A Novel Lattice-Based Ciphertext-Policy Attribute-Based Proxy Re-encryption for Cloud Sharing

Juyan Li[1,3], Chunguang Ma[2,3], and Kejia Zhang[1](✉)

[1] College of Data Science and Technology, Heilongjiang University,
Harbin 150080, People's Republic of China
lijuyan587@163.com, zhangkejia@hlju.edu.cn

[2] College of Computer Science and Technology, Harbin Engineering University,
Harbin 150001, People's Republic of China
machunguang@hrbeu.edu.cn

[3] State Key Laboratory of Information Security, Institute of Information Engineering,
Chinese Academy of Sciences, Beijing 100093, People's Republic of China

Abstract. Proxy re-encryption plays an important role in cloud sharing. Ciphertext-policy attribute-based proxy re-encryption (CP-ABPRE) scheme supports access control and can convert the ciphertext under an access policy to a ciphertext under another access policy, 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 comes. In this paper, a unidirectional single-hop CP-ABPRE scheme with small size of public parameters was presented by using trapdoor sampling, and proved secure under learning with errors assumption which is widely believed secure in quantum computer attacks.

Keywords: LWE · Proxy re-encryption · Attribute-based encryption · Cloud sharing

1 Introduction

Proxy re-encryption (PRE) allows the proxy to convert the ciphertext of delegator to the ciphertext of delegatee who can be specified by the delegator, while the proxy will not know the message in this process, which can be used for cloud sharing. At present, many types of PRE have been constructed such as conditional proxy re-encryption (CPRE) [1], homomorphic proxy re-encryption (HPRE) [2], proxy broadcast re-encryption (PBRE) [3], identity-based proxy re-encryption (IBPRE) [4], Attribute-Based Proxy Re-Encryption (ABPRE) [5].

Attribute-Based Encryption (ABE) was introduced by Sahai et al. [6] which is an extension of identity-based encryption (IBE). ABE can achieve fine-grained access control of encrypted data and provide a one-to-many encryption. Goyal et al. [7] introduced two variants of ABE, that is key policy attribute-based

W. Meng and S. Furnell (Eds.): SocialSec 2019, CCIS 1095, pp. 32–46, 2019.
https://doi.org/10.1007/978-981-15-0758-8_3

encryption (KP-ABE) and ciphertext policy attribute-based encryption (CP-ABE). In a KP-ABE (CP-ABE) system, the ciphertext (private key) is associated with an attribute set S, the private key (ciphertext) is associated with an access structure W, the private key can decrypt the ciphertext if and only if S satisfies W.

Because of the resource-limited of the terminal device, it is impossible for users to backup all data (in the plain format) and make heavy compute. In cloud networks, a user (e.g., Alice) can use CP-ABE to encrypt her data with access structure W, and then store the ciphertext to cloud for sharing data and protecting her privacy. Suppose the access structure W needs to be updated to another policy W' for the new needs of other users (e.g., Bob), then Alice should download and decrypt the ciphertext, and then again encrypt the data with W'. If the access structure is renewed frequently, the computational overhead of this strategy at Alice will be too heavy.

Ciphertext-policy attribute-based proxy re-encryption (CP-ABPRE) can make data cloud sharing more effective. ABPRE only needs Alice to generate a re-encryption key and send it to proxy who can convert the ciphertext under W to a ciphertext under another W'. Cloud sharing should also consider issues such as authentication [8–10]. Liang et al. [11] constructed the first CP-ABPRE supporting AND gates over positive and negative attributes. Luo et al. [12] extended [5]to a CP-ABPRE supporting AND gates on multi-valued and negative attributes. Liang et al. [13] constructed the first adaptively CCA-secure CP-ABPRE. Zhang et al. [14] presented a ciphertext policy attribute-based encryption (ABE) scheme based on LWE which is widely believed secure in quantum computer attacks.

