Communications of the CCISA
Vol. 31 No. 1 Feb. 2025

Ciphertext-Policy Attribute-Based Proxy Re-Encryption with Non-Interactivity from Lattices

Er-Shuo Zhuang[1], Ya-Chih Chang[2], Chun-I Fan[1,2,3*]
[1]Information Security Research Center, National Sun Yat-sen University, Kaohsiung, Taiwan,
[2]Department of Computer Science and Engineering, National Sun Yat-sen University, Kaohsiung, Taiwan, [3]Intelligent Electronic Commerce Research Center, National Sun Yat-sen University, Kaohsiung, Taiwan
[1]zhaunges@gmail.com, [2]yachihchang1104@gmail.com,
[3*]cifan@mail.cse.nsysu.edu.tw (Corresponding author)

Abstract

Attribute-based encryption (ABE) is suitable for one-to-many encryption scenarios. In ABE, the encryptor can perform encryption by specifying the attributes of the recipients. However, along with the gradual increase in data encryption applications, it is required to transform access permissions of ciphertexts in some scenarios. Therefore, how to efficiently convert ciphertext has become an important issue. Furthermore, with the development of quantum computers, new encryption schemes need to be resistant to quantum computer attacks. In quantum-resistant ABE schemes, it is not easy to change the access structure of a ciphertext. To solve those issues, we propose a ciphertext-policy attribute-based proxy re-encryption scheme with non-interactivity from lattices. The proposed scheme combines proxy re-encryption with ABE to enhance the convenience of sharing encrypted data in the cloud. In addition to being able to resist quantum attacks, the proposed scheme also provides collusion-resistance, multi-hop re-encryption, and non-interactivity to increase the practicality. Finally, we give formal security proofs for the proposed scheme under the D-LWE problem.

Keywords: Lattice-Based Cryptography, Attribute-Based Encryption, Proxy Re-Encryption, Collusion-Resistance, Non-Interactivity, Multi-Hop.

* Corresponding author.

1 Introduction

Rapid technological advancements have resulted in considerable growth in information processing requirements; thus, cloud services have been introduced to reduce the computational and storage costs associated with these requirements. A public-key cryptosystem is a common tool for protecting the privacy of cloud users and the confidentiality of their data. The encryption scheme of such a system has various forms; for example, functional encryption involves encryption with a specific function, such as identity-based encryption and attribute-based encryption (ABE). Ciphertext-policy ABE is particularly advantageous in an environment with a frequently changing authority.

In 1994, Shor proposed a quantum algorithm that solves mathematical problems with large prime factors in polynomial time [17]. This algorithm threatens cryptosystems based on mathematical problems and can destroy such systems if the computational capacity of quantum computers improves to a certain level, which can considerably undermine data confidentiality. Recent research on ciphertext-policy attribute-based proxy re-encryption (CP-ABPRE) has predominantly focused on developing discrete logarithm problems for cryptography. To resist attacks from future quantum computers, scholars have increasingly studied cryptosystems resistant to quantum computation and have termed this area of study as Post-Quantum Cryptography (PQC). Of all cryptosystems, researchers are particularly interested in lattice-based cryptography because it offers various forms of functional computation and a flexible structure. In early July 2022, the US National Institute of Standards and Technology released the result of the third round of its PQC Standardization Process, and three of the final four standard algorithms were lattice-based.

With advances in PQC research, various lattice-based cryptographic primitives have been proposed for use in the establishment of PQC systems. In 1996, Ajtai proposed the first one-way collision-resistant function based on short-integer solutions (SIS) [1]. In the following year, Ajtai and Dwork verified that the worst-case hardness of short-integer-solution-based lattice problems equals the average-case hardness of SIS [3]. In 2005, Regev proposed the learning with errors (LWE) problem [16] and proved that its hardness is identical to the worst-case hardness of two lattice problems, namely the gap shortest vector problem (GapSVP) and the shortest independent vector problem. The LWE problem is widely considered a universal cryptographic primitive, and several lattice-based schemes based on the LWE problem have been proposed, such as an LWE-based, identity-based encryption scheme with a trapdoor function (proposed by Gentry *et al.* in 2008) [9] and a lattice-based ABE scheme (proposed by Boneh in 2013) [4].

Different features can be added to ABE to adapt to the requirements of various settings. For example, for User A to share a piece of encrypted data with User B (whose attributes do not satisfy the access structure), User A must convert the data encrypted using their public key into ciphertext encrypted using User B's public key. The simplest approach for achieving this requirement involves User A decrypting the data before encrypting them by using User B's public key to generate the ciphertext. To reduce computational costs, Liang *et al.* combined ABE with conventional proxy re-encryption (PRE) and proposed attribute-based PRE (ABPRE) in 2009 [12]. In ABPRE, a data owner generates a conversion key for the proxy to translate the ciphertext such that the ciphertext is made accessible to a group of data receivers without revealing the plaintext to the proxy or disclosing the data owner's key. Moreover, CP-ABPRE is suitable for managing encrypted data in a company. This scheme is particularly efficient and practical in situations in which a supervisor must delegate an encrypted file to its secretaries with different access levels (Figure 1) because the proxy can convert the file to a format that is within the decryption authority of the secretaries.

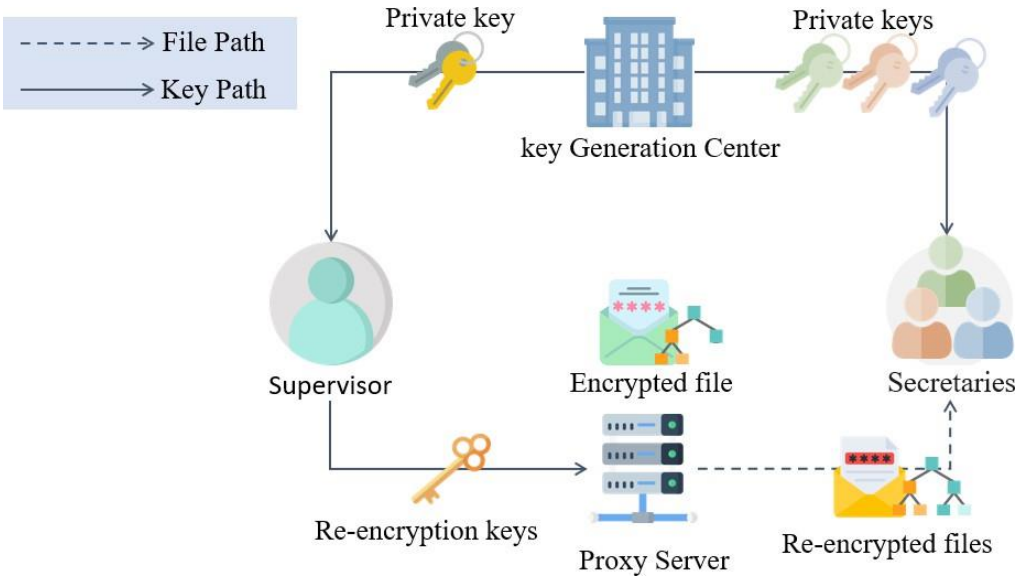

Figure 1: The CP-ABPRE Scenario

In the proposed manuscript, a CP-ABPRE scheme was developed. This scheme can be implemented in cloud environments and achieves high efficiency in ciphertext conversion because of its ciphertext-policy ABE and PRE components, respectively. The developed CP-ABPRE scheme enables the convenient sharing of encrypted data and has strong resistance to attacks by quantum algorithms because of its lattice-based structure. Although lattice-based CP-ABPRE schemes have been proposed in the literature, the proposed scheme

added several useful features, including collusion-resistance, noninteractivity, multi-hop behavior, and proxy invisibility, to the proposed scheme to facilitate the generation of re-encryption keys without the assistance of third parties. In addition, the proposed scheme overcomes the problem of increases in error terms with increases in the number of conversions. Finally, the size of an original ciphertext is equal to a re-encrypted ciphertext. The proposed scheme also enables access control, which increases the flexibility and efficiency of sharing encrypted data in a proxy server (cloud server).

1.1 Contributions

The proposed scheme is a CP-ABPRE scheme that first simultaneously achieves the following features:

- To resist quantum attacks, the scheme is lattice-based.
- It supports multi-hop re-encryption, allowing for more than one re-encryption operation. This feature enhances the ease of sharing encrypted data by increasing the number of re-encryption operations.
- This scheme is non-interactive, which reduces the transmission and communication costs in the generation of re-encryption keys.
- The proposed CP-ABPRE scheme provides AND-gate and OR-gate operations for access control based on a tree access structure, which offers high flexibility in fine-grained access control.
- With collusion-resistance, adversaries cannot decrypt unauthorized ciphertext through collusion.
- The proposed scheme has proxy invisibility. A single decryption algorithm can process the ciphertext generated directly by the data owner and the re-encrypted ciphertext without users knowing which.
- The scheme is proved to reach indistinguishability under chosen-plaintext attack (IND-CPA) security under the LWE assumption.

2. Related Works

This section introduces some identity-based PRE (IB-PRE) schemes, attribute-based PRE(AB-PRE), and ciphertext-policy AB-PRE (CP-ABPRE) schemes.

2.1. Related Works

Singh *et al*. proposed two IB-PRE schemes in 2020 [18]. The difference between the two schemes lies in their transferability, with one of them (named "IB-PRE+") being non-transferable and allowing only the delegator to execute the algorithm for re-encryption key generation; the other scheme lacks accuracy. In addition, the IB-PRE+ scheme uses a random number to control the direction of re-encryption and employs two levels of ciphertext to achieve non-transferability. To ensure non-transferability, this scheme limits the authority to execute the re-encryption algorithm to only the delegator.

