Computing and Informatics, Vol. 37, 2018, 327–348, doi: 10.4149/cai_2018_2_327

FINE-GRAINED ACCESS CONTROL SYSTEMS SUITABLE FOR RESOURCE-CONSTRAINED USERS IN CLOUD COMPUTING

Yinghui Zhang*, Dong Zheng

National Engineering Laboratory for Wireless Security
Xi'an University of Posts and Telecommunications
Xi'an 710121, P.R. China
&
State Key Laboratory of Cryptology
P.O. Box 5159, Beijing 100878, P.R. China
e-mail: yhzhaang@163.com, zhengdong@xupt.edu.cn

Rui Guo, Qinglan Zhao

National Engineering Laboratory for Wireless Security
Xi'an University of Posts and Telecommunications
Xi'an 710121, P.R. China
e-mail: guorui@xupt.edu.cn, zhaoqinglan@foxmail.com

Abstract. For the sake of practicability of cloud computing, fine-grained data access is frequently required in the sense that users with different attributes should be granted different levels of access privileges. However, most of existing access control solutions are not suitable for resource-constrained users because of large computation costs, which linearly increase with the complexity of access policies. In this paper, we present an access control system based on ciphertext-policy attribute-based encryption. The proposed access control system enjoys constant computation cost and is proven secure in the random oracle model under the decision Bilinear Diffie-Hellman Exponent assumption. Our access control system supports AND-gate access policies with multiple values and wildcards, and it can efficiently support direct user revocation. Performance comparisons indicate that the proposed solution is suitable for resource-constrained environment.

* Corresponding author

Keywords: Attribute-based encryption, constant computation, access control, revocation, cloud computing

1 INTRODUCTION

Cloud computing is a promising computing paradigm in which vast and scalable resources are provided as services over the Internet. As the development of cloud computing, users' concerns about data security become main obstacles that impede cloud computing from wide adoptions. However, traditional access control technologies are no longer suitable for cloud computing environment because the service provider is fully trusted by users. In cloud computing, the data service manager is not trusted by users and is assumed to be honest-but-curious, that is, it will honestly execute the tasks assigned by legitimate participants in the system. Meanwhile, it would like to learn secret information as much as possible.

Attribute-based encryption (ABE) is known as an important tool for implementing secure and fine-grained access control over untrusted cloud storage. In an attribute-based system, access control over encrypted data is closely related to attributes, which are used to describe users in the system and define fine-grained access policies. There are two kinds of ABE constructions: key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In a KP-ABE scheme, the access policy is necessary for generation of attribute secret keys and ciphertexts are computed based on a set of attributes. In CP-ABE, access policies are used to generate ciphertexts and every secret key is corresponding to an attribute set. A user can successfully decrypt a ciphertext only if the attribute set associated with the user's secret key matches the access policy specified for the ciphertext by data owners.

Although promising in designing fine-grained access control system in cloud computing, efficiency challenges still remain there before ABE can be widely deployed in practical cloud platforms. Specifically, the computation cost of most existing ABE schemes linearly grows with the complexity of the access formula. The drawback appears more serious in resource-constrained scenarios such as wireless sensors and mobile phones. Moreover, an efficient revocation mechanism is necessary in secure and scalable ABE systems.

Aiming at tackling the challenges described above, we present a fine-grained data access control system in cloud computing, where CP-ABE serves as a fundamental building block. The proposed access control system enjoys small and constant computation cost and it can efficiently support direct user revocation. It is proved that the system is secure against adaptively chosen ciphertexts attacks (CCA2) in the random oracle model under the decision m-BDHE assumption, where m is an upper bound of the total number of users in the system. Particularly, our access control system enables AND-gate access policy with multiple attribute values and wildcards. Performance comparisons indicate that our solution is suitable for real-world application scenarios where users are resource-constrained.

2 RELATED WORK

The notion of ABE was introduced by Sahai and Waters [1] as a fuzzy identity-based encryption, and was firstly dealt with by Goyal et al. [2]. There are two complementary notions of ABE: KP-ABE and CP-ABE. The first KP-ABE construction [2] realized the monotonic access structure for key policies, while the first CP-ABE scheme supporting tree-based access structures in generic group models was proposed by Bethencourt et al. [3]. To achieve enhanced security, Cheung and Newport [4] presented a CP-ABE scheme supporting AND-gate policy with positive and negative attribute values and wildcards in the standard model.