In this paper, we constructed a CP-ABE scheme by modifying the ABE scheme of Zeng et al. [15]. Compared with the ABE scheme of [14,15], our CP-ABE scheme has smaller size of public parameters. The existing CP-ABPRE schemes are constructed by bilinear pairing or multi-linear maps which are fragile when the post-quantum comes. We constructed a CP-ABPRE based on the new CP-ABE scheme by using trapdoor sampling from LWE which is widely believed secure in quantum computer attacks. Our CP-ABPRE scheme is the first CP-ABPRE from LWE and can implement the transfer of ciphertext access structure.

The rest of this paper is organized as follows. Section 2 is preliminaries. Section 3 describes the constructed ABPRE scheme. At last, our work is concluded in Sect. 4.

2 Preliminaries

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

2.1 Notation

We employ some initial notations listed in Table 1. For an integer q and a vector $\boldsymbol{x} \in \mathbb{Z}_q{}^n$, let $l = \lceil \log q \rceil$, $P2\left(\boldsymbol{x}\right) = \left(1\boldsymbol{x}; 2\boldsymbol{x}; \cdots ; 2^{l-1}\boldsymbol{x}\right) \in \mathbb{Z}_q^{nl}$, $BD\left(\boldsymbol{x}\right) = \left(\boldsymbol{u}_1 | \cdots | \boldsymbol{u}_l\right) \in \{0,1\}^{nl}$, where $\boldsymbol{x} = \sum\limits_{k=1}^{l} 2^{k-1}\boldsymbol{u}_k$. 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
$\boldsymbol{x}$	Vector
A	Matrix or set
$\Vert\boldsymbol{x}\Vert_\infty$	l_∞ norm of $\boldsymbol{x}$
$\Vert\boldsymbol{x}\Vert$	l_2 norm of $\boldsymbol{x}$
$[k]$	Set $\{1, 2, \cdots, k\}$
$\vert L \vert$	The order of set L
$S \vDash (\nvDash) W$	Attribute set S satisfies (or does not satisfy) access structure W
$[X \vert Y] \in \mathbb{Z}_q^{m\times(n_1+n_2)}$	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 χ
$x \leftarrow S$	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 $\boldsymbol{c}$: $\forall \boldsymbol{x} \in \mathbb{R}^m$,

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

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

$$\chi_{\Lambda,\sigma,\boldsymbol{c}}(\boldsymbol{x}) = \frac{\rho_{s,\boldsymbol{c}}\left(\boldsymbol{x}\right)}{\rho_{\sigma,\boldsymbol{c}}\left(\Lambda\right)},$$

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

Lemma 1 *([16]). For any $\boldsymbol{c} \in \Lambda \subset \mathbb{Z}^m$, let $\boldsymbol{x} \leftarrow D_{\Lambda+\boldsymbol{c},\sigma}$, $\sigma > \eta_\epsilon(\Lambda)$ for some $\epsilon \in (0,1)$, then with overwhelming probability $\|\boldsymbol{x}\| < \sigma\sqrt{m}$. Moreover, if $\boldsymbol{c} = 0$ then the bound holds for any $\sigma > 0$, with $\epsilon = 0$.*

Lemma 2 *([17]). Let q, n, m be positive integers with $q \geq 2$ and $\mathrm{m} \geq 6nlogq$. There is a probabilistic polynomial-time algorithm TrapGen(q, n, m) that outputs a pair $(A, T) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}^{m\times m}$ such that A is statistically close to uniform in $\mathbb{Z}_q^{n\times m}$ and T is a basis for $\Lambda_q^{\perp}(A) = \{\boldsymbol{e} \in \mathbb{Z}^m, s.t. A\boldsymbol{e} = 0 \bmod q\}$, satisfying $\|T\| \leq O(nlogq)$ 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 3 *([18]). Let $q \geq 2$ and a matrix $A \in \mathbb{Z}_q^{n\times m}$. Let T_{A} be a basis for $\Lambda_q^{\perp}(A)$, $\sigma \geq \left\|\widetilde{T}\right\|\omega\left(\sqrt{\log m}\right)$. Then for $\boldsymbol{c} \in \mathbb{Z}^m, \boldsymbol{u} \in \mathbb{Z}_q^n$. There is a PPT algorithm SamplePre$(A, T_{\mathrm{A}}, \boldsymbol{u}$, $\boldsymbol{c})$ that returns $\boldsymbol{x} \in \Lambda_q^{\boldsymbol{u}}(A) = \{\boldsymbol{e} \in \mathbb{Z}^m, s.t. A\boldsymbol{e} = \boldsymbol{u} \bmod q\}$ sampled from a distribution statistically close to $D_{\Lambda_q^{\boldsymbol{u}}(\boldsymbol{A}),\sigma,\boldsymbol{c}}$.*

