Multi-Authority Attribute-Based Encryption with Dynamic Membership from Lattices

Er-Shuo Zhuang\(^1\), Chun-I Fan\(^2\)(Senior Member, IEEE), and I-Hua Kuo\(^3\).

\(^1\)Department of Computer Science and Engineering, National Sun Yat-sen University, Kaohsiung 80424, Taiwan. E-mail: zhuanges@gmail.com

\(^2\)Department of Computer Science and Engineering, National Sun Yat-sen University, Kaohsiung 80424, Taiwan. E-mail: cifan@mail.cse.nsysu.edu.tw

\(^3\)Department of Computer Science and Engineering, National Sun Yat-sen University, Kaohsiung 80424, Taiwan. E-mail: evaave860302@gmail.com

Corresponding author: Chun-I Fan (cifan@mail.cse.nsysu.edu.tw).

ABSTRACT

Attribute-based encryption is useful for one-to-many encrypted message sending. However, most attribute-based encryption schemes authorize and issue attributes to users by a single authority. Such a scenario conflicts with practical requirements and may cause the key-escrow problem. Hence, decentralization of authority is a critical issue in attribute-based encryption. Besides, dynamic membership management is another important issue in attribute-based encryption. With dynamic membership management, a system may update the user’s attributes without affecting other users, making the system more flexible and practical. On the other hand, with the rapid development of quantum computers nowadays, encryption schemes based on traditional mathematical problems are at the risk of quantum attacks. Among the existing quantum-resistant mathematical architectures, lattice-based cryptography is the most widely studied. Thus, we propose a multi-authority attribute-based encryption scheme with dynamic membership from lattices to solve the above problems. Moreover, we also formally prove the security of the proposed scheme under the decisional learning with errors assumption.

INDEX TERMS

Attribute-based encryption, Decentralization of authority, Dynamic membership management, Lattice-based cryptography

I. INTRODUCTION

To protect the personal privacy of messages sent over the network, public key encryption (PKE) schemes have been widely researched and used to protect the confidentiality of the data. In a PKE scheme, each user owns a key pair called a public key and a private key. The sender encrypts the plaintext with the public key, and the receiver decrypts the ciphertext with the private key. Moreover, there are many different aspects of research on PKE, such as identity-based encryption (IBE)\(^1\), attribute-based encryption (ABE)\(^2\), dynamic encryption\(^3\), re-encryption\(^4\), searchable encryption\(^5\), and so on. However, to prevent man-in-the-middle attacks, a certificate authority (CA) is needed to issue and manage a certificate for each user’s public key.

ABE is a kind of PKE suitable for one-to-many message sending. To reduce the requirements for certificates in PKE schemes, IBE is proposed where the user’s public key is related to its identity. However, the IBE scheme is only appropriate to the one-to-one message sending scenarios. When a sender wants to send the same message to a group of receivers, he/she must first know the identity of each receiver and then individually encrypt the message with each identity. To improve efficiency for one-to-many encrypted message sending, in 2005, Sahai and Waters\(^6\) proposed the first fuzzy identity-based encryption (Fuzzy IBE) scheme. In their scheme, each user is recognized by a specific set of attributes. A sender designates a policy for encrypting the plaintext, and receivers can decrypt the ciphertext only when their attribute set matches the policy. Thus, Fuzzy IBE is considered a pioneer of ABE.

ABE can be split into two categories according to the different strategies of access structures, namely key-policy ABE (KP-ABE)\(^7\) and ciphertext-policy ABÊ (CP-ABE)\(^8\). In KP-ABE, the key generation center (KGC) is responsible for embedding an access structure into the user’s private key. Then the sender can determine the attribute set of the
ciphertext during the encryption process. By contrast, in CP-ABE, KGC is responsible for embedding an attribute set into the user’s private key. Then the sender can determine the access structure of the ciphertext during the encryption process. For example, in Figure 1, assume that a Hospital-A only provides its disease reports of the COVID-19 to doctors or those who suffer from COVID-19. In KP-ABE, each user is able to recover the plaintext only when the attribute set of the ciphertext matches his/her access structure. On the contrary, a user is able to recover the plaintext only if his/her attribute set matches the access structure of the ciphertext in CP-ABE.

CP-ABE is more suitable for one-to-many encryption than KP-ABE. Since a sender can choose the distinct access structure for every ciphertext in CP-ABE, it is more elastic and feasible than KP-ABE. Furthermore, in CP-ABE, KGC may update the user’s private key independently when a user’s attributes change. However, in KP-ABE, revoking or updating a user’s private key may invoke other users’ private keys.

Decentralization of authority is another important issue in ABE. In general ABE, a single KGC distributes and manages all users’ keys, which may cause the key escrow problem where the system may face severe impacts if KGC is under the attacker’s control. To solve the above problem, Chase [9] proposed the first multi-authority ABE (MA-ABE) scheme in 2007 which permits a set of attribute authorities to manage and issue users’ keys independently. After that, Lin et al. [10] proposed an MA-ABE scheme that eliminates the demand for a central authority in 2008, and Lewko and Waters [11] proposed an MA-ABE scheme with a novel key-binding technique in 2011. The concept of MA-ABE removes the risk of malicious KGC and makes ABE more practical. In addition, the multi-authority structure can also disperse the computation and make the key distribution process more efficient.

Apart from the multi-authority architecture, dynamic membership management is also important in ABE. Fan et al. [12] proposed the first ABE supporting dynamic membership management (ABE-DM). According to their definition, there are four features to reach DM, which are Expandability, Revocability, Renewability, and Independence. With those features, any user can join the system whenever needed, and the system can update a user’s attributes without affecting other users. However, there is a flaw in the above scheme. Therefore, Fan et al. [13] proposed a new scheme to fix the flaw in 2015, but the security of their scheme is proved in the random oracle model. Finally, Fan et al. [14] proposed an ABE-DM scheme in 2021, and its security is proved in the standard model. Besides, Chang [15] applied the concept of DM to a multi-authority ABE (MA-ABE-DM) scheme in 2019.

Lattice-based encryption is one of the most popular quantum-resistant encryption. In 1994 Shor [16] proposed the quantum algorithm which may solve traditional hard problems such as discrete logarithm, elliptic curve discrete logarithm, and large integer factorization problems. Therefore, all the above schemes may be insecure, and various quantum-resistant encryption methods have been proposed in recent years. Among them, lattice-based encryption has received attention for its ability to incorporate functional encryption. The security of lattice-based encryption is based on the shortest vector problem (SVP) and its derived problems. Moreover, no known algorithm can solve SVP in polynomial time, and only approximate-SVP can be solved in polynomial time [17].

Lattice-based ABE has been studied in recent years. In 2012, Agrawal et al. [18] proposed a lattice-based Fuzzy IBE scheme, and Zhang et al. [19] improved it to a lattice-based CP-ABE scheme in the same year. Then, Boyen [20] proposed the first lattice-based KP-ABE scheme in 2013. After that, the first lattice-based MA-ABE scheme was proposed by Zhang et al. [21] in 2015, and a variant is proposed by Liu et al. [22] in 2018. However, both Zhang et al.’s scheme and Liu et al.’s scheme are KP-ABE. Finally, in 2021, Datta et al. [23] proposed the first lattice-based MA-ABE scheme, which is CP-ABE. Although some works for MA-ABE on lattices are proposed, to the best of our knowledge, there has been no lattice-based MA-ABE scheme, which supports dynamic membership management.

A. PROBLEM STATEMENTS

In summary, to meet the needs of the practical environment, a one-to-many encryption scheme should satisfy the following requirements:

- The sender may choose the access structure of the ciphertext. Therefore, the sender can easily decide who can decrypt the ciphertext.
- Private keys of users may be updated independently. Other users’ private keys will not be influenced during the key-update phase.
- Decentralization of authority should be provided to reduce the damage of the key escrow problem of a single authority.
- The encryption scheme should resist quantum attacks.

Therefore, we propose an MA-ABE-DM scheme on lattices to satisfy the above requirements.

B. CONTRIBUTIONS

To highlight the advantages of the proposed MA-ABE-DM scheme on lattices, it provides the features as follows:

- The proposed scheme is a CP-ABE scheme. Therefore, the sender can choose the access structure of the ciphertext.
- Since the proposed scheme allows dynamic membership management, all private keys can be updated independently.
- It supports multi-authority scenarios, which resolves the key escrow problem of a single authority.
- The proposed structure is based on lattices, which can resist quantum attacks.
It can resist collusion attacks from users. Any unauthorized users cannot decrypt the ciphertext through cooperation.

