symmetry

*Article*

# A Novel Lattice-Based CP-ABPRE Scheme for Cloud Sharing

**Juyan Li** [1], **Chunguang Ma** [2,3] **and Kejia Zhang** [1,*]

[1] College of Data Science and Technology, Heilongjiang University, Harbin 150080, China; lijuyan587@163.com
[2] College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao 266590, China; machunguang@hrbeu.edu.cn
[3] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
* Correspondence: zhangkejia@hlju.edu.cn

Received: 7 September 2019; Accepted: 3 October 2019; Published: 9 October 2019

**Abstract:** The ciphertext-policy attribute-based proxy re-encryption (CP-ABPRE) scheme supports access control and can transform a ciphertext under an access policy to a ciphertext under another access policy without decrypting the ciphertexts, which is flexible and efficient for cloud sharing. The existing CP-ABPRE schemes are constructed by bilinear pairing or multi-linear maps which are fragile when the post-quantum future comes. This paper presents an efficient unidirectional single-hop CP-ABPRE scheme with small public parameters from a lattice. For the transformation between two access structures, they are required to be disjoint. This paper uses the trapdoor sampling technique to generate the decryption key and the re-encryption key in constructing the scheme, and uses the decompose vectors technique to produce the re-encrypted ciphertexts in order to control their noise. Finally, we extended the scheme to a unidirectional single-hop CP-ABPRE scheme with keyword search for searching the encrypted data. Both schemes were proved secure under the learning with errors assumption, which is widely believed to be secure in quantum computer attacks. To the best of our knowledge, our scheme is the first CP-ABPRE scheme based on the learning with errors assumption.

**Keywords:** LWE; proxy re-encryption; attribute-based encryption; cloud sharing

## 1. Introduction

The encryption of cloud data can protect the security of data effectively. There are two types of encryption system: symmetric and asymmetric. In a symmetric encryption system, the encryption key and decryption key are the same. In an asymmetric encryption system, the encryption key and the decryption key are different. Attribute-based encryption (ABE) is an asymmetric approach.

In an ABE system, ciphertexts are labeled with a public attribute $x$, and private keys are associated with some descriptive values $y$. A private key decrypts the ciphertext and recovers the message if and only if $x$ satisfies $y$. By assigning common attributes of these decryptors, a user can use ABE to encrypt data and store the encrypted data in the cloud for sharing data, protecting privacy, and obtaining fine-grained access control. Hierarchical key assignment schemes (HKASs) [1,2] can be used to achieve fine-grained access control. There are two variants of ABE [3]: key-policy attribute-based encryption (KP-ABE) and ciphertext-policy attribute-based encryption (CP-ABE). In a CP-ABE (KP-ABE) system, the private key (ciphertext) is associated with an arbitrary number of attributes expressed as strings $S$, the ciphertext (private key) is associated with an access structure $W$ over attributes, and the private key can decrypt the ciphertext if and only if $S$ satisfies $W$.

Using CP-ABE, a user (e.g., Alice) can encrypt her data under access structure $W$, then any user with attribute $S$ can decrypt the encrypted data, where $S$ satisfies $W$. If Alice wants to share the encrypted data with Bob, but the attribute set of Bob does not satisfy $W$, then Bob can not get them from the cloud. Due to the resource-limited nature of the terminal device, it is impossible for users to backup all data with plain format. Thus, Alice needs to download and decrypt the ciphertext, and encrypt the data with another access structure $W'$. The computational overhead of this strategy is too heavy for Alice.

For example, in an electronic health record (EHR) system [4], the set $L$ of all attributes in the EHR system consists of all kinds of diseases, such as cold, lipomyoma, lung cancer, diabetes, and nephropathy. A patient encrypts their detailed personal information under access structure $W$, where $W$ may be (cold and lipomyoma) or (diabetes and nephropathy). The physician's attributes $S$ consist of many kinds of diseases that the physician is professional in, where $S$ could be {cold,lipomyoma}.

Proxy re-encryption (PRE) allows a proxy to transform a ciphertext of a delegator to a ciphertext of a delegatee specified by the delegator, and the proxy will not know the message in this process, which can be used for cloud sharing. The cloud sharing can become more efficient with ciphertext-policy attribute-based proxy re-encryption (CP-ABPRE). In the CP-ABPRE scheme, Alice only needs to generate a re-encryption key and send it to a proxy, then the proxy can transform the ciphertext under $W$ to another ciphertext under $W'$ [5–7]. Although CP-ABPRE can effectively achieve cloud sharing, the search on the encrypted data is powerless. It is interesting to combine the concept of CP-ABPRE and keyword search to construct CP-ABPRE with keyword search (CP-ABPRE-KS), which can not only achieve the data sharing effectively, but can also search the encrypted data.

### *1.1. Related Work*

At present, many types of lattice-based PRE scheme have been constructed. One example is conditional proxy re-encryption (CPRE) [8], whereby only ciphertexts satisfying a condition set by a delegator can be transformed by the proxy. Homomorphic proxy re-encryption (HPRE) [9,10] can homomorphically evaluate original or re-encrypted ciphertexts. In identity-based proxy re-encryption (IBPRE) [11], ciphertexts are transformed from one identity to another. Proxy re-encryption with keyword search (PRE-KS) [12] simultaneously realizes the functionality of proxy re-encryption and keyword search. However, there is no lattice-based attribute-based proxy re-encryption (ABPRE) [13] whereby ciphertexts are transformed from one access policy to another.

Liang et al. [13] constructed the first CP-ABPRE scheme based on bilinear maps, supporting and-gates over positive and negative attributes. Luo et al. [14] extended [13] to a CP-ABPRE supporting and-gates on multi-valued and negative attributes, but the scheme is selective-policy chosen plaintext secure. Liang et al. [15] constructed the first adaptively CCA-secure CP-ABPRE. The existing CP-ABPRE schemes are constructed by bilinear pairing or multi-linear maps, which are fragile when the post-quantum future comes. Zhang et al. [16] presented a ciphertext policy attribute-based encryption (ABE) scheme based on learning with errors (LWE), which is widely believed to be secure in quantum computer attacks. Zeng et al. [17] presented an authorized searchable encryption with special keyword based on [16].

Boneh et al. [18] constructed a public key encryption with keyword search for searching encrypted data. Shao et al. [19] constructed the first PRE-KS, which simultaneously realizes the functionality of proxy re-encryption and keyword search. Wang et al. [20] extended [19] to a constrained single-hop unidirectional proxy re-encryption supporting conjunctive keywords search. Shi et al. [21] formalized the syntax and security definitions for ABPRE with keyword search (ABPRE-KS), and constructed two ABPRE-KS by multi-linear maps; that is, CP-ABPRE-KS and KP-ABPRE-KS. Hong et al. [22] also presented an ABPRE-KS by bilinear pairing for flexible and secure data sharing in the cloud. None of these schemes can resist quantum computation attacks. Yang et al. [12] proposed a novel lattice-based semantic keyword searchable proxy re-encryption scheme for secure cloud storage which is resistant to quantum attack.

### *1.2. Our Contributions*

In this paper, (1) we constructed a lattice-based CP-ABE scheme by modifying the ABE scheme of Zeng et al. [17]. Compared with the ABE schemes of [16,17], our CP-ABE scheme has smaller public parameters. (2) We constructed a CP-ABPRE scheme based on the new CP-ABE scheme by using trapdoor sampling from LWE, which is widely believed to be secure in quantum computer attacks. The CP-ABPRE scheme is the first CP-ABPRE based on LWE. (3) We extended the CP-ABPRE scheme to a CP-ABPRE-KS scheme.

The rest of this paper is organized as follows: Section 2 presents preliminaries; Section 3 describes the constructed ABPRE scheme; Section 4 extends the ABPRE to the ABPRE-KS scheme; finally, our work is concluded in Section 5.

## **2. Preliminaries**

We introduce some notations, Gaussian distribution, the LWE hardness assumption, and the definition of CP-ABPRE in this section.

### *2.1. Notation*

We employed some initial notations, as listed in Table 1. For an integer $q$ and a vector $\vec{x} \in {\mathbb{Z}_q}^n$, let $l = \lceil \log q \rceil$, $P2\left(\vec{x}\right) = \left(1\vec{x}; 2\vec{x}; \cdots ; 2^{l-1}\vec{x}\right) \in \mathbb{Z}_q^{nl}$, $BD\left(\vec{x}\right) = \left(\vec{u}_1 | \cdots | \vec{u}_l\right) \in \{0,1\}^{nl}$, where $\vec{x} = \sum\limits_{k=1}^{l} 2^{k-1}\vec{u}_k$. When $A$ is a matrix, let $P2(A)$ $(BD(A))$ be the matrix formed by applying the operation to each row (column) of $A$.

**Table 1.** Notation.

| | |
|---|---|
| $x$ | scalar |
| $\vec{x}$ | vector |
| $A$ | matrix or set |
| $\|\|\vec{x}\|\|_\infty$ | $l_\infty$ norm of $\vec{x}$ |
| $\|\|\vec{x}\|\|$ | $l_2$ norm of $\vec{x}$ |
| $[k]$ | set $\{1, 2, \cdots, k\}$ |
| $\|L\|$ | the order of set $L$ |
| $S \vDash (\nvDash) W$ | attribute set S satisfies (or does not satisfy) access structure W |
| $[X\|Y] \in \mathbb{Z}_q^{m \times (n_1+n_2)}$ | the concatenation of the columns of $X \in \mathbb{Z}_q^{m \times n_1}, Y \in \mathbb{Z}_q^{m \times n_2}$ |
| $[X; Y] \in \mathbb{Z}_q^{(n_1+n_2) \times m}$ | the concatenation of the rows of $X \in \mathbb{Z}_q^{n_1 \times m}, Y \in \mathbb{Z}_q^{n_2 \times m}$ |
| $x \leftarrow \chi$ | $x$ is sampled according to a probability distribution $\chi$ |
| $x \leftarrow S$ | $x$ is sampled uniformly from a set S |
| $X \approx_c (\approx_s) Y$ | $X$ and $Y$ are computationally (statistically) indistinguishable |

### *2.2. Gaussian Distributions and the LWE Hardness Assumption*

For any positive parameter $\sigma > 0$, define the Gaussian function on $\mathbb{R}^m$, centered at $\vec{c}$: $\forall \vec{x} \in \mathbb{R}^m$,

$$\rho_{\sigma,\vec{c}}(\vec{x}) = \exp\left(-\pi \|\vec{x} - \vec{c}\|^2 \big/ \sigma^2\right).$$

For any vector $\vec{c} \in \mathbb{R}^m$ and positive parameter $\sigma > 0$, let $\Lambda$ be a discrete subset of $\mathbb{Z}^m$, define the discrete Gaussian distribution over $\Lambda$ as: $\forall \vec{x} \in \mathbb{R}^m$,

$$D_{\Lambda,\sigma,\vec{c}}(\vec{x}) = \frac{\rho_{s,\vec{c}}(\vec{x})}{\rho_{\sigma,\vec{c}}(\Lambda)},$$

where $\rho_{\sigma,\vec{c}}(\Lambda) = \sum_{\vec{x}\in\Lambda} \rho_{\sigma,\vec{c}}(\vec{x})$.