For the correctness of our CP-ABPRE, we recall a distribution $\overline{\Psi}_\alpha$ over $\mathbb{Z}_q$ in which the random variable is $\lfloor qX\rceil \mod q$, where $\alpha \in (0,1)$ is a real, p is a prime, X is a normal random variable with mean 0 and deviation $\alpha^2/\ 2\pi$.

Lemma 4 *([18]). Let $\boldsymbol{r} \in \mathbb{Z}^m$, $\boldsymbol{e} \leftarrow \overline{\Psi}_\alpha^m$. Then with overwhelming probability in m*

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

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

The LWE (learning with errors) problem is a classic hard problem on lattices, which is as hard as the worst-case SIVP and GapSVP with certain noise distributions χ, such as $\overline{\Psi}_\alpha$.

Theorem 1 *([19]). Let $q \geq 2$, and χ be a distribution over $\mathbb{Z}$. The decisional $LWE_{n,q,\chi}$ problem is to distinguish the following two distributions: one is $(\boldsymbol{a_i}; b_i) \leftarrow \mathbb{Z}_q^{n+1}$, the other is $(\boldsymbol{a_i}, b_i) \in \mathbb{Z}_q^{n+1}$, where $\boldsymbol{a_i} \leftarrow \mathbb{Z}_q^n, b_i = \boldsymbol{a_i}^T\boldsymbol{s} + e_i$, $\boldsymbol{s} \leftarrow \mathbb{Z}_q^n$, $e_i \leftarrow \chi$. The $LWE_{n,q,\chi}$ assumption is that the $LWE_{n,q,\chi}$ problem is infeasible.*

2.3 Attribute and Access Structure

In this paper, we study CP-ABE that supports and-gates on positive and negative attributes. Let $L = [|L|]$ be the set of all attributes in system. For $i \in [L]$, each user has or does not have attribute i. If a user does not have attribute i, we say the user has attribute $-i$ which means each attribute i is associated with $-i$. We use i and $-i$ as positive and negative attribute, respectively.

Definition 1. *For an access structure W organized by and-gates on positive and negative attributes, 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, L is the set of all attributes in system.

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 don't need 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.

2.4 Definition and Security Model of CP-ABPRE

A Single-Hop Unidirectional CP-ABPRE scheme has four participants.

(1) Trusted Authority (TA). TA generates public parameters, master secret key, re-encryption key and can be trusted by all participants.
(2) Cloud Services Provider (CSP). CSP can store data which were uploaded by DO, compute the re-encrypted ciphertext by the original ciphertext and re-encryption key. CSP is semi-trusted.
(3) Data Owner (DO). DO encrypts his data and stores the encrypted data in cloud.
(4) Data User (DU). DU queries the CSP for re-encrypted data which belongs to DO.

Based on the definition and the security model of Liang et al. [5], we give the following definition.

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

1. *Setup (κ, L): Given a security parameter κ, a set of attribute L, the TA returns public parameters pp and master secret key msk.*
2. *KeyGen (pp, msk, S): Given pp, msk and an attribute set S of the DO or DU, the TA returns secret key sk_S for S. Note that each secret key sk_S is associated with an attribute set S.*
3. *Encrypt (pp, W, μ): Given pp, a message μ, and an access structure W over the attribute set L, the DO returns ciphertext C_W. Note that each ciphertext C_W is associated with an access structure W.*
4. *Decrypt (pp, sk_S, C_W, S): Given pp, C_W, S and its corresponding secret key sk_S, the DO or DU returns plaintext μ 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): Given pp, attribute set S and two access structures W, W^1, the TA returns a re-encryption key $rk_{W \rightarrow W^1}$ which can be used to transform a ciphertext with W to another ciphertext with W^1 if $S \vDash W$ or a symbol $\perp$ if $S \nvDash W$. The access structure W and W^1 are required to be disjoint, that is $S^+ \subseteq S^{1,-}, S^- \subseteq S^{1,+}$, where $S^+, S^{1,+}(S^-, S^{1,-})$ are the positive (negative) attribute set in W, W^1.*

