Adv_{\mathcal{A}}^{IND-CPA}(1^\lambda) = \left| Pr[Exp_{\mathcal{A}}^{IND-CPA}(1^\lambda)] - \frac{1}{2} \right|$$

is negligible for any PPT adversary $\mathcal{A}$, where the experiment $Exp_{\mathcal{A}}^{IND-CPA}(1^\lambda)$ is depicted in Fig. 2.

Definition 5: (EU-CMA) The EU-CMA security for a LMIBE scheme means that the advantage

$$Adv_{\mathcal{A}}^{EU-CMA}(1^\lambda) = Pr[Exp_{\mathcal{A}}^{EU-CMA}(1^\lambda) = 1]$$

```
$\mathbf{Exp}_{\mathcal{A}}^{IND-CPA}(1^\lambda)$
$rcv^* \longleftarrow \mathcal{A}(1^\lambda)$;
$(pk, msk) \longleftarrow$ Setup$(1^\lambda)$;
$(m_0, m_1, \sigma_0, \sigma_1) \longleftarrow \mathcal{A}^{O}(pk)$;
$b \longleftarrow \{0, 1\}$;
$ek_{\sigma_b} \longleftarrow SKGen(msk, \sigma_b)$;
$CT_b \longleftarrow Enc(ek_{\sigma_b}, rcv^*, m_b)$;
$b' \longleftarrow \mathcal{A}^{O}(CT_b)$;
If $(b' = b)$ return 1 ;
Else return 0.
```

```
Oracle $O_{SKGen}(\sigma)$
$ek \longleftarrow SKGen(msk, \sigma)$;
return $ek$.

Oracle $O_{RKGen}(\rho)$
$dk \longleftarrow RKGen(msk, \rho)$;
return $dk$.
```

FIGURE 2. Experiment of IND-CPA. $\mathcal{O}_{SKGen}(\cdot)$ and $\mathcal{O}_{RKGen}(\cdot)$ are executed by $SKGen(msk, \cdot)$ and $RKGen(msk, \cdot)$ respectively.

```
$\mathbf{Exp}_{\mathcal{A}}^{EU-CMA}(1^\lambda)$
$snd^* \longleftarrow \mathcal{A}(1^\lambda)$;
$(pk, msk) \longleftarrow$ Setup$(1^\lambda)$;
$c^* \longleftarrow \mathcal{A}^{O}(mpk)$;
return 1 iff Verify$(snd^*, c^*) = 1$, and
$\forall snd \in Q_{O_{SKGen()}}$: $snd \neq snd^*$, and
$\forall c \in Q_{O_{Enc()}}$: $c^* \neq c$.
```

```
Oracle $O_{SKGen}(\sigma)$
$ek \longleftarrow SKGen(msk, \sigma)$;
return $ek$.

Oracle $O_{RKGen}(\rho)$
$dk \longleftarrow RKGen(msk, \rho)$;
return $dk$.

Oracle $O_{Enc}(ek, M, rcv)$
$c \longleftarrow Enc(ek, M, rcv)$
return $c$.
```

FIGURE 3. Experiment of EU-CMA. $\mathcal{O}_{SKGen}(\cdot)$, $\mathcal{O}_{RKGen}(\cdot)$ and $\mathcal{O}_{Enc}(\cdot)$ are executed by $SKGen(msk, \cdot)$, $RKGen(msk, \cdot)$ and $Enc(ek_{\sigma_1}, \cdot, rcv)$ respectively.

is negligible for any PPT adversary $\mathcal{A}$, where the experiment $Exp_{\mathcal{A}}^{EU-CMA}(1^\lambda)$ is depicted in Fig. 3.

V. CONSTRUCTION OF LMIBE

We now provide the process of concrete construction of LMIBE and the secure proof.