The security of the proposed scheme is proved to be selective indistinguishability under chosen-plaintext attack (IND-CPA) secure under the hardness of the decisional learning with errors (D-LWE) problem.

C. ORGANIZATION
In section 2, we introduce some cryptographic primitives on lattices and the hard problem applied in the proposed scheme. In section 3, we show some MA-ABE schemes on lattices and a traditional MA-ABE scheme that supports dynamic membership management. Then, we present the details of the proposed scheme and its security proof in section 4 and section 5, respectively. Finally, we show some comparisons between the proposed scheme and the related works in section 6 and make a conclusion for this work in section 7.

II. PRELIMINARIES
In this section, we first introduce some background knowledge of lattices. We adopt the trapdoor generation and sample techniques proposed by Micciancio and Peikert [24] in 2012 and prove the security of the proposed scheme under the assumption of the D-LWE problem introduced by Regev [25] in 2005. Furthermore, we present the concept of dynamic membership (DM) and show the composition of MA-ABE-DM schemes.

A. NOTATIONS
In the rest of this work, lowercase bold letters are used to represent column vectors, and uppercase bold letters are used to represent matrices, such as vector \( \mathbf{v} \) and matrix \( \mathbf{V} \). Also, the transpose of \( \mathbf{v} \) and \( \mathbf{V} \) will be \( \mathbf{v}^\top \) and \( \mathbf{V}^\top \), respectively. Moreover, a horizontal concatenation matrix of two matrices is denoted as \( [\mathbf{V}_1 | \mathbf{V}_2] \). Besides, we denote scalars with lowercase regular letters and denote sets with uppercase regular letters, such as scalar \( r \) and set \( U \). The size of the set \( U \) will be represented as \( |U| \).

B. LATTICE
Given a set of \( m \)-dimensional linearly independent vectors \( V = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\} \), where \( \mathbf{v}_i \in \mathbb{R}^m \) for \( 1 \leq i \leq n \). A lattice \( \Lambda \) with \( V \) can be defined as follows:

**Definition II.1.** The \( m \)-dimensional lattice is defined as

\[
\Lambda = \left\{ \sum_{i=1}^{n} s_i \mathbf{v}_i \mid s_i \in \mathbb{Z} \right\}
\]

For integer lattices, there are three common mathematical architectures as follows.
Definition II.2. Given a prime \( q \), a vector \( t \in \mathbb{Z}_q^n \), and a matrix \( A \in \mathbb{Z}_q^{n \times m} \), define:

\[
\Lambda_q(A) := \{ s \in \mathbb{Z}^m | \exists y \in \mathbb{Z}_q^n \text{ where } A^\top y = s \mod q \}
\]

\[
\Lambda_q^\pm(A) := \{ s \in \mathbb{Z}^m | As = 0 \mod q \}
\]

\[
\Lambda_q^t(A) := \{ s \in \mathbb{Z}^m | As = t \mod q \}
\]

Note that \( \Lambda_q^\pm(-) \) is a shift of \( \Lambda_q^\pm(-) + x \).

C. SHORT INTEGER SOLUTION (SIS)

According to the research done by Ajtai [26] in 1998, the following problems have been proved to be NP-Hard in the worst case.

Definition II.3. The Short Integer Solution (SIS)

Input an arbitrary matrix \( A \in \mathbb{Z}_q^{n \times m} \), a prime \( q \) and a factor \( \gamma \), find a nonzero vector \( x \in \mathbb{Z}_q^n \), where \( Ax = 0 \mod q \) and \( ||x|| \leq \gamma \).

Definition II.4. The Inhomogeneous Short Integer Solution (ISIS)

Input an arbitrary matrix \( A \in \mathbb{Z}_q^{n \times m} \), a prime \( q \), a target vector \( t \in \mathbb{Z}_q^n \) and a factor \( \gamma \), find a nonzero vector \( x \in \mathbb{Z}_q^n \), where \( Ax = t \mod q \) and \( ||x|| \leq \gamma \).

D. LEARNING WITH ERRORS (LWE)

In 2005, Regev [27] firstly defined the learning with errors (LWE) problem and demonstrated that for specific noise distribution \( \chi \), the LWE problem is as difficult as the worst-case of the gap shortest vector problem or shortest independent vectors problem under the quantum reduction shown by Peikert in [28]. The security of the proposed scheme is based on the hardness assumption of the D-LWE problem as shown in Figure 2 and Definition II.7.

Definition II.5. Oracle \( O_\chi \) and Oracle \( O_\Psi \):

Given a positive integer \( n \), a prime \( q \), and a specific discrete Gaussian distribution \( \chi \) over \( \mathbb{Z}_q \). Let \( O_\chi \) be a pseudo-random noise sampler with some random secret-vector \( s \in \mathbb{Z}_q^n \), and let \( O_\Psi \) be a truly-random sampler. The outputs of \( O_\chi \) and \( O_\Psi \) are defined as follows:

\( O_\chi \):
- Output a set of pseudo-random noise samples. Each sample is in the form of \( (u_i, v_i = u_i^\top s + x_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q \), where \( u_i \in \mathbb{Z}_q^n \) is a uniformly random vector, \( s \in \mathbb{Z}_q^n \) is a fixed secret-vector, \( x_i \in \mathbb{Z}_q \) is an ephemeral noise value sampled from \( \chi \).

\( O_\Psi \):
- Output a set of truly random samples \( (u_i, v_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q \), which is independently and uniformly random sampled from the whole domain \( \mathbb{Z}_q^n \times \mathbb{Z}_q \).

Definition II.6. The Search Learning With Errors (S-LWE) problem:

Instance arbitrary polynomial number of \( (\mathbb{Z}_q^n \times \mathbb{Z}_q) \) samples from \( O_\chi \), find the fixed secret-vector \( s \).

Definition II.7. The Decision Learning With Errors (D-LWE) problem:

Instance arbitrary polynomial number of \( (\mathbb{Z}_q^n \times \mathbb{Z}_q) \) samples from \( O_\chi \) or \( O_\Psi \), return YES if the samples are from \( O_\chi \), and return NO if the samples are from \( O_\Psi \).

An algorithm \( A \) can solve the D-LWE problem only if

\[
\text{Adv}^{D-LWE}(A) := |Pr[A_{O_\chi} = 1] - Pr[A_{O_\Psi} = 1]| > \epsilon
\]

where \( \epsilon \) is non-negligible, \( A_{O_\chi} = 1 \) denotes the case that \( A \) guesses correctly when the D-LWE problem generates samples from oracle \( O_\chi \), and \( A_{O_\Psi} = 1 \) denotes the case that \( A \) guesses correctly when the D-LWE problem generates samples from oracle \( O_\Psi \).

E. LATTICE TRAPDOOR

The proposed scheme applies the trapdoor generation function proposed by Micciancio and Peikert [24] since it is more efficient. The algorithms of the trapdoor functions are introduced as follows:

Let a gadget vector \( g = [1 \ 2 \ 4 \ \cdots \ 2^{k-1}] \in \mathbb{Z}_q^{k} \), where \( k = \log_2 q \) and \( q = 2^k \). There exists a matrix \( T_g \) such that

\[
T_g = \begin{bmatrix}
2 & 0 & \cdots & 0 \\
-1 & 2 & \cdots & 0 \\
0 & -1 & \cdots & \vdots \\
0 & 0 & \cdots & 2 \\
\vdots & \vdots & \ddots & \vdots \\
0 & \cdots & \cdots & -1
\end{bmatrix}, \text{ where } g \cdot T_g = 0 \mod q.
\]

Then, a gadget matrix \( G \) can be defined as

\[
G = I_n \otimes g = \begin{bmatrix}
g & 0 & \cdots & 0 \\
0 & g & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & \cdots & 0 & g
\end{bmatrix} \in \mathbb{Z}_q^{n \times w}, \text{ where } w = n k.
\]

And there also exists a matrix \( T_{G} \) corresponding to \( G \), such that

\[
T_G = I_w \otimes T_g = \begin{bmatrix}
T_g & 0 & \cdots & 0 \\
0 & T_g & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & \cdots & 0 & T_g
\end{bmatrix} \in \mathbb{Z}_q^{w \times w}.
\]

With the matrix \( T_G \), any SIS problem constructed with \( G \) can be simply solved.