However, most existing ABE schemes are inefficient because the computation overhead is linearly proportional to the complexity of access policies. In many real-world application scenarios, users often have constrained computing power [5, 6, 7, 8, 9, 10, 11] and cannot afford the computation cost of many previous ABE solutions. Therefore, computationally efficient ABE schemes [12, 13, 14] have received a lot of attention recently. Emura et al. [13] proposed a CP-ABE scheme, which only needs three exponentiation and two pairing operations in encryption and decryption phases, respectively. However, the scheme only supports AND-gate policies with multiple values without wildcards. If a decryptor's attributes are different from the access policy, he/she cannot decrypt corresponding ciphertexts. Similarly, the CP-ABE scheme [12] suffers the disadvantage [13] in that it supports AND-gate policies with single positive value without wildcards. Chen et al. [14] proposed two CP-ABE constructions, which support AND-gate policies with positive and negative attribute values and wildcards. Zhang et al. [15] proposed a CP-ABE scheme supporting AND-gate policies with multiple attribute values and wildcards. Very recently, Li et al. [16] have proposed a data deduplication technique suitable for cloud storage. As a promising technique, data deduplication has been widely adopted in cloud storage to save storage resources and bandwidth. There are also many other ABE constructions, such as multi-authority ABE [17, 18], outsourced ABE [19, 20, 21], anonymous ABE [22, 23, 24, 25], and traceable ABE [26, 27, 28], etc. In the multi-authority ABE scheme [17], any polynomial number of attribute authorities are allowed to control attributes and issue attribute secret keys. It is worth noting that these authorities are mutually independent. A data owner can encrypt his/her data so as to a user can decrypt the corresponding ciphertext only if he/she has particular attributes controlled by an attribute authority. Certainly, multi-authority ABE schemes must resist the collusion attacks of multiple malicious attribute authorities. In outsourced ABE schemes, intensive computing tasks during encryption and decryption phases are outsourced to cloud servers without revealing any private data or secret keys. Outsourced ABE has wide applications considering the mobile cloud computing environment. It enables resource-constrained users to complete heavy computation tasks with the help of cloud servers. Different from traditional ABE schemes, outsourced ABE has to introduce corresponding outsourcing servers. In the outsourced ABE scheme [20], secure outsourced decryption and key distribution are realized. In anonymous ABE schemes, access policies informa-

tion is not revealed in ciphertexts. Therefore, any people cannot learn of policy information from ciphertexts, and even legitimate decryptors fail to guess what access policies are adopted by encryptors. Anonymous ABE can realize users' privacy protection and hence it has a wide range of applications. Particularly, in the anonymous ABE scheme [25], a novel technique called match-then-decrypt is proposed, in which a matching phase is additionally introduced before the anonymous decryption phase. The match-then-decrypt technique can significantly improve the efficiency in decryption phase of anonymous ABE. ABE with attribute hierarchies further realize the expressiveness of access policies.

Furthermore, efficient revocation mechanisms are indispensable for ABE schemes in that some secret keys might get compromised at some point. Yu et al. [29] proposed a CP-ABE scheme supporting immediate attribute revocation mechanism with the help of a semi-trusted proxy server. Yang et al. [30] proposed an attribute revocation method to cope with the dynamic changes of users' access privileges. However, all the above ABE schemes only support indirect revocation, that is, the attribute authority indirectly enables revocation by forcing revoked users to be unable to update their secret keys. Direct revocation enjoys a desirable property that revocation can be done without affecting any non-involved users. Attrapadung et al. [31] suggested two directly user-revocable CP-ABE schemes by combining the techniques of ABE and broadcast encryption (BE). Since Fiat et al. [32] first introduced the notion of BE, Boneh et al. [33] proposed a collusion resistant BE scheme, which features short ciphertexts and private keys and is adopted in our construction to realize direct user revocation. There are many other researches on revocation, offline computation and policy update [34, 35, 36]. However, the computation cost of the above schemes linearly increases with the complexity of access structures and the number of revoked users.