A. CONCRETE CONSTRUCTION OF OUR SCHEME

- Setup(1^λ): Suppose q is a prime number and n, m are positive integers, they satisfy $q \geq 2$ and $m > 6n \log q$. Let $H_1 : \{0, 1\}^* \rightarrow \mathbb{Z}_q^{n \times m}$, $H_2, H_3 : \{0, 1\}^* \rightarrow \mathbb{Z}_q^n$, and input a security parameter λ. Next do:
  1) By running the TrapGen(q, n) algorithm, the KGC generates a random matrix $A_0 \in \mathbb{Z}_q^{n \times m}$ with a short basis T_{A_0} for $\Lambda_q^{\perp}(A_0)$ such that $\|\widetilde{T_{A_0}}\| \leq \mathcal{O}(\sqrt{n \log q})$.
  2) The KGC defines public parameter as $pk = A_0$ and the master secret key as $msk = T_{A_0}$.
- SKGen(msk, σ_1): Given the master key msk and identity $\sigma_1 \in \{0, 1\}^*$ of the sender, next do:
  1) The KGC runs the SampleBasis$(A_0|H_1(\sigma_1), T_{A_0}, r = \{1\}, \sigma)$ algorithm to generate a matrix $B_1 \in \mathbb{Z}^{m \times m}$.
  2) Return the encryption key $ek_{\sigma_1} = B_1$.
- RKGen(msk, ρ_1): Given the master key msk and identity $\rho_1 \in \{0, 1\}^*$ of the receiver, next do:
  1) The KGC runs the SamplePre$(A_0, T_{A_0}, H_2(\rho_1), \sigma)$ $\rightarrow e_1$ algorithm, where $e_1 \in \mathbb{Z}_q^m$ satisfies $A_0 e_1 = H_2(\rho_1) \in \mathbb{Z}_q^n$.

  2) Return the decryption key $dk_{\rho_1} = e_1$.

- Enc(ek_{σ_1}, M, rcv): Given a encryption key $ek_{\sigma_1} = B_1$ of the sender, a target identity $rcv \in \{0, 1\}^*$ of the receiver and a plaintext $M \in \{0, 1\}$, next do:
  1) Select a vector $v \in \mathbb{Z}_q^n$ at random.
  2) Select noise vectors $x \leftarrow \chi$, and $y \leftarrow \chi^m$.
  3) Set $p = A_0^T v + y \in \mathbb{Z}_q^m, c_0 = H_2(rcv)^T v + x + M\left\lfloor \frac{q}{2} \right\rfloor \in \mathbb{Z}_q$.
  4) Use algorithm SamplePre($A_0|H_1(\sigma_1), B_1, H_3(p, c_0), \sigma$) $\rightarrow \mu$, where $\mu \in \mathbb{Z}_q^{2m}$ satisfies $(A_0|H_1(\sigma_1))\mu = H_3(p, c_0) \in \mathbb{Z}_q^n$.
  5) Output the ciphertext $CT = (p, c_0, \mu)$.
- Verify(CT, snd): On input ciphertext $CT = (p, c_0, \mu)$, a target identity $snd \in \{0, 1\}^*$, do:
  1) Check $(A_0|H_1(snd))\mu \overset{?}{=} H_3(p, c_0)$.
  2) If the equation holds, returns 1; else it stops the communication.
- Dec(CT, dk_{ρ_1}, snd): On input ciphertext $CT = (p, c_0, \mu)$, a decryption key $dk_{\rho_1} = e_1$ and a target identity $snd \in \{0, 1\}^*$, do:
  1) Compute $\omega = c_0 - dk_{\rho_1}^T p$.
  2) Compare ω and $\lfloor \frac{q}{2} \rfloor$ in $\mathbb{Z}_q$. If $|\omega - \lfloor \frac{q}{2} \rfloor| < \lfloor \frac{q}{4} \rfloor$, then outputs 1, else outputs 0.

B. PARAMETERS AND CORRECTNESS

If CT is a valid ciphertext, $rcv = \rho_1$ and $snd = \sigma_1$, we have

$$\begin{aligned}\omega &= c_0 - dk_{\rho_1}^T p \\ &= H_2(\rho_1)^T v + x + M\left\lfloor \frac{q}{2} \right\rfloor - e_1^T (A_0^T v + y) \\ &= H_2(\rho_1)^T v + x + M\left\lfloor \frac{q}{2} \right\rfloor - H_2(\rho_1)^T v - e_1^T y \\ &= M\left\lfloor \frac{q}{2} \right\rfloor + x - e^T y.\end{aligned}$$

The formula $x - e^T y$ is the error term. To ensure the system correctly work, we need the bound of the error term to be controled by $\frac{q}{5}$, and the TrapGen algorithm works very well (that means $m > 6n \log q$), and σ is large enough for SampleBasis and SamplePre algorithms, and Regev's reduction applies (that means $q > 2\sqrt{n}/\alpha$). In order to meet the above demands, we take n as the security parameter and let (m, α, σ, q) satisfy $m = 6n^{1+\delta}$, $\alpha = \left[m^2 w(\log n)\right]^{-1}$, $\sigma = mw(\log n)$, $q = m^2\sqrt{n}w(\log n)$.