For constructing the CP-ABPRE scheme, we sample vectors from the discrete Gaussian distribution $D$. The algorithm *SamplePre* can sample vectors from a distribution statistically close to $D_{\Lambda(A)}$, but it needs the basis of $\Lambda^{\perp}(A)$. Lemmas 1 and 2 can meet our needs. Lemma 1 can output a basis of $\Lambda^{\perp}(A)$, and Lemma 2 can sample vectors from a distribution statistically close to $D_{\Lambda(A)}$.

**Lemma 1** ([23])**.** *For any positive integers $n$, $\mathrm{m} \geq 6n\log q$, $q \geq 2$, the probabilistic polynomial-time algorithm TrapGen$(q,n,m)$ can output a pair $(A,T) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}^{m\times m}$, where*

*(1) $A$ is statistically close to uniform in $\mathbb{Z}_q^{n\times m}$;*

*(2) $T$ is a basis for $\Lambda_q^{\perp}(A) = \left\{\vec{e}\in\mathbb{Z}^m, s.t. A\vec{e} = \vec{0} \bmod q\right\}$;*

*(3) $\|T\| \leq O(n\log q)$ and $\left\|\widetilde{T}\right\| \leq O\left(\sqrt{n\log q}\right)$.*

Alwen and Peikert assert that the constant hidden in the first $O(\cdot)$ is no more than 20.

**Lemma 2** ([24])**.** *For any positive integer $q \geq 2$, vector $\vec{c}\in\mathbb{Z}^m, \vec{u}\in\mathbb{Z}_q^n$ and matrix $A\in\mathbb{Z}_q^{n\times m}$, the probabilistic polynomial-time algorithm SamplePre$(A, T_{\mathrm{A}}, \vec{u}, \vec{c})$ can output vector $\vec{x}\in\Lambda_q^{\vec{u}}(A) = \{\vec{e}\in\mathbb{Z}^m, s.t. A\vec{e} = \vec{u} \bmod q\}$, which in a distribution statistically close to $D_{\Lambda_q^{\vec{u}}(A),\sigma,\vec{c}}$, where $T_{\mathrm{A}}$ is a basis of $\Lambda_q^{\perp}(A)$, $\sigma \geq \left\|\widetilde{T}\right\|\omega\left(\sqrt{\log m}\right)$.*

Let $X$ be a normal random variable with mean 0 and deviation ${}^{\alpha^2}\!/_{2\pi}$, where $\alpha\in(0,1)$ is a real number. For prime $q$, define the random variable in distribution $\overline{\Psi}_\alpha$ over $\mathbb{Z}_q$ as $\lfloor qX\rceil \bmod q$. For the correctness of our CP-ABPRE scheme, we need Lemmas 3 and 4, which show bounds for random variables.

**Lemma 3** ([25])**.** *For any $\vec{c}\in\Lambda\subset\mathbb{Z}^m$, let $\vec{x}\leftarrow D_{\Lambda+\vec{c},\sigma}$, $\sigma > \eta_\epsilon(\Lambda)$ for some $\epsilon\in(0,1)$, then with overwhelming probability $\|\vec{x}\| < \sigma\sqrt{m}$. Moreover, if $\vec{c} = 0$ then the bound holds for any $\sigma > 0$, with $\epsilon = 0$.*

**Lemma 4** ([24])**.** *For any $\vec{r}\in\mathbb{Z}^m$, let $\vec{e}\leftarrow\overline{\Psi}_\alpha^m$, then with overwhelming probability in $m$*

$$\left|\vec{r}^T\vec{e}\right| \leq \|\vec{r}\|\, q\alpha\omega\left(\sqrt{\log m}\right) + \|\vec{r}\|\sqrt{m}/2.$$

*In particular, if $e\leftarrow\overline{\Psi}_\alpha$, then $|e| \leq q\alpha\omega\left(\sqrt{\log m}\right) + 1/2$ with overwhelming probability in $m$.*

The LWE (learning with errors) problem [26] is as hard as the worst-case SIVP and GapSVP with certain noise distributions $D$ (e.g., $\overline{\Psi}_\alpha$), which is a classic hard problem on lattices. The decisional $LWE_{n,q,\chi}$ problem is to distinguish $(\vec{a}_i;\bar{b}_i)\leftarrow\mathbb{Z}_q^{n+1}$ and $(\vec{a}_i, b_i)\in\mathbb{Z}_q^{n+1}$, where $\vec{a}_i\leftarrow\mathbb{Z}_q^n, b_i = \vec{a}_i{}^T\vec{s} + e_i$, $\vec{s}\leftarrow\mathbb{Z}_q^n$, $e_i\leftarrow D$, $q\geq 2$, and $D$ is a distribution over $\mathbb{Z}$.

### 2.3. Attribute and Access Structure

We denote $L = [|L|]$ as the set of all attributes in the system. For $i\in[L]$, the user either has the attribute $i$ or does not have it. If a user does not have attribute $i$, we say the user has attribute $-i$. Thus, $i$ and $-i$ appear in pairs. We denote $i$ and $-i$ as positive and negative attribute, respectively. In this paper, we study the CP-ABE scheme which supports and-gates on positive and negative attributes.

**Definition 1.** *Let L be the set of all attributes. If the access structure W is organized by and-gates on positive and negative attributes, then an attribute set S satisfies W if and only if*

$$S^+ \subseteq S, S^- \subseteq L \backslash S,$$

*where $S^+$ ($S^-$) is the positive (negative) attribute set in $W$.*

For instance, let $L = [4]$, access structure $W = (1\, and\, -3)$, if $S \vDash W$, then we only need $1 \in S, 3 \notin S$, and do not need to consider $2, 4$. The attribute sets $S_1 = \{1\}, S_2 = \{1,2\}, S_3 = \{1,4\}, S_4 = \{1,2,4\}$ all satisfy $W$.

For two access structures $W$ and $W^1$, let $S^+, S^{1,+} (S^-, S^{1,-})$ be the positive (negative) attribute set in $W$ and $W^1$. If $S^+ \subseteq S^{1,-}, S^- \subseteq S^{1,+}$, then we say $W$ and $W^1$ are disjoint.

### 2.4. Definition and Security Model of CP-ABPRE Scheme

There are four participants in the single-hop unidirectional CP-ABPRE scheme for cloud sharing, as shown in Figure 1.

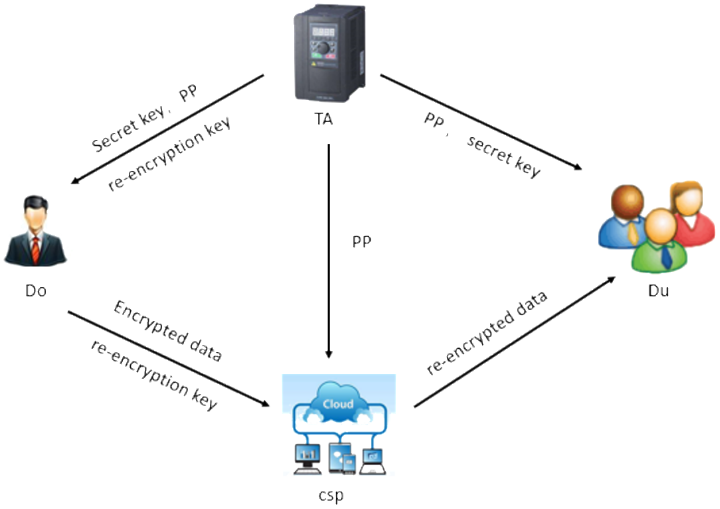

**Figure 1.** System model of the ciphertext-policy attribute-based proxy re-encryption (CP-ABPRE) scheme. CSP : cloud services provider; DO: data owner; DU: data user; TA: trusted authority.

(1) Trusted authority (TA). The TA is trusted by all participants. TA generates master secret key, public parameters and re-encryption key.

(2) Cloud services provider (CSP). The CSP is semi-trusted by all participants. The CSP stores data uploaded by the DO, and computes the re-encrypted ciphertext using the original ciphertext and re-encryption key.

(3) Data owner (DO). The DO encrypts their data and stores the encrypted data in the cloud.

(4) Data user (DU). The DU queries the CSP for re-encrypted data which belongs to them.

We give the following definition based on the definition and security model of Liang et al. [27].

**Definition 2.** *A single-hop unidirectional CP-ABPRE scheme consists of the following six algorithms:*

1. *Setup($\kappa, L$): For a set L of attribute and security parameter $\kappa$, the TA outputs public parameters $pp$ and master secret key $msk$.*
2. *KeyGen($pp, msk, S$): For $pp, msk$ and an attribute set $S$ of user (DO or DU), the TA outputs secret key $sk_S$ for $S$. Note that each secret key $sk_S$ is associated with an attribute set $S$.*

3. *Encrypt($pp, W, \mu$): For $pp$, a message $\mu$, and an access structure $W$ over the attribute set $L$, the DO outputs ciphertext $C_W$. Note that each ciphertext $C_W$ is associated with an access structure $W$.*
4. *Decrypt($pp, sk_S, C_W, S$): For $pp, C_W, S$ and its corresponding secret key $sk_S$, the user (DO or DU) outputs plaintext $\mu$ if $S \vDash W$ or a symbol $\perp$ indicating either $C_W$ is invalid or $S \nvDash W$.*
5. *ReKeyGen($pp, S, W, W^1$): For $pp$, two access structures $W, W^1$ and an attribute set $S$, if $S \vDash W$, and $W$ and $W^1$ are disjoint, the TA outputs the re-encryption key $rk_{W \to W^1}$, and otherwise outputs a symbol $\perp$.*
6. *ReEnc($pp, C_W, rk_{W \to W^1}$): For $pp$, $C_W$, $rk_{W \to W^1}$, the CSP outputs the re-encrypted ciphertext $C_{W^1}$.*

*Correctness—There are two requirements for correctness:*

1. *Decrypt($pp, sk_S, C_W$)= $\mu$, where $C_W = Encrypt(pp, W, \mu)$ and $S \vDash W$.*
2. *Decrypt($pp, sk_{S^1}, C_{W^1}$)= $\mu$, where $C_{W^1} = ReEnc(pp, rk_{W \to W^1}, C_W)$, $C_W = Encrypt(pp, W, \mu)$, $rk_{W \to W^1} = ReKeyGen(pp, W, W^1)$, $S^1 \vDash W^1$.*