With the special matrix \( G \), anyone may generate a trapdoor \( R \) and compute the corresponding matrix \( A \). Then he/she may solve the ISIS problem for matrix \( A \). The trapdoor generation function \( \text{GenTrap} \) and the function \( \text{SampleD} \) used to solve ISIS problem are described as follows:

- \( \text{GenTrap}(\bar{A}, H) \rightarrow (R, A) \)
  - Given a matrix \( \bar{A} \in \mathbb{Z}_q^{n \times m} \), an invertible matrix \( H \in \mathbb{Z}_q^{n \times n} \), and a distribution \( \chi \) over \( \mathbb{Z}_q^{m \times w} \). If \( \bar{A} \) and \( H \) are not given, then uniformly choose \( \bar{A} \in \mathbb{Z}_q^{n \times m} \) at random and set \( H \) as an identity matrix \( I \in \mathbb{Z}_q^{n \times n} \).
  - Let \( R \in \mathbb{Z}_q^{m \times w} \) be a matrix chosen from distribution

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3179110, IEEE Access
\(\chi\). Output a matrix \(A = [\tilde{A}|A_1] \in \mathbb{Z}^{n \times m}\), where \(m = m + w\) and \(A_1 = [H G - AR]\). The matrix \(R\) with tag \(H\) will be the trapdoor of \(\Lambda_q^t(A)\), with its quality guaranteed that \(s_1(R) \leq \sqrt{m} \omega(\sqrt{\log q})\), where the \(s_1(\cdot)\) function extracts the Euclidean length of the input matrix or vector.

- **SampleD(\(A, H, R, t, \sigma\)) \rightarrow x**
  
  Given a matrix \(\tilde{A} \in \mathbb{Z}^{m \times n}\), a trapdoor matrix \(R \in \mathbb{Z}^{m \times n}\), an invertible matrix \(H \in \mathbb{Z}^{q \times m}\) and a target vector \(t \in \mathbb{Z}^n\). Then, output a vector \(x \in \mathbb{Z}^n\) with the Gaussian parameter \(\sigma\), such that \(Ax = t \in \mathbb{Z}^n\), where \(A = [\tilde{A}|HG - AR]\). The details of generating the vector \(x\) is described as follows:

First, the algorithm randomly chooses a perturbation vector \(p \in \mathbb{Z}_q^m\) with \(\sigma\). The vector \(p\) can be divided into

\[p = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}, \text{ where } p_1 \in \mathbb{Z}_q^m \text{ and } p_2 \in \mathbb{Z}_q^n.\]

Further, the algorithm constructs an ISIS problem with \(G\) by computing

\[y_1 = \tilde{A}(p_1 - Rp_2) \in \mathbb{Z}_q^n \text{ and } y_2 = Gp_2 \in \mathbb{Z}_q^n.\]

and choosing a vector \(z \in \mathbb{Z}_q^n\) from \(\Lambda_q^x(G)\), where

\[v = H^{-1}(t - y_1) - y_2 = H^{-1}(t - A p) \in \mathbb{Z}_q^n.\]

Finally, the algorithm outputs

\[x = p + \begin{bmatrix} R \\ I_w \end{bmatrix} z, \text{ where } x \in \Lambda_q^t(A).\]

**F. DISCRETE GAUSSIANS**

**Definition II.8.** For any real number \(\sigma > 0\), Gaussian function with \(\sigma\) as the parameter and \(z\) as the center on \(\mathbb{R}^n\) can be defined as follows:

\[
\forall y \in \mathbb{R}^n, \rho_{\sigma,z}(y) = \exp\left(-\frac{\pi \|y - z\|^2}{\sigma^2}\right)
\]

And the corresponding discrete Gaussian distribution will be:

\[
\mathcal{D}_{\sigma, z}(y) = \sum_{x \in \mathbb{Z}_q^n} \rho_{\sigma, z}(x)
\]

Given a lattice \(L\), which is a subset of \(\mathbb{Z}^n\),

\[
\rho_{\sigma, z}(L) = \sum_{y \in L} \rho_{\sigma, z}(y)
\]

The discrete Gaussian distribution over \(L\) can be defined as:

\[
\forall x \in L, \mathcal{D}_{L, \sigma, z}(x) = \frac{\rho_{\sigma, z}(x)}{\rho_{\sigma, z}(L)}
\]

Note that, we usually omit the subscript if \(z\) is the origin or \(\sigma = 1\) and denote \(\chi = \mathcal{D}_{\sigma, z}(y)\).

**G. ACCESS STRUCTURE**

In ABE, a certain rule of attributes designed by a sender is called an access structure. The receivers can decrypt the ciphertext if and only if their attributes suffice the access structure of the ciphertext. Let \(U\) be the set of all attributes in the system, and \(U_{ID} \subseteq U\) be the attribute set of the user with identity \(ID\). Then, a sender chooses an access structure \(\tau\) that defined a rule of the attribute set \(U_{\tau} \subseteq U\) to encrypt the message. If we illustrate \(\tau\) with a tree structure, the leaf
nodes of $\tau$ will be the attributes in $U_C$, and each parent node may be one of the two types of operation gates, namely AND and OR. The user with the identity $ID$ can get the message only if $U_{ID}$ suffices the access structure $\tau$.

H. DYNAMIC MEMBERSHIP (DM)

The aims of dynamic membership management (DM) were proposed by Fan et al. [12] in 2013, which contains the following features:

- **Expandability**: Any user may enroll into the system whenever needed.
- **Renewability**: The system may update users’ attributes and get the corresponding private key.
- **Revocability**: The system may remove any attribute of a user, and make sure that the ciphertext encrypted by the new public parameters is unable to be decrypted by a revoked private key.
- **Independence**: Any user’s revocation and the updating process may be performed without affecting other users.

There are two ways to achieve revocability, namely indirect revocation and direct revocation. In an indirect revocation mechanism, the system needs to maintain a revocation list for each attribute. After each revocation, all unrevoked users have to update their private keys to ensure its effectiveness, which is a complicated work. On the other hand, a direct revocation mechanism simplifies the revocation process. In a direct revocation mechanism, none of unrevoked users will be affected after any revocation, this feature also called Independence. However, to carry out a direct revocation process, such a mechanism usually asks the sender to embed the revocation list into the ciphertext during encryption. The disclosure of the revocation list may cause some privacy issues.

I. MA-ABE-DM SCHEME

The proposed MA-ABE-DM scheme is composed of the following seven algorithms:

- **Setup($\lambda, D$)**: This algorithm takes a security parameter $\lambda$ and a set of attribute authorities $D$ as input and outputs the global public parameters $GP$.
- **AuthoritySetup($GP$)**: This algorithm takes the global public parameters $GP$ as input and outputs the master private key $MK_d$ and the public key $PK_d$ for the $d$-th attribute authority $AA_d$ in the attribute authority set $D$.
- **Enroll($GP, PK_d, MK_d, ID, U_{ID}$)**: This algorithm takes the user’s identity $ID$, the user’s attribute set $U_{ID}$, the public key $PK_d$, and the master private key $MK_d$ as input and outputs the partial private key $SK_{d, ID}$ for the user $ID$.
- **Revoke($GP, PK_d, ID, t$)**: This algorithm takes a public key $PK_d$, a user’s identity $ID$, and a target attribute $t$ as input and outputs the updated public key $PK_d'$. The algorithm updates $SK_{d, ID}$ to ensure the updated public key $PK_d'$.
- **Extend($GP, PK_d, MK_d, ID, t, SK_{d, ID}$)**: This algorithm takes a public key $PK_d$, a master private key $MK_d$, a user’s identity $ID$, a target attribute $t$, and the user’s partial private key $SK_{d, ID}$ as input and outputs the updated partial private key $(SK_{d, ID})'$. The algorithm takes a single-bit message $b$, an access tree $\tau$, and the public keys $\{PK_d\}_{d \in D_C}$ as input and outputs the ciphertext $C$, where $D_C$ is the set of attribute authorities monitoring attributes in $\tau$.
- **Decryp($GP, C, SK_{ID}$)**: This algorithm takes the ciphertext $C$ and the user’s private key $SK_{ID}$ as input and outputs the plaintext $b'$.