C. SECURITY PROOF

We now show the following theorem to ensure the security of our proposed LMIBE scheme based on the LWE assumption.

Theorem 4: If the decisional LWE assumption holds, then there is no PPT adversaries that can break the IND-CPA security for our proposed LMIBE scheme with parameters $(n, m, \sigma, \alpha, q)$ similar to section V-B.

Proof: Assume LMIBE does not satisfy IND-CPA security definition. Then there exists an adversary $\mathcal{A}$ that can break the proposed scheme with a non-negligible advantage ϵ. Therefore, we can construct an algorithm $\mathcal{B}$ that interacts with the adversary $\mathcal{A}$ to settle the decisional LWE problem. The challenge sends a LWE instance $(u_i \in \mathbb{Z}_q^n, \theta_i \in \mathbb{Z}_q)$ $(0 \leqslant i \leqslant m)$ to $\mathcal{B}$, where $\theta_i = u_i^T v + y_i$ $(y_i \leftarrow \chi)$ or randomly selected. To settle the LWE problem, algorithm $\mathcal{B}$ communicates with $\mathcal{A}$ as follows.

Initial: $\mathcal{A}$ submits rcv^* as challenge.

Setup: $\mathcal{B}$ assembles $A_0 \in \mathbb{Z}_q^{n\times m}$ by setting $A_0 = (u_1, u_2, \cdots, u_m)$. Then $\mathcal{B}$ returns $pk = A_0$ to $\mathcal{A}$.

H_1 **queries**: $\mathcal{A}$ queries the random oracle H_1 as follows. If the query σ_i is in the list $\{\sigma_i, A_i, C_i\} \in \mathcal{L}_1$, then $\mathcal{B}$ sends $H_1(\sigma_i) = A_i$ to the adversary $\mathcal{A}$. Else, $\mathcal{B}$ uses the algorithm TrapGen to generate $A_i \in \mathbb{Z}_q^{n\times m}$ and a short basis $C_i \in \mathbb{Z}_q^{m\times m}$ for lattice $\Lambda_q^{\perp}(A_i)$, where $A_i \in \mathbb{Z}_q^{n\times m}$ is random, then adds $\{\sigma_i, A_i, C_i\}$ to $\mathcal{L}_1$, and sends A_i to $\mathcal{A}$.

H_2 **queries**: $\mathcal{A}$ asks the oracle H_2 at most q_{H_2} queries. $\mathcal{B}$ selects $q^* \in [1, q_{H_2}]$ at random. If the q_i-th query ρ_i is in the list $\{q_i, \rho_i, u_i, e_i\} \in \mathcal{L}_2$. $\mathcal{B}$ returns $H_2(q_i) = u_i$ to $\mathcal{A}$. Otherwise, if $q_i = q^*$, $\mathcal{B}$ defines $u_i = u_0$, and chooses $e_i \in \mathbb{Z}_q^{2m}$ at random. Else, $\mathcal{B}$ samples e_i from the distribution $D_{\mathbb{Z}^m,\sigma}$ such that $A_0 e_i = u_i$, and adds $\{q_i, \rho_i, u_i, e_i\}$ to $\mathcal{L}_2$, then returns u_i to the adversary $\mathcal{A}$.

Query phase 1:

1) SKGen queries: the adversary $\mathcal{A}$ submits σ_i. The algorithm $\mathcal{B}$ first searches for $\{\sigma_i, A_i, C_i\}$ in the list $\mathcal{L}_1$, if it not found, $\mathcal{B}$ queries the oracle H_1 to obtain $\{\sigma_i, A_i, C_i\}$. Else, $\mathcal{B}$ uses algorithm SampleBasis($A_0|A_i, C_i, r = \{2\}, \sigma$) to generate a matrix $B_i \in \mathbb{Z}^{m\times m}$, and returns $ek_{\sigma_i} = B_i$ as encryption key to the adversary $\mathcal{A}$.
2) RKGen queries: the adversary $\mathcal{A}$ submits ρ_i. The algorithm $\mathcal{B}$ first searches for $\{q_i, \rho_i, u_i, e_i\}$ in the list $\mathcal{L}_2$, if it not found, $\mathcal{B}$ queries the oracle H_2 to obtain $\{q_i, \rho_i, u_i, e_i\}$. If $q_i = q^*$, $\mathcal{B}$ aborts. Else, $\mathcal{B}$ returns $dk_{\rho_i} = e_i$ as decryption key to the adversary $\mathcal{A}$.