Dutta *et al*. proposed several IB-PRE schemes and termed the ones with unidirectionality as "IB-uPRE" schemes. They proposed the first IB-uPRE scheme in 2020 [6] and then proposed another one in the following year to address the first scheme's lack of collusion safety [7], with both schemes being unidirectional and single-hop schemes. The re-encryption key generation structures of these schemes are similar to those of the IB-PRE schemes of Singh *et al*. Moreover, after some modifications, the re-encryption key generation structures of the schemes of Dutta *et al*. do not exhibit the accuracy problem. However, although the original and re-encrypted ciphertexts have an equal size in these schemes, the computations involved in decrypting the two types of ciphertext are different; thus, the decryption algorithm must distinguish the type of ciphertext before performing decryption. In addition, only one re-encryption operation is allowed in the aforementioned schemes of Dutta *et al.*

2.2. AB-PRE-Schemes

In 2021, Liang *et al.* proposed the first attribute-based conditional PRE schemes based on the LWE assumption [13]. They proposed two unidirectional schemes, one of which is a single-hop scheme and the other a multi-hop scheme. The multi-hop scheme consists of a Boolean circuit as the access structure, a fully key-homomorphic encryption algorithm, and a key-switching algorithm. Given that each user has their public key in this scheme, the transfer of access to a ciphertext involves the delegator designating the users to be authorized and their access level and defining access limitations during re-encryption. Nevertheless, the lack of master and private keys in the scheme suggests that the generation of users' public and private keys requires only the public parameters.

Yao *et al.* proposed a unidirectional, single-hop, conditional attribute-based PRE scheme [21] and established an honest re-encryption attacks (HRA) security model for this scheme. The aforementioned scheme is composed of two encryption algorithms, one of which generates the

original ciphertext (first-level ciphertext) and the other of which generates the re-encrypted ciphertext (second-level ciphertext). When the access structure and conditions are satisfied, the re-encrypted ciphertext can be converted into the original ciphertext. Therefore, although the proposed AB-PRE scheme is based on the ABE component of Yao *et al.*'s scheme, the two schemes differ in that the second- and first-level ciphertexts are the input and output, respectively, of the re-encryption algorithm of the scheme of Yao *et al*.

In 2021, Luo *et al*. proposed the first key-policy attribute-based PRE scheme based on the LWE assumption [14]. This scheme is a multi-hop scheme, exhibits unidirectionality, employs a Boolean circuit as its access structure, and adopts a fully key-homomorphic encryption algorithm. However, because the encryption and decryption operations require attributes and because the input attributes of the decryption algorithm are determined by the encryptor, the scheme requires the disclosure of user attribute sets. Moreover, the aforementioned multi-hop scheme limits the number of re-encryption operations.

Susilo *et al*. proposed another key-policy attribute-based PRE scheme [19], which is a single-hop unidirectional scheme, and established an HRA security model for this scheme. The encryption structure of this scheme is similar to that of the scheme of Luo *et al*. [14]. However, in contrast to schemes that adopt encryption key generation algorithms, the scheme of Susilo *et al*. embeds the delegator's private key into the re-encryption key by using a switching algorithm, which increases the size of the re-encryption key and thus increases the errors resulting from decrypting and re-encrypting ciphertexts.

2.3. CP-ABPRE Schemes

Zhang *et al*. proposed a CP-ABPRE scheme in 2018 [22]. This scheme is a single-hop, unidirectional, and non-interactive scheme and uses a linear secret-sharing scheme (LSSS) as the access structure. However, this CP ABPRE scheme relies on a ring structure in which commutative multiplication is performed for re-encryption and is based on a scheme developed by Fun *et al*. [8]. The ciphertext structure in the CP-ABPRE scheme of Zhang *et al*. differs from those in LWE-based schemes, which protect the sent message only by adding an error, in that it multiplies the error by a public parameter. However, the ciphertext error term used in the scheme of Zhang *et al*. can be eliminated by attacks designed by Chen *et al*. [5]; thus, this scheme is not secure against chosen plaintext attacks.

Li *et al*. proposed a CP-ABPRE scheme based on the LWE assumption [10], which uses a key-switching algorithm in conjunction with LWE problems to transfer re-encrypted keys and employs positive and negative attributes in the access structure to facilitate AND-gate

computation. However, because a trusted third party is required to generate re-encryption keys, this scheme does not satisfy the fundamental requirement of noninteractivity in PRE. Moreover, the access structure of the scheme is not embedded in the ciphertext; instead, a ciphertext is generated in accordance with the presence or absence of each attribute, which is denoted using a positive or negative sign, respectively. Therefore, the scheme allows for only one re-encryption operation because a ciphertext that is re-encrypted twice is identical to the original ciphertext.

In 2022, Li *et al*. proposed a CP-ABPRE scheme based on ring LWE [11]. This scheme is a single-hop and unidirectional scheme, has a threshold access structure, and facilitates the concurrent encryption of multiple bits through its ring structure. However, the aforementioned scheme prevents expansion to multi-hop re-encryption and involves interactive PRE because of its requirement of collaboration between a trusted third party and the user to generate a re-encryption key.

Jinqiu *et al*. proposed a CP-ABPRE based on the LWE assumption [20] in 2024. This scheme is a multi-hop, unidirectional, and non-interactive scheme and uses an LSSS scheme as the access structure.

It is worth noting that none of these CP-ABPRE schemes [10, 11, 20, 22] are resistant to collusion attacks. In those schemes, users with the same attributes will obtain the same decryption key. This would enable malicious attackers to collude to decrypt unauthorized ciphertext. Therefore, those schemes are not suitable for environments with high security requirements. To achieve collusion-resistance, we apply the method of Zhuang *et al*.'s scheme [23] in the proposed scheme.

3. Preliminaries

This section introduces the background knowledge of the technology used in the proposed scheme. First, the lattice and hard problems will be defined, and then the core technology used in the proposed scheme will be introduced. Finally, the system model and security model will be defined.

In this section, lowercase and uppercase bold letters are used to denote column vectors and matrices, respectively. For example, $\mathbf{a}^T$ and $\mathbf{A}^T$ refer to the transposes of vector a and matrix A, respectively; $(\mathbf{a}_1 — \mathbf{a}_2)$ or $[\mathbf{A}_1 — \mathbf{A}_2]$ denote two column vectors or matrices; and $\| \mathbf{a} \|$ represents the length of a vector. $\mathbb{Z}_q$ represents the set of integers modulo q.

3.1. Lattice

Definition 3.1. A lattice Λ of dimension m is a set of all integer linear combinations of linearly independent vectors $\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_n \in \mathbb{Z}^m$.

$$\Lambda = \left\{ \sum_{i=1}^{n} x_i \mathbf{a}_i \mid x_i \in \mathbb{Z} \right\}$$

Among them, the integer m is the dimension of the lattice Λ, the integer n is the rank of the lattice Λ, and the set of vectors $\{\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_n\}$ is the basis of the lattice Λ, and can also be determined by the matrix $\mathbf{A} = [\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_n]$ represents it.

In addition, the lattice Λ can satisfy $q\mathbb{Z}^m \subseteq \Lambda \subseteq \mathbb{Z}^m$ under some integers q, it can be called $q - ary$. Two common lattice types are introduced below.

$$\Lambda_q^{\perp}(\mathbf{A}) := \{\mathbf{x} \in \mathbb{Z}^m \mid \mathbf{Ae} = 0 \, mod \, q\},$$

$$\Lambda_q^{\mathbf{u}}(\mathbf{A}) := \{\mathbf{x} \in \mathbb{Z}^m \mid \mathbf{Ax} = \mathbf{u} \, mod \, q\}.$$

3.2. Discrete Gaussians

Definition 3.2. For an arbitrary positive Gaussian parameter $r \in \mathbb{R}^+$ and an arbitrary vector $c \in \mathbb{R}^n$, the parameters and center of a discrete Gaussian distribution are defined respectively as:

$$\forall y \in \mathbb{R}^n,$$

$$\rho_{r,\boldsymbol{c}}(\Lambda) = \sum_{y \in \mathbf{L}} \rho_{r,\boldsymbol{c}}(\mathbf{y}),$$

$$\rho_{r,c}(\mathbf{y}) = exp(-\pi \frac{\| \mathbf{y} - c \|^2}{r^2}).$$

If c is the origin or $r = 1$, the subscript of the parameter $\rho_{r,c}$ can be omitted.

Definition 3.3. For any $c \in \mathbb{R}^n$, $r \in \mathbb{R}^+$ and a lattice Λ of dimension n, the discrete Gaussian distribution on the lattice is defined as follows.

$$\forall y \in \mathbb{R}^n, D_{\mathbf{L},r,\mathbf{c}}(\boldsymbol{y}) = \frac{\rho_{r,c}(\mathbf{y})}{\rho_{r,c}(\Lambda)}$$

3.3. Inhomogeneous Short Integer Solution

The Inhomogeneous Short Integer Solution (ISIS) problem is a well-known hard problem on lattices. No known quantum algorithm can solve the ISIS problem. It is defined as follows:
Definition 3.4. Given an integer q, a random matrix $\mathbf{A} \in \mathbb{Z}^{n\times m}$, a target vector $\mathbf{u} \in \mathbb{Z}^n$, and a parameter $\beta \in \mathbb{R}$, find a non-zero vector $\mathbf{e} \in \mathbb{Z}^m$, such that $\mathbf{Ae} = \mathbf{u} \bmod q$ and $\| \mathbf{e} \| \leq \beta$.

3.4. Decisional Learning with Errors

In addition to being a well-known hard problem on lattices, the Decision Learning with Errors (D-LWE) problem is also used in many fields of cryptography. Given two oracles $\mathcal{O}_s$ and $\mathcal{O}_\$$, the D-LWE problem is defined as follows:

- $\mathcal{O}_s$: A pseudo-random sampler, outputs $(\mathbf{a}_i, b_i) = (\mathbf{a}_i, \mathbf{a}_i^T\mathbf{s} + x_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, where x_i is sampled from distribution $\chi, s \in \mathbb{Z}_q^n$ is a fixed secret vector among all samples, and $\mathbf{a}_i \in \mathbb{Z}_q^n$ is a uniform random vector.
- $\mathcal{O}_\$$: A truely random sampler, outputs uniformly random $(\mathbf{a}_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$.

Definition 3.5. Decision Learning with Error (D-LWE). Given a prime q, a positive integer n a distribution χ, and a polynomial number of samples $(\mathbf{a}_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ from an unspecified oracle $\mathcal{O}$, distinguish whether $\mathcal{O}$ is either $\mathcal{O}_s$ or $\mathcal{O}_\$$.

The advantage of a polynomial-time adversary A to win the D-LWE problem is defined as:

Definition 3.6. $Adv_{D-LWE}(A) = |Pr[A^{\mathcal{O}_s} = 1] - Pr[A^{\mathcal{O}_\$} = 1]|$

Definition 3.7. D-LWE Assumption. There is no polynomial-time adversary A that can win the D-LWE problem with a non-negligible advantage.