J. SECURITY MODEL OF MA-ABE-DM

**Definition II.9.** Let $A$ be a polynomial-time adversary, and $S$ be a challenger. $S$ simulates an IND-CPA$_{MA-ABE-DM}$ game under the selective model as follows:

- **Init**: $A$ declares a target access tree $\tau$ and the target user’s identity $ID^*$ and sends them to $S$, where $\tau$ is form with some operation gates and a set of attributes $U_C$. Besides, $A$ also provides a list of corrupted attribute authorities $D_{corrupt}$. Note that, $D_C$ is the set of attribute authorities monitoring attributes in $U_C$ which is restricted not to be a subset of $D_{corrupt}$.
- **Setup**: $S$ runs Setup to generate the global public parameters $GP$ and sends it to $A$.
- **AuthoritySetup**: $S$ runs AuthoritySetup to generate public key $PK_d$ and master private key $MK_d$ of each attribute authority $AA_d$. Then, $S$ sends public keys $\{PK_d\}_{d \in D}$ to $A$. For those corrupted attribute authorities, $S$ provides the corresponding master private keys $\{MK_d\}_{d \in D_{corrupt}}$ to $A$ as well.
- **Phase I**: $A$ may issue the following queries.
  - **Enroll**: $A$ submits $(ID, U_{ID})$ to $S$, where $ID$ is a user’s identity and $U_{ID}$ is an attribute set for $ID$. If $ID = ID^*$, $S$ provides only the public parameter $B^{d, P}_{A_d \ast}$ to $A$. Otherwise, $S$ runs Enroll to create the user’s private key $SK_{ID}$ and adds the public parameters $\{B^{d, ID}_{A_d}\}_{d \in U_{ID}}$ into the corresponding public key $PK_d$, and then returns $SK_{ID}$ to $A$.
  - **Revoke**: $A$ submits $(ID, t)$ to $S$, where $t$ is an attribute monitored by $AA_d$ in $U_{ID}$. If $ID = ID^*$ and $t$ is an element in $U_C$, abort the query. Otherwise, $S$ runs Revoke to revoke the attribute $t$ for $ID$ and update the public key $PK_d$.
  - **Extend**: $A$ submits $(ID, t)$ to $S$, where $t$ is an attribute monitored by $AA_d$ but not an element in $U_{ID}$. If $ID = ID^*$ and $t$ is an element in $U_C$, $S$ provides only the public parameter $B^{d, P}_{A_d \ast}$ to $A$. Otherwise, $S$ runs Extend to create the private key $e^{d, ID}_{A_d \ast}$ and adds the public parameter $B^{d, ID}_{A_d \ast}$ into the corresponding public key $PK_d$, and then returns $e^{d, ID}_{A_d \ast}$ to $A$. 
Challend:
\( \mathcal{A} \) delivers two distinct single-bit messages \((m_0, m_1)\) to \( \mathcal{S} \). Then, \( \mathcal{S} \) randomly selects \( b \in \{0, 1\} \) and generates the ciphertext \( C_b \) corresponding to \( b \) and the access tree \( \tau \). Then, \( \mathcal{S} \) sends \( C_b \) to \( \mathcal{A} \) as the challenge.

Phase 2:
\( \mathcal{A} \) may issue more queries as defined in Phase 1.

Guess:
In the end, \( \mathcal{A} \) answers a bit \( b' \in \{0, 1\} \) and wins the \( \text{IND-CPA}_{\mathcal{MA}, \mathcal{ABE}-\mathcal{DM}} \) game if \( b' = b \). The advantage of \( \mathcal{A} \) winning the \( \text{IND-CPA}_{\mathcal{MA}, \mathcal{ABE}-\mathcal{DM}} \) game is defined as
\[
\text{Adv}_{\text{IND-CPA}_{\mathcal{MA}, \mathcal{ABE}-\mathcal{DM}}} (\mathcal{A}) = \left| Pr[b' = b] - \frac{1}{2} \right|.
\]

An MA-ABE-DM scheme is selectively \( \text{IND-CPA}_{\mathcal{MA}, \mathcal{ABE}-\mathcal{DM}} \) secure if there does not exist any polynomial-time adversary that can win the \( \text{IND-CPA}_{\mathcal{MA}, \mathcal{ABE}-\mathcal{DM}} \) game with non-negligible advantage.

III. RELATED WORKS
In this section, we introduce some traditional MA-ABE schemes and some ABE schemes based on lattices. Moreover, we show the properties comparison between the proposed scheme and related works.

A. PROPERTIES COMPARISON
The proposed scheme achieves the dynamic membership management property with the security guaranteed, which is more functional than others. The details of the properties comparison are shown in TABLE I.

As shown in TABLE I, Chang’s scheme and Ming et al.’s scheme lack quantum-resistance property. Both Zhang et al.’s scheme and Liu et al.’s scheme lack renewability, revocability, and independence properties. Furthermore, those schemes are KP-ABE, which is worse than CP-ABE in one-to-many encryption. Wang et al.’s scheme lacks independence property due to its indirect revocation process. Meng’s scheme lacks renewability property due to the private key of each user is fixed by the key generation phase. Moreover, both Wang et al.’s scheme and Meng’s scheme don’t support Multi-Authority. Thus, the proposed scheme provides the most complete properties for an MA-ABE scheme.

B. TRADITIONAL MA-ABE SCHEMES
1) Chang’s Traditional MA-ABE-DM Scheme
In 2019, Chang [13] proposed an MA-ABE-DM scheme. In Chang’s scheme, any authority can be the "Initializer" who may set up and aggregate public parameters from all attribute authorities without a central authority. This scheme grasped the advantages of both direct and indirect revocation mechanisms to design a new approach that holds privacy and independence simultaneously. The trick of Chang’s scheme is to generate a unique key for each attribute value of every user, which implies that even if there are two users having the same attribute value, their attribute keys are distinct. After a user enrolled, there will be a correlated public parameter for each attribute key so that anyone can encrypt the message by adding the corresponding public parameters of the chosen attributes. This scheme was proved to be secure under the hardness of the decisional bilinear Diffie-Hellman (DBDH) problem. However, the DBDH problem is unable to resist the quantum attacks proposed by Shor [16].

2) Ming et al.’s Traditional MA-ABE Scheme
Ming et al. [23] proposed a pairing-free MA-ABE scheme with revocability. Without pairing operations, their scheme has a lower computational cost. However, unrevoked users need to update their private keys in the revocation mechanism. Moreover, this scheme was proved to be IND-CPA secure under the decisional Diffie-Hellman (DDH) assumption, which is also unable to resist the quantum attacks.

C. LATTICE-BASED REVOCABLE CP-ABE SCHEMES
We introduce some CP-ABE schemes on lattices with revocation or updating mechanisms here. Wang et al. [29] added the attribute modification mechanism into the CP-ABE and proved their scheme was secure under the random oracle model. After that, Meng [30] proposed a directly revocable CP-ABE scheme in 2020, which is more intuitive than the previous works. However, both schemes were constructed under a single authority, which is not suitable for reality.

1) Wang et al.’s Revocable and Grantable CP-ABE Scheme on Lattices
In Wang et al.’s [29] scheme, they presented an efficient revocable and grantable CP-ABE scheme. They built a binary tree for each attribute and constructed the key-update process with the KUNodes algorithm. Also, they proved that their scheme was secure under the selective and random oracle model. However, the revocation mechanism in Wang et al.’s scheme is indirect, which means that the other users will be affected after the revocation process. Moreover, the scheme is based on a single authority scenario, which does not match the practical condition.

2) Meng’s Revocable CP-ABE Scheme on Lattices
In Meng’s [30] work, there are two directly revocable CP-ABE schemes on lattices. One can achieve user-level revocation, and another can achieve attribute-level revocation. To directly revoke a user or an attribute, the sender embeds the revocation list into the ciphertext during encryption. As mentioned above, the benefit of a direct revocation mechanism is that there is no other user will be affected. Besides, the attribute authority is able to perform revocation without issuing any updated key, which reduces lots of work. However, the revocation list in Meng’s scheme reveals the identities of revoked users, which invades the privacy of the revoked users. Furthermore, their scheme is based on a single authority scenario, which conflicts with the practical condition.
TABLE 1: Properties Comparison

| Notations | Quantum-Resistance | Multi-Authority | CP-ABE | Dynamic Membership | Collusion-Resistance | Security Proof |
|-----------|--------------------|-----------------|--------|--------------------|----------------------|----------------|
| Chang [15] | ×                  | ✓               | ✓      | ✓                  | ✓                    | CCA            |
| Ming et al. [28] | ×                  | ✓               | ✓      | ✓                  | ✓                    | CCA            |
| Wang et al. [29] | ✓                  | ×               | ✓      | ✓                  | ✓                    | CCA            |
| Meng [30] | ✓                  | ×               | ✓      | ✓                  | ✓                    | CPA³          |
| Zhang et al. [21] | ✓                  | ✓               | ×      | ✓                  | ✓                    | CPA            |
| Liu et al. [22] | ✓                  | ✓               | x     | x                  | x                    | CPA            |
| Datta et al. [23] | ✓                  | ✓               | ✓      | ✓                  | ✓                    | CPA            |
| Ours      | ✓                  | ✓               | ✓      | ✓                  | ✓                    | CPA            |

1 Exp, Ren, Rev, and Ind denote expandability, renewability, revocability, and independence, respectively.

2 Although Wang et al. claimed that their scheme is CCA secure, they did not simulate the decryption oracle in their proof.