**Definition 3.** *For a single-hop unidirectional CP-ABPRE scheme, let $\kappa$ be a security parameter. Consider the following games, denoted by $\mathrm{Expt}_{\mathrm{CP-ABPRE},\mathcal{A}}^{\mathrm{IND-sAS-CPA-Or}}(\kappa)$, between challenger and adversary.*

**Initialization**. *The adversary chooses a challenge access structure $W^*$ for the challenger.*

**Setup Phase**: *The challenger runs Setup( $\kappa$, $L$) and sends $pp$ to the adversary.*

**Learning Phase**: *In this phase, the adversary can access the following oracles polynomially many times, and the challenger needs to answer these oracles.*

(1) *Secret key oracle $\mathcal{O}_{\mathrm{sk}}(S)$: The adversary inputs an attribute set $S$. If $\mathrm{S} \nvDash \mathrm{W}^*$, then the challenger returns $\mathrm{sk}_S \leftarrow \mathrm{KeyGen}(\mathrm{pp}, \mathrm{msk}, \mathrm{S})$, and otherwise returns $\perp$.*

(2) *Re-encryption key oracle $\mathcal{O}_{\mathrm{rk}}(S, W, W')$: The adversary inputs two access structures $W, W'$ and $S$. If $S \vDash W$, $W$ and $W'$ are disjoint, and $\mathcal{O}_{\mathrm{sk}}(S')$ has been accessed for any $\mathrm{S}' \vDash \mathrm{W}'$, then the challenger returns $rk_{W \to W'} \leftarrow \mathrm{ReKeyGen}(\mathrm{pp}, S, \mathrm{W}, W')$, and otherwise returns $\perp$.*

(3) *Re-encryption oracle $\mathcal{O}_{\mathrm{re}}(rk_{W \to W'}, W', C_W)$: The adversary inputs $W'$, $C_W$, $rk_{W \to W'}$. If $rk_{W \to W'} \leftarrow \mathrm{ReKeyGen}(\mathrm{pp}, S, \mathrm{W}, W')$, $\mathrm{sk}_S \leftarrow \mathrm{KeyGen}(\mathrm{pp}, \mathrm{msk}, \mathrm{S})$, $S \vDash W$, then the challenger returns $C_{W'} \leftarrow \mathrm{ReEnc}(\mathrm{pp}, C_W, rk_{W \to W'})$, and otherwise returns $\perp$.*

**Challenge**: *If the adversary finishes all of the oracles' queries, then the adversary sends $\mu \in \{0, 1\}$ to the challenger. For a coin $b \in \{0, 1\}$, the challenger returns a random ciphertext $C$ if $b = 0$ or the real ciphertext $\mathrm{C}_{W^*} \leftarrow \mathrm{Encrypt}(\mathrm{pp}, \mathrm{W}^*, \mu)$ if $b = 1$.*

**Gauss**: *Finally, the adversary outputs a guess $b' \in \{0, 1\}$. If $b' = b$, the adversary wins.*

*We say a single-hop unidirectional CP-ABPRE scheme is IND-sAS-CPA secure at the original ciphertext if for any PPT adversary, the advantage*

$$\mathrm{Adv}_{\mathrm{CP-ABPRE},\mathcal{A}}^{\mathrm{IND-sAS-CPA-Or}}(\kappa) = \left| Pr\left[b = b'\right] - \frac{1}{2} \right|$$

*of the adversary is negligible.*

**Definition 4.** *For a single-hop unidirectional CP-ABPRE scheme, let $\kappa$ be a security parameter. We say a single-hop unidirectional CP-ABPRE scheme is IND-sAS-CPA secure at re-encrypted ciphertext if for any PPT adversary, the advantage*

$$\mathrm{Adv}^{\mathrm{IND-sAS-CPA-Re}}_{\mathrm{CP-ABPRE},\mathcal{A}}(\kappa) = \left| Pr\left[\begin{array}{l} b = b' : \\ (W^*, state_1) \leftarrow \mathcal{A}(1^\kappa); \\ (pp, msk) \leftarrow Setup(1^\kappa, L); \\ (\mu, W, state_2) \leftarrow \mathcal{A}^{\mathcal{O}_1}(pp, state_1); \\ b \leftarrow \{0,1\}; \\ C^*_{W^*} \leftarrow ReEnc(rk_{W\to W^*}, C_W); \\ b' \leftarrow \mathcal{A}^{\mathcal{O}_1}(C^*_{W^*}, state_2) \end{array}\right] - \frac{1}{2} \right|$$

*of the adversary is negligible, where $\mathcal{O}_1 = \{\mathcal{O}_{\mathrm{sk}}, \mathcal{O}_{\mathrm{rk}}, \mathcal{O}_{\mathrm{re}}\}$ and $\mathcal{O}_{\mathrm{sk}}$ (it is forbidden to $S \vDash W^*$), $\mathcal{O}_{\mathrm{rk}}, \mathcal{O}_{\mathrm{re}}$ (it is forbidden to $C_W$ is an valid original ciphertext or a re-encrypted ciphertext) as in Definition 3, $State_1$ and $State_2$ are the state information, $W^*$ is challenge access structure, and $W, W^*$ are disjoint, $C_W$ is a random ciphertext $C$ if $b = 0$ or the real ciphertext $\mathrm{C_W} \leftarrow \mathrm{Encrypt(pp, W, \mu)}$ if $b = 1$, $\mu \in \{0,1\}$.*

## 3. A CP-ABPRE Scheme

First, we propose a single-hop unidirectional CP-ABPRE scheme, then prove the correctness and security of the scheme, and finally compare the schemes.

### 3.1. Concrete Scheme

A single-hop unidirectional CP-ABPRE scheme consists of the following six algorithms.

1. Setup$(n, m, q, L)$: Given positive integers $n, m, q$, and a set of attributes $L$, the TA samples $\vec{u} \leftarrow \mathbb{Z}_q^n$, computes $(A_{i,b}, T_{i,b}) \leftarrow TrapGen(q, n)$ for $i \in L$, where $b \in \{0,1\}$ and returns public parameters $pp = \left(\{A_{i,b}\}_{i\in L}^{b\in\{0,1\}}, \vec{u}\right)$ and master secret key $msk = \left(\{T_{i,b}\}_{i\in L}^{b\in\{0,1\}}\right)$.
2. KeyGen$(pp, msk, S)$: Given $pp, msk$ and an attribute set $S$ of the DU, where $S \subseteq L$, the TA lets $A_i = \begin{cases} A_{i,0}, & i \in L \backslash S \\ A_{i,1}, & i \in S \end{cases}$, computes $\vec{s} \leftarrow \mathrm{SamplePre}(A, T, \vec{u})$, and returns secret key $sk_S = \vec{s}$, where $A = \left(A_1 | \cdots | A_{|L|}\right)$, $T = \begin{bmatrix} T_1 & & \\ & \ddots & \\ & & T_{|L|} \end{bmatrix}$, $T_i$ is the basis for $\Lambda_q^\perp(A_i)$, $i \in L$.
3. Encrypt$(pp, W, \mu)$: Given $pp$, a message $\mu \in \{0,1\}$, and an access structure $W$, the DO denotes $S^+ (S^-)$ as the positive (negative) attribute set in $W$, computes

$$c = \vec{u}^T \vec{f} + x_c + \left\lfloor \frac{q}{2} \right\rfloor \mu,$$

$$\vec{c}_{i,0} = \begin{cases} \vec{z}_{i,0}, & i \in S^+ \\ A_{i,0}^T \vec{f} + \vec{x}_{i,0}, & i \in S- \end{cases},$$

$$\vec{c}_{i,1} = \begin{cases} A_{i,1}^T \vec{f} + \vec{x}_{i,1}, & i \in S^+ \\ \vec{z}_{i,1}, & i \in S^- \end{cases},$$

$$\begin{pmatrix} \vec{c}_{j,0} \\ \vec{c}_{j,1} \end{pmatrix} = \begin{pmatrix} A_{j,0}^T \\ A_{j,1}^T \end{pmatrix} \vec{f} + \begin{pmatrix} \vec{x}_{j,0} \\ \vec{x}_{j,1} \end{pmatrix},$$

$j \in L \backslash \left(S^+ \cup S^-\right)$, and returns ciphertext

$$C_W = \left(c; \{\vec{c}_{i,0}, \vec{c}_{i,1}\}_{i \in L}\right),$$

where $x_c \leftarrow \chi, \vec{f} \leftarrow \chi^n, \vec{z}_{i,0}, \vec{z}_{i,1}, \vec{x}_{i,0}, \vec{x}_{i,1} \leftarrow \chi^m$.

4. Decrypt($pp, C_W, sk_S, S$): After receiving the cipthertext $C_W$ from the CSP, the DU computes $\vec{y} = \left(\vec{y}_1; \cdots; \vec{y}_{|L|}\right)$ by $\vec{y}_i = \begin{cases} \vec{c}_{i,1}, & i \in S \\ \vec{c}_{i,0}, & else \end{cases}$, and then outputs 0 if $\left(-\vec{s}^T|1\right)\left(\vec{y}^T; c\right) = c - \vec{y}^T\vec{s}$ is closer to 0 than to $\left\lfloor \frac{q}{2} \right\rfloor$ modulo q, and 1 otherwise.
5. ReKeyGen($pp, S, W, W^1$): After receiving $pp, S$, two access structures $W, W^1$ from the DO, if $W, W^1$ are not disjoint or $S \nvDash W$, then the TA outputs $\perp$, and otherwise denotes the positive (negative) attribute set in $W^1$ as $S^{1,+}\left(S^{1,-}\right)$, noting $S^{1,+} \subseteq L, S^{1,-} \subseteq L$, then computes

$$Q_{i,0} \leftarrow \begin{cases} \overline{X}_i, & i \in S^{1,+} \\ \mathrm{P2}\left(R_{i,1\to 0}^T\right) + X_i, & i \in S^{1,-} \end{cases},$$

$$Q_{i,1} \leftarrow \begin{cases} \mathrm{P2}\left(R_{i,0\to 1}^T\right) + X_i, & i \in S^{1,+} \\ \overline{X}_i, & i \in S^{1,-} \end{cases},$$

$$Q_{i,0} \leftarrow P2\left(R_{i,1\to 0}^T\right) + X_{i,0}, i \in \left(L \backslash \left(S^{1,+} \cup S^{1,-}\right)\right),$$

$$Q_{i,1} \leftarrow P2\left(R_{i,0\to 1}^T\right) + X_{i,1}, i \in \left(L \backslash \left(S^{1,+} \cup S^{1,-}\right)\right),$$