Challenge: The adversary $\mathcal{A}$ selects two plaintexts $M_0, M_1 \in \{0, 1\}$, and two identities $\sigma_0, \sigma_1 \in \{0, 1\}^*$ with the limitation that σ_0 and σ_1 have never been queried in Query phase 1. $\mathcal{B}$ first chooses $\zeta \in \{0, 1\}$, then queries σ_ζ to oracle H_1 and obtains $\{\sigma_\zeta^*, A_\zeta^*, C_\zeta^*\}$. Then $\mathcal{B}$ uses algorithm SampleBasis$\Big(A_0|A_\zeta^*, C_\zeta^*, r = \{2\}, \sigma\Big)$ to generate a matrix $B_\zeta^* \in \mathbb{Z}^{m\times m}$, and the encryption key is $ek_{\sigma_\zeta} = B_\zeta^*$. If $q_i \neq q^*$, $\mathcal{B}$ aborts, else, $\mathcal{B}$ defines the ciphertext CT^* as follows:

1) Set $\theta^* = (\theta_1, \theta_2, \cdots, \theta_m)^T \in \mathbb{Z}_q^m$.
2) Encrypt a plaintext M_ζ by setting $c_0^* = \theta_0 + M_\zeta\left\lfloor \frac{q}{2} \right\rfloor \in \mathbb{Z}_q$.
3) Run algorithm SamplePre$\Big(A_0|A_\zeta^*, B_\zeta^*, H_3(\theta^*, c_0^*), \sigma\Big)$ to generate a vector $\mu^* \in \mathbb{Z}_q^m$.
4) Send $CT^* = (\theta^*, c_0^*, \mu^*)$ to the adversary $\mathcal{A}$.

Query phase 2: The adversary $\mathcal{A}$ can acquire the encryption key and decryption key by querying the algorithm $\mathcal{B}$ as described in the Query Phase 1, however, $\sigma_i \neq \sigma_0$ and σ_1.

Guess: $\mathcal{A}$ outputs a bit ζ'. Then $(u_i, \theta_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ belongs to the distribution $\mathcal{O}_s$ if $\zeta' = \zeta$. Otherwise, $(u_i, \theta_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ is uniformly sampled from $\mathbb{Z}_q^n \times \mathbb{Z}_q$.

Now let's analyze the probability of successful simulation. The termination probabilities of the game are $\frac{1}{q_{H_2}}$ and $1-\frac{1}{q_{H_2}}$ in Query phase 1 and Challenge phase respectively. So the probability of success of the simulation is $1-\frac{1}{q_{H_2}}\left(1-\frac{1}{q_{H_2}}\right)$.

If $(u_i, \theta_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ belongs to the distribution $\mathcal{O}_s$, then we have $\theta_i = u_i^T v + y_i$ ($y_i \leftarrow \chi$). Thus, the ciphtertext $CT^* = (\theta^*, c_0^*, \mu^*)$ constructed in Challenge phase satisfies

$$\begin{aligned} \theta^* &= (\theta_1, \theta_2, \cdots, \theta_m)^T \\ &= A_0^T v + y, \\ c_0^* &= \theta_0 + M_\zeta \left\lfloor \frac{q}{2} \right\rfloor \\ &= u_0^T v + y_0 + M_\zeta \left\lfloor \frac{q}{2} \right\rfloor, \\ (A_0|A_\zeta^*)\mu^* &= H_3(\theta^*, c_0^*), \end{aligned}$$

and CT^* is a valid challenge ciphtertext. Therefore, the adversary $\mathcal{A}$ holds his ϵ advantage, and $\left|Pr[\zeta' = \zeta]\right| \geq \frac{1}{2}+\epsilon$.

If $(u_i, \theta_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ is uniformly sampled from $\mathbb{Z}_q^n \times \mathbb{Z}_q$, then θ_i is random in $\mathbb{Z}_q$ and then leads to c_0^* is also random in $\mathbb{Z}_q$. Therefore, the challenge ciphtertext CT^* does not reveal any information about $\zeta \in \{0, 1\}$ to any legitimate adversary. Hence, $\left|Pr[\zeta' = \zeta]\right| = \frac{1}{2}$.