3.5. Trapdoor Functions

There are two types of methods for generating trapdoors. Ajtai proposed trapdoor functions based on anti-collision hash functions, which are type-1 trapdoor functions [2]. Their security is built on the short integer solution problem. The type-2 trapdoor functions are proposed by Regev [16], and their security is built on the LWE problem. Then, Micciancio and Peikert proposed more efficient type-2 trapdoor functions [15]. The proposed scheme uses the type-2 trapdoor

functions, and they are defined here. Before introducing the type-2 functions, a special matrix that is used in the trapdoor functions is defined as follows, where $k = \lceil \log\ q \rceil$

$$\mathbf{g}^T := [1\ \ 2\ \ 4\ \ \ldots\ \ 2^{k-1}] \in \mathbb{Z}_q^{1\times k}$$

$$\mathbf{G} := \begin{bmatrix} \mathbf{g}^T & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{g}^T & \mathbf{0} & \vdots \\ \vdots & \mathbf{0} & \ddots & \mathbf{0} \\ \mathbf{0} & \cdots & \mathbf{0} & \mathbf{g}^T \end{bmatrix} \in \mathbb{Z}_q^{n\times nk}$$

Definition 3.8. GenTrap($\overline{\mathbf{A}}$,H). Given a matrix $\overline{\mathbf{A}} \in \mathbb{Z}_q^{n\times m'}$ and an invertible matrix $\boldsymbol{H} \in \mathbb{Z}_q^{n\times n}$ as input, randomly generate a matrix $\mathbf{R} \in \mathbb{Z}^{m'\times d}$ from a discrete Gaussian distribution $\mathcal{D}$, and output $\mathbf{A} = (\overline{\mathbf{A}}|\mathbf{HG} - \overline{\mathbf{A}}\mathbf{R}) \in \mathbb{Z}_q^{n\times m}$, where $m = m' + d$. Then, $\mathbf{R}$ is a trapdoor of $\Lambda_{\mathrm{q}}^{\perp}(\mathbf{A})$, and $\mathbf{H}$ is a tag. At the same time, this algorithm can ensure that the Euclidean length of $\mathbf{R}$ must be less than or equal to $\sqrt{m}\cdot d(\sqrt{\log\ q})$.

Given $(\mathbf{A}, \overline{\mathbf{A}}, \mathbf{H}, \mathbf{G})$, the difficulty of finding a trapdoor $\mathbf{R}$ is equivalent to solving the *ISIS* problem, which means that the attacker needs to find a small matrix $\mathbf{Y}$ such that $\mathbf{AY} = \mathbf{AR}$.

Definition 3.9. SampleD $(\mathbf{R}, \overline{\mathbf{A}}, \mathbf{H}, \mathbf{u}, \sigma)$**.** Given a trapdoor $\mathbf{R} \in \mathbb{Z}^{m'\times d}$, a matrix $\boldsymbol{A} = (\overline{\mathbf{A}}|\mathbf{HG} - \overline{\mathbf{A}}\mathbf{R})$, an invertible matrix $\mathbf{H} \in \mathbb{Z}_q^{n\times n}$, a target vector $\mathbf{u} \in \mathbb{Z}_q^n$ and a Gaussian parameter σ as input, output a small vector $\mathbf{x} \in \mathbb{Z}^m$ such that $\mathbf{Ax} = \mathbf{u}\ mod\ q$.

The details of generating the vector x is presented as follows:

- First, a Gaussian perturbation vector $\mathbf{p} \in \mathbb{Z}^m$ is randomly selected, where the vector can be split into two parts:

$$\mathbf{p} = \begin{bmatrix} \mathbf{p_1} \\ \mathbf{p_2} \end{bmatrix}, \text{where } \mathbf{p_1} \in \mathbb{Z}^{m\prime} \text{ and } \mathbf{p_2} \in \mathbb{Z}^d.$$

- Compute $\mathbf{v}$ by the following steps:

$$\mathbf{y_1} = \overline{\mathbf{A}}(\mathbf{p_1} - \mathbf{Rp_2}) \in \mathbb{Z}_q^n,$$
$$\mathbf{y_2} = \mathbf{Gp_2} \in \mathbb{Z}_{\mathrm{q}}^{\mathrm{n}},$$

$$\begin{aligned} \mathbf{v} &= \mathbf{H}^{-1}(\mathbf{u} - \mathbf{y_1}) - \mathbf{y}_2 \\ &= \mathbf{H}^{-1}(\mathbf{u} - \mathbf{Ap}) \in \mathbb{Z}_q^n. \end{aligned}$$

- Choose a vector $\mathbf{z} \in \Lambda_{\mathrm{q}}^{\mathrm{v}}(\mathbf{G})$.
- Compute $\boldsymbol{y} = \begin{bmatrix} \mathbf{R} \\ \mathbf{I}_d \end{bmatrix}$.
- Compute $\mathbf{x} = \mathbf{p} + \mathbf{y} \in \Lambda_q^{\mathbf{u}}(\mathbf{A})$.

Definition 3.10. $\mathbf{DelTrap}(\mathbf{A}' = [\mathbf{A}|\mathbf{A_1}], \mathbf{R}, \mathbf{H}', \sigma)$. Givenamatrix $\mathbf{A}' = [\mathbf{A}|\mathbf{A_1}] \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^{n\times d}$, a corresponding trapdoor $\mathbf{R}$ of $\Lambda_q^{\perp}(\mathbf{A})$, an invertible matrix $\mathbf{H}' \in \mathbb{Z}_q^{n\times n}$ and a Gaussian parameter σ as input. Then, by continuously executing the **SampleD** algorithm, the **DelTrap** algorithm will output a trapdoor $\mathbf{R}'$ of $\Lambda_q^{\perp}(\mathbf{A}')$ such that $\mathbf{AR}' = \mathbf{H}'\mathbf{G} - \mathbf{A_1}$.

3.6. Access Structure

The access structure used in the proposed scheme is shown here. An access structure is embedded into a ciphertext by the data owner during encryption. During re-encryption, a new access structure might be selected and replaced by the data owner. In the decryption phase, data receivers whose set of attributes satisfies the access structure can decrypt the ciphertext and access the plaintext.

Let L be the set of all attributes in the proposed scheme, and $S_{ID} \subseteq L$ is the attributes set of User ID. The proposed scheme uses a tree structure as the access structure τ, in which the leaf nodes of τ are the attributes in the attribute set S_{ID}, and the non-leaf nodes are operands. The term $\overline{\mathbf{T}}$ denotes the value of the parent node, $\mathbf{T}_{\tau,x_i}$ represents the value of the leaf node, and M denotes the number of child nodes.

How to compute $\mathbf{T}_{\tau,x_i}$ is as follows. First, the root nodes are used to create a unit matrix $\mathbf{I} \in \{0,1\}^{n\times n}$. If the gates between node $\overline{\mathbf{T}}$ and its child nodes are AND gates, M invertible matrices are generated, with $\mathbf{T}_{\tau,x_i} \in \{-1,0,1\}^{n\times n}$, where $\overline{\mathbf{T}} = \sum_{i=1}^{M} \mathbf{T}_{\tau,x_i}$. If the gates between node $\overline{\mathbf{T}}$ and its child nodes are OR gates, the values of all child nodes are identical to the value of the parent node, namely $\mathbf{T}_{\tau,x_i} = \overline{\mathbf{T}}$. Subsequently, the node value $\mathbf{T}_{\tau,x_i} \in \{-1,0,1\}^{n\times n}$ that corresponds to each attribute gleaned from the access structure τ is embedded into the ciphertext, and the node value is an invertible matrix. Finally, the ciphertext is decrypted by obtaining the root node $\mathbf{I}$ on the basis of the node value.

3.7. System Model

There are four roles in the proposed CP-ABPRE scheme.

- Key Generation Center (KGC): Responsible for generating public parameters and users' public and private key pairs. KGC belongs to a trusted third party.
- Proxy Server (PS): PS can be regarded as a cloud server and assists in storing encrypted data and re-encryption keys. PS performs re-encryption to convert the access structure of the ciphertext and transmits the re-encrypted ciphertext to DRs. PS is semi-trusted.

- Data Owner (DO): DO encrypts the file and uploads the ciphertext to PS. DO is the owner of the original ciphertext.
- Data Receiver (DR): Obtain the re-encrypted ciphertext from PS.

The data users of the system include DOs and DRs. Users in the system may have single or multiple roles at the same time.

The proposed CP-ABPRE scheme consists of the following six algorithms:

- $\boldsymbol{Setup}\ (\lambda)$: Take a security parameter λ as input, output the public parameter PP and the master private key MSK.
- $\boldsymbol{KeyGen}\ (PP, MSK, S_{ID})$: Take public parameters PP, master private key MSK, and an attribute set S_{ID} as input, generate the public and private keys $(PK_{S_{ID}}, SK_{S_{ID}})$ of the user ID.
- $\boldsymbol{Enc}\ (PK_{S_{ID}}, \mu, \tau, U^{ID})$: Take the public key $PK_{S_{ID}}$, the message $\boldsymbol{\mu}$, a chosen access structure τ, and the set of all users in the system U^{ID} as input, output a ciphertext C_τ.
- $\boldsymbol{Re\text{-}KeyGen}\ (PK_{S_{ID1}}, PK_{S_{ID2}}, SK_{S_{ID1}}, \tau, \tau')$: Take $(PK_{S_{ID1}}, SK_{S_{ID1}})$, $PK_{S_{ID2}}$, the original access structure τ, and a new access structures τ' as input, output a re-encryption key $RK_{\tau\to\tau'}$.
- $\boldsymbol{Re\text{-}Enc}\ (RK_{\tau\to\tau'}, C_\tau)$: Take a re-encryption key $RK_{\tau\to\tau'}$ and C_τ as input, output the re-encrypted ciphertext $C_{\tau'}$.
- $\boldsymbol{Dec}\ (SK_{S_{ID}}, C)$: Take the private key $SK_{S_{ID}}$ and a ciphertext C as input, output the plaintext message μ.