3 PRELIMINARIES

3.1 Cryptographic Background

Definition 1 (Bilinear pairing)**.** Let $\mathbb{G}$ be a cyclic multiplicative group of a prime order p, $g \in_R \mathbb{G}$ be a generator, and $\mathbb{G}_T$ be a cyclic multiplicative group of the same order, identity of which we denote as 1. We call $\hat{e}$ a bilinear pairing if $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a map with the following properties:

1. Bilinear: $\hat{e}(g^a, g^b) = \hat{e}(g, g)^{ab}$ for all $a, b \in \mathbb{Z}_p^*$.
2. Non-degenerate: There exists $g_1, g_2 \in \mathbb{G}$ such that $\hat{e}(g_1, g_2) \neq 1$.
3. Computable: $\hat{e}(g_1, g_2)$ can be efficiently computed for all $g_1, g_2 \in \mathbb{G}$.

Definition 2 (Decision (t, ϵ, ℓ)-BDHE assumption)**.** Security of our construction is based on a complexity assumption called the Bilinear Diffie-Hellman Exponent assumption (BDHE). Let $\mathbb{G}$ be a bilinear group of prime order p, and g, h two independent generators of $\mathbb{G}$. Denote $\overrightarrow{y}_{g,\alpha,\ell} = (g_1, g_2, \cdots, g_\ell, g_{\ell+2}, \cdots, g_{2\ell}) \in \mathbb{G}^{2\ell-1}$,

where $g_i = g^{(\alpha^i)}$ for some unknown $\alpha \in \mathbb{Z}_p^*$. An algorithm $\mathcal{B}$ that outputs $\mu \in \{0,1\}$ has advantage ϵ in solving the decision ℓ-BDHE problem if

$$|\Pr[\mathcal{B}(g, h, \overrightarrow{y}_{g,\alpha,\ell}, \hat{e}(g_{\ell+1}, h)) = 1] - \Pr[\mathcal{B}(g, h, \overrightarrow{y}_{g,\alpha,\ell}, Z) = 1]| \geq \epsilon.$$

We say that the decision (t, ϵ, ℓ)-BDHE assumption holds in $\mathbb{G}$ if no t-time algorithm has advantage at least ϵ in solving the decision ℓ-BDHE problem in $\mathbb{G}$.

3.2 Access Policy

Usually, notation $L \models W$ is used to represent the fact that the attribute list L satisfies the access policy W, and the case of L does not satisfy W is denoted by $L \not\models W$. In our construction, we consider AND-gate policy supporting multiple attribute values and wildcards, which is a generalization of the access policy in [4] and is also adopted in [23]. Formally, given an attribute list $L = [L_1, L_2, \cdots, L_n]$ and an access policy $W = [W_1, W_2, \cdots, W_n] = \bigwedge_{i \in \mathcal{I}_W} W_i$, where $\mathcal{I}_W$ is a subscript index set and $\mathcal{I}_W = \{i | 1 \leq i \leq n, W_i \neq *\}$, we say $L \models W$ if $L_i = W_i$ or $W_i = *$ for all $1 \leq i \leq n$ and $L \not\models W$ otherwise. Note that the wildcard $*$ in W plays the role of "do not care" value.

4 SYSTEM ARCHITECTURE AND ADVERSARY MODEL

4.1 System Architecture

As shown in Figure 1, the system architecture of access control in cloud computing consists of four entities AA (Attribute Authority), CSP (Cloud Service Provider), DO (Data Owner), and DU (Data User).

AA is an entity who generates public parameters and master secret keys for the system. It is in charge of issuing attribute secret keys for users. It is fully trusted by all entities joining the system.

CSP is an entity that hosts the encrypted files of DO. It consists of cloud storage servers and a data service manager. Encrypted files from data owners are stored in cloud storage servers. The data service manager is in charge of controlling the accesses from outside users to the encrypted files.

DO is an entity who owns files, and wishes to upload them to the cloud storage servers provided by CSP. It is responsible for defining attribute-based access policy, and enforcing it on its own files by encrypting the files under the access policy before uploading them.

DU is an entity who intends to access the encrypted files hosted in the cloud storage servers. If DU is not revoked and his/her attributes match the underlying access policy in the encrypted files specified by DO, then he/she will succeed in decrypting the encrypted files.