D. LATTICE-BASED MA-ABE SCHEMES

We show some MA-ABE schemes on lattices here.

1) Zhang et al.’s MA-ABE Scheme on Lattices

Zhang et al. [21] firstly proposed a lattice-based MA-ABE scheme in 2015. Although the scheme requires a central authority (CA) to authenticate identities and handle attributes of users, they avoid the key escrow problem by depriving the key generating ability of the central authority. However, there are some shortages of Zhang et al.’s scheme. First, there are neither revocation nor updating mechanisms in the scheme, which is inconvenient for member management. Second, their scheme is KP-ABE. Third, the probability of two distinct users having the same attribute private key is non-negligible in their scheme, which may cause a collusion attack.

2) Liu et al.’s MA-ABE Scheme on Lattices

Liu et al. [22] proposed an efficient MA-ABE scheme on lattices in 2018. Taking advantage of the theory in Micciancio and Peikert et al.’s work, they constructed an optimized sampling function to create stronger trapdoors in the key generation process. Besides, they also proved their scheme to be IND-CPA secure, but there is still a lack of modification mechanism for attributes. Precisely, there are neither revocation nor updating mechanisms in the scheme as well, which is inconvenient for member management. Moreover, their scheme is KP-ABE, too.

3) Datta et al.’s MA-ABE Scheme on Lattices

In 2021, Datta et al. [23] proposed an MA-ABE scheme on lattices, which is CP-ABE. Moreover, their scheme supports access policies described in disjunctive normal form. However, neither revocation nor updating mechanisms are provided in their scheme.

IV. CONSTRUCTION

In the proposed lattice-based MA-ABE-DM scheme, as shown in Figure 3, an initializer firstly runs Setup to generate the global public parameters, and each attribute authority runs AuthoritySetup to create its own public key and private key. After that, each attribute authority runs Enroll to generate the partial private key of each user. Once a user’s attribute changes, the attribute authority runs Revoke or Extend algorithm to update the public key and user’s partial private key. When sending a message, the sender runs Encrypt to generate the ciphertext and sends it to the receivers. Then, receivers run Decrypt to recover the message. The notations are shown in TABLE 2.

A. THE PROPOSED SCHEME

We show the details of the proposed scheme, which consists of seven algorithms: Setup, AuthoritySetup, Enroll, Revoke, Extend, Encrypt and Decrypt.

TABLE 2: The Notations

| Notation | Meaning |
|----------|---------|
| D        | the set of all attribute authorities |
| L        | the set of all enrolled users’ identities |
| AA_d     | the d-th attribute authority |
| |       | the number of the elements in some set |
| ID       | the identity of some user |
| X        | a Gaussian distribution |
| U        | the set of all attributes |
| U_d      | the set of attributes monitored by AA_d |
| U_{ID}   | the set of attributes of ID |
| U_{ID}   | the intersection of U_{ID} and U_d |
| U_{C}    | the set of attributes associated with the ciphertext C |
| D_C     | the set of attribute authorities monitoring attributes in U_C |
| U_{C}    | the intersection of U_C and U_d |
| U_{ID}   | the intersection of U_{ID} and U_C |
| P_{K_d}  | the public key of AA_d |
| M_{K_d}  | the master private key of AA_d |
| S_{P_{ID}} | the partial private key of ID for AA_d |
| S_{K_{ID}} | the private key of ID |
| G        | a gadget matrix |
public parameters:

1) With a security parameter \( \lambda \), select a prime \( q \), three positive integers \( n, \tilde{m}, w \) and two positive Gaussian parameters \( \sigma, \alpha \). Note that \( m = \tilde{m} + w \).

2) Let \( D \) be the set of all attribute authorities, \( U \) be the set of all attributes, and \( L \) be the set of all enrolled users’ identities.

3) Set the Gaussian distribution \( \chi \) with the parameters \( \sigma \) and \( \alpha \).

4) Randomly choose a vector \( u \in \mathbb{Z}_q^n \).

5) Publish the global public parameters \( GP = \{q, n, \tilde{m}, w, \sigma, \alpha, \chi, u, G, D, U, L\} \), where \( G \) is the gadget matrix defined in Section II-E.

C. AUTHORITY SETUP

After the Initializer publishes \( GP \), each \( AA_d \) runs the following steps to create its own public key and private key:

1) Let \( U_d \) be the set of attributes monitored by \( AA_d \). For each attribute in \( U_d \), randomly choose two matrices \( \bar{A}_{d,i} \in \mathbb{Z}_q^{\tilde{m} \times m} \) and \( H_{d,i} \in \mathbb{Z}_q^{\tilde{m} \times n} \), where \( H_{d,i} \) is an invertible matrix.

2) Initialize an empty set \( B_d = \{\emptyset\} \) and set \( A_d = \{\bar{A}_{d,i}\}_{i \in U_d} \). Then, publish \( \{A_d, B_d\} \) as the public key \( PK_d \).

3) Set \( \{H_{d,i}\}_{i \in U_d} \) as the master private key \( MK_d \).

D. ENROLL

An enrollment request for \( AA_d \) includes the user’s identity \( ID \) and a set of attribute \( U_d^{ID} \), where \( U_d^{ID} \) denotes the set of attributes of \( ID \) monitored by \( AA_d \). After receiving the enrollment request, each \( AA_d \) generates the private key for \( U_d^{ID} \) through the following steps:

1) \( \forall i \in U_d^{ID} \):
   a) Run \( \text{GenTrap}(\bar{A}_{d,i}, H_{d,i}) \) defined in Section II-E to sample a matrix \( T_{d,i}^{ID} \in \mathbb{Z}_q^{\tilde{m} \times w} \) and generate \( \bar{B}_{d,i}^{ID} = [\bar{A}_{d,i} | H_{d,i} G - \bar{A}_{d,i} T_{d,i}^{ID}] \in \mathbb{Z}_q^{\tilde{m} \times m} \), where \( T_{d,i}^{ID} \) is the trapdoor of \( \Lambda_q^{\tilde{m}}(\bar{B}_{d,i}^{ID}) \).

b) Set \( \{\bar{B}_{d,i}^{ID}\}_{i \in U_d^{ID}} \) and \( \{e_{d,i}^{ID}\}_{i \in U_d^{ID}} \).

2) \( \forall i \in U_d - U_d^{ID} \):
   a) Randomly choose a matrix \( R \in \mathbb{Z}_q^{n \times w} \).
   b) Set \( B_{d,i}^{ID} = \lfloor \bar{A}_{d,i} | R \rfloor \).

3) Add \( \{B_{d,i}^{ID}\}_{i \in U_d} \) into \( B_d \) in \( PK_d \).

4) Set the user’s partial private key \( SK_d^{ID} = \{e_{d,i}^{ID}\}_{i \in U_d^{ID}} \) and send it to \( ID \).

5) Add \( ID \) into \( L \) if \( ID \notin L \).

Finally, \( ID \) sets his/her private key \( SK_d^{ID} = \{SK_d^{ID}\}_{d \in D} = \{e_{d,j}^{ID}\}_{j \in U_d^{ID}, d \in D} \).

E. REVOKE

A revoking request for \( AA_d \) includes the target attribute \( t \) and the user’s identity \( ID \). After receiving the revoking request, \( AA_d \) revokes the target attribute for \( ID \) through the following steps:

1) Randomly choose a matrix \( R' \in \mathbb{Z}_q^{n \times w} \).

2) Set \( \{B_{d,t}^{ID}'\} = \lfloor \bar{A}_{d,t} | R' \rfloor \).

3) Replace \( B_{d,t}^{ID} \) with \( \{B_{d,t}^{ID}'\} \).

F. EXTEND

An extending request for \( AA_d \) includes the target attribute \( t \) and the user’s identity \( ID \). After receiving the extending request, \( AA_d \) generates the private key of the target attribute for \( ID \) through the following steps:

1) Run \( \text{GenTrap}(\bar{A}_{d,t}, H_{d,t}) \) to generate \( \{B_{d,t}^{ID}'\} \) and \( \{T_{d,t}^{ID}\} \).