The correctness of the proposed scheme must meet the following two conditions:

1. If the attribute set S_{ID2} satisfies the access structure τ, $\boldsymbol{Dec}\ (SK_{S_{ID}}, C_\tau) = \mu$, where $C_\tau \leftarrow \boldsymbol{Enc}\ (PK_{S_{ID}}, \mu, \tau, U^{ID})$.
2. If the attribute set S_{ID2} satisfies the access structure τ', $\boldsymbol{Dec}\ (SK_{S_{ID2}}, C_{\tau'}) = \mu$, where $C_{\tau'} \leftarrow \boldsymbol{Re-Enc}\ (RK_{\tau\to\tau'}, C_\tau)$ and $C_\tau \leftarrow \boldsymbol{Enc}\ (PK_{S_{ID}}, \mu, \tau, U^{ID})$.

3.8. Security Model of CP-ABPRE

The security model of the proposed CP-ABPRE scheme is defined here.

Definition 3.11. The proposed CP-ABPRE scheme achieves indistinguishability under the Selective Access Structure and Chosen Plaintext Attack (IND-sAS-CPA), if no polynomial time attacker has a non-negligible advantage in successfully winning the following IND-sAS-CPA game.

Suppose there is a polynomial time attacker $\mathcal{A}$ and a challenger $\mathcal{C}$, where $\mathcal{C}$ simulate the

IND-sAS-CPA game as follows.

- ***Initialization***: $\mathcal{A}$ selects a target access structure τ^* and the target user ID^*. Then $\mathcal{A}$ sends them to $\mathcal{C}$.
- ***Setup***: $\mathcal{C}$ executes $\boldsymbol{Setup}(\lambda)$ and sends the public parameters PP to $\mathcal{A}$.
- ***Query phase 1***: $\mathcal{A}$ can query the following oracle $\mathcal{O}$ polynomial times.
  - ***KeyGen oracle*** $\boldsymbol{\mathcal{O}_{KeyGen}}$: $\mathcal{A}$ sends (ID, S_{ID}) to $\mathcal{C}$, where S_{ID} is the attribute set of ID. If $ID = ID^*$, $\mathcal{C}$ only returns the public key PK_{SID^*} to $\mathcal{A}$. Otherwise, C executes $\mathbf{KeyGen}(PP, MSK, S_{ID})$ and returns the public key $PK_{S_{ID}}$ and the private key $SK_{S_{ID}}$ to $\mathcal{A}$.
  - ***Re - KeyGen oracle*** $\boldsymbol{\mathcal{O}_{\mathbf{Re-KeyGen}}}$: $\mathcal{A}$ sends $(ID, S_{ID}, PK_{S_{ID2}}, \tau, \tau')$ to $\mathcal{C}$, where τ is the original access structure and τ' is a new access structure. If $ID = ID^*$, then $\mathcal{C}$ returns $\perp$ to $\mathcal{A}$. Otherwise, $\mathcal{C}$ executes $\boldsymbol{Re\text{-}KeyGen}(\boldsymbol{KeyGen}(PP, MSK, S_{ID}), PK_{SID2}, \tau, \tau')$ and returens the re-encryption key $RK_{\tau \to \tau'}$ to $\mathcal{A}$.
- ***Challenge query***: $\mathcal{A}$ sends two different messages $(\mu_0, \mu_1) \in \{0,1\}^2$ to $\mathcal{C}$. Then $\mathcal{C}$ randomly selects $b \in \{0,1\}$ and uses τ^* to generate the corresponding ciphertext C_b. Finally, C returns C_b to $\mathcal{A}$.
- ***Query phase 2***: $\mathcal{A}$ may continue the queries as in ***Query phase 1***.
- ***Guess***: Finally, $\mathcal{A}$ sends $b' \in \{0,1\}$ to $\mathcal{C}$, if $b' = b$ then $\mathcal{A}$ win the game.

The advantage of a polynomial-time adversary $\mathcal{A}$ to win the $IND\text{-}sAS\text{-}CPA$ game is defined as:

$$Adv_{IND-sAS-CPA}(\mathcal{A}) = \left|\Pr[b = b'] - \frac{1}{2}\right|$$

4. Construction

This section introduces the proposed CP-ABPRE scheme, which contains four roles and consists of six algorithms. The six algorithms are ***Setup, KeyGen, Enc, Re-KeyGen, Re-Enc,*** and ***Dec.*** The process of the proposed scheme is shown in Figure 2. First, the system is initialized through KGC, and KGC generates the users' public and private key pairs. Then, DO generates ciphertext and uploads it to PS. If DO wants to delegate data permissions to some DRs, DO needs to generate the re-encryption keys and send them to PS. Then, PS performs ciphertext re-encryption so that DRs can decrypt the re-encrypted ciphertext. Table 1 lists the symbols used in the proposed scheme. Finally, the correctness of the algorithms will be verified.

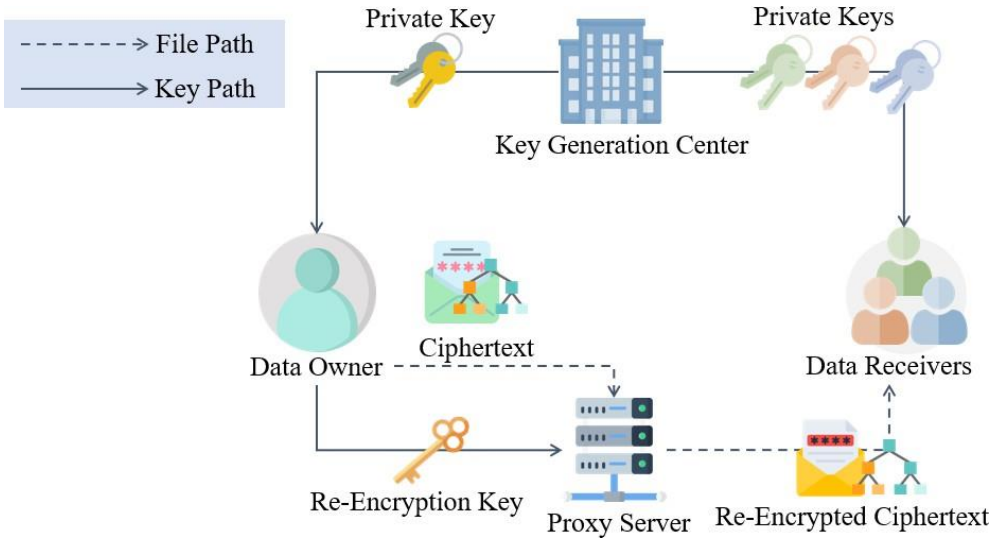

Figure 2: The System Architecture

4.1 Setup

$(PP, MSK) \leftarrow \boldsymbol{Setup}(\lambda)$:
KGC performs the following steps to generate system public parameters PP and master private key MSK:

1. Based on a security parameter λ, choose a Gaussian distribution χ, a Gaussian parameter σ, a prime number q, and three integers (n, m, d), and set $m' = m - d$.

Table 1: The Notations

Notation	Meaning
λ	a security parameter
σ	a Gaussian parameter
χ	a Gaussian distribution
x_i	the *i-th* attribute
ID	user ID
U^{ID}	the set of all users in the system $U^{ID} = \{ID_1, \ldots, ID_{\lvert U^{ID} \rvert}\}$
L	the set of all attributes in the system $L = \{x_1, \ldots, x_{\lvert L \rvert}\}$
τ	an access structure

S_{ID}	the set of all attributes of *ID*, $S_{ID} = \{x_i | x_i \in L\} \subseteq L$
S_τ	the set of all attributes of τ , $S_\tau = \{x_i | x_i \in L\} \subseteq L$
$PK_{S_{ID}}$	the public key related to S_{ID}
$SK_{S_{ID}}$	the private key related to S_{ID}
C_τ	a ciphertext related to τ
$RK_{\tau\to\tau'}$	a re-encryption key used to convert τ to $\tau'$of a ciphertext
H_1	a hash function
μ	a one-bit message

2. Choose a random matrix $\mathbf{A}_0 \in \mathbb{Z}_q^{n\times m'}$ and an invertible matrix $\mathbf{H}_0 \in \mathbb{Z}_q^{n\times n}$.
3. Execute **GenTrap**($\mathbf{A}_0, \mathbf{H}_0$) (defined in section 3.5), to generate a matrix $\mathbf{A} = [\mathbf{A}_0 | -\mathbf{A}_0\mathbf{R}_0 + \mathbf{H}_0\mathbf{G}] \in \mathbb{Z}_q^{n\times m}$ and a trapdoor $\mathbf{R}_0$ *of* $\Lambda_q^{\perp}(\mathbf{A})$.
4. Set the set of all attributes $L = \{x_1, \ldots, x_{|L|}\}$.
5. Randomly select a vector $\mathbf{u} \in \mathbb{Z}_q^n$.
6. Select a hash function $H_1: \{0,1\}^* \to Z_q^{n\times n}$.
7. Publish public parameters $PP = (\mathbf{A}, \mathbf{u}, n, m, q, d, \sigma, \chi, H_1)$ and store the master key $MSK = \mathbf{R}_0$.

4.2 KeyGen

$(PK_{S_{ID}}, SK_{S_{ID}}) \leftarrow \boldsymbol{KeyGen}(PP, MSK, S_{ID})$:
According to the user's attribute set S_{ID}, KGC performs the following steps to generate the user's public key $PK_{S_{ID}}$ and private key $SK_{S_{ID}}$:

1. Generate private key
   - $\forall x_i \in S_{ID}$:
     (a) Select a random matrix $\mathbf{A}_{x_i} \in \mathbb{Z}_q^{n\times d}$ and compute the invertible matrix $\mathbf{H}_{ID,x_i} = H_1(ID||x_i) \in \mathbb{Z}_q^{n\times n}$.
     (b) Execute $\boldsymbol{DelTrap}(\mathbf{A}'_{ID,x_i} = [\mathbf{A}|\mathbf{A}_{x_i}], \mathbf{R}_0, \mathbf{H}_{ID,xi}, \sigma)$ (defined in section 3.5), to generate a trapdoor $\mathbf{R}'_{ID,x_i}$ of $\Lambda_q^{\perp}(\mathbf{A}'_{ID,x_i})$.
     (c) Set the public key $\mathbf{A}'_{ID,x_i}$ and private key $\mathbf{R}'_{ID,x_i}$ corresponding to this attribute.
   - $\forall xi \notin S_{ID}$:
     (a) Select a random matrix $\bar{\mathbf{B}} \in \mathbb{Z}_q^{n\times d}$.
     (b) Set the public key $\mathbf{A}'_{ID,x_i} = [\mathbf{A}|\bar{\mathbf{B}}]$ corresponding to this attribute.