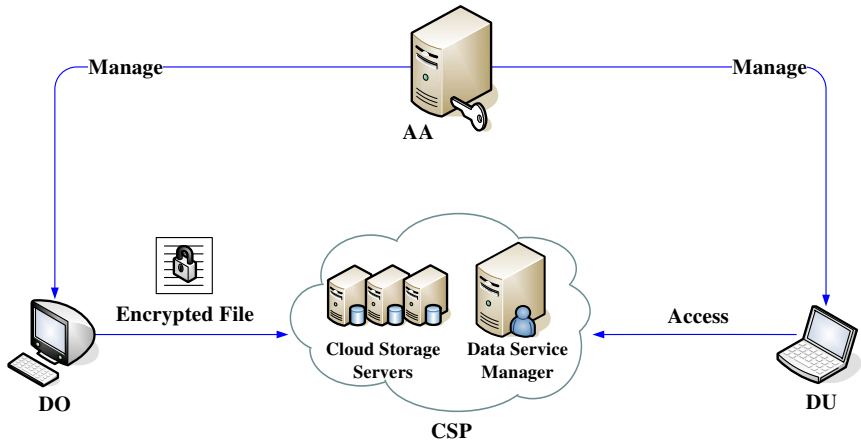


Figure 1. System architecture of access control in cloud computing

We give an overview of access control in cloud computing.

System Setup. AA generates public parameters and master secret keys for the system, and keeps master secret keys secretly.

User Registration. When a user wants to join the system, AA issues attribute secret keys to him/her based on his/her attributes.

New File Creation. When DO wants to share a file with some users, he/she encrypts the file under a specific access policy and uploads the resulted ciphertext to CSP.

File Access. When DU wants to access an outsourced file, he/she downloads the ciphertext from CSP and decrypts it.

4.2 Adversary Model and Security Goals

Similar to the previous systems, CSP is assumed to be honest-but-curious. In our system, the adversary is modeled as users colluding with CSP. The security goal is semantic security of data and it is reflected in the following three security requirements.

Data Confidentiality. Unauthorized DU who does not have enough attributes matching the access policy specified for a ciphertext by DO should be prevented from accessing the plaintext of the files. In addition, unauthorized access from CSP to the plaintext of the encrypted files should also be prevented.

Collusion-Resistance. If multiple DU and CSP collude, they may be able to access the plaintext of an encrypted file by combining attributes even if each of them cannot decrypt encrypted files alone. In practical attribute-based data

sharing systems, these colluders should not succeed in decrypting encrypted files.

Revocation. Any user involved in a revocation event fails to access the plaintext of subsequent ciphertexts exchanged after he/she is revoked from the system.

5 BUILDING BLOCK CP-ABE

5.1 Definition of CP-ABE

A CP-ABE scheme consists of the following four algorithms:

Setup$(1^\lambda) \rightarrow (PK, MK)$**:** On input a security parameter λ, it returns the system public key PK which is distributed to DO and DU, and the master key MK which is kept private.

KeyGen$(PK, MK, L) \rightarrow SK_L$**:** On input the system public key PK, the master key MK and an attribute list L, it outputs SK_L as the attribute secret key associated with L.

Encrypt$(PK, M, W, \mathcal{R}) \rightarrow CT_W$**:** On input the system public key PK, a message M, an access policy W specified by DO and a revocation set $\mathcal{R}$ issued by AA, it generates a ciphertext CT_W as the encryption of M with respect to W and $\mathcal{R}$, which is outsourced to CSP. Note that $\mathcal{R}$ specifies the users who are revoked from the system.

Decrypt$(PK, CT_W, SK_L) \rightarrow M$ **or** $\perp$**:** On input the system public key PK, a ciphertext CT_W of a message M under W and $\mathcal{R}$, and a secret key SK_L associated with L, it outputs the message M if the user is not revoked and $L \models W$, and the error symbol $\perp$ otherwise.

5.2 Formalized Security Models for CP-ABE

In the proof of our construction, we adopt a security model called indistinguishability against selective ciphertext-policy and adaptively chosen-ciphertext attacks (IND-sCP-CCA2), which is demonstrated in the following IND-sCP-CCA2 game.

Init: The adversary $\mathcal{A}$ commits to a challenge ciphertext policy W^* and a revocation information set $\mathcal{R}^*$.