2) Run \( \text{SampleD}(\bar{A}_{d,t}, H_{d,t}, T_{d,t}^{ID}, u, \sigma) \) to generate \( e_{d,t}^{ID} \), where \( \{B_{d,t}^{ID}'\} e_{d,t}^{ID} = u \).

3) Replace \( B_{d,t}^{ID} \) with \( \{B_{d,t}^{ID}'\} \).

4) Set the partial private key \( \{SK_d^{ID}'\} = SK_d^{ID} \cup \{e_{d,t}^{ID}\} \) and send it to \( ID \).
Finally, \( ID \) updates his/her private key \((SK_{ID})' = (SK_{ID} - SK_d) \cup (SK_d')\).

G. ENCRYPT

A sender encrypts a single-bit message \( b \) with a chosen access tree \( \tau \) by the following steps:

1. Randomly choose a noise value \( x \in \chi \).
2. Choose a access tree \( \tau \) which is form with some operation gates and a set of attributes \( U_C = \{U_d^c\}_{d \in D_C} \), where \( D_C \) is the set of attribute authorities monitoring attributes in \( U_C \).
3. For each attribute \( j \in U_d^c \), randomly choose a noise vector \( x_d,j \in \chi^m \).
4. For each \( ID \in L \), choose a random value \( r^{ID} \in \mathbb{Z}_q \) and a vector \( s^{ID} \in \mathbb{Z}_q^n \) and set
   \[ C^{ID} = u^T s^{ID} \cdot r^{ID} + x + b|q \over 2| (\text{mod } q) \in \mathbb{Z}_q. \]
5. Set the root node value of \( \tau \) as \( r^{ID} \). Then, starting from the root node, assign a value to each leaf node according to the operation gates in \( \tau \):
   - When comes a AND gate, and \( M \) be the set of all its child nodes. Divide the parent node into \( |M| \) parts, where \( r^{ID} = \sum_{j \in M} r_{j}^{ID} (\text{mod } q) \).
     Set each child node value as one of parts \( r_{j}^{ID} \).
   - When comes a OR gate, and \( M \) be the set of all its child nodes. Set each child node value as same as the value of their parent node such that \( \forall j \in M, r_{j}^{ID} = r^{ID} \).
6. For each attribute \( j \in \{U_d^c\}_{d \in D_C} \), generate the partial ciphertext for each \( ID \) as follows:
   \[ C_{d,j}^{ID} = (B_{d,j}^T) s^{ID} \cdot r_{j}^{ID} + x_{d,j} (\text{mod } q) \in \mathbb{Z}_q^m. \]
7. Then set the ciphertext
   \[ C = \{C^{ID}, \{C_{d,j}^{ID}\}_{j \in U_d^c}, \{\tau\}_{ID \in L}\}. \]
8. Send the ciphertext \( C \) to the receivers.

H. DECRYPT

After receiving the ciphertext \( C \), any user whose attribute set satisfies \( \tau \) inputs his/her private key \( SK_{ID} = \{e_{d,j}\}_{j \in U_d, d \in D} \) and runs the following steps:

1. Compute \( b' \) according to the operation gates in \( \tau \). For the convenience of explanation, we show the case where all operation gates are AND and the case where all operation gates are OR as follows:
   - When \( \tau \) is composed with only AND gates:
     \[ b' = C^{ID} - \sum_{j \in \tau} (e_{d,j}^{ID})^T C_{d,j}^{ID} (\text{mod } q) \]
   - When \( \tau \) is composed with only OR gates:
     \[ b' = C^{ID} - (e_{d,j}^{ID})^T C_{d,j}^{ID} (\text{mod } q), \text{ where } j \in U_C. \]
2. Output \( b \) if \( |b' - \frac{q}{4}| < \frac{q}{4} \), else output \( b = 0 \).

I. CORRECTNESS

We show the correctness of the formulas in decryption as follows. For the convenience of explanation, assume that \( \tau \) only composed with AND gates:

\[
\begin{align*}
b' &= C^{ID} - \frac{\sum_{j \in \tau} (e_{d,j}^{ID})^T C_{d,j}^{ID} (\text{mod } q)}{(\text{mod } q)} \\
&= C^{ID} - \frac{\sum_{j \in \tau} (e_{d,j}^{ID})^T (B_{d,j}^T) s^{ID} \cdot r_{j}^{ID} + x_{d,j} (\text{mod } q)}{(\text{mod } q)} \\
&= u^T (s^{ID} \cdot r^{ID} + x + b|q \over 2|) - \frac{\sum_{j \in \tau} (e_{d,j}^{ID})^T (B_{d,j}^T) s^{ID} \cdot r_{j}^{ID} + x_{d,j} (\text{mod } q)}{(\text{mod } q)} \\
&= u^T s^{ID} \cdot r^{ID} + x + b|q \over 2| - \frac{\sum_{j \in \tau} (e_{d,j}^{ID})^T x_{d,j} (\text{mod } q)}{(\text{mod } q)} \\
&= \frac{b|q \over 2| + x + \sum_{j \in \tau} (e_{d,j}^{ID})^T x_{d,j}}{(\text{mod } q)} \\
&= \frac{b|q \over 2| + x + \sum_{j \in \tau} (e_{d,j}^{ID})^T x_{d,j}}{(\text{mod } q)} \]
\end{align*}
\]

Thus, compute \( |b' - \frac{q}{4}| \). If \( b' = 1 \), the result will be less than \( \frac{q}{4} \). Otherwise, if \( b' = 0 \), the result will be large or equal to \( \frac{q}{4} \).

V. SECURITY PROOF

In this section, we prove the proposed scheme to be selectively IND-CPA_{MA-ABE-DM} secure under the D-LWE assumption. The flows of IND-CPA_{MA-ABE-DM} game are shown in Figure 4

Proof. If any polynomial-time adversary \( A \) can win the IND-CPA_{MA-ABE-DM} game defined in Section II with non-negligible advantage \( \epsilon \), it implies that the challenger \( S \) can solve the D-LWE problem by simulating the following game:

- Init:
  1. \( A \) determines a set of corrupted attribute authorities \( D_{\text{corrupt}} \).
  2. Without loss of generality, we consider the most extreme condition that only one attribute authority \( AA_d \) is corrupted, so that \( D_{\text{corrupt}} = D - AA_d \).
  3. \( A \) determines the target access tree \( \tau \), where \( \tau \) is form with some operation gates and a set of attributes \( U_C = \{U_d^c\}_{d \in D_C} \).
  4. Besides, \( A \) also determines the target user's ID'. Note that, \( U_C \) must contain at least one attribute monitored by \( AA_d \). In other words, \( D_C \) cannot be a subset of \( D_{\text{corrupt}} \).
  5. Let \( |U_C'| = k' \) and \( |D| = k \). \( S \) gets \( m \times |U_C| + 1 \) samples from D-LWE oracle as follows:
     \[ (u_{i_0}, v_0), \]
     \[ \{(u_{i_1}, v_{i_1}), (u_{i_2}, v_{i_2}), \ldots, (u_{i_m}, v_{i_m})\}, \]
     \[ \{(u_{i_1}, u_{i_2}, v_{i_1}), (u_{i_2}, u_{i_1}, v_{i_2}), \ldots, (u_{i_m}, u_{i_m}, v_{i_m})\}, \]
     \[ \ldots \]
     \[ \{(u_{i_1}, v_{i_1}), (u_{i_2}, v_{i_2}), \ldots, (u_{i_m}, v_{i_m})\}, \]
     \[ \{(u_{i_1}, v_{i_1}), (u_{i_2}, v_{i_2}), \ldots, (u_{i_m}, v_{i_m})\}, \]
     \[ \ldots \]
     \[ \{(u_{i_1}, v_{i_1}), (u_{i_2}, v_{i_2}), \ldots, (u_{i_m}, v_{i_m})\}, \]
     \[ \{(u_{i_1}, v_{i_1}), (u_{i_2}, v_{i_2}), \ldots, (u_{i_m}, v_{i_m})\}, \]
     \[ \ldots \]
     \[ \{(u_{i_1}, v_{i_1}), (u_{i_2}, v_{i_2}), \ldots, (u_{i_m}, v_{i_m})\}. \]

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/
Er-Shuo Zhuang et al.: Preparation of Papers for IEEE Access

FIGURE 4: The Security Proof

- **Setup:**
  1. $S$ sets $u = u_0$.
  2. $S$ follows the Setup algorithm defined in Section IV-B to obtain the global public parameters $GP = \{q, n, m, \sigma, \alpha, \chi, u, G, D, U, L\}$.