where $R_{i,1\to 0} \leftarrow \mathrm{SamplePre}\left(A_{i,1}, T_{i,1}, A_{i,0}\right)$, $R_{i,0\to 1} \leftarrow \mathrm{SamplePre}\left(A_{i,0}, T_{i,0}, A_{i,1}\right)$, $X_i, X_{i,0}, X_{i,1} \leftarrow D_{\mathbb{Z}^{m\times m\lceil \log q\rceil}}, \overline{X_i} \leftarrow D_{\mathbb{Z}_q^{m\times m\lceil \log q\rceil}}$ and finally returns the re-encryption key $rk_{W\to W^1} = \left(\{Q_{i,0}, Q_{i,1}\}_{i\in L}\right)$.
6. ReEnc($pp, C_W, rk_{W\to W^1}$): Given $pp, C_W, rk_{W\to W^1}$, the CSP computes

$$\vec{c}_{i,0}^{1} = \begin{cases} Q_{i,0}BD\left(\vec{c}_{i,1}\right) + \vec{x}_{i,0}^{1}, & i \in S^{1,-} \\ \vec{z}_{i,0}^{1}, & i \in S^{1,+} \end{cases},$$

$$\vec{c}_{i,1}^{1} = \begin{cases} Q_{i,1}BD\left(\vec{c}_{i,0}\right) + \vec{x}_{i,1}^{1}, & i \in S^{1,+} \\ \vec{z}_{i,1}^{1}, & i \in S^{1,-} \end{cases},$$

$$\vec{c}_{j,0}^{1} = Q_{i,0}BD\left(\vec{c}_{j,1}\right) + \vec{x}_{j,0}^{1},$$

$$\vec{c}_{j,1}^{1} = Q_{i,1}BD\left(\vec{c}_{j,0}\right) + \vec{x}_{j,1}^{1},$$

$$j \in \left(L \backslash \left(S^{1,+} \cup S^{1,-}\right)\right),$$

where $\vec{x}^1_{i,0}, \vec{x}^1_{j,0} \leftarrow D_{\mathbb{Z}^m}, \vec{z}^1_{i,0}, \vec{z}^1_{i,1} \leftarrow \mathbb{Z}_q^m$ and outputs the re-encrypted ciphertext

$$C_{W^1} = \left(c; \left\{\vec{c}^1_{i,0}, \vec{c}^1_{i,1}\right\}_{i\in L}\right).$$

### 3.2. Correctness and Parameters

We show the correctness and parameters in this subsection.

Firstly, we prove that Decrypt($pp, sk_S, C_W$)= $\mu$, where $C_W = Encrypt(pp, W, \mu)$ and $S \vDash W$.

For an attribute set $S$, let $A_i = \begin{cases} A_{i,0}, & i \in L\backslash S \\ A_{i,1}, & i \in S \end{cases}$, $A = \left(A_1|\cdots|A_{|L|}\right)$. Since $T_i$ is the basis for $\Lambda_q^{\perp}(A_i)$, $i \in L$, $AT = \left(A_1|\cdots|A_{|L|}\right)\begin{bmatrix} T_1 & & \\ & \ddots & \\ & & T_{|L|} \end{bmatrix} = 0$, and $|T| = \prod\limits_{i\in L} |T_i| \neq 0$, we have $T = \begin{bmatrix} T_1 & & \\ & \ddots & \\ & & T_{|L|} \end{bmatrix}$ is a basis for $\Lambda_q^{\perp}(A)$, then TA can compute $\vec{s} = \left(\vec{s}_1; \cdots, \vec{s}_{|L|}\right) \leftarrow \text{SamplePre}\left(A, T, \vec{u}\right)$ such that $\vec{u} = A\vec{s} = \sum\limits_{i=1}^{|L|} A_i\vec{s}_i$. Since $S \vDash W$, we know that

$$\vec{y} = \left(\vec{y}_1; \cdots; \vec{y}_{|L|}\right) = A^T\vec{f} + \vec{x},$$

where $\vec{x} = \left(\vec{x}_1; \cdots; \vec{x}_{|L|}\right)$, $\vec{x}_i = \begin{cases} \vec{x}_{i,0}, & i \in L\backslash S \\ \vec{x}_{i,1}, & i \in S \end{cases}$. Thus,

$$\begin{aligned} & c - \vec{s}^T\vec{y} \\ & = \vec{u}^T\vec{f} + x_c + \left\lfloor \tfrac{q}{2} \right\rfloor \mu - \vec{s}^T\left(A^T\vec{f} + \vec{x}\right) . \\ & = \left\lfloor \tfrac{q}{2} \right\rfloor \mu + \left(x_c - \vec{s}^T\vec{x}\right). \end{aligned}$$

If $\left|x_c - \vec{s}^T\vec{x}\right| < \left\lfloor \frac{q}{2} \right\rfloor /2$, then we can get $\mu$.

Then, we prove that Decrypt($pp, sk_{S^1}, C_{W^1}$)= $\mu$, where $C_{W^1} = ReEnc(pp, rk_{W\to W^1}, C_W)$, $rk_{W\to W^1} = ReKeyGen(pp, W, W^1)$, $C_W = Encrypt(pp, W, \mu)$, $S^1 \vDash W^1$.

Let $S^{1,+}, S^{1,-}$ be the positive and negative attribute set in $W^1$, $C_W = \left(c; \{\vec{c}_{i,0}, \vec{c}_{i,1}\}_{i\in L}\right)$ be a ciphertext under $W$, and $rk_{W\to W^1} = \left(\{Q_{i,0}, Q_{i,1}\}_{i\in L}\right)$ be a re-encryption key. Since the access structures $W$ and $W^1$ are disjoint, we know that if $i \in S^{1,-}$, then

$$\begin{aligned} \vec{c}^1_{i,0} & = Q_{i,0}^T BD\left(\vec{c}_{i,1}\right) + \vec{x}^1_{i,0} \\ & = \left[\mathrm{P2}\left(R^T_{i,1\to 0}\right) + X_i\right] BD\left(\vec{c}_{i,1}\right) + \vec{x}^1_{i,0} \\ & = R^T_{i,1\to 0}\vec{c}_{i,1} + X_i BD\left(\vec{c}_{i,1}\right) + \vec{x}^1_{i,0} \\ & = R^T_{i,1\to 0}A^T_{i,1}\vec{f} + R^T_{i,1\to 0}\vec{x}_{i,1} + X_i BD\left(\vec{c}_{i,1}\right) + \vec{x}^1_{i,0} \\ & = A^T_{i,0}\vec{f} + R^T_{i,1\to 0}\vec{x}_{i,1} + X_i BD\left(\vec{c}_{i,1}\right) + \vec{x}^1_{i,0} \end{aligned}$$

that is

$$\vec{c}^1_{i,0} = \begin{cases} A^T_{i,0}\vec{f} + \vec{x}^2_{i,0}, & i \in S'^{-} \\ \vec{z}^1_{i,0}, & i \in S'^{+} \end{cases},$$

where $\vec{x}^2_{i,0} = R^T_{i,1\to 0}\vec{x}_{i,1} + X_i BD\left(\vec{c}_{i,1}\right) + \vec{x}^1_{i,0}$. Similarly, we have

$$\vec{c}^1_{i,1} = \begin{cases} A^T_{i,1}\vec{f} + \vec{x}^2_{i,1}, & i \in S'^{+} \\ \vec{z}^1_{i,1} & i \in S'^{-} \end{cases},$$

where $\vec{x}^2_{i,1} = R^T_{i,0\to 1}\vec{x}_{i,0} + X_i BD\left(\vec{c}_{i,0}\right) + \vec{x}^1_{i,1}$,

$$\vec{c}^1_{j,0} = A^T_{j,0}\vec{f} + \vec{x}^2_{j,0},$$

$$\vec{c}^1_{j,1} = A^T_{j,1}\vec{f} + \vec{x}^2_{j,1},$$

where $\vec{x}^2_{i,0} = R^T_{i,1\to 0}\vec{x}_{i,1} + X_{i,0} BD\left(\vec{c}_{i,1}\right) + \vec{x}^1_{i,0}$, $\vec{x}^2_{i,1} = R^T_{i,0\to 1}\vec{x}_{i,0} + X_{i,1} BD\left(\vec{c}_{i,0}\right) + \vec{x}^1_{i,1}$, $i \in \left(L \backslash \left(S^{1,+} \cup S^{1,-}\right)\right)$.

For the attribute set $S^1$, let $A_i = \begin{cases} A_{i,0}, & i \in L\backslash S^1 \\ A_{i,1}, & i \in S^1 \end{cases}$, $A^1 = \left(A_1 | \cdots | A_{|L|}\right)$. TA can compute $\vec{s}^1 \leftarrow \mathrm{SamplePre}\left(A^1, T^1, \vec{u}\right)$ such that $A^1\vec{s}^1 = \vec{u}$, where $T^1 = \begin{pmatrix} T_1 & & \\ & \ddots & \\ & & T_{|L|} \end{pmatrix}$ is the basis of $\Lambda^{\perp}_q\left(A^1\right)$. Since $S^1 \vDash W^1$, we know that $\vec{y}^1 = \left(\vec{y}^1_1; \cdots; \vec{y}^1_{|L|}\right) = {A^1}^T\vec{f} + \vec{x}^1$, where $\vec{x}^1 = \left(\vec{x}^1_1; \cdots; \vec{x}^1_{|L|}\right)$, $\vec{x}^1_i = \begin{cases} \vec{x}^2_{i,0}, & i \in L\backslash S^1 \\ \vec{x}^2_{i,1}, & i \in S^1 \end{cases}$. Thus,

$$c - \vec{s}^{1T}\vec{y}^1 = \left\lfloor \frac{q}{2} \right\rfloor \mu + \left(x_c - \vec{s}^{1T}\vec{x}^1\right).$$

If $\left|x_c - \vec{s}^{1T}\vec{x}^1\right| < \left\lfloor \frac{q}{2} \right\rfloor / 2$, then we can get $\mu$.

Finally, we set the parameters.

1. Algorithm TrapGen requires $m \geq 6n \log q$.
2. Algorithm SamplePre requires $\sigma \geq \left\|\widetilde{\mathbf{T}}\right\| \omega\left(\sqrt{\log m}\right)$.
3. Decrypting the ciphertext requires $\left|x_c - \vec{s}^T\vec{x}\right| < \left\lfloor \frac{q}{2} \right\rfloor / 2$.
4. Decrypting the re-encrypted ciphertext requires $\left|x_c - \vec{s}^{1T}\vec{x}^1\right| < \left\lfloor \frac{q}{2} \right\rfloor / 2$.
5. The hardness of LWE requires $\alpha q > 2\sqrt{n}$.