Setup: The challenger $\mathcal{S}$ chooses a sufficiently large security parameter λ, and runs the Setup algorithm to get a master key SK and the corresponding system public key PK. It retains SK and gives PK to $\mathcal{A}$.

Phase 1: In addition to hash queries, $\mathcal{A}$ issues a polynomially bounded number of queries to the following oracles:

- **KeyGen Oracle** $\mathcal{O}_{KeyGen}$: $\mathcal{A}$ submits an attribute list L, if $L \not\models W^*$, $\mathcal{S}$ gives $\mathcal{A}$ the secret key SK_L and outputs $\perp$ otherwise.

- **Decrypt Oracle** $\mathcal{O}_{Dec}$: $\mathcal{A}$ submits a ciphertext CT_W of a message M. If CT_W is well-formed, $\mathcal{S}$ returns the message M. Otherwise, $\perp$ is returned.

Challenge: Once $\mathcal{A}$ decides that **Phase 1** is over, it outputs two equal length messages M_0 and M_1 from the message space, on which it wishes to be challenged with respect to W^* and $\mathcal{R}^*$. The challenger $\mathcal{S}$ randomly chooses a bit $b \in \{0,1\}$, computes $CT_{W^*} = \mathsf{Encrypt}(PK, M_b, W^*, \mathcal{R}^*)$ and sends CT_{W^*} to $\mathcal{A}$.

Phase 2: The same as **Phase 1**, except that CT_{W^*} may not be submitted for oracle $\mathcal{O}_{Dec}$.

Guess: $\mathcal{A}$ outputs a guess bit $b' \in \{0,1\}$ and wins the game if $b' = b$. The advantage of $\mathcal{A}$ in the IND-sCP-CCA2 game is defined as follows:

$$\mathrm{Adv}_{\mathrm{CP-ABE}}^{\mathrm{IND-sCP-CCA2}}(\mathcal{A}) = \left| \Pr[b' = b] - \frac{1}{2} \right|.$$

Definition 3. A CP-ABE scheme is said to be IND-sCP-CCA2 secure if no probabilistic polynomial-time adversary can break the IND-sCP-CCA2 game with non-negligible advantage.

6 PROPOSED ACCESS CONTROL SYSTEM

6.1 Main Idea

In the proposed scheme, the decryption cost is constant and it does not linearly increase with the complexity of access policies. The scheme can support AND-gate access policies with multiple values and wildcards and it is IND-sCP-CCA2 secure. In order to realize constant decryption cost, we use the idea of ciphertext aggregation. That is, in the new file creation phase, DO generates ciphertext components by aggregating the system public key components which are specified by the attribute values in access policies. To allow authorized DU to decrypt ciphertexts, in the user registration phase, AA generates attribute secret key components for attribute values appeared in the attribute list of DU. In the file access phase, to successfully decrypt a ciphertext, DU just uses some attribute secret key components in his/her secret key which are specified by values of the access policy. In order to efficiently support AND-gate access policies with multiple values and wildcards, AA only chooses three master secret key components in the system setup phase. Then, for each attribute value, a system public key component is generated by binding the attribute index with a master secret key component based on hash functions. For the sake of CCA2 security, the last ciphertext component is generated from the first three ciphertext components based on a random factor and system public key components. Based on the bilinear pairing, the last ciphertext component helps to answer decryption queries in security proof.

6.2 Our Scheme

In this section, we present an access control system. Let $\mathbb{G}$ and $\mathbb{G}_T$ be two cyclic multiplicative groups of a prime order p. Also, let g be a generator of $\mathbb{G}$ and $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ be a bilinear map. Suppose the attribute set of the system is $\mathcal{U} = \{\omega_1, \omega_2, \cdots, \omega_n\}$. Attribute ω_i has n_i values and $S_i = \{v_{i,1}, v_{i,2}, \cdots, v_{i,n_i}\}$ is the multi-value set. Define collision-resistant hash functions $H_0 : \mathbb{Z}_p^* \times \{0,1\}^* \to \mathbb{Z}_p^*$, $H_1 : \mathbb{Z}_p^* \to \mathbb{G}$, and $\hat{H} : \{0,1\}^* \times \mathbb{G}_T \times \mathbb{G}^2 \to \mathbb{Z}_p^*$. The system is described as follows.