6. *ReEnc* $(pp, C_W, rk_{W\to W^1})$*: Given* pp*,* C_W*,* $rk_{W\to W^1}$*, the CSP outputs the re-encrypted ciphertext* C_{W^1} *or a symbol* $\perp$ *indicating* W *and* W^1 *are not disjoint.*

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

Initialization. *The adversary chooses a challenge access structure* W^* *to challenger.*

Setup Phase: *The challenger runs Setup (*κ*, L) and sends pp to adversary.*

Learning Phase: *In this phase, the adversary can access to 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* $\mathrm{sk}_S \leftarrow \mathrm{KeyGen}(\mathrm{pp}, \mathrm{msk}, \mathrm{S})$*. Otherwise, the challenger returns* $\perp$*.*

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

(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* $rk_{W\to W'} \leftarrow \mathrm{ReKeyGen}(\mathrm{pp}, \mathrm{W}, W')$*,* $\mathrm{sk}_S \leftarrow \mathrm{KeyGen}(\mathrm{pp}, \mathrm{msk}, \mathrm{S})$*,* $S \vDash W$*, then the challenger returns* $C_{W'} \leftarrow \mathrm{ReEnc}(\mathrm{pp}, \mathrm{C}_W, rk_{W\to W'})$*. Otherwise, the challenger returns* $\perp$*.*

Challenge: *If the adversary finishes all of the oracles' queries, then he 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 original ciphertext if for any PPT adversary, the advantage

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

of adversary is negligible.

Definition 4. *For a single-hop unidirectional CP-ABPRE scheme, let κ 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*

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

of 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 Definition3, $State_1$ 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

In this section, a single-hop unidirectional CP-ABPRE scheme was presented at first, then the correctness and security of CP-ABPRE were proved.

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 attribute L, the TA samples $\boldsymbol{u} \leftarrow \mathbb{Z}_q^n$, computes $(A_{i,b}, T_{i,b}) \leftarrow TrapGen(q, n)$ for $i \in L$, where $b \in \{0,1\}$ and returns public parameters $pp = \left(\{A_{i,b}\}_{i \in L}^{b \in \{0,1\}}, \boldsymbol{u}\right)$ 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 $\boldsymbol{s} \leftarrow$ SamplePre$(A, T, \boldsymbol{u})$ and returns secret key $sk_S = \boldsymbol{s}$, where $A = (A_1 | \cdots | A_{|L|})$, $T = \begin{bmatrix} T_1 & & \\ & \ddots & \\ & & T_{|L|} \end{bmatrix}$, T_i is the basis for $\Lambda_q^\perp(A_i)$, $i \in L$.
3. Encrypt(pp, W, μ): 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
$$c = \boldsymbol{u}^T \boldsymbol{f} + x_c + \left\lfloor \frac{q}{2} \right\rfloor \mu,$$

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

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

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

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

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

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

4. Decrypt(pp, C_W, sk_S, S): After receiving the cipthertext C_W from CSP, the DU computes $\boldsymbol{y} = \left(\boldsymbol{y}_1; \cdots; \boldsymbol{y}_{|L|}\right)$ by $\boldsymbol{y}_i = \begin{cases} \boldsymbol{c}_{i,1}, & i \in S \\ \boldsymbol{c}_{i,0}, & else \end{cases}$, and then outputs 0 if $\left(-\boldsymbol{s}^T|1\right)\left(\boldsymbol{y}^T; c\right) = c - \boldsymbol{y}^T\boldsymbol{s}$ 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 $\perp$, 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

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

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

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

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

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

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

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

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

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

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

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

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

3.2 Correctness and Parameters

We show the correctness and parameters in this subsection.