2. Set the public key $PK_{S_{ID}} = \{\mathbf{A'}_{ID,x_i}\}_{x_i \in L}$ and private key $SK_{S_{ID}} = \{R'_{ID,x_i}\}_{x_i \in S_{ID}}$.
3. Publish $PK_{S_{ID}}$ and send $SK_{S_{ID}}$ to user ID

4.3 Enc

$(C_\tau) \leftarrow \boldsymbol{Enc}(PK_{S_{ID}}, \mu, \tau, U^{ID})$:
DO encrypts a one-bit message $\mu \in \{0, 1\}$ with a chosen access structure τ by executing the following steps:

1. Select a noise value $e_2 \in \chi$.
2. $\forall ID \in U^{ID}$: Select a secret vector $s \in \mathbb{Z}_q^n$, and set the partial ciphertext
$$c_2^{ID} = \boldsymbol{u}^T s + \mu \lfloor \frac{q}{2} \rfloor + e_2 \in \mathbb{Z}_q.$$
3. Rely on the access structure τ to obtain a node value corresponding to each attribute $\mathbf{T}_{\tau,x_i} \in \{-1, 0, 1\}^{n \times n}$ (defined in section 3.6).
4. $\forall ID \in U^{ID}$: Select the noise values $e_{1,i} \in \chi^{m+d}$ and compute the ciphertex
   1. $\forall x_i \in S_\tau$:
$$c_{1,x_i}^{ID} = \mathbf{A'}_{ID,x_i}{}^T \mathbf{T}_{\tau,x_i} \mathbf{s} + \mathbf{e}_{1,i} \in \mathbb{Z}_q^{m+d}$$
5. Set the ciphertext as $C_\tau = \{\{c_{1,x_i}^{ID}\}_{x_i \in S_\tau}, c_2^{ID}, \tau = \{\mathbf{T}_{\tau,x_i}\}_{x_i \in S\tau}\}_{ID \in U^{ID}}$ and upload C_τ to PS.

Note: For users with the same attributes, the public and private keys are different, so malicious adversaries cannot crack the ciphertext by sharing the decryption keys. Therefore, the proposed scheme is collusion-resistant.

4.4 Re-KeyGen

$(RK_{\tau \to \tau'}) \leftarrow \boldsymbol{Re\text{-}KeyGen}(PK_{S_{ID_1}}, PK_{S_{ID_2}}, SK_{S_{ID_1}}, \tau, \tau')$:
DO ID_1 selects a new access structure τ' and a DR's $PK_{S_{ID_2}}$. Then DO performs the following steps to generate the re-encryption key $RK_{\tau \to \tau'}$:

1. For each $\mathbf{T}_{\tau,x_i}$, compute $\mathbf{T}_{\tau,x_i}{}^{-1}$.
2. Rely on the access structure τ' to obtain a node value corresponding to each attribute $\mathbf{T}_{\tau',x_i} \in \{-1, 0, 1\}^{n \times n}$.
3. $\forall x_i \in (S_{ID_1} \cap S_\tau)$:
   (a) $\forall x_i \in S_{\tau'}$:

i. Compute $\mathbf{A}'_{ID_2,x_i}{}^{\mathrm{T}} \cdot \mathbf{T}_{\tau\prime,x_i} \cdot \mathbf{T}_{\tau,x_i}{}^{-1}$

ii. Set:

$$(\mathbf{a}'_1,\ldots,\mathbf{a}'_{m+d}) = \mathbf{A}'_{ID_2,x_i}{}^{\mathrm{T}} \cdot \mathbf{T}_{\tau\prime,x_i} \cdot \mathbf{T}_{\tau,x_i}{}^{-1}$$

iii. Execute $\boldsymbol{SampleD}\ (\mathbf{R}'_{ID_1,x_i}, \mathbf{A}'_{ID_1,x_i}, \mathbf{H}_{x_i}, \mathbf{a}'_i, \sigma)$ (defined in section 3.5) to get $\mathbf{R}'_{\tau\to\tau\prime,x_i}$ such that:$\mathbf{R}'_{\tau\to\tau\prime,x_i}{}^{\mathrm{T}} \mathbf{A}'_{ID_1,x_i}{}^{\mathrm{T}} = \mathbf{A}'_{ID_2,x_i}{}^{\mathrm{T}} \cdot \mathbf{T}_{\tau\prime,x_i} \cdot \mathbf{T}_{\tau,x_i}{}^{-1}$

iv. Set $\mathbf{R}_{x_i} = \mathbf{R}'_{\tau\to\tau',x_i}$.

(b) $\forall x_i \notin S_{\tau'}$: Set $\mathbf{R}_{x_i}$ to a zero matrix.

4. Send the re-encryption key $RK_{\tau\to\tau'} = \{\mathbf{R}_{x_i}\}_{x_i\in S_\tau}$ to PS.

Note: If $\mathbf{R}_{x_i}$ is a zero matrix, there is no need to send $\mathbf{R}_{x_i}$ to PS.

4.5 Re-Enc

$(C_{\tau'}) \leftarrow \boldsymbol{Re\text{-}Enc}(RK_{\tau\to\tau'}, C_\tau)$:

PS uses the re-encryption key $RK_{\tau\to\tau'}$ to perform the following steps to generate the re-encrypted ciphertext $C_{\tau'}$:

1. $\forall x_i \in S_\tau$: Compute

$$c_{1,x_i}^{ID'} = RK_{\tau\to\tau'}{}^{\mathrm{T}} \cdot c_{1,x_i}^{ID}$$

If $c_{1,x_i}^{ID'} = 0$, discard $c_{1,x_i}^{ID'}$.

2. Set $c_2^{ID'} = c_2^{ID}$

3. Set $C_{\tau'} = \{\{c_{1,x_i}^{ID'}\}_{x_i\in S_{\tau'}}, c_2^{ID'}, \tau' = \{T_{\tau\prime,x_i}\}_{x_i\in S_{\tau'}}\}_{ID\in U^{ID}}$

4. Send the re-encrypted ciphertext $C_{\tau'}$ to DR ID_2.

Note: As shown in 4.7, the format of $C_{\tau\prime}$ is similar to the format of C_τ, where $e'_{1,i} = \mathbf{R}'_{\tau\to\tau\prime,x_i}{}^{\mathrm{T}} e_{1,i}$. Through appropriate parameter selection, the error term can be controlled within an acceptable range, and the ciphertext can undergo multiple re-encryption operations. Therefore, the proposed scheme supports multi-hop re-encryption.

4.6 Dec

$(\mu) \leftarrow \boldsymbol{Dec}(SK_{S_{ID}}, C)$:

The data user ID can decrypt an original ciphertext or a re-encrypted ciphertext by performing the following steps to retrieve the plaintext message μ:

1. $\forall x_i \in S_{ID}$:

   (a) Execute $\boldsymbol{SampleD}$ $(\mathbf{R}'_{ID,x_i}, \mathbf{A}'_{ID,x_i}, \mathbf{H}_{x_i}, \mathbf{u}, \sigma)$ to generate $\mathbf{x}_{x_i} \in \mathbb{Z}^{m+d}$ such that $\mathbf{A}'_{ID,x_i}\, \mathbf{x}_{x_i} = \mathbf{u}$.

   (b) Store the private key for decryption $SK_{2,S_{ID}} = \{\mathbf{x}_{x_i}\}_{x_i \in S_{ID}} \in \mathbb{Z}^{m+d}$.

2. According to the access structure τ, compute

$$b' = c_2^{ID} - \sum SK_{2,S_{ID}}^{T}\, c_{1,x_i}^{ID}$$

3. If $|b' - \lfloor \frac{q}{2} \rfloor| < \frac{q}{4}$, then set $\mu = 1$. On the contrary, set $\mu = 0$.

4. Output the plaintext message μ.

4.7 Correctness

The correctness of the decryption is presented, and the process is divided into two parts. One is decrypting an original ciphertext, and the other is decrypting a re-encrypted ciphertext.

• If the ciphertext is an original ciphertext C_τ, then

$$\begin{aligned} b' &= c_2^{ID} - \sum SK_{2,S_{ID}}^{T}\, c_{1,x_i}^{ID} \\ &= \mathbf{u}^{\mathrm{T}} s + \mu \lfloor \frac{q}{2} \rfloor + e_2 - \sum \mathbf{x}_{x_i}{}^{\mathrm{T}} (\mathbf{A}'_{ID,x_i}{}^{T}\, \mathbf{T}_{\tau,x_i}\, \mathbf{s} + \mathbf{e}_{1,i}) \\ &= \mathbf{u}^{\mathrm{T}} s + \mu \lfloor \frac{q}{2} \rfloor + e_2 - \sum \mathbf{u}^{\mathrm{T}}\, \mathbf{T}_{\tau,x_i}\, s + \mathbf{x}_{x_i}{}^{T} \mathbf{e}_{1,i}) \\ &= \mathbf{u}^{\mathrm{T}} s + \mu \lfloor \frac{q}{2} \rfloor + e_2 - \mathbf{u}^{\mathrm{T}} s + \sum \mathbf{x}_{x_i}{}^{T} \mathbf{e}_{1,i}) \\ &= \mu \left\lfloor \frac{q}{2} \right\rfloor + e^2 - \sum \mathbf{x}_{x_i}{}^{T} \mathbf{e}_{1,i}) \end{aligned}$$

To ensure the correctness of the decryption, the error term must meet the following restriction

$$|e_2 - \sum \mathbf{x}_{x_i}{}^{T} \mathbf{e}_{1,\mathrm{i}}| < \frac{q}{4}$$

Therefore, if $|b' - \lfloor \frac{q}{2} \rfloor| < \frac{q}{4}$, then $b = 1$, otherwise $b = 0$.