Let $\chi = \overline{\Psi}_\alpha$, the parameters can be set as follows:

$n = \kappa$, $q =$ the prime nearest to $2^{n^\delta}$, $m = 6n \lceil \log q \rceil$, $\sigma = m\omega\left(\sqrt{\log m}\right)$, $\alpha = \left[5m^3\sigma^2 |L| \, \omega\left(\sqrt{\log m}\right)\right]^{-1}$, where $\delta$ is constant between 0 and 1.

We verify (4), the others can be easily computed. From the element of $\vec{x}^1$, we know

$$\left\|\vec{x}^1\right\|_\infty \leq \left|\vec{r}^T\vec{x}'\right| + m\lceil \log q \rceil \left\|\vec{x}''\right\|_\infty + \left\|\vec{x}'''\right\|_\infty,$$

where $\vec{x}', \vec{x}''' \leftarrow \chi^m$, $\vec{x}'' \leftarrow \chi^{m \times m\lceil \log q \rceil}$, $\vec{r}$ is a column of $R_{i,1\to 0}, R_{i,0\to 1}$. By Lemmas 2 and 3, we have $||\vec{r}|| \leq \sigma\sqrt{m}$. By Lemma 4, we have

$$\begin{aligned}
&\left\|\vec{x}^1\right\|_\infty \leq \left|\vec{r}^T\vec{x}'\right| + m\left\lceil \log q\right\rceil \left\|\vec{x}''\right\|_\infty + \left\|\vec{x}'''\right\|_\infty \\
&\leq \sigma\sqrt{m}q\alpha\omega\left(\sqrt{\log m}\right) + \sigma m/2 + m\left\lceil \log q\right\rceil\left(q\alpha\omega\left(\sqrt{\log m}\right) + 1/2\right) + q\alpha\omega\left(\sqrt{\log m}\right) + 1/2 \\
&= q\alpha\omega\left(\sqrt{\log m}\right)\left[\sigma\sqrt{m} + m\left\lceil \log q\right\rceil + 1\right] + \sigma m/2 + m\left\lceil \log q\right\rceil/2 + 1/2 \\
&\leq 2\sigma\sqrt{m}q\alpha\omega\left(\sqrt{\log m}\right) + \sigma m
\end{aligned} .$$

Thus,

$$\begin{aligned}
&\left|x_c - \vec{s}^{1T}\vec{x}^1\right| \leq \left|x_c\right| + \left|\vec{s}^{1T}\vec{x}^1\right| \leq \left|x_c\right| + m\sqrt{|L|}\left\|\vec{s}^1\right\|\left\|\vec{x}^1\right\|_\infty \\
&\leq q\alpha\omega\left(\sqrt{\log m}\right) + 1/2 + m\sqrt{|L|}\sigma\sqrt{|L|\,m}\left[2\sigma\sqrt{m}q\alpha\omega\left(\sqrt{\log m}\right) + \sigma m\right] \\
&= q\alpha\omega\left(\sqrt{\log m}\right)\left[1 + 2m^2\sigma^2\left|L\right|\right] + 1/2 + m^{\frac{5}{2}}\sigma^2\left|L\right| \\
&< q\alpha\omega\left(\sqrt{\log m}\right)m^3\sigma^2\left|L\right| \\
&\leq \tfrac{q}{5}
\end{aligned} .$$

### *3.3. Security*

We show the CP-ABPRE scheme is IND-sAS-CPA secure under the LWE problem in this subsection. Theorem 1 shows that the CP-ABPRE scheme is IND-sAS-CPA secure at the original ciphertext, Theorem 2 shows the CP-ABPRE scheme is IND-sAS-CPA secure at the re-encrypted ciphertext.

**Theorem 1.** *Let $n, q, m, \sigma, \alpha$ be as in the aforementioned. Then if LWE is hard, our CP-ABPRE scheme is IND-sAS-CPA secure at the original ciphertext.*

**Proof.** Consider the following games.

*$Game_0^b$*: This is the real game $\mathrm{Expt}_{\mathrm{CP-ABPRE},\mathcal{A}}^{\mathrm{IND-sAS-CPA-Or}}(\kappa)$ with $b \in \{0,1\}$. Suppose $W^*$ is the adversary's access structure, the challenger denotes the positive (negative) attribute set in $W^*$ as $S^{*,+}$ $(S^{*,-})$. The challenger answers the ciphertext of the adversary's issue about $\mu \in \{0,1\}$ as follows:

- If $b = 0$, output $\vec{c} \leftarrow \mathbb{Z}_q^{1+2|L|m}$.
- If $b = 1$, output $\mathrm{C}_{W^*} \leftarrow \mathrm{Encrypt}(\mathrm{pp}, \mathrm{W}^*, \mu)$.

Finally, the adversary outputs a guess $b' \in \{0,1\}$.

*$Game_1^b$*: We modify the secret key oracle $\mathcal{O}_{\mathrm{sk}}(S)$. If the adversary inputs an attribute set $S$ and $S \vDash W^*$, then the challenger returns $\perp$. If $S \nvDash W^*$, the challenger lets $A_i = \begin{cases} A_{i,0}, & i \in L\backslash S \\ A_{i,1}, & i \in S \end{cases}$, samples $\vec{s}_i^+ \leftarrow D_{\mathbb{Z}^m,\sigma}$, $i \in [|L| - 1]$, computes $\vec{u}' = \vec{u} - \sum_{i=1}^{|L|-1} A_i\vec{s}_i^+$, $\vec{s}_{|L|}^+ \leftarrow \mathrm{SamplePre}\left(A_{|L|}, T_{|L|}, \vec{u}'\right)$ and outputs the secret key $\vec{s}^+ = \left(\vec{s}_1^+, \cdots, \vec{s}_{|L|}^+\right)$. The others are the same as *$Game_0^b$*.

From Lemma 2, we know the distribution of $\vec{s}^+$ statistically closes to $D_{\Lambda_q^{\vec{u}'}(A),\sigma}$. The distribution of the real secret key $\vec{s}$ in the CP-ABPRE scheme also statistically closes to $D_{\Lambda_q^{\vec{u}'}(A),\sigma}$. Thus the distribution of $\vec{s}^+$ is same as the real secret key $\vec{s}$. In addition, because $A\vec{s}^+ = \vec{u}$, we have $\vec{s}^+ \approx_s \vec{s}$. Thus, $\mathrm{Game}_0^b \approx_s \mathrm{Game}_1^b$.

*$Game_2^b$*: We modify the re-encryption key oracle $\mathcal{O}_{\mathrm{rk}}(W, W')$. We replace $\mathrm{P2}\left(R_{i,1\to 0}^T\right) + X_i$, $i \in S^{1,-}$, $\mathrm{P2}\left(R_{i,0\to 1}^T\right) + X_i$, $i \in S^{1,+}$, and $Q_{i,0}, Q_{i,1}$, $i \in \left(L\backslash\left(S^{1,+} \cup S^{1,-}\right)\right)$ with $Q_{i,1\to 0}^*, Q_{i,0\to 1}^*, Q_{i,0}^*, Q_{i,1}^* \leftarrow D_{\mathbb{Z}^{m \times m\lceil \log q \rceil},\sigma}$, respectively. The others are the same as *$Game_1^b$*.

Since $R_{i,1\to 0} \leftarrow \mathrm{SamplePre}\left(A_{i,1}, T_{i,1}, A_{i,0}\right)$, $R_{i,0\to 1} \leftarrow \mathrm{SamplePre}\left(A_{i,0}, T_{i,0}, A_{i,1}\right)$, $X_i, X_{i,0}, X_{i,1} \leftarrow D_{\mathbb{Z}^{m\times m\lceil\log q\rceil}}$ in the CP-ABPRE scheme, we know the distribution of $\mathrm{P2}\left(R^T_{i,1\to 0}\right) + X_i$, $i \in S^{1,-}$, $\mathrm{P2}\left(R^T_{i,0\to 1}\right) + X_i$, $i \in S^{1,+}$, $Q_{i,0}, Q_{i,1}$ statistically close to $D_{\mathbb{Z}^{m\times m\lceil\log q\rceil},\sigma}$. Since the distribution of $Q^*_{i,0}, Q^*_{i,1} \leftarrow D_{\mathbb{Z}^{m\times m\lceil\log q\rceil},\sigma}$ are the same as $Q_{i,0}, Q_{i,1}$, respectively, we have $Q^*_{i,0} \approx_s Q_{i,0}$, $Q^*_{i,1} \approx_s Q_{i,1}$. Thus, $\mathrm{Game}^b_0 \approx_s \mathrm{Game}^b_1$.

*Game*$^b_3$: We modify the re-encryption oracle $\mathcal{O}_{\mathrm{re}}\left(rk_{S\to W'}, W', C_W\right)$. We replace $\vec{c}^{\,1}_{i,0}, \vec{c}^{\,1}_{i,1}$ with $\vec{c}^{\,1,+}_{i,0}, \vec{c}^{\,1,+}_{i,1} \leftarrow \mathbb{Z}^m_q$, respectively, $i \in [|L|]$. The others are the same as *Game*$^b_2$.

Since $Q^*_{i,0}, Q^*_{i,1} \leftarrow D_{\mathbb{Z}^{m\times m\lceil\log q\rceil},\sigma}$ and $\vec{x}^{\,1}_{i,0}, \vec{x}^{\,1}_{i,1} \leftarrow D_{\mathbb{Z}^m,\sigma}$, we cannot distinguish between the distribution of $\vec{c}^{\,1}_{i,0}, \vec{c}^{\,1}_{i,1}$ and the uniform distribution on $\mathbb{Z}^m_q$ under the LWE problem. Since $\vec{c}^{\,1,+}_{i,0}, \vec{c}^{\,1,+}_{i,1} \leftarrow \mathbb{Z}^m_q$, we have $\vec{c}^{\,1,+}_{i,0} \approx_s \vec{c}^{\,1}_{i,0}, \vec{c}^{\,1,+}_{i,1} \approx_s \vec{c}^{\,1}_{i,1}$. Furthermore, $\mathrm{Game}^b_3 \approx_s \mathrm{Game}^b_2$.

*Game*$^b_4$: We replace $\mathrm{C}_{W^*} \leftarrow \mathrm{Encrypt}(\mathrm{pp}, \mathrm{W}^*, \mu)$ with $\vec{c}^{\,+} \leftarrow \mathbb{Z}_q^{1+2|L|m}$, where $\vec{c}^{\,+} = \left(c^+; \left\{\vec{c}^{\,+}_{i,0}, \vec{c}^{\,+}_{i,1}\right\}_{i\in L}\right)$. The others are the same as *Game*$^b_3$.