- **AuthoritySetup:**
  1. For each attribute in $U_d = U_d^C$, $S$ follows the AuthoritySetup algorithm defined in Section IV-C to select two matrices $\tilde{A}_{d,i}$ and $H_{d,i}$.
  2. For each attribute in $U_d$, $S$ sets the matrix $\tilde{A}_{d,i} = [u_{d,i}^1 | \cdots | u_{d,i}^m]$ and selects $H_{d,i}$ randomly.
  3. $S$ publishes $\mathcal{A}_d = \{\tilde{A}_{d,i}\}_{i \in U_d}$ and $B_d = \{0\}$ as the public key $PK_d$ and sets $\{H_{d,i}\}_{i \in U_d}$ as the master private key $MK_d$. If $AA_d$ is corrupted, send $MK_d$ to $A$ as well.

- **Phase 1:** $A$ may issue the following queries.
  - **Enroll:** Take $(ID, U_{1D})$ as input. If $ID = ID^*$, for each attribute in $U_{1D}^C$, $S$ sets the matrix $B_{d,i}^{ID^*} = [\tilde{A}_{d,i} | u_{d,i}^{m+1} | \cdots | u_{d,i}^m]$, which also means that $B_{d,i}^{ID^*} = [u_{d,i}^1 | \cdots | u_{d,i}^m]$. Then, $S$ updates the public key $PK_d$ with $B_{d,i}^{ID^*}$. Otherwise, $S$ follows the Enroll algorithm defined in Section IV-D to generate the matrix $B_{d,i}^{ID}$ and the vector $e_{d,i}^{ID}$ for each attribute in $U_{1D}$. Then, $S$ returns the private key $SK_{1D} = \{e_{d,i}^{ID}\}_{i \in U_{1D}}$ to $A$ and updates the public key $PK_d$ with $\{B_{d,i}^{ID}\}_{i \in U_{1D}}$.
  - **Revoke:** Take $(ID, t)$ as input, where $t$ is an attribute monitored by $AA_d$ in $U_{1D}$. If $ID = ID^*$ and $t$ is an element in $U_C$, abort the query. Otherwise, $S$ follows the Revoke algorithm defined in Section IV-E to remove $t$ from $U_{1D}$ by updating the public key $PK_d$.

- **Challenge:**
  - **Extend:** Take $(ID, t)$ as input. If $ID = ID^*$ and $t$ is an element in $U_C$, $S$ sets the matrix $B_{d,t}^{ID^*} = [\tilde{A}_{d,t} | u_{d,t}^{m+1} | \cdots | u_{d,t}^m]$, which also means that $B_{d,t}^{ID^*} = [u_{d,t}^1 | \cdots | u_{d,t}^m]$. Then, $S$ updates the public key $PK_d$ with $B_{d,t}^{ID^*}$. Otherwise, $S$ follows the Extend algorithm defined in Section IV-F to generate the matrix $B_{d,t}^{ID}$ and the vector $e_{d,t}^{ID}$. Then, $S$ returns the private key $e_{d,t}^{ID}$ to $A$ and updates the public key $PK_d$ with $B_{d,t}^{ID}$.

- **Challenge:**
  - **Challenge:** $A$ delivers two distinct single-bit messages $(m_0, m_1)$ to $S$. Then, $S$ randomly chooses a message $b \in (m_0, m_1)$ and performs the following steps to encrypt $b$ with $\tau$.
  1. For each attribute in $U_C$, set $v_{d,j} = (v_{d,j}^1, \ldots, v_{d,j}^m)$.
  2. Set the ciphertext $C = v_0 + b \cdot \frac{q}{2} \in \mathbb{Z}_q \mod q$.
  3. For each attribute in $\{U_{d}^C\}_{d \in D_C}$, generate the partial ciphertext $C_{d,j} = v_{d,j} \in \mathbb{Z}_q^m$.
  4. Then get $C_b = \{C, \{C_{d,j}\}_{j \in U_{d}^C, d \in D_C, U_C}\}$.
  5. $S$ sends the ciphertext $C_b$ to $A$ as the challenge.

- **Phase 2:**
  - $A$ may issue more queries as defined in Phase 1.
Guess:
In the end, \( A \) answers a bit \( b' \in \{0, 1\} \) to \( S \). If \( b' = b \), \( S \) outputs \( \mathcal{O}_x \) to the D-LWE oracle. Otherwise, \( S \) outputs \( \mathcal{O}_q \) to the D-LWE oracle.

If the samples are chosen from \( \mathcal{O}_x \), we will have that
\[
C = v_0 + b\left[\frac{q}{2}\right] = u_1^\top s + x + b\left[\frac{q}{2}\right] \pmod{q} \in \mathbb{Z}_q
\]
and
\[
C_{d,j} = v_{d,j} = [u_{d,j}^1 | u_{d,j}^2 | \cdots | u_{d,j}^m]^\top s + x_{d,j} \pmod{q}.
\]
The ciphertext will be
\[
C_b = \{ C, \{ C_{d,j} \}_{j \in U_q^D}, d \in D_C, U_C \}.
\]
Since \( A \) is able to win the IND-CPA\textsubscript{MA-ABE-DM} game with advantage \( \epsilon \), the probability that \( A \) wins the IND-CPA\textsubscript{MA-ABE-DM} game is \( \frac{1}{2} + \epsilon \). Therefore, in this case, the probability that \( S \) correctly guesses the D-LWE oracle is \( \frac{1}{2} + \epsilon \).

Otherwise, if the samples from the D-LWE oracle are uniformly random chosen from \( \mathcal{O}_q \), the ciphertext \( C_b \) is uniformly random. In this case, the probability that \( S \) correctly guesses the D-LWE oracle is \( \frac{1}{2} \).

Thus, the advantage for \( S \) to solve the D-LWE problem will be:
\[
\left| \Pr[S^{O_x} = 1] - \Pr[S^{O_q} = 1] \right| = \frac{1}{2} + \epsilon - \frac{1}{2} = \epsilon.
\]
Therefore, if \( A \) can win the IND-CPA\textsubscript{MA-ABE-DM} game with non-negligible advantage \( \epsilon \), it implies that \( S \) can solve the D-LWE problem in polynomial-time with non-negligible advantage \( \epsilon \).

VI. COMPARISON
In this section, we present the comparison between the proposed scheme, Zhang et al.’s [21] scheme, Liu et al.’s [22] schemes, and Datta et al.’s [23] schemes, which are MA-ABE schemes on lattices. For a fair comparison, the corresponding parameters in all schemes are set to the same values, as shown in TABLE 3.

Note that properties comparison is shown in Section III-A.

A. COMPUTATION COST
We estimate the cost with the set of practical parameters given in TABLE 4. Also, we implement the operations via python(3.8.3) with library Numpy(1.19.3) and perform on the environment of Windows 10 Enterprise system with Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz and 8.00GB RAM. The notations of the operators and their computation cost are given in TABLE 4 and the computation cost of the encryption and the decryption are listed in TABLE 5.

As shown in TABLE 5, the computation cost of the encryption in the proposed scheme is \( g \) times of the related works, which is the cost of achieving independence property.

Nevertheless, the encryption cost of the proposed scheme with \( g = 100 \) is 3.2093 (s), which is still within an acceptable range. Moreover, we provide more flexible access structures than the related works with the much lower decryption cost, which makes the proposed scheme more efficient and functional.

B. TRANSMISSION COST
The estimation is performed under the set of practical parameters given in TABLE 3. Let \( U_C \) with size \( h \) be the set of attributes associated with the ciphertext, and \( U_C' \) with size \( h' \) be the smallest set of attributes that satisfies \( U_C \). Assume that \( g \) is the total number of the users and \( k \) is the total number of the attribute authorities.

As shown in TABLE 6, the ciphertext length of the proposed scheme has to multiply the total number of the users \( g \), which is the cost of achieving independence property. Besides, due to the form of ciphertext in Zhang et al.’s work and Liu et al.’s work is nearly the same, the transmission cost and the computation cost are almost the same as well.

VII. CONCLUSION
In this research, a lattice-based multi-authority ABE with dynamic membership management has been proposed. First, the sender can design the access structure, since the proposed scheme is a CP-ABE scheme. Second, with dynamic membership management, all private keys may be updated independently. Third, it supports multi-authority to resolve the key escrow problem. Fourth, based on lattice hard problems, the proposed scheme resists quantum attacks. Fifth, it can effectively prevent collusion attacks by users. Finally, the proposed scheme is provably IND-CPA secure under the D-LWE assumption, which ensures the confidentiality of the ciphertext.