• If the ciphertext is a re-encrypted ciphertext $C_{\tau\prime}$, then

– $\forall x_i \in (S_\tau \cap S_{\tau\prime})$:

$$c_{1,i}^{ID'} = RK_{\tau\to\tau\prime}{}^{\mathrm{T}} \cdot c_{1,x_i}^{ID}$$
$$= \mathbf{R'}_{\tau\to\tau\prime,x_i}{}^{\mathrm{T}} (\mathbf{A'}_{ID_1,x_i}{}^{\mathrm{T}} \mathbf{T}_{\tau,x_i}\, \mathbf{s} + \mathbf{e}_{1,i})$$
$$= \mathbf{A'}_{ID_2,x_i}{}^{\mathrm{T}} \mathbf{T}_{\tau\prime,x_i}\, \mathbf{T}_{\tau,x_i}{}^{-1} (\mathbf{T}_{\tau,x_i}\, s) + \mathbf{R'}_{\tau\to\tau\prime,x_i}{}^{\mathrm{T}} \mathbf{e}_{1,i}$$
$$= \mathbf{A'}_{ID_2,x_i}{}^{\mathrm{T}}\, \mathbf{T}_{\tau\prime,x_i}\, s + \mathbf{R'}_{\tau\to\tau\prime,x_i}{}^{\mathrm{T}} \mathbf{e}_{1,i}$$
$$= \mathbf{A'}_{ID_2,x_i}{}^{\mathrm{T}} \mathbf{T}_{\tau\prime,x_i}\, s + \mathbf{e'}_{1,i}$$

, where $e'_{1,i} = \mathbf{R'}_{\tau\to\tau',x_i}{}^{\mathrm{T}} e_{1,i}$. Then, compute

$$b' = c_2^{ID'} - \sum SK_{2,S_{ID_2}}^{T}\, \boldsymbol{c}_{1,x_i}^{ID'}$$

$$= \mathbf{u}^{\mathrm{T}}\mathbf{s} + \mu \lfloor \frac{q}{2} \rfloor + e_2 - \sum \mathrm{x}_{x_i}{}^{\mathrm{T}} (\mathbf{A'}_{ID_2,x_i}{}^{T}\, \mathbf{T}_{\tau',x_i}\, \mathbf{s} + \mathbf{e'}_{1,i})$$

$$= \mathbf{u}^{\mathrm{T}}\mathbf{s} + \mu \lfloor \frac{q}{2} \rfloor + e_2 - \sum \mathbf{u}^{\mathrm{T}} (\mathbf{T}_{\tau',x_i}\, s) + \mathbf{x}_{x_i}{}^{T} \mathbf{e'}_{1,i}$$

$$= \mathbf{u}^{\mathrm{T}}\mathbf{s} + \mu \lfloor \frac{q}{2} \rfloor + e_2 - \mathbf{u}^{\mathrm{T}}\mathbf{s} - \sum \mathbf{x}_{x_i}{}^{T} \mathbf{e'}_{1,i}$$

$$= \mu \lfloor \frac{q}{2} \rfloor + e_2 - \sum \mathbf{x}_{x_i}{}^{T} \mathbf{e'}_{1,i}$$

To ensure the correctness of the decryption, the error term must meet the following restriction

$$|e_2 - \sum \mathrm{x}_{x_i}{}^{T} \mathbf{e'}_{1,i}| < \frac{q}{4}$$

Therefore, if $|b' - \lfloor \frac{q}{2} \rfloor| < \frac{q}{4}$, then $b = 1$, otherwise $b = 0$.

5 Security Proof

The proposed scheme is IND-sAS-CPA safe under the D-LWE assumption defined in section 3.4. Proof by contradiction will be used to prove the security of the proposed scheme. The simulation process is shown in Figure 3. The security model is defined in section 3.8.

Theorem 1. If there is a polynomial time attacker $\mathcal{A}$ that has a non-negligible advantage to successfully win the IND-sAS-CPA game, then the challenger $\mathcal{C}$ will have a non-negligible advantage to solve the D-LWE problem:

- **Initialization:**
  1. $\mathcal{A}$ selects an access structure $\tau^* = \{\mathbf{T}_i^*\}_{i\in S_{\tau^*}}$ and a target user ID^* and

sends them to $\mathcal{C}$.

2. D-LWE oracle (defined in section 3.4) sends a set of samples $(\mathbf{a}_i, b_i) \in (\mathbb{Z}_q^n \times \mathbb{Z}_q)$ to $\mathcal{C}$, where the samples are as follows:

$\{\mathbf{a}_0, b_0\}, \{(\mathbf{a}_{1,1}^1, b_{1,1}^1), \ldots, (\mathbf{a}_{1,1}^{m+d}, b_{1,1}^{m+d})\}, \{(\mathbf{a}_{1,2}^1, b_{1,2}^1), \ldots, (\mathbf{a}_{1,2}^{m+d}, b_{1,2}^{m+d})\}, \ldots,$
$\{(\mathbf{a}_{1,S_{\tau^*}}^1, b_{1,S_{\tau^*}}^1), \ldots, (\mathbf{a}_{1,S_{\tau^*}}^{m+d} b_{1,S_{\tau^*}}^{m+d})\}$

- ***Setup:*** $\mathcal{C}$ generates public parameters PP by executing the algorithm **Setup** defined in section 4.1 and sends PP to $\mathcal{A}$.

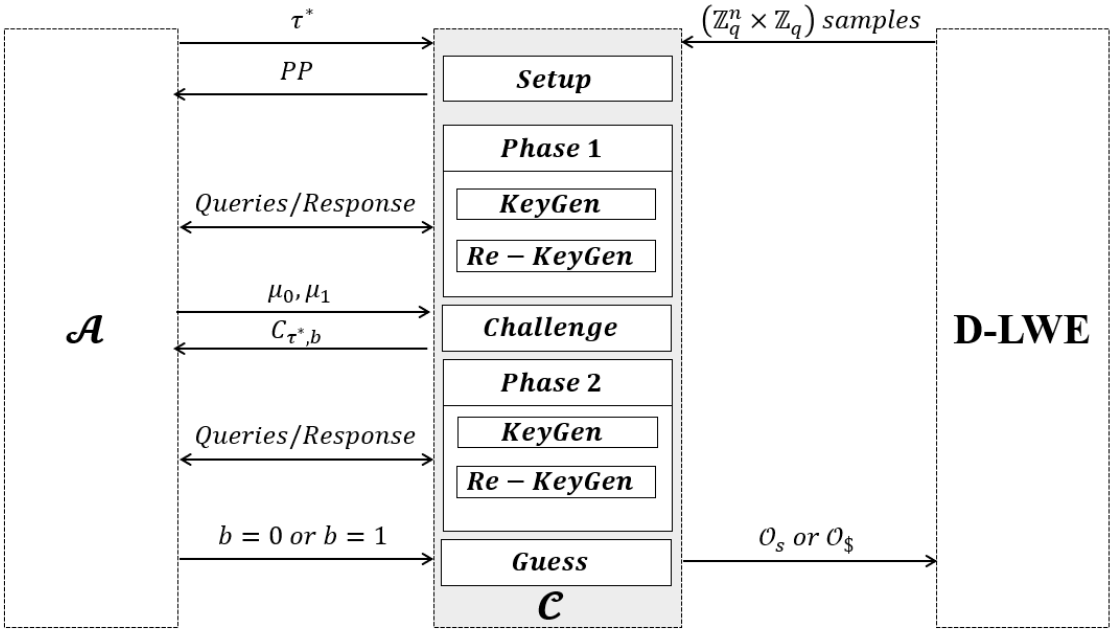

Figure 3: The IND-sAS-CPA Game

- ***Query phase 1***: $\mathcal{A}$ may send the following queries.
- $\mathcal{O}_{\mathbf{KeyGen}}$**:** $\mathcal{A}$ sends (ID, S_{ID}) to $\mathcal{C}$. If $ID = ID^*$, then $\mathcal{C}$ sets a public key for each attribute $\mathbf{A}_{S_{ID^*},i} = ([\mathbf{a}_{1,i}^1 \ldots, \mathbf{a}_{1,i}^{m+d}]^{\mathrm{T}} \cdot \mathbf{T}_i^{*-1})^{\mathrm{T}}$ such that $\mathbf{A}^T{}_{S_{ID^*},i}\, \mathbf{T}_i^* = [\mathbf{a}_{1,i}^1 \ldots, \mathbf{a}_{1,i}^{m+d}]^{\mathrm{T}}$ and sends the public keys to $\mathcal{A}$. On the contrary, $\mathcal{C}$ executes the algorithm **KeyGen** defined in section 4.2 to generate the private key and transmits the public key $PK_{S_{ID}}$ and the private key $SK_{S_{ID}}$ to $\mathcal{A}$.
- $\mathcal{O}_{\mathbf{Re-KeyGen}}$**:** $\mathcal{A}$ sends $(ID, S_{ID}, PK_{S_{ID_2}}, \tau, \tau')$ to $\mathcal{C}$. If $ID = ID^*$, then $\mathcal{C}$ returns $\perp$ to $\mathcal{A}$. On the contrary, $\mathcal{C}$ executes the algorithm **Re-KeyGen** defined in section 4.4 to generate the re-encryption key $RK_{\tau \to \tau'}$ and sends it to $\mathcal{A}$.

- ***Challenge query***: $\mathcal{A}$ sends two different messages $(\mu_0, \mu_1) \in \{0,1\}^2$. Then $\mathcal{C}$ randomly selects $b \in \{0,1\}$ and uses τ^* to perform the following steps to encrypt the message μ_b.

  1. For each attribute j in the access structure τ^*, set $\boldsymbol{b}_{ID^*,j} = (b_{1,j}^1, \ldots, b_{1,j}^{m+d})$.
  2. Set ciphertext:
  $$c_2 = b_0 + \mu_b \lfloor \frac{q}{2} \rfloor \in \mathbb{Z}_q$$
  3. Generate ciphertext
  $$c_{1,j} = \mathbf{b}_{ID^*,j} \in \mathbb{Z}_q^{m+d}$$
  4. Get the ciphertext
  $$C_{\tau^*,b} = (\{c_{1,j}\}_{j \in S_{\tau^*}}, c_2)$$
  5. C sends the ciphertext $C_{\tau^*,b}$ as a challenge to $\mathcal{A}$.
- ***Query phase 2:*** $\mathcal{A}$ may send more queries as in ***Query phase 1***.
- ***Guess:*** Finally, $\mathcal{A}$ guesses $b' \in \{0,1\}$. If $b' = b$, then $\mathcal{C}$ outputs $\mathcal{O}_s$ to D-LWE oracle. On the contrary, $\mathcal{C}$ outputs $\mathcal{O}_\$$ to D-LWE oracle.