We have $c^+ \approx_c c$, $\vec{c}^{\,+}_{i,1} \approx_c \vec{c}_{i,1}$,$i \in S^+ \cup L\backslash\left(S^+ \cup S^-\right)$, $\vec{c}^{\,+}_{i,0} \approx_c \vec{c}_{i,0}$, $i \in S^- \cup L\backslash\left(S^+ \cup S^-\right)$ under the LWE assumption and $\vec{c}^{\,+}_{i,1} \approx_s \vec{c}_{i,1}$, $i \in S^-$, $\vec{c}^{\,+}_{i,0} \approx_s \vec{c}_{i,0}$, $i \in S^+$. Thus $\mathrm{C}_{W^*} \approx_c \vec{c}^{\,+}$. Furthermore, $\mathrm{Game}^b_3 \approx_c \mathrm{Game}^b_4$.

Finally, we can get $\mathrm{Game}^0_0 \approx_c \mathrm{Game}^1_0$ by $\mathrm{Game}^0_4 \approx_c \mathrm{Game}^1_4$. This completes the proof. □

**Theorem 2.** *Let $n, q, m, \sigma, \alpha$ be as in the aforementioned. Then if LWE is hard, our CP-ABPRE scheme is IND-sAS-CPA secure at the re-encrypted ciphertext.*

**Proof.** For $(W^*, state_1) \leftarrow \mathcal{A}\left(1^\kappa\right)$, $(\mu, W, state_2) \leftarrow \mathcal{A}^{\mathcal{O}_1}\left(pp, state_1\right)$ which are chosen by the adversary, The challenger encrypts $\mu \in \{0,1\}$ under access structure $W$ and gets a corresponding ciphertext $C_W$ which is a random ciphertext $C$ if $b = 0$ or the real ciphertext $\mathrm{C}_W \leftarrow \mathrm{Encrypt}(\mathrm{pp}, \mathrm{W}, \mu)$ if $b = 1$. By the *Game*$^b_4$ of Theorem 1, we know that the adversary cannot distinguish a random ciphertext $C$ from the real ciphertext $\mathrm{C}_W \leftarrow \mathrm{Encrypt}(\mathrm{pp}, \mathrm{W}, \mu)$. For the re-encryption key $rk_{W\to W^*}$, the adversary cannot distinguish the real $rk_{W\to W^*}$ from a random Gaussian distribution by *Game*$^b_2$ of Theorem 1. Thus, the adversary cannot obtain any useful things for winning the game. At last, the challenger outputs the challenge re-encrypted ciphertext $C^*_{W^*} \leftarrow ReEnc\left(rk_{S\to W^*}, C_W\right)$. By the LWE, we have $Q_{i,0}BD\left(\vec{c}_{i,1}\right) + \vec{x}^{\,1}_{i,0}$, $i \in S^{1,-} \cup \left(L\backslash\left(S^{1,+} \cup S^{1,-}\right)\right)$ and the random uniform distributions are computationally indistinguishable, $Q_{i,1}BD\left(\vec{c}_{i,0}\right) + \vec{x}^{\,1}_{i,1}$, $i \in S^{1,+} \cup \left(L\backslash\left(S^{1,+} \cup S^{1,-}\right)\right)$ and the random uniform distributions are computationally indistinguishable. Thus, the advantage $\mathrm{Adv}^{\mathrm{IND-sAS-CPA-Re}}_{\mathrm{CP-ABPRE},\mathcal{A}}\left(\kappa\right)$ of the adversary is negligible. □

### *3.4. Comparison*

We compare the related works in this subsection.

(1) Our scheme was constructed based on the LWE problem, and supports and-gates on positive and negative attributes. There are only two lattice-based ABE schemes that support this operation. Compared with the ABE scheme of [16,17], our scheme not only supports proxy re-encryption but also has smaller public parameters. The comparison results are given in Table 2. $S$ is a set of all attributes in the access structure.

**Table 2.** Comparison of ciphertext-policy attribute-based encryption (CP-ABE) schemes. LWE: learning with errors; pp: public parameters; sk: secret key.

| Cryptosystem | The Size of pp | Size of sk | Size of Ciphertext | Support and-Gates on Positive and Negative Attributes | LWE Assumption |
|---|---|---|---|---|---|
| [28] | $(2\,\lvert L\rvert+1)\,n\times(2\,\lvert L\rvert+1)\,m+n$ | $\lvert L\rvert m$ | $(2\lvert L\rvert+1-\lvert S\rvert)m$ | YES | YES |
| [17] | $(2\,\lvert L\rvert+1)\,n\times(2\,\lvert L\rvert+1)\,m+n$ | $\lvert L\rvert m$ | 1+$(2\lvert L\rvert+1)m$ | YES | YES |
| Our scheme | $2\,\lvert L\rvert\,n\times 2\,\lvert L\rvert\,m+n$ | $\lvert L\rvert m$ | 1+2$\lvert L\rvert m$ | YES | YES |

(2) The existing CP-ABPRE schemes are constructed by bilinear pairing [15,27,29], which are fragile when the post-quantum future comes. Our CP-ABPRE was constructed based on LWE, which is widely believed to be secure in quantum computer attacks.

(3) Compared with the PRE based on LWE, our scheme is the first CP-ABPRE scheme based on LWE and has the same computational complexity $O(n^2)$. The comparison results are in Table 3.

**Table 3.** Comparison for proxy re-encryption (PRE) schemes.

| Cryptosystem | Interactivity | Directionality | Security | LWE Assumption | Access Control |
|---|---|---|---|---|---|
| [8] | NO | Unidirectional | CPA | YES | NO |
| [9] | NO | Unidirectional | CPA | YES | NO |
| [10] | NO | Unidirectional | CPA | YES | NO |
| [30] | YES | Bidirectional | CPA | YES | NO |
| [31] | NO | Unidirectional | CPA | YES | NO |
| [32] | NO | Unidirectional | CPA | YES | NO |
| Our scheme | NO | Unidirectional | CPA | YES | YES |

## 4. Extension

In this section, we extend our CP-ABPRE scheme to a CP-ABPRE-KS scheme based on [17].

**Definition 5.** *A single-hop unidirectional CP-ABPRE-KS scheme consists of the following eight algorithms:*

*1. Setup$(n, m, q, L)$: For positive integers $n, m, q$, and a set of attributes $L$, the TA outputs public parameters $pp$ and master secret key $msk$.*

*2. KeyGen$(pp, msk, S)$: For $pp, msk$ and an attribute set $S$ of user (DO or DU), the TA outputs secret key $sk_S$ for $S$.*

*3. Encrypt$(pp, W, kw, \mu)$: For $pp$, a message $\mu$, a keyword $kw$, and an access structure $W$ over the attribute set $L$, the DO outputs ciphertext $C_W$.*

*4. Decrypt$(pp, C_{W,kw}, sk_S, S)$: For $pp, C_{W,kw}, S$ and its corresponding secret key $sk_S$, the user (DO or DU) outputs plaintext $\mu$ if $S \vDash W$ or a symbol $\perp$ indicating either $C_W$ is invalid or $S \nvDash W$.*

*5. ReKeyGen$(pp, S, W, W^1)$: For $pp$, two access structures $W, W^1$ and an attribute set $S$, if $S \vDash W$, and $W$ and $W^1$ are disjoint, the TA outputs re-encryption key $rk_{W\to W^1}$, otherwise outputs a symbol $\perp$.*

*6. ReEnc$(pp, C_{W,kw}, rk_{W\to W^1})$: For $pp$, $C_{W,kw}$, $rk_{W\to W^1}$, the CSP outputs the re-encrypted ciphertext $C_{W^1,kw}$.*

*7. Trapdoor$(pp, msk, S, kw)$: For $pp, msk, kw$, and a DU's attribute set $S$, the TA returns the trapdoor $T_{kw}$.*

*8. Test $(pp, T_{kw}, C_{W,kw'}, R)$: For $pp, T_{kw} = \vec{e}, C_{W,kw'}$, the DU constructs a list $R$ about the positive or negative information of attributes, and sends $R$ to CSP. The CSP returns $\eta$, where $\eta = 1$ means $kw = kw'$, $\eta = 0$ means $kw \neq kw'$.*

The CP-ABPRE-KS scheme is shown below.

1. Setup($n, m, q, L$): Given positive integers $n, m, q$, and a set of attributes $L$, the TA chooses a hash function $H : \{0,1\}^* \to \mathbb{Z}_q^n$, samples $\vec{u} \leftarrow \mathbb{Z}_q^n$, computes $(A_{i,b}, T_{i,b}) \leftarrow TrapGen\,(q, n)$ for $i \in L$, where $b \in \{0,1\}$ and returns public parameters $pp = \left(\{A_{i,b}\}_{i\in L}^{b\in\{0,1\}}, \vec{u}, H\right)$ and master secret key $msk = \left(\{T_{i,b}\}_{i\in L}^{b\in\{0,1\}}\right)$.

2. KeyGen($pp, msk, S$): Given $pp, msk$, and an attribute set $S$ of the DU, where $S \subseteq L$, the TA lets $A_i = \begin{cases} A_{i,0}, & i \in L\backslash S \\ A_{i,1}, & i \in S \end{cases}$, computes $\vec{s} \leftarrow \text{SamplePre}\,(A, T, \vec{u})$, and returns secret key $sk_S = \vec{s}$, where $A = \left(A_1|\cdots|A_{|L|}\right)$, $T = \begin{bmatrix} T_1 & & \\ & \ddots & \\ & & T_{|L|} \end{bmatrix}$, $T_i$ is the basis for $\Lambda_q^\perp\,(A_i)$, $i \in L$.

3. Encrypt($pp, W, kw, \mu$): Given $pp$, a message $\mu \in \{0,1\}$, a keyword $kw$, and an access structure $W$, the DO denotes $S^+\,(S^-)$ as the positive (negative) attribute set in $W$, computes

$$c = \vec{u}^T\vec{f} + x_c + \left\lfloor \frac{q}{2} \right\rfloor \mu,$$

$$p = H(kw)^T\vec{f} + x_p,$$

$$\vec{c}_{i,0} = \begin{cases} \vec{z}_{i,0}, & i \in S^+ \\ A_{i,0}^T\vec{f} + \vec{x}_{i,0}, & i \in S\text{–} \end{cases},$$

$$\vec{c}_{i,1} = \begin{cases} A_{i,1}^T\vec{f} + \vec{x}_{i,1}, & i \in S^+ \\ \vec{z}_{i,1}, & i \in S^- \end{cases},$$

$$\begin{pmatrix} \vec{c}_{j,0} \\ \vec{c}_{j,1} \end{pmatrix} = \begin{pmatrix} A_{j,0}^T \\ A_{j,1}^T \end{pmatrix}\vec{f} + \begin{pmatrix} \vec{x}_{j,0} \\ \vec{x}_{j,1} \end{pmatrix},$$

$j \in L\backslash\,(S^+ \cup S^-)$, and returns ciphertext

$$C_{W,kw} = \left(c; p; \{\vec{c}_{i,0}, \vec{c}_{i,1}\}_{i\in L}\right),$$

where $x_c, x_p \leftarrow \chi$, $\vec{f} \leftarrow \chi^n$, $\vec{z}_{i,0}, \vec{z}_{i,1}, \vec{x}_{i,0}, \vec{x}_{i,1} \leftarrow \chi^m$.