System Setup. AA chooses a security parameter λ and runs the following algorithm Setup of CP-ABE to generate a public parameter PK and a master secret key MK for the system. Then AA publishes PK and keeps MK secretly.

- Setup(1^λ): AA chooses $x, y \in_R \mathbb{Z}_p^*$, and computes $X_{i,k_i} = g^{-H_0(x||i||k_i)}$, $Y_{i,k_i} = \hat{e}(g,g)^{H_0(y||i||k_i)}$ for $1 \le i \le n$ and $1 \le k_i \le n_i$. It also chooses $\alpha, \beta \in_R \mathbb{Z}_p^*$ and sets $v = g^\beta$. Suppose the total number of users in the system is bounded above by some natural number m. For notational simplicity, we let $\mathcal{I}_m = \{1, 2, \cdots, m\}$ in the following. For $1 \le i \le 2m$ and $i \ne m+1$, AA computes $g_i = g^{(\alpha^i)}$. In addition, AA chooses $\delta_1, \delta_2, \delta_3 \in \mathbb{G}$. Finally, the system public key is published by AA as

$$PK = \langle g, \{X_{i,k_i}, Y_{i,k_i}\}_{1 \le i \le n, 1 \le k_i \le n_i}, \{g_i\}_{1 \le i \le 2m, i \ne m+1}, v, \delta_1, \delta_2, \delta_3 \rangle,$$

  and the master key is $MK = \langle x, y, \beta \rangle$.

User Registration. When a user with an attribute list L wants to join the system, AA runs the following algorithm KeyGen of CP-ABE to obtain an attribute secret key SK_L and gives it to the user.

- KeyGen(PK, MK, L): AA chooses $sk \in_R \mathbb{Z}_p^*$ for the user. Then for $1 \le i \le n$, suppose $L_i = v_{i,k_i}$, AA computes

$$\overline{\sigma}_i = \sigma_{i,k_i} = g^{H_0(y||i||k_i)} H_1(sk)^{H_0(x||i||k_i)}.$$

  Also, AA computes $d = g_{sn}^\beta$, where $sn \in \{1, 2, \cdots, m\}$ is a serial number and it is used by AA to indicate that the current user is the sn^{th} one to join the system. Finally, the corresponding attribute secret key is $SK_L = \langle sn, sk, \{\overline{\sigma}_i\}_{1 \le i \le n}, d \rangle$.

New File Creation. Whenever DO wants to upload a file $\mathcal{F}$ to CSP, he/she chooses a symmetric key K and encrypts $\mathcal{F}$ with K based on a typical symmetric encryption scheme such as AES to obtain a ciphertext CT_0. Then DO defines a ciphertext policy W for $\mathcal{F}$, and runs the following algorithm Encrypt of CP-ABE to encrypt K to get a ciphertext CT_W. Finally, DO sets $CT_\mathcal{F} = \{CT_0, CT_W\}$ and uploads $CT_\mathcal{F}$ to CSP.

- $\mathsf{Encrypt}(PK, M, W, \mathcal{R})$: Suppose $W_i = v_{i,k_i}$, in order to encrypt a message $M = K$ under a ciphertext policy $W = \bigwedge_{i \in \mathcal{I}_W} W_i$ such that the revoked users specified by $\mathcal{R}$ cannot access it, DO computes

$$\langle X_W, Y_W \rangle = \left\langle \prod_{i \in \mathcal{I}_W} \overline{X}_i, \prod_{i \in \mathcal{I}_W} \overline{Y}_i \right\rangle,$$

where $\langle \overline{X}_i, \overline{Y}_i \rangle = \langle X_{i,k_i}, Y_{i,k_i} \rangle$. Then, DO chooses $s, \hat{s} \in_R \mathbb{Z}_p^*$, computes $K_{\mathcal{R}} = \hat{e}(g_1, g_m)^s$ and $C_{\mathcal{R}} = \left(v \cdot \prod_{i \in \mathcal{I}_m - \mathcal{R}} g_{m+1-i}\right)^s$. It also computes $C_0 = M Y_W^s K_{\mathcal{R}}$, $C_1 = g^s$, $C_2 = X_W^s$, $\hat{h} = \hat{H}(W||C_0||C_1||C_2)$, and $C_3 = (\delta_1^{\hat{h}} \delta_2^{