Thus, $\mathcal{B}$ has advantage $\frac{1}{2}\left[1 - \frac{1}{q_{H_2}}(1 - \frac{1}{q_{H_2}})\right]\epsilon$ in solving the LWE assumption. □

Theorem 5: If the SIS assumption holds, there is no PPT adversaries that can break the EU-CMA security for our proposed LMIBE scheme with parameters $(n, m, \sigma, \alpha, q)$ similar to section V-B.

Proof: Assume LMIBE does not satisfy EU-CMA security definition. Then there exists an adversary $\mathcal{A}$ that can break the proposed scheme with a non-negligible advantage ϵ. Therefore, we can construct an algorithm $\mathcal{B}$ that interacts with $\mathcal{A}$ to settle the SIS problem. To resolve the SIS problem, algorithm $\mathcal{B}$ communicates with $\mathcal{A}$ in the following way.

Initial: $\mathcal{A}$ submits snd^* as challenge.

Setup: $\mathcal{B}$ selects a random matrix $A_0 \in \mathbb{Z}_q^{n\times m}$ and sends $pk = A_0$ to $\mathcal{A}$.

H_1 **queries**: This is the same as Theorem 4.

H_2 **queries**: $\mathcal{A}$ queries the random oracle H_2 as follows. If the query ρ_i is in the list $\{\rho_i, u_i, e_i\} \in \mathcal{L}_4$. $\mathcal{B}$ returns $H_2(q_i) = u_i$ to $\mathcal{A}$. Else, $\mathcal{B}$ samples a arbitrary vector e_i from the distribution $D_{\mathbb{Z}^m,\sigma}$ such that $A_0 e_i = u_i$, and adds $\{\rho_i, u_i, e_i\}$ to $\mathcal{L}_4$, then returns u_i to $\mathcal{A}$.

SKGen queries: This is the same as theorem 4.

RKGen queries: $\mathcal{A}$ submits ρ_i. $\mathcal{B}$ first looks for $\{\rho_i, u_i, e_i\}$ in the list $\mathcal{L}_4$, if it not found, $\mathcal{B}$ queries the oracle H_2 to obtain $\{\rho_i, u_i, e_i\}$. Else, $\mathcal{B}$ returns $dk_{\rho_i} = e_i$ as decryption key to $\mathcal{A}$.

Enc queries: $\mathcal{A}$ submits (σ_i, rcv_i, m_i). $\mathcal{B}$ selects a uniformly random vector $v \in \mathbb{Z}_q^n$. Then $\mathcal{B}$ obtains two list $\{\sigma_i, A_i, C_i\}$ and $\{rcv_i, u_i, e_i\}$ by querying the oracle H_1 and H_2, respectively. $\mathcal{B}$ uses algorithm SampleBasis($A_0|A_i, C_i, r = \{2\}, \sigma$) to generate a matrix $B_i \in \mathbb{Z}^{m\times m}$. Then computes $p = A_0^T v + y \in \mathbb{Z}_q^m$, $c_0 = u_i^T v + y_0 + m\lfloor\frac{q}{2}\rfloor \in \mathbb{Z}_q$. $\mathcal{B}$ runs algorithm SamplePre($A_0|A_i, B_i, H_3(p, c_0), \sigma$) to generate a vector $\mu \in \mathbb{Z}_q^m$. $\mathcal{B}$ sends (p, c_0, μ) to $\mathcal{A}$.

Forgery: $\mathcal{A}$ sends $\left(p', c_0', \mu'\right)$ to $\mathcal{B}$. If $\left(p', c_0', \mu'\right)$ is valid, then $\left(A_0|H_1(snd^*)\right)\mu' = H_2(p', c_0') \in \mathbb{Z}_q^n$ and $\| \mu' \| \leq \sigma\sqrt{2m}$. Because $(A_0|H_1(snd^*))\mu^* = H_2\left(p', c_0'\right) \in \mathbb{Z}_q^n$, so we have $\left(A_0|H_1(snd^*)\right)(\mu'-\mu^*) = 0 \mod q$ and $\| \mu'-\mu^* \| \leq \| \mu' \| + \| \mu^* \| \leq 2\sigma\sqrt{2m}$. Because this solution is a non-zero solution to SIS problem with $\left(q, 2m, 2\sigma\sqrt{2m}, A_0|H_1(snd^*)\right)$, by the preimage min-entropy property, this non-zero solution with probability no less than $1 - \frac{1}{2^{w(\log 2m)}}$. So the non-zero solution to this $SIS_{q,2m,2\sigma\sqrt{2m},A_0|H_1(snd^*)}$ problem with negligible probability $\left(1 - \frac{1}{2^{w(\log 2m)}}\right)\epsilon$. □

VI. THEORETICAL EVALUATION

In the present section, we will make a comparison to evaluate our proposed LMIBE scheme and partial existing IBE schemes based on lattices [25], [36], [37] with respect to communication and computation costs in theory. In addition, we also compare our scheme and other related schemes [7], [25], [36], [37] in respect of features of post-quantum and access control for the sender.