4. Decrypt($pp, C_{W,kw}, sk_S, S$): After receiving the cipthertext $C_{W,kw}$ from CSP, the DU computes $\vec{y} = \left(\vec{y}_1; \cdots; \vec{y}_{|L|}\right)$ by $\vec{y}_i = \begin{cases} \vec{c}_{i,1}, & i \in S \\ \vec{c}_{i,0}, & else \end{cases}$, and then outputs 0 if $\left(-\vec{s}^T|1\right)\left(\vec{y}^T; c\right) = c - \vec{y}^T\vec{s}$ is closer to 0 than to $\left\lfloor \frac{q}{2} \right\rfloor$ modulo q, and 1 otherwise.

5. ReKeyGen($pp, S, W, W^1$): After receiving $pp, S$, two access structures $W, W^1$ from DO, if $W, W^1$ are not disjoint or $S \nvDash W$, then the TA outputs $\perp$, and otherwise denotes the positive (negative) attribute set in $W^1$ as $S^{1,+}\,\left(S^{1,-}\right)$, noting $S^{1,+} \subseteq L, S^{1,-} \subseteq L$, then computes

$$Q_{i,0} \leftarrow \begin{cases} \overline{X}_i, & i \in S^{1,+} \\ \text{P2}\left(R_{i,1\to 0}^T\right) + X_i, & i \in S^{1,-} \end{cases},$$

$$Q_{i,1} \leftarrow \begin{cases} \text{P2}\left(R_{i,0\to 1}^T\right) + X_i, & i \in S^{1,+} \\ \overline{X}_i, & i \in S^{1,-} \end{cases},$$

$$Q_{i,0} \leftarrow P2\left(R^T_{i,1\to 0}\right) + X_{i,0}, i \in \left(L\backslash\left(S^{1,+} \cup S^{1,-}\right)\right),$$

$$Q_{i,1} \leftarrow P2\left(R^T_{i,0\to 1}\right) + X_{i,1}, i \in \left(L\backslash\left(S^{1,+} \cup S^{1,-}\right)\right),$$

where $R_{i,1\to 0} \leftarrow \text{SamplePre}\left(A_{i,1}, T_{i,1}, A_{i,0}\right)$, $R_{i,0\to 1} \leftarrow \text{SamplePre}\left(A_{i,0}, T_{i,0}, A_{i,1}\right)$, $X_i, X_{i,0}, X_{i,1} \leftarrow \chi^{m\times m\lceil\log q\rceil}$, $\overline{X_i} \leftarrow \mathbb{Z}_q^{m\times m\lceil\log q\rceil}$ and finally returns re-encryption key $rk_{W\to W^1} = \left(\{Q_{i,0}, Q_{i,1}\}_{i\in L}\right)$.

6. ReEnc($pp, C_{W,kw}, rk_{W\to W^1}$): Given $pp, C_{W,kw}, rk_{W\to W^1}$, the CSP computes

$$\vec{c}^{\,1}_{i,0} = \begin{cases} Q_{i,0}BD\left(\vec{c}_{i,1}\right) + \vec{x}^{\,1}_{i,0}, & i \in S^{1,-} \\ \vec{z}^{\,1}_{i,0}, & i \in S^{1,+} \end{cases},$$

$$\vec{c}^{\,1}_{i,1} = \begin{cases} Q_{i,1}BD\left(\vec{c}_{i,0}\right) + \vec{x}^{\,1}_{i,1}, & i \in S^{1,+} \\ \vec{z}^{\,1}_{i,1}, & i \in S^{1,-} \end{cases},$$

$$\vec{c}^{\,1}_{j,0} = Q_{i,0}BD\left(\vec{c}_{j,1}\right) + \vec{x}^{\,1}_{j,0},$$

$$\vec{c}^{\,1}_{j,1} = Q_{i,1}BD\left(\vec{c}_{j,0}\right) + \vec{x}^{\,1}_{j,1},$$

$$j \in \left(L\backslash\left(S^{1,+} \cup S^{1,-}\right)\right),$$

where $\vec{x}^{\,1}_{i,0}, \vec{x}^{\,1}_{j,0} \leftarrow \chi^m$, $\vec{z}^{\,1}_{i,0}, \vec{z}^{\,1}_{i,1} \leftarrow \mathbb{Z}_q^m$ and outputs the re-encrypted ciphertext

$$C_{W^1,kw} = \left(c; p; \left\{\vec{c}^{\,1}_{i,0}, \vec{c}^{\,1}_{i,1}\right\}_{i\in L}\right).$$

7. Trapdoor($pp, msk, S, kw$): Given $pp, msk, kw$ and a DU's attribute set $S$, the TA computes $H(kw)$ and a matrix $A = \left(A_1|\cdots|A_{|L|}\right)$, where $A_i = \begin{cases} A_{i,0}, & i \in L\backslash S \\ A_{i,1}, & i \in S \end{cases}$, and computes $\vec{e} \leftarrow \text{SamplePre}\left(A, T, H(kw)\right)$ and returns the trapdoor $T_{kw} = \vec{e}$, where $T = \begin{bmatrix} T_1 & & \\ & \ddots & \\ & & T_n \end{bmatrix}$, $T_i$ is the basis for $\Lambda_q^{\perp}\left(A_i\right), i \in L$.

8. Test ($pp, T_{kw}, C_{W,kw'}, R$): Given $pp, T_{kw} = \vec{e}, C_{W,kw'}$, the DU constructs a list $R$ about the positive or negative information of attributes, and sends $R$ to CSP. The CSP computes $\vec{y} = \left(\vec{y}_1; \cdots; \vec{y}_{|L|}\right)$ by $\vec{y}_i = \begin{cases} \vec{c}_{i,1}, & i\, is\, positive\, attribute \\ \vec{c}_{i,0}, & else \end{cases}$, and returns $\eta = \begin{cases} 1, & \left|p - \vec{e}^T\vec{y}\right| < \frac{q}{4} \\ 0, & else \end{cases}$, where $\eta = 1$ means $kw = kw'$, $\eta = 0$ means $kw \neq kw'$.

Figure 2 shows the sequence diagram of the whole scheme. Since the $c, p$ in the original ciphertext are same as the $c$ in the re-encrypted ciphertext, and the construction of $c = \vec{u}^T\vec{f} + x_c + \left\lfloor\frac{q}{2}\right\rfloor\mu$ and $p = H(kw)^T\vec{f} + x_p$ are similar. Therefore, the correctness of the CP-ABPRE-KS scheme can be proved by the correctness of the CP-ABPRE scheme.

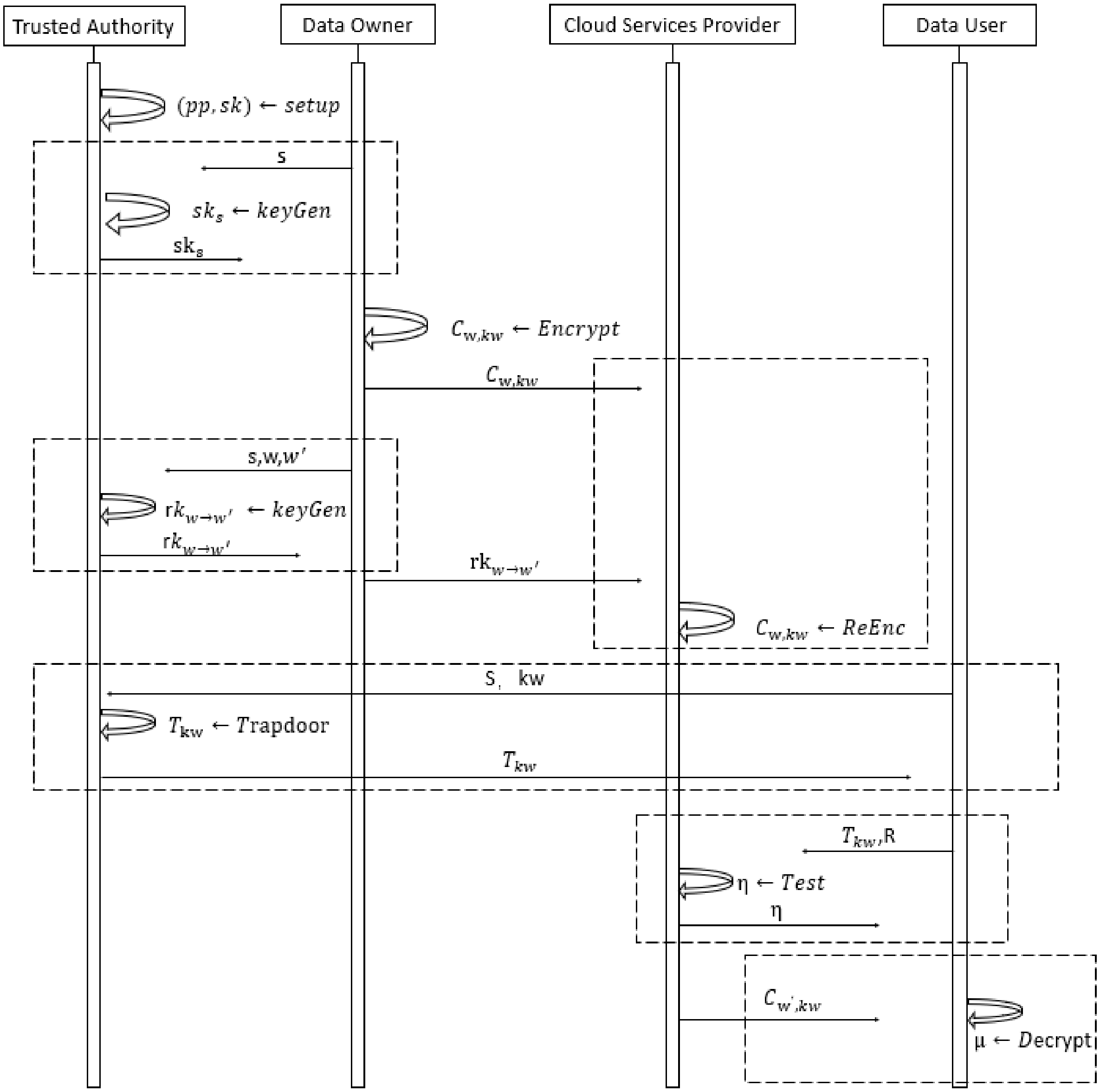

**Figure 2.** The sequence diagram of the CP-ABPRE with keyword search (CP-ABPRE-KS) scheme.

Based on the security definition of [17,21], we can define the IND-sAS-CKA (chosen keyword attacks) secure at the original ciphertext for the CP-ABPRE-KS scheme by modifying Definition 3 as follows:

(1) Adding Trapdoor oracle $\mathcal{O}_{\text{tr}}\,(pp, S, kw)$ to the Learning Phase.