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

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

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

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

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

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

Then, we prove that Decrypt(pp, sk_{S^1}, C_{W^1})= μ, 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 $S^{1,+}, S^{1,-}$ are the positive and negative attribute set in W^1, $C_W = \left(c; \left\{\boldsymbol{c}_{i,0}, \boldsymbol{c}_{i,1}\right\}_{i\in L}\right)$ is a ciphertext under W, and $rk_{W\to W^1} = \left(\left\{Q_{i,0}, Q_{i,1}\right\}_{i\in L}\right)$ is a re-encryption key. Since the access structure W and W^1 are disjoint, we know that if $i \in S^{1,-}$, then

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

that is

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

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

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

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

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

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

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

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 $\boldsymbol{s}^1 \leftarrow \mathrm{SamplePre}\left(A^1, T^1, \boldsymbol{u}\right)$ such that $A^1\boldsymbol{s}^1 = \boldsymbol{u}$, where $T^1 = \begin{pmatrix} T_1 & & \\ & \ddots & \\ & & T_{|L|} \end{pmatrix}$ is the basis for $\Lambda^\perp_q\left(A^1\right)$. Since $S^1 \vDash W^1$, we know that $\boldsymbol{y}^1 = \left(\boldsymbol{y}^1_1; \cdots; \boldsymbol{y}^1_{|L|}\right) = {A^1}^T\boldsymbol{f} + \boldsymbol{x}^1$, where $\boldsymbol{x}^1 = \left(\boldsymbol{x}^1_1; \cdots; \boldsymbol{x}^1_{|L|}\right)$, $\boldsymbol{x}^1_i = \begin{cases} \boldsymbol{x}^2_{i,0}, & i \in L\backslash S^1 \\ \boldsymbol{x}^2_{i,1}, & i \in S^1 \end{cases}$. Thus,

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

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

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) Correctly decrypt the ciphertext requires $\left|x_c - \boldsymbol{s}^T \boldsymbol{x}\right| < \left\lfloor \frac{q}{2} \right\rfloor / 2$.
(4) Correctly decrypt the re-encrypted ciphertext requires $\left|x_c - \boldsymbol{s}^{1T} \boldsymbol{x}^1\right| < \left\lfloor \frac{q}{2} \right\rfloor / 2$.
(5) The hardness of LWE requires $\alpha q > 2\sqrt{n}$.

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

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

We only verify (4) that is $\left|x_c - \boldsymbol{s}^{1T} \boldsymbol{x}^1\right| < \left\lfloor \frac{q}{2} \right\rfloor / 2$. The others can be easily computed.

From the element of $\boldsymbol{x}^1$, we know

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

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

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

Thus,

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

3.3 Security

Theorem 2. *Let n, q, m, σ, α be as in the aforementioned. Then if LWE is hard, our CP-ABPRE scheme is IND-sAS-CPA secure at 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 follow,

- If $b = 0$, output $\boldsymbol{c} \leftarrow \mathbb{Z}_q^{1+2|L|m}$.
- 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 $\mathcal{O}_{\text{sk}}(S)$. 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 $\boldsymbol{s}_i^+ \leftarrow D_{\mathbb{Z}^m,\sigma}$, $i \in [|L|-1]$, computes $\boldsymbol{u}' = \boldsymbol{u} - \sum\limits_{i=1}^{|L|-1} A_i \boldsymbol{s}_i^+$, $\boldsymbol{s}_{|L|}^+ \leftarrow \text{SamplePre}\left(A_{|L|}, T_{|L|}, \boldsymbol{u}'\right)$ and outputs the secret key $\boldsymbol{s}^+ = \left(\boldsymbol{s}_1^+, \cdots, \boldsymbol{s}_{|L|}^+\right)$. The others are the same as *Game*$_0^b$.