We reveal the communication cost in Table 1 and the computation cost in Table 2 for our LMIBE scheme. Specifically, we compare the communication cost of LMIBE with the existing lattice-based IBE schemes in aspects of public parameters, encryption keys size, decryption keys size, and ciphertext size in Table 1. We also make a comparison for the computation cost of algorithms such as Setup, SKGen, RKGen, Enc, Verify, and Dec between our LMIBE scheme and the existing schemes. In Table 2, T_{TG}, T_{SB}, T_{SP}, T_{SL}, T_{SD} refer to the cost of computing algorithms TrapGen, SampleBasis, SamplePre, SampleLeft, and SampleD respectively. Using T_{ha} as the cost of a hash function. We use $(\cdot)_{mul}$ to denote the multiplication cost between matrixes or vectors.

In terms of communication cost demonstrated in Table 1, the public parameter size and Decryption keys size in LMIBE is smaller than that of other listed schemes [25], [36], [37]. Even though LMIBE needs to store the encryption key, it supports access control for the sender. The ciphertext size of the LMIBE scheme is slightly bigger than those of [25], [36], and [37] since our LMIBE scheme supports the verifying function for the identity of the sender.

For computation cost, from Table 2, our LMIBE scheme has analogous computation cost in the Setup with the schemes from [25] and [36] since they demand to run TrapGen to acquire public parameters and master secret keys. We also note that the computation cost of the scheme [37] in the Setup is more than that of LMIBE. Schemes of [25], [36], and [37] in Table 2 have no requirements for encryption key generation algorithm because of their unidirectional access control. Our LMIBE scheme supports outsourcing sender verification by sanitizer, but the other schemes [25], [36], [37] do not support it. In addition, the computation costs are less than those of [25], [36], [37] for RKGen, Enc and Dec, and thus are more efficient than other schemes in Table 2.

TABLE 1. Communication cost.

Schemes	Public parameter size	Encryption keys size	Decryption keys size	Ciphertext size
[25]	$(3nm+n)\|\mathbb{Z}_q\|$	$-$	$2m\|\mathbb{Z}_q\|$	$(2m+1)\|\mathbb{Z}_q\|$
[36]	$(3nm+n)\|\mathbb{Z}_q\|$	$-$	$2m\|\mathbb{Z}_q\|$	$(2m+1)\|\mathbb{Z}_q\|$
[37]	$(nm+n^2)\|\mathbb{Z}_q\|$	$-$	$nm\|\mathbb{Z}_q\|$	$(n+m)\|\mathbb{Z}_q\|$
LMIBE	$nm\|\mathbb{Z}_q\|$	$m^2\|\mathbb{Z}_q\|$	$m\|\mathbb{Z}_q\|$	$(3m+1)\|\mathbb{Z}_q\|$

TABLE 2. Computation cost.

Schemes	Setup	SKGen	RKGen	Enc	Verify	Dec
[25]	T_{TG}	$-$	$T_{ha}+T_{SL}$ $+(n^2m)_{mul}$	$(n^2m+m^2)_{mul}$ $+(2nm+n+1)_{mul}$	$-$	$(2m)_{mul}$
[36]	T_{TG}	$-$	$T_{ha}+T_{SL}$ $+(2nm)_{mul}$	$(2nm+n+1)_{mul}$	$-$	$(2m)_{mul}$
[37]	$T_{TG}+T_{ha}$	$-$	$T_{ha}+T_{SD}$	$(nm+n+n^2)_{mul}$ $+3T_{ha}$	$-$	$(nm)_{mul}$
LMIBE	T_{TG}	T_{SB}	T_{SP}	$(nm)_{mul}$	$2m_{mul}+2T_{ha}$	m_{mul}

TABLE 3. Feature comparison.