If the sample obtained by D-LWE oracle is sampled from $\mathcal{O}_s$, then the structure of the ciphertext will be the same as the proposed scheme:

$$\begin{aligned} c_2 &= b_0 + \mu_b \lfloor \frac{q}{2} \rfloor \\ &= \mathbf{a}_0^T s + x + \mu_b \left\lfloor \frac{q}{2} \right\rfloor \in \mathbb{Z}_q \\ c_{1,j} &= \mathbf{b}_{ID^*,j} \\ &= (b_{1,j}^1, \ldots, b_{1,j}^{m+d}) \\ &= [\mathbf{a}_{1,j}^1] \ldots [\mathbf{a}_{1,j}^{m+d}]^{\mathrm{T}} \mathbf{s} + \mathbf{x}_{1,j} \\ &= \mathbf{A}^T{}_{S_{ID^*,j}} \mathbf{T}_j^* s + \mathbf{x}_{1,j} \in \mathbb{Z}_q^{m+d} \\ C_{\tau^*,b} &= (\{c_{1,j}\}_{j \in S_{\tau^*}}, c_2) \end{aligned}$$

Because $\mathcal{A}$ has a non-negligible advantage ε successfully winning the *IND-sAS-CPA* game, the probability for $\mathcal{C}$ to correctly guess D-LWE oracle is $\frac{1}{2} + \in$.

On the contrary, if the sample is randomly sampled from $\mathcal{O}_\$$, then the ciphertext C_b is a uniform random value. In this case, the probability for $\mathcal{C}$ to correctly guess D-LWE oracle is $\frac{1}{2}$.

Therefore, for $\mathcal{C}$, the advantage of solving the D-LWE problem is

$$|Pr[\mathcal{C}^{O_s} = 1] - Pr[\mathcal{C}^{O_\$} = 1]| = \frac{1}{2} + \epsilon - \frac{1}{2} = \epsilon$$

Therefore, if a polynomial time attacker $\mathcal{A}$ has a non-negligible advantage ϵ successfully wins the IND-sAS-CPA game, then $\mathcal{C}$ has a non-negligible advantage ϵ to solve the D-LWE problem.

6 Comparison

This section provides a comparison between the proposed CP-ABPRE scheme and the PRE schemes discussed in Section 2 with reference to their properties, ciphertext lengths, and performance.

6.1 Properties Comparison

The proposed CP-ABPRE scheme exhibits multi-hop behavior, noninteractivity, proxy invisibility, and collusion-resistance under the LWE assumption, thereby serving as a functional scheme with safety assurance. Table 2 presents a comparison between the properties of the proposed scheme and other related schemes. All previous CP-ABPRE schemes do not provide collusion-resistance.

Table 2: The Properties Comparison

Scheme	CP-ABPRE	access structure	multi-hop	Non-interactivity	Proxy invisibility	Collusion-resistance	Hard problem
Singh *et al.* [18]	×	×	×	✓	×	✓	LWE
Dutta *et al.* [7]	×	×	×	✓	×	✓	LWE
Liang *et al.* [13]	×	Boolean Circuit	✓	✓	✓	✓	LWE
Yao *et al.* [21]	×	t-CNF	×	✓	×	✓	LWE
Luo *et al.* [14]	×	Boolean Circuit	✓	✓	×	✓	LWE
Susilo *et al.* [19]	×	Boolean Circuit	×	✓	×	✓	LWE
Zhang *et al.* [22]	✓	LSSS	×	✓	✓	×	R-LWE
Li *et al.* [11]	✓	Threshold	×	×	×	×	R-LWE
Li *et al.* [10]	✓	AND	×	×	×	×	LWE
Jinqiu *et al.* [20]	✓	LSSS	✓	✓	✓	×	LWE
CP-ABPRE	✓	AND, OR	✓	✓	✓	✓	LWE

Furthermore, the multi-hop feature of the proposed CP-ABPRE scheme facilitates the decryption of a given re-encrypted ciphertext $C_{\tau'}$ through $SK_{2,S_{ID_1}}$,where the set of attributes S_{ID_1}satisfies the access structure τ'. Moreover, $\boldsymbol{SampleD}(\mathbf{R'}_{S_{ID_1}}, \mathbf{A'}_{S_{ID_1}}, \mathbf{H}, \mathbf{a'}_{\boldsymbol{i}}, \sigma)$

can be used to generate the reencryption key $\mathbf{R}_{\tau\prime\to\tau\prime\prime}$ such that $\mathbf{A}'_{S_{ID_1}}\mathbf{R}_{\tau\prime\to\tau\prime\prime} = \mathbf{A}'_{S_{ID_2}}$; the re-encryption key $\mathbf{R}_{\tau\prime\to\tau\prime\prime}$ and re-encrypted ciphertext $C_{\tau\prime}$ can then be used in computation to acquire a new re-encrypted ciphertext $C_{\tau\prime\prime}$. This new ciphertext can be decrypted using the private key $SK_{2,S_{ID_2}}$, where the set of attributes S_{ID_2} satisfies the access structure τ''. Therefore, the proposed scheme uses the aforementioned process to achieve multi-hop re-encryption, with the number of re-encryption operations being limited by the selected value q.

6.2 Ciphertext Comparison

This subsection provides a comparison of the transmission costs of ABPRE schemes. Considering that a scheme might require only one key to be generated, the transmission cost comparison was conducted on the basis of the ciphertext length. Table 3 presents the parameter settings employed in the comparison; L and u denote the total numbers of attributes and users in the scheme, respectively.

Table 3: Parameters

Notation	Description	Value
n	security parameter	284
m	basis dimension	13812
d	increased basis dimension	6816
q	module	2^{24}
$\boldsymbol{L}$	the number of all attributes in the system	50
$\boldsymbol{S}$	the number of attributes of an access structure	5
u	the number of users	10/50/100

Table 4 presents the lengths of original ciphertexts in the schemes. The comparison reveals that the schemes of Liang *et al*., Luo et al., and Susilo *et al*. produce ciphertexts with a length that approximates the number of attributes. The use of multiple algorithms in the scheme of Yao *et al*. results in the creation of a ciphertext structure that differs from those of the other schemes. The ring structure in the scheme of Zhang *et al*. resulted in shorter cyphertexts than those in the other schemes. Both schemes of Li *et al*. generate ciphertexts with a length that is twice the number of attributes. In the present study's scheme, the length of ciphertexts is equal to the number of attributes in the access structure. However, the ciphertexts are multiplied by the number of users u and extended by d dimensions, which are the costs incurred for preventing collusion and for obviating the need to involve a key generation center in re-encryption key

generation, respectively. Table 4 also presents the final lengths of ciphertexts after their multiplication by different numbers of users.

Table 4: Comparison

Scheme	Ciphertext length
Liang *et al.* [13]	$(L+2)*\mathbb{Z}_q^m \approx 1.867\times10^7$ (bits)
Yao *et al.* [21]	$\mathbb{Z}_q^{(n+1)\lceil log\ q\rceil+2n}+L*\mathbb{Z}_q^m+(L+2)*\mathbb{Z}_q^{\lceil log\ q\rceil} \approx 1.798\times10^7$ (bits)
Luo *et al.* [14]	$(L+2)*\mathbb{Z}_q^m \approx 1.867\times10^7$ (bits)
Susilo *et al.* [19]	$(L+2)*\mathbb{Z}_q^m \approx 1.867\times10^7$ (bits)
Zhang *et al.* [22]	$(L+1)*R_q \approx 1.224\times10^3$ (bits)
Li *et al.* [11]	$(L+\frac{1}{3}L)*R_q^m+2*R_q \approx 3.867\times10^7$ (bits)
Li *et al.* [10]	$2*L*\mathbb{Z}_q^m+\mathbb{Z}_q \approx 3.591\times10^7$(bits)
Jinqiu *et al.* [20]	$S*\mathbb{Z}_q^{2m}+\mathbb{Z}_q \approx 3.593\times10^6$ (bits)
CP-ABPRE	$u*(S*\mathbb{Z}_q^{m+d}+\mathbb{Z}_q) \approx u*(2.682\times10^6)$ (bits)

	$u=10$	$u=50$	$u=100$
CP-ABPRE	$\approx 2.682\times10^7$(bits	$\approx 1.341\times10^8$(bits)	$\approx 2.682\times10^8$ (bits)

6.3 Computation Cost

The computational cost of the proposed scheme was also compared with those of the other ABPRE schemes. Table 3 presents the parameter settings used for the comparison. The Numpy 1.22.4 library in Python 3.10.2 was used to run matrix and ring-structure computations on a macOS Monterey 12.4 AppleSilicon M1 computer with a 3.2-GHz (eight-core) processor with 16 GB of random-access memory and a 1-TB solid-state drive. Table 5 presents the variables used in the computation and the corresponding computational costs.

Table 5: Operation Cost

Notation	Operation	Computation cost
T_{add1}	$(\mathbb{Z}_q^{n\times m}+\mathbb{Z}_q^{n\times m})$	10.817 (ms)
T_{mul_1}	$(\mathbb{Z}_q^{m\times n}+\mathbb{Z}_q^{n\times 1})$	6.368 (ms)
T_{mul_2}	$(\mathbb{Z}_q^{1\times n}+\mathbb{Z}_q^{n\times m})$	5.388 (ms)
T_{mul_3}	$(\mathbb{Z}_q^{1\times n}+\mathbb{Z}_q^{n\times 1})$	0.643 (ms)
T_{mulR_1}	$(R_q\times R_q\times R_q\times R_q)$	0.007 (ms)
T_{mulR_2}	$(R_q\times R_q\times R_q)$	0.006 (ms)
T_{mulR_3}	$(R_q^m\times R_q)$	0.041 (ms)
T_{mulR_4}	$(R_q\times R_q)$	0.001 (ms)

T_{mul_4}	$(\mathbb{Z}_q^{(m+d)\times n} \times \mathbb{Z}_3^{n\times n} \times \mathbb{Z}_q^{n\times 1})$	1015.777 (ms)
T_{mul_5}	$(\mathbb{Z}_q^{1\times 2m} \times \mathbb{Z}_q^{2m\times 2m})$	5334.267 (ms)
T_{mul_6}	$(\mathbb{Z}_q^{(1\times((n+1)\lceil \log q\rceil+2n+m))} \times \mathbb{Z}_q^{((n+1)\lceil \log q\rceil+2n+m)\times 1})$	0.107 (ms)
T_{mul_7}	$(\mathbb{Z}_q^{m\times 2m} \times \mathbb{Z}_q^{2m\times 1})$	898.175 (ms)
T_{mulR_5}	$(R_q^{1\times m} \times R_q^{m\times 1})$	0.149 (ms)
T_{mul_8}	$(\mathbb{Z}_q^{1\times m} \times \mathbb{Z}_q^{m\times 1})$	0.098 (ms)
T_{mul_9}	$(\mathbb{Z}_q^{1\times(m+d)} \times \mathbb{Z}_q^{(m+d)\times 1})$	0.141 (ms)
$T_{mul_{10}}$	$(\mathbb{Z}_q^{2m\times n} \times \mathbb{Z}_q^{n\times 1})$	7.705 (ms)

For the comparison of computational cost, Table 6 presents the encryption and decryption times of each scheme. The proposed scheme's computational cost during encryption is increased by the d-dimensional extension of the public key; the cost attributable to multiplying the ciphertext by the number of users u is also shown in Table 6. Regarding decryption, the proposed scheme facilitates the selection of specific private keys that have attributes relevant to the access structure for decryption, which results in this scheme having a shorter computational time compared with the other schemes.