Since the distribution of $\boldsymbol{s}^+$ is same as the real secret key $\boldsymbol{s}$, and $A\boldsymbol{s}^+ = \boldsymbol{u}$, we have $\boldsymbol{s}^+ \approx_s \boldsymbol{s}$. Thus, $\text{Game}_0^b \approx_s \text{Game}_1^b$.

Game$_2^b$: We modify the re-encryption key oracle $\mathcal{O}_{\text{rk}}(W, W')$. We replace $\text{P2}\left(R_{i,1\to 0}^T\right) + X_i$, $i \in S^{1,-}$, $\text{P2}\left(R_{{}_{i,0\to 1}}^T\right) + X_i$, $i \in S^{1,+}$, 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 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, $\text{Game}_0^b \approx_s \text{Game}_1^b$.

Game$_3^b$: We modify the re-encryption oracle $\mathcal{O}_{\text{re}}(rk_{S\to W'}, W', C_W)$. We replace $\boldsymbol{c}_{i,0}^1, \boldsymbol{c}_{i,1}^1$ with $\boldsymbol{c}_{i,0}^{1,+}, \boldsymbol{c}_{i,1}^{1,+} \leftarrow D_{\mathbb{Z}_q^m,\sigma}$, respectively, $i \in [|L|]$. The others are the same as *Game*$_2^b$.

Since $Q_{{}_{i,0}}^*, Q_{{}_{i,1}}^* \leftarrow D_{Z^{m \times m\lceil \log q \rceil},\sigma}$ and $\boldsymbol{x}_{{}_{i,0}}^1, \boldsymbol{x}_{{}_{i,1}}^1 \leftarrow D_{Z^m,\sigma}$, we have the distribution of $\boldsymbol{c}_{i,0}^1, \boldsymbol{c}_{i,1}^1$ and $\boldsymbol{c}_{i,0}^{1,+}, \boldsymbol{c}_{i,1}^{1,+}$ are same. Thus, $\boldsymbol{c}_{i,0}^{1,+} \approx_s \boldsymbol{c}_{i,0}^1$, $\boldsymbol{c}_{i,1}^{1,+} \approx_s \boldsymbol{c}_{i,1}^1$. Furthermore, $\text{Game}_3^b \approx_s \text{Game}_2^b$.

Game$_4^b$: we replace $\text{C}_{W^*} \leftarrow \text{Encrypt}(\text{pp}, \text{W}^*, \mu)$ with $\boldsymbol{c}^+ \leftarrow \mathbb{Z}_q^{1+2|L|m}$, where $\boldsymbol{c}^+ = \left(c^+; \left\{\boldsymbol{c}_{{}_{i,0}}^+, \boldsymbol{c}_{{}_{i,1}}^+\right\}_{i \in L}\right)$. The others are the same as *Game*$_3^b$.

We have $c^+ \approx_c c$, $\boldsymbol{c}_{{}_{i,1}}^+ \approx_c \boldsymbol{c}_{i,1}$,$i \in S^+ \cup L \backslash \left(S^+ \cup S^-\right)$, $\boldsymbol{c}_{{}_{i,0}}^+ \approx_c \boldsymbol{c}_{i,0}$, $i \in S^- \cup L \backslash \left(S^+ \cup S^-\right)$ under the LWE assumption and $\boldsymbol{c}_{{}_{i,1}}^+ \approx_s \boldsymbol{c}_{i,1}$, $i \in S^-$, $\boldsymbol{c}_{{}_{i,0}}^+ \approx_s \boldsymbol{c}_{i,0}$, $i \in S^+$. Thus $\text{C}_{W^*} \approx_c \boldsymbol{c}^+$. Furthermore, $\text{Game}_3^b \approx_c \text{Game}_4^b$.