Schemes	Post-quantum	Access control for sender
MIBE [7]	No	Yes
[25]	Yes	No
[36]	Yes	No
[37]	Yes	No
LMIBE	Yes	Yes

As shown in Table 3, we also note that although the scheme [7] has access control for the sender, it cannot resist quantum attack. The schemes [25], [36], [37] have the function of post-quantum, but without restriction for the identity of the sender. Our proposed scheme LMIBE supports the above-stated two properties simultaneously.

VII. CONCLUSION

To ensure secure messages of IoT transferring, we construct the LMIBE scheme based on lattice that supports bilateral identity access control and against quantum attacks. Such system models allow the receiver to have the permission to identify ciphertexts from unauthorized senders with little costly data decryption. Furthermore, by outsourcing a large amount of work load of verification to the sanitizer, it can prevent the dangerous information from invading computers through messages, and reduce the burden of the terminal equipment at the same time. In short, we trust that LMIBE meets some requirements in various IoT application areas for providing data privacy, ciphertext identification, and post-quantum attacks simultaneously.

REFERENCES

[1] O. Vermesan and P. Fries, *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*. Aalborg, Denmark: River, 2013, pp. 153–204.

[2] L. Vishwakarma and D. Das, "SCAB–IoTA: Secure communication and authentication for IoT applications using blockchain," *J. Parallel Distrib. Comput.*, vol. 154, pp. 94–105, Aug. 2021.

[3] C. H. Choi, "Adoptation of Weil pairing IBE for secure file sharing," in *Proc. 12th Int. Conf. Netw.*, 2013, pp. 59–65.

[4] D. Unal, A. Al-Ali, F. O. Catak, and M. Hammoudeh, "A secure and efficient Internet of Things cloud encryption scheme with forensics investigation compatibility based on identity-based encryption," *Future Gener. Comput. Syst.*, vol. 125, pp. 433–445, Dec. 2021.

[5] H. Yan, Y. Wang, C. Jia, J. Li, Y. Xiang, and W. Pedrycz, "IoT-FBAC: Function-based access control scheme using identity-based encryption in IoT," *Future Gener. Comput. Syst.*, vol. 95, pp. 344–353, Jun. 2019.

[6] L. Wu, Y. Zhang, K.-K. R. Choo, and D. He, "Efficient and secure identity-based encryption scheme with equality test in cloud computing," *Future Generat. Comput. Syst.*, vol. 73, pp. 22–31, Aug. 2017.

[7] G. Ateniese, D. Francati, D. Nuez, and D. Venturi, *Match Me If You Can: Matchmaking Encryption and Its Applications*. Cham, Switzerland: Springer, 2019.

[8] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Jun. 2010.

[9] V. Ovidiu, M. Harrison, H. Vogt, K. Kalaboukas, M. Tomasella, K. Wouters, S. Gusmeroli, and S. Haller, "Internet of Things strategic research roadmap," in *European Commission-Information Society and Media DG*. River, 2009.

[10] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Cham, Switzerland: Springer, 1984, pp. 47–53.

[11] C. Cocks, "An identity based encryption scheme based on quadratic residues," in *Proc. IMA Int. Conf. Cryptogr. Coding*. Cham, Switzerland: Springer, 2001, pp. 360–363.

[12] D. Boneh, C. Gentry, and M. Hamburg, "Space-efficient identity based EncryptionWithout pairings," in *Proc. 48th Annu. IEEE Symp. Found. Comput. Sci. (FOCS)*, Oct. 2007, pp. 647–657.

[13] D. Boneh1, X. Boyen, and E.-J. Goh, "Hierarchical identity based encryption with constant size ciphertext," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2005, pp. 440–456.

[14] B. Waters, "Efficient identity-based encryption without random oracles," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2005, pp. 114–127.

[15] C. Gentry, "Practical identity-based encryption without random oracles," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2006, pp. 445–464.

[16] B. Waters, "Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2009, pp. 619–636.

[17] A. Lewko and B. Waters, "Why proving hibe systems secure is difficult," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2014, pp. 58–76.

[18] J. Horwitz and B. Lynn, "Toward hierarchical identity-based encryption," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2002, pp. 466–481.

[19] J. Wu, Y. Long, Q. Huang, and W. Wang, "Design and application of IBE email encryption based on pseudo RSA certificate," in *Proc. 12th Int. Conf. Comput. Intell. Secur. (CIS)*, 2016, pp. 282–286.

[20] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science). Berlin, Germany: Springer 2005, pp. 457–473.