Moreover, in contrast to the other LWE-assumption-based schemes, which use the ***GenTrap*** trapdoor function for parameter setting, the proposed scheme employs the ***TrapGen*** trapdoor function for parameter setting. The numbers of dimensions required by these two functions are $m \approx 6n\log q$ and $m \approx 2n\log q$, respectively; therefore, to ensure a fair comparison, the parameter requirement of the GenTrap trapdoor function was employed to set the parameters. Given that dimension constitutes a crucial part of cost calculation, the proposed scheme might have produced an even better result than that shown in Table 6.

Table 6: Computation Cost

Scheme	Encryption	Decryption
Liang *et al.* [13]	$L * T_{add1} + (L+2) * T_{mul_1} \approx 871.978\ (ms)$	$T_{mul_5} \approx 5334.267\ (ms)$
Yao *et al.* [21]	$(L+1) * T_{mul_2} + (2 + L\lceil log\ q\rceil) * T_{mul_3} \approx 1048.066\ (ms)$	$L\lceil log\ q\rceil * T_{mul_6} \approx 128.853\ (ms)$
Luo *et al.* [14]	$L * T_{add1} + (L+2) * T_{mul_1} \approx 871.978\ (ms)$	$T_{mul_7} \approx 898.175\ (ms)$
Susilo *et al.* [19]	$L * T_{add1} + (L+2) * T_{mul_1} \approx 871.978\ (ms))$	$T_{mul_7} \approx 898.175\ (ms)$
Zhang *et al.* [22]	$L * T_{mulR_1} + T_{mulR_2} \approx 0.377\ (ms)$	$S * T_{mulR_1} + T_{mulR_3} \approx 0.076\ (ms)$
Li *et al.* [11]	$(S+1) * T_{mulR_3} + 2 * T_{mulR_4} \approx 1.06\ (ms)$	$(\frac{1}{3}L + 1) * T_{mulR_5} \approx 2.626\ (ms)$
Li *et al.* [10]	$(2L-S) * T_{mul_1} + T_{mul_3} \approx 478.213\ (ms)$	$L * T_{mul8} \approx 4.888\ (ms)$
Jinqiu *et al.* [20]	$S * T_{mul_{10}} + T_{mul_3} \approx 39.168\ (ms)$	$S * T_{mul_8} \approx 0.488\ (ms)$

CP-ABPRE	$u * (S * T_{mul_3} + T_{mul_2}) \approx u * 8.603\ (ms)$	$S * T_{mul_9} \approx 0.703\ (ms)$

Encryption	$u = 10$	$u = 50$	$u = 100$
CP-ABPRE	$\approx 86.03\ (ms)$	$\approx 430.15\ (ms)$	$\approx 860.3\ (ms)$

7 Conclusions

Although lattice-based CP-ABPRE schemes exist, the proposed CP-ABPRENI scheme has some more features than these schemes. The proposed scheme provides multi-hop re-encryption operations for the easier sharing of encrypted data, has a non-interactive design that reduces KGC's load and reduces the transmission costs involved in an interaction, uses an invisible proxy that facilitates the decryption process for users, supports collision-resistance to prevent adversaries from colluding in decryption, and embeds AND-gate and OR-gate access structures into the ciphertexts. In addition, the proposed scheme reaches the IND-CPA security under the decision LWE assumption. However, this scheme does not surpass all the other schemes considered for comparison in terms of transmission and computational costs. An increase in ciphertext complexity increases the encryption costs and ciphertext length.

Overall, the proposed scheme is suitable for data-sharing environments, such as companies or schools, in which a higher-level data owner with more attributes might need to transfer its authority to access encrypted data to a lower-level user with fewer attributes. The encrypted data can be stored in the proxy server in advance. When the data owner wants to share the data with others, it simply sends the re-encryption keys to the proxy server. The proxy server can then share the re-encrypted data with other users by re-encrypting the original encrypted data.

Despite the additional features of the proposed scheme, it still requires improvements in its encryption costs and access structure. Therefore, future works will attempt to enhance the efficiency and flexibility of this scheme, particularly by reducing the computational and transmission costs for ciphertexts. Alternatively, attempts may be made to extend ciphertexts into multibit messages to enhance the proposed scheme's practicality. Another possible direction for future research involves investigating the proposed scheme's security against chosen-ciphertext attacks.

References

[1] M. Ajtai. "Generating hard instances of lattice problems," *In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp. 99–108, 1996.

[2] M. Ajtai. "Generating hard instances of the short basis problem," *In International*

Colloquium on Automata, Languages, and Programming, pp. 1–9. Springer, 1999.

[3] M. Ajtai and C. Dwork. "A public-key cryptosystem with worst-case/average-case equivalence," *In Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pp. 284–293, 1997.

[4] X. Boyen. "Attribute-based functional encryption on lattices," *In Theory of Cryptography Conference*, pp. 122–142. Springer, 2013.

[5] Z. Chen, P. Zhang, F. Zhang, and J. Huang. "Ciphertext policy attribute-based encryption supporting unbounded attribute space from R-LWE," *KSII Transactions on Internet and Information Systems (TIIS)*, 11(4):2292–2309, 2017.

[6] P. Dutta, W. Susilo, D. H. Duong, J. Baek, and P. S. Roy. "Identity-based unidirectional proxy re-encryption in standard model: A lattice-based construction," *In International Conference on Information Security Applications*, pp. 245–257. Springer, 2020.

[7] P. Dutta, W. Susilo, D. H. Duong, and P. S. Roy. "Collusion-resistant identity-based proxy re-encryption: Lattice-based constructions in standard model," *Theoretical Computer Science*, 871:16–29, 2021.

[8] T. S. Fun and A. Samsudin. "Lattice ciphertext-policy attribute-based encryption from Ring-LWE," In 2015 *International Symposium on Technology Management and Emerging Technologies (ISTMET)*, pp. 258–262. IEEE, 2015.

[9] C. Gentry, C. Peikert, and V. Vaikuntanathan. "Trapdoors for hard lattices and new cryptographic constructions," *In Proceedings of the fortieth annual ACM symposium on Theory of computing*, pp. 197–206, 2008.

[10] J. Li, C. Ma, and K. Zhang. "A novel lattice-based ciphertext-policy attribute-based proxy re-encryption for cloud sharing," *In International Symposium on Security and Privacy in Social Networks and Big Data*, pp. 32–46. Springer, 2019.

[11] J. Li, J. Peng, and Z. Qiao. "A ring learning with errors-based ciphertext-policy attribute-based proxy re-encryption scheme for secure big data sharing in cloud environment," *Big Data*, 2022.

[12] X. Liang, Z. Cao, H. Lin, and J. Shao. "Attribute based proxy re-encryption with delegating capabilities," In Proceedings of the 4th International Symposium on Information, *Computer, and Communications Security*, pp. 276–286, 2009.

[13] X. Liang, J. Weng, A. Yang, Lisha Yao, Zike Jiang, and Zhenghao Wu. "Attribute-based conditional proxy re-encryption in the standard model under LWE," *In European Symposium on Research in Computer Security*, pp. 147–168. Springer, 2021.

[14] F. Luo, S. Al-Kuwari, F. Wang, and K. Chen. "Attribute-based proxy re-encryption from standard lattices," *Theoretical Computer Science*, 865:52–62, 2021.

[15] D. Micciancio and C. Peikert. “Trapdoors for lattices: Simpler, tighter, faster, smaller,” *In Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 700–718. Springer, 2012.

[16] O. Regev. “On lattices, learning with errors, random linear codes, and cryptography,” *Journal of the ACM (JACM)*, 56(6):1–40, 2009.

[17] P. W. Shor. “Algorithms for quantum computation: Discrete logarithms and factoring,” *In Proceedings 35th annual symposium on foundations of computer science*, pp. 124–134. IEEE, 1994.

[18] K. Singh, C. P. Rangan, R. Agrawal, and S. Sheshank. “Provably secure lattice based identity based unidirectional pre and pre+ schemes,” *Journal of Information Security and Applications*, 54:102569, 2020.

[19] W. Susilo, P. Dutta, D. H. Duong, and P. S. Roy. “Lattice-based HRA-secure attribute-based proxy re-encryption in standard model,” *In European Symposium on Research in Computer Security*, pp. 169–191. Springer, 2021.

[20] W. Tan, H. Ding, J. Hou, C. Peng. “Quantum resistant multi-feature attribute-based proxy re-encryption scheme for cloud services,” *Computer Modeling in Engineering & Sciences*, 138(1):917–938, 2024.

[21] L. Yao, J. Weng, and B. Wang. “Conditional attribute-based proxy re-encryption and its instantiation,” *Cryptology ePrint Archive*, 2022.

[22] E. Zhang, P. Yaoyao, and D. Jiao. “RLWE-based ciphertext-policy attribute proxy re-encryption,” *Journal on Communications*, 39(11):129, 2018.

[23] E. S. Zhuang, C. I. Fan, and I. H. Kuo. “Multiauthority attribute-based encryption with dynamic membership from lattices,” *IEEE Access*, 10:58254–58267, 2022.