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

Theorem 3. *Let n, q, m, σ, α be as in the aforementioned. Then if LWE is hard, our CP-ABPRE scheme is IND-sAS-CPA secure at re-encrypted ciphertext.*

Proof. For $(W^*, state_1) \leftarrow \mathcal{A}(1^\kappa)$, $(\mu, W, state_2) \leftarrow \mathcal{A}^{\mathcal{O}_1}(pp, state_1)$ 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 $\text{C}_W \leftarrow \text{Encrypt}(\text{pp}, \text{W}, \mu)$ if $b = 1$. By the *Game*$_4^b$ of Theorem 2, we know that the adversary can't distinguish a random ciphertext C from the real ciphertext $\text{C}_W \leftarrow \text{Encrypt}(\text{pp}, \text{W}, \mu)$. For the re-encryption key $rk_{W\to W^*}$, the adversary can't distinguish the real $rk_{W\to W^*}$ from a random Gaussian distribution by the *Game*$_2^b$ of Theorem 2. Thus, the adversary can't obtain any useful things for winning the game. At last, the challenger outputs the challenge re-encrypted ciphertext $C_{W^*}^* \leftarrow ReEnc(rk_{S\to W^*}, C_W)$. By the LWE, we have $Q_{i,0}BD\left(\boldsymbol{c}_{i,1}\right)+\boldsymbol{x}_{i,0}^{1}$, $i \in S^{1,-} \cup \left(L\backslash\left(S^{1,+} \cup S^{1,-}\right)\right)$ and the random uniform distribution are computationally indistinguishable, $Q_{i,1}BD\left(\boldsymbol{c}_{i,0}\right)+\boldsymbol{x}_{i,1}^{1}$, $i \in S^{1,+} \cup \left(L\backslash\left(S^{1,+} \cup S^{1,-}\right)\right)$ and the random uniform distributions are computationally indistinguishable. Thus, the advantage $\mathrm{Adv}_{\mathrm{CP-ABPRE},\mathcal{A}}^{\mathrm{IND-sAS-CPA-Re}}(\kappa)$ of adversary is negligible.

3.4 Comparison

We compare the related works in this subsection.

(1) Our scheme was constructed based on [14]. Compared with the ABE scheme of [14,15], our scheme not only supports proxy re-encryption but also has smaller size of public parameters. The comparison results in Table 2. The S is a set of all attribute in access structure.

(2) The existing CP-ABPRE schemes are constructed by bilinear pairing [5,13,20], which are fragile when the post-quantum comes. Our CP-ABPRE was constructed based on LWE which is widely believed 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 in Table 3.

Table 2. Comparison for CP-ABE

Cryptosystem	The size of pp	The size of sk	The size of ciphertext
[14]	$(2\lvert L\rvert+1)\,n \times (2\lvert L\rvert+1)\,m+n$	$\lvert L\rvert m$	$(2\lvert L\rvert+1-\lvert S\rvert)m$
[15]	$(2\lvert L\rvert+1)\,n \times (2\lvert L\rvert+1)\,m+n$	$\lvert L\rvert m$	$1+(2\lvert L\rvert+1)m$
our scheme	$2\lvert L\rvert\,n \times 2\lvert L\rvert\,m+n$	$\lvert L\rvert m$	$1+2\lvert L\rvert m$

Table 3. Comparison for PRE

Cryptosystem	Interactivity	Directionality	Security	LWE assumption	Access control
[2]	NO	Unidirectional	CPA	YES	NO
[21]	YES	Bidirectional	CPA	YES	NO
[22]	NO	Unidirectional	CPA	YES	NO
[23]	NO	Unidirectional	CPA	YES	NO
Our scheme	NO	Unidirectional	CPA	YES	YES

4 Conclusion

This paper constructs a ciphertext-policy attribute-based proxy re-encryption over lattice. The lattice-based cryptography is an alternative to resist quantum computer attacks. The constructed scheme not only supports access control but also can convert the ciphertext C_W under access structure W to a ciphertext $C_{W'}$ under another access structure W' without decrypt the ciphertext C_W. Thus, the scheme is flexible for cloud sharing. At last, the scheme is proved secure under LWE assumption.

Acknowledgements. 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).