[21] J. Baek, W. Susilo, and J. Zhou, "New constructions of fuzzy identity-based encryption," in *Proc. 2nd ACM Symp. Inf., Comput. Commun. Secur.*, Mar. 2007, pp. 368–370.

[22] Y. Ren, D. Gu, S. Wang, and X. Zhang, "New fuzzy identity-based encryption in the standard model," *Informatica*, vol. 21, no. 3, pp. 393–407, Jan. 2010.

[23] Y. Mao, J. Li, M.-R. Chen, J. Liu, C. Xie, and Y. Zhan, "Fully secure fuzzy identity-based encryption for secure IoT communications," *Comput. Standards Interfaces*, vol. 44, pp. 117–121, Feb. 2016.

[24] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, *Report on Post-Quantum Cryptography*, vol. 12. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2016.

[25] S. Agrawal, D. Boneh, and X. Boyen, "Efficient lattice (H)IBE in the standard model," in *Advances in Cryptology-EUROCRYPT* (Lecture Notes in Computer Science), vol. 6110, H. Gilbert, Ed. Berlin, Germany: Springer, 2010, pp. 553–572.

[26] R. W. F. Lai, H. K. F. Cheung, and S. S. M. Chow, "Trapdoors for ideal lattices with applications," in *Proc. 10th Int. Conf.* Cham, Switzerland: Springer, 2015, pp. 239–256.

[27] L. Ducas, V. Lyubashevsky, and P. Thomas, "Efficient identity-based encryption over NTRU lattices," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Cham, Switzerland: Springer, 2014, pp. 22–41.

[28] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. 14th Annu. ACM Symp. Theory Comput.*, May 2008, pp. 197–206.

[29] H. Zhu, Y. Wang, C. Wang, and X. Cheng, "An efficient identity-based proxy signcryption using lattice," *Future Gener. Comput. Syst.*, vol. 117, pp. 321–327, Apr. 2021.

[30] O. Regev. (2004). *Lattices in Computer Science*. [Online]. Available: https://cims.nyu.edu/regev/teaching/lattices_fall_2009/index.html

[31] M. Ajtai, "Generating hard instances of the short basis problem," in *Automata, Languages and Programming*. Berlin, Germany: Springer, 1999, pp. 1–9.

[32] J. Alwen and C. Peikert, "Generating shorter bases for hard random lattices," *Theory Comput. Syst.*, vol. 48, pp. 535–553, Apr. 2011.

[33] O. Regev, "New lattice-based cryptographic constructions," *J. ACM*, vol. 51, no. 6, pp. 899–942, 2004.

[34] D. Cash, D. Hofheinz, and E. Kiltz, "How to delegate a lattice basis," *IACR Cryptol. ePrint Arch.*, vol. 25, no. 4, pp. 601–639, 2009.

[35] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proc. 37th Annu. ACM Symp. Theory Comput.*, May 2005, pp. 84–93.

[36] S. Yamada, "Adaptively secure identity-based encryption from lattices with asymptotically shorter public parameters," in *Proc. 35th Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Vienna, Austria: Springer, 2016, pp. 32–62.

[37] J. Zhang, Y. Chen, and Z. Zhang, "Programmable hash functions from lattices: Short signatures and IBEs with small key sizes," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2016, pp. 303–332.

XUFENG TAO received the B.S. degree in mathematics and applied mathematics from Shanxi Datong University, China, in 2013. He is currently pursuing the postgraduate degree with the College of Information and Computer, Taiyuan University of Technology. His main research interests include lattice-based cryptography and information security.

YAN QIANG received the M.S. and Ph.D. degrees in computer applications technology from the Taiyuan University of Technology, China, in 1999 and 2010, respectively. He is currently a Professor with the College of Information and Computer, Taiyuan University of Technology. His current research interests include cloud computing, image big data processing, medical image computer-aided diagnosis technology, and cryptography.

PENG WANG received the Ph.D. degree in computer science from Chongqing University, China, in 2020. He is currently a Lecturer with the School of Intelligent Technology and Engineering, Chongqing University of Science and Technology, China. His current research interests include public-key cryptography, lattice-based cryptography, and access control.

YINGSEN WANG (Graduate Student Member, IEEE) received the B.C.S. degree in computer applications technology from the Taiyuan University of Technology, China, in 2012, where he is currently pursuing the joint master's and Ph.D. degree with the College of Information and Computer. His main research interests include blockchain and cryptography.