Although the transmission cost and the computation cost in the encryption process of the proposed scheme are higher than in the previous works, these costs are worth sacrificing for adding more practical features. Besides, the computation cost of the decryption of the proposed scheme is much lower than the previous works, which is more beneficial to the receivers. In the future, we will try to enhance the performance of the proposed scheme. Specifically, how to
TABLE 4: The Notations and Operation Cost

| Notation | Meaning | Cost |
|----------|---------|------|
| $T_{mul1}$ | The computation time of a multiplication $(\mathbb{Z}_q^n \times \mathbb{Z}_q)$ | 0.003 (ms) |
| $T_{mul2}$ | The computation time of a multiplication $(\mathbb{Z}_q^n \times \mathbb{Z}_q)$ | 3.080 (ms) |
| $T_{mul3}$ | The computation time of a multiplication $(\mathbb{Z} \times \mathbb{Z}_q)$ | 0.084 (ms) |
| $T_{mul4}$ | The computation time of a multiplication $(\mathbb{Z} \times \mathbb{Z}_q)$ | 0.002 (ms) |
| $T_{mul5}$ | The computation time of a multiplication $(\mathbb{Z}_q^n \times \mathbb{Z}_q)$ | 2.679 (ms) |
| $T_{mul6}$ | The computation time of a multiplication $(\mathbb{Z}_q^n \times \mathbb{Z}_q)$ | 0.013 (ms) |
| $T_{add1}$ | The computation time of an addition $(\mathbb{Z}_q^n \times \mathbb{Z}_q)$ | 0.045 (ms) |

TABLE 5: Computation Cost

| Encryption Cost |
|-----------------|
| **Zhang et al.** | $T_{mul1} + h \ast (T_{mul2} + T_{mul3} + T_{add1})$ | $\approx 0.003 + (3.209)h \approx 32.093$ (ms) |
| **Liu et al.** | $T_{mul1} + h \ast (T_{mul2} + T_{mul3} + T_{add1})$ | $\approx 0.003 + (3.209)h \approx 32.093$ (ms) |
| **Datta et al.** | $h \ast T_{mul2} + h \ast k \ast (T_{mul2} + T_{add1})$ | $\approx (3.080)h + (3.125)hk \approx 187.050$ (ms) |
| **The Proposed Scheme** | $g \ast (T_{mul1}) + g \ast h \ast (T_{mul2} + T_{mul3} + T_{add1})$ | $\approx (0.003 + (3.209)h)g \approx 32.093g$ (ms) |

| Encryption Cost | $g = 10$ | $g = 50$ | $g = 100$ |
|-----------------|----------|----------|----------|
| **Zhang et al.** | 0.32093 (s) | 1.60465 (s) | 3.2093 (s) |
| **Liu et al.** | 0.32093 (s) | 1.60465 (s) | 3.2093 (s) |
| **Datta et al.** | 0.32093 (s) | 1.60465 (s) | 3.2093 (s) |
| **The Proposed Scheme** | 0.32093 (s) | 1.60465 (s) | 3.2093 (s) |

| Decryption Cost |
|-----------------|
| **Zhang et al.** | $h' \ast (T_{mul4} + T_{mul5}) + k \ast T_{mul4} + h' \ast T_{mul6}$ | $\approx 2.681h' + 0.002k + 0.013h' \approx 2.694h' + 0.002k \approx 13.48$ (ms) |
| **Liu et al.** | $h' \ast (T_{mul4} + T_{mul5}) + h' \ast T_{mul4} + k \ast T_{mul4} + h' \ast T_{mul6}$ | $\approx 2.681h' + 0.002h' + 0.002k + 0.013h' \approx 2.696h' + 0.002k \approx 13.49$ (ms) |
| **Datta et al.** | $k \ast T_{mul3} + 2k \ast T_{mul6} + k \ast T_{add1}$ | $\approx 0.084k + 0.026k + 0.045k \approx 0.155k \approx 0.775$ (ms) |
| **The Proposed Scheme** | $h \ast T_{mul6}$ | $\approx 0.013h \approx 0.13$ (ms) |

- $h$ represents the size of the attribute set associated with the ciphertext.
- $h'$ represents the size of the smallest attribute set that can satisfy the ciphertext.
- $g$ represents the total number of users.
- $k$ represents the total number of attribute authorities.

reduce the transmission cost and the computation cost of the proposed scheme will be our future research.

**ACKNOWLEDGEMENTS**

This work was partially supported by the Ministry of Science and Technology of Taiwan under grants MOST 110-2218-E-110-007-MBK, MOST 109-2221-E-110-044-MY2, and MOST 110-2923-E-110-001-MY3. It also was financially supported by the Information Security Research Center at National Sun Yat-sen University in Taiwan and the Intelligent Electronic Commerce Research Center from The Featured Areas Research Center Program within the framework of the Higher Education Sprout Project by the Ministry of Education (MOE) in Taiwan.

**REFERENCES**

[1] C. Cao, Y. Tang, D. Huang, W. Gan, and C. Zhang, “Iibe: an improved identity-based encryption algorithm for wsn security,” Security and Communication Networks, vol. 2021, 2021.

[2] P. S. K. Oberko, V.-H. K. S. Obeng, and H. Xiong, “A survey on multi-authority and decentralized attribute-based encryption,” Journal of Ambient Intelligence and Humanized Computing, vol. 13, no. 1, pp. 515-533, 2022.

[3] A. D. Dwivedi, “Brisk: Dynamic encryption based cipher for long
TABLE 6: Ciphertext Length

| Proposed Scheme | Ciphertext length |
|-----------------|------------------|
| Zhang et al.     | $h \approx 13812 \times 24 + 24 \approx (3.314 \times 10^5) \times 10^6$ (bits) |
| Liu et al.       | $h \approx 13812 \times 24 + 24 \approx (3.314 \times 10^5) \times 10^6$ (bits) |
| Datta et al.     | $2h \approx 13812 \times 24 + 1 \approx (6.628 \times 10^5) \times 10^6$ (bits) |
| The Proposed Scheme | $g \approx (h \times 13812 \times 24 + 24) \approx ((3.314 \times 10^5) \times 10^6)$ (bits) |

| Proposed Scheme | Cipher length |
|-----------------|---------------|
| $g = 10$        | $3.314024 \times 10^8$ (bits) |
| $g = 50$        | $1.657012 \times 10^8$ (bits) |
| $g = 100$       | $3.314024 \times 10^8$ (bits) |

- $h$ represents the size of the attribute set that associated with the ciphertext.
- $g$ represents the total number of users.
ER-SHUO ZHUANG was born in Taipei, Taiwan. He received the M.S. degree in computer science and engineering from National Sun Yat-sen University, Kaohsiung, Taiwan, in 2007. His research interests include post-quantum cryptography, homomorphic encryption, secret sharing, and block chain.

CHUN-I FAN received the MS degree in computer science and information engineering from National Chiao Tung University, Taiwan, in 1993, and the PhD degree in electric engineering at National Taiwan University in 1998. From 1999 to 2003, he was an associate researcher and project leader of Telecommunication Laboratories, Chunghwa Telecom Co., Ltd, Taiwan. In 2003, he joined the faculty of the department of computer science and engineering, National Sun Yat-sen University, Kaohsiung, Taiwan, and has been a full professor since 2010. His current research interests include applied cryptology, cryptographic protocols, information and communication security, and he has published over 100 technical papers. He won the Dragon PhD Thesis Award from Aser Foundation, Best PhD Thesis Award from Institute of Information & Computing Machinery in 1999, Best Student Paper Awards in National Conference on Information Security 1998. He advised his graduate students to win the Best Student Paper Awards in National Conference on Information Security 2007, Best Master Thesis Award from Taiwan Association for Web Intelligence Consortium in 2011, Outstanding Master Dissertation Award from Institute of Information & Computing Machinery in 2012, and Outstanding PhD Dissertation Award from Institute of Information & Computing Machinery in 2012. He also was the editor-in-chief of Information Security Newsletter and is an executive director of Chinese Cryptology and Information Security Association.

I-HUA KUO was born in Kaohsiung, Taiwan. She received the B.S. degree in Department of Information and Learning Technology at National University of Tainan, Tainan, Taiwan, in 2019, and the M.S. degree in Computer Science and Engineering at National Sun Yat-sen University in 2021. She current research interests include applied cryptography and lattice-based cryptography.