$\mathcal{O}_{\text{tr}}\,(pp, S, kw)$: The adversary inputs an attribute set $S$ and $H(kw)$. If $\mathrm{S} \nvDash \mathrm{W}^*$, then challenger returns $\vec{e} \leftarrow Trapdoor(pp, msk, S, kw)$, where $A = \left(A_1|\cdots|A_{|L|}\right)$, $A_i = \begin{cases} A_{i,0}, & i \in L\backslash S \\ A_{i,1}, & i \in S \end{cases}$, $T = \begin{bmatrix} T_1 & & \\ & \ddots & \\ & & T_n \end{bmatrix}$, $T_i$ is the basis for $\Lambda_q^{\perp}\,(A_i)$, $i \in L$.

(2) Modifying the **Challenge**.

**Challenge**: If the adversary finishes all of the oracles' queries, then the adversary sends $kw_0, kw_1$ to the challenger. For a coin $b \in \{0,1\}$, the challenger returns a random ciphertext $C$ if $b = 0$ or the real ciphertext $\mathrm{C}_{W^*} \leftarrow \mathrm{Encrypt}(\mathrm{pp}, \mathrm{W}^*, kw)$ if $b = 1$.

The others are the same as Definition 3.

Note that $H$ is a hash function (random oracle) and $\vec{e} \in D_{\mathbb{Z}^m,\sigma}$, the security of the CP-ABPRE-KS scheme in the random model can be proved by the security of the CP-ABPRE scheme.

## 5. Conclusions

Focusing on the safe and efficient issue of cloud sharing, we construct the first CP-ABPRE scheme based on LWE. The CP-ABPRE scheme consists of six algorithms, and has small public parameters. Then, we show the correctness and parameters of the scheme, and prove the security under LWE. Because the data owner encrypts the data using the ABE scheme and then uploads the ciphertexts to the cloud, the data owner can implement fine-grained access control on the data. When the data owner wants to share the data with the data user who cannot access the data, the data owner only needs to send the re-encryption key to the cloud. The cloud implements the tedious re-encrypted ciphertexts generation calculation, and converts the ciphertexts under one access structure into re-encrypted ciphertexts under another access structure without decrypting the ciphertexts. The CP-ABPRE-KS scheme can search data without compromising data confidentiality, and can also transfer heavy data search operations to the cloud which reduces the computing burden of the user. In addition, because the LWE assumption is generally considered to be able to resist quantum computing attacks, the two schemes in this paper can guarantee the security under quantum computing attacks. However, the two schemes can only transform the ciphertexts under disjoint access structures. We will further study the conversion under more general access structures and the hierarchical key assignment schemes (HKASs) to achieve fine-grained access control.

**Author Contributions:** All authors contributed to the paper. J.L. and K.Z. wrote the manuscript with supervision from C.M. and J.L. is responsible for the design of the cryptosystem.

**Funding:** This work was supported by the National Natural Science Foundation of China (61472097), the Natural Science Foundation of Heilongjiang Province of China (JJ2019LH1770), the Special Funds of Heilongjiang University of the Fundamental Research Funds for the Heilongjiang Province (RCCXYJ201812), and the Open Fund of the State Key Laboratory of Information Security (2019-ZD-05).

**Conflicts of Interest:** The authors declare no conflicts of interest.

## References

1. Castiglione, A.; De Santis, A.; Masucci, B.; Palmieri, F.; Huang, X.; Castiglione, A. Supporting dynamic updates in storage clouds with the Akl-Taylor scheme. *Inf. Sci.* **2017**, *387*, 56–74. [CrossRef]
2. Crampton, J.; Gagarin, A.; Gutin, G.; Jones, M.; Wahlström, M. On the workflow satisfiability problem with class-independent constraints for hierarchical organizations. *ACM Trans. Priv. Secur.* **2016**, *19*, 3. [CrossRef]
3. Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. Attribute-based encryption for finegrained access control of encrypted data. In Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 30 October–3 November 2006; pp. 89–98.
4. Xhafa, F.; Li, J.; Zhao, G.; Li, J.; Chen, X.; Wong, D.S. Designing cloud-based electronic health record system with attribute-based encryption. *Multimed. Tools Appl.* **2015**, *74*, 10, 3441–3458. [CrossRef]
5. Wang, D.; Ma, C.; Shi, L.; Wang, Y. On the Security of an Improved Password Authentication Scheme Based on ECC. In *Information Computing and Applications, ICICA 2012*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7473, pp. 181–188.

6. He, D.; Wang, D.; Wu, S. Cryptanalysis and improvement of a password-based remote user authentication scheme without smart cards. *Inf. Technol. Control.* **2013**, *42*, 105–112. [CrossRef]
7. Wang, D.; Ma, C.; Zhang, Q.; Zhao, S. Secure password-based remote user authentication scheme against smart card security breach. *J. Netw.* **2013**, *8*, 148–155. [CrossRef]
8. Ma, C.; Li, J.; Ouyang, W. Lattice-Based Identity-Based Homomorphic Conditional Proxy Re-Encryption for Secure Big Data Computing in Cloud Environment. *Int. J. Found. Comput. Sci.* **2017**, *28*, 645–660. [CrossRef]
9. Ma, C.; Li, J.; Ouyang, W. A Homomorphic Proxy Re-encryption from Lattices. In *Provable Security. ProvSec 2016*; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2016; Volume 10005, pp. 353–372.
10. Li, J,; Ma, C.; Zhang, L.; Yuan, Q. Unidirectional FHPRE Scheme from Lattice for Cloud Computing. *Int. J. Netw. Secur.* **2019**, *21*, 592–600.
11. Singh, K.; Rangan, C.P.; Banerjee, A.K. Lattice Based Identity Based Proxy Re-Encryption Scheme. *J. Internet Serv. Inf. Secur* .**2013**, *3*, 38–51.
12. Yang, Y.; Zheng, X.; Chang, V.; Tang, C. Semantic keyword searchable proxy re-encryption for postquantum secure cloud storage. *Concurr. Comput. Pract. Exp.* **2017**, *29*, e4211. [CrossRef]
13. Liang, X.; Cao, Z.; Lin, H.; Shao, J. Attribute based proxy re-encryption with delegating capabilities. In Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, Sydney, Australia, 10–12 March 2009; pp. 276–286.
14. Luo, S.; Hu, J.; Chen, Z. Ciphertext Policy Attribute-Based Proxy Re-encryption. In *Information and Communications Security, ICICS 2010*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6476, pp. 401–415.
15. Liang, K.; Man, H.; Liu, J.; Susilo, W.; Wong, D.S.; Yang, G.; Yu, Y.; Yang, A. A secure and efficient Ciphertext-Policy Attribute-Based Proxy Re-Encryption for cloud data sharing. *Future Gener. Comput. Syst.* **2015**, *52*, 95–108. [CrossRef]
16. Zhang, J.; Zhang, Z.; Ge, A. Ciphertext policy attribute-based encryption from lattices. In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, Seoul, Korea, 2–4 May 2012; pp. 16–17.
17. Zeng, F.; Xu, C. A novel model for lattice-based authorized searchable encryption with special keyword. *Math. Probl. Eng.* **2015**, *314621*. [CrossRef]
18. Boneh, D.; Di Crescenzo, G.; Ostrovsky, R.; Persiano, G. Public key encryption with keyword search. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, 2–6 May 2004; pp. 506–522.
19. Shao, J.; Cao, Z.; Liang, X.; Lin, H. Proxy re-encryption with keyword search. *Inf. Sci.* **2010**, *180*, 2576–2587. [CrossRef]
20. Wang, X.; Huang, X.; Yang, X.; Liu, L.; Wu, X. Further observation on proxy re-encryption with keyword search. *J. Syst. Softw.* **2012**, *85*, 643–654. [CrossRef]
21. Shi, Y.; Liu, J.; Han, Z.; Zheng, Q.; Zhang, R.; Qiu, S. Attribute-Based Proxy Re-Encryption with Keyword Search. *PLoS ONE* **2015**, *9*, e116325. [CrossRef] [PubMed]
22. Hong, H.; Sun, Z. Towards secure data sharing in cloud computing using attribute based proxy re-encryption with keyword search. In Proceedings of the 2017 IEEE 2nd International Conference on Cloud Computing and Big Data Analysis, ICCCBDA2017, Chengdu, China, 28–30 April 2017; pp. 218–223, .
23. Alwen, J.; Peikert, C. Generating shorter bases for hard random lattices. *Theory Comput. Syst.* **2011**, *48*, 535–553. [CrossRef]
24. Agrawal. S.; Boneh. D.; Boyen X. Efficient Lattice (H)IBE in the Standard Model. In *Advances in Cryptology-EUROCRYPT 2010, EUROCRYPT 2010*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6110, pp. 553–572.
25. Micciancio, D.; Peikert, C. Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller. In *Advances in Cryptology-EUROCRYPT 2012, EUROCRYPT 2012*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7237, pp. 700–718.
26. Regev, O. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM* **2005**, *56*, 34.

27. Liang, K.; Fang, L.; Susilo, W.; Wong, D.S. A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security. In Proceedings of the 5th International Conference on Intelligent Networking and Collaborative Systems, INCoS2013, Xi'an, China, 9–11 September 2013; pp. 55–559.
28. Zhang, J.; Zhang, Z. A Ciphertext Policy Attribute-Based Encryption Scheme without Pairings. In *Information Security and Cryptology. Inscrypt 2011*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2011; Volume 7537, pp. 324–340.
29. Zeng, P.; Choo, K. A New Kind of Conditional Proxy Re-Encryption for Secure Cloud Storage. *IEEE Access* **2018**, *6*, 70017–70024 [CrossRef]
30. Xagawa, K. Cryptography with Lattices. Ph.D. Thesis, Department of Mathematical and Computing Sciences, Tokyo Institute of Technology, Tokyo, Japan, 2010.
31. Jiang, M.; Hu, Y.; Wang, B.; Wang, F.H.; Lai, Q.Q. Lattice-based multi-use unidirectional proxy re-encryption. *Secur. Commun. Netw.* **2016**, *8*, 3796–3803. [CrossRef]
32. Hou, J.; Jiang, M.; Guo, Y.; Song, W. Identity-Based Multi-bit Proxy Re-encryption Over Lattice in the Standard Model. In *Frontiers in Cyber Security, FCS 2018, Communications in Computer and Information Science*; Springer: Singapore, 2018; Volume 879, pp. 110–118.

© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).