References

1. 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. **28**(6), 645–660 (2017)
2. Ma, C., Li, J., Ouyang, W.: A homomorphic proxy re-encryption from lattices. In: Chen, L., Han, J. (eds.) ProvSec 2016. LNCS, vol. 10005, pp. 353–372. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-47422-9_21
3. Chow, S.S.M., Weng, J., Yang, Y., Deng, R.H.: Efficient unidirectional proxy re-encryption. In: Bernstein, D.J., Lange, T. (eds.) AFRICACRYPT 2010. LNCS, vol. 6055, pp. 316–332. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-12678-9_19
4. Green, M., Ateniese, G.: Identity-based proxy re-encryption. In: Katz, J., Yung, M. (eds.) ACNS 2007. LNCS, vol. 4521, pp. 288–306. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-72738-5_19
5. Liang, K., Fang, L., Susilo, W., et al.: 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, INCoS 2013, Xi'an, China, October, pp. 55–559 (2013)
6. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005). https://doi.org/10.1007/11426639_27
7. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Wright, R., Vimercati, S. (eds.) Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, Virginia, USA, pp. 89–98 (2006)
8. Wang, D., Ma, C., Shi, L., Wang, Y.: On the security of an improved password authentication scheme based on ECC. In: Liu, B., Ma, M., Chang, J. (eds.) ICICA 2012. LNCS, vol. 7473, pp. 181–188. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34062-8_24
9. He, D., Wang, D., Wu, S.: Cryptanalysis and improvement of a password-based remote user authentication scheme without smart cards. Inf. Technol. Control **42**(2), 105–112 (2013)

10. Wang, D., Ma, C., Zhang, Q., et al.: Secure password-based remote user authentication scheme against smart card security breach. J. Netw. **8**(1), 148 (2013)
11. Liang, X., Cao, Z., Lin, H., Shao, J.: Attribute based proxy re-encryption with delegating capabilities. In: Safavi-Naini, R., Varadharajan, V. (eds.) proceedings of the 4th International Symposium on Information, Computer, and Communications Security, Sydney, Australia, pp. 276–286 (2009)
12. Luo, S., Hu, J., Chen, Z.: Ciphertext policy attribute-based proxy re-encryption. In: Soriano, M., Qing, S., López, J. (eds.) ICICS 2010. LNCS, vol. 6476, pp. 401–415. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-17650-0_28
13. Liang, K., Man, H., Liu, J., et al.: A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing. Futur. Gener. Comput. Syst. **52**, 95–108 (2015)
14. Zhang, J., Zhang, Z.: A ciphertext policy attribute-based encryption scheme without pairings. In: Wu, C.-K., Yung, M., Lin, D. (eds.) Inscrypt 2011. LNCS, vol. 7537, pp. 324–340. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34704-7_23
15. Zeng, F., Xu, C.: A novel model for lattice-based authorized searchable encryption with special keyword. Math. Probl. Eng. (2015). Article ID 314621 https://doi.org/10.1155/2015/314621
16. Micciancio, D., Peikert, C.: Trapdoors for lattices: simpler, tighter, faster, smaller. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 700–718. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_41
17. Alwen, J., Peikert, C.: generating shorter bases for hard random lattices. Theory Comput. Syst. **48**(3), 535–553 (2011)
18. Agrawal, S., Boneh, D., Boyen, X.: Efficient Lattice (H)IBE in the standard model. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 553–572. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_28
19. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: STOC, pp. 84C93. ACM (2005)
20. Zeng, P., Choo, K.: A new kind of conditional proxy re-encryption for secure cloud storage. IEEE Access. **6**, 70017–70024 (2018)
21. Xagawa, K.: Cryptography with Lattices. Ph.D. thesis. Department of Mathematical and Computing Sciences Tokyo Institute of Technology (2010)
22. Jiang, M., Hu, Y., Wang, B., et al.: Lattice-based multi-use unidirectional proxy re-encryption. Secur. Commun. Netw. **8**(18), 3796–3803 (2016)
23. Hou, J., Jiang, M., Guo, Y., Song, W.: Identity-based multi-bit proxy re-encryption over lattice in the standard model. In: Li, F., Takagi, T., Xu, C., Zhang, X. (eds.) FCS 2018. CCIS, vol. 879, pp. 110–118. Springer, Singapore (2018). https://doi.org/10.1007/978-981-13-3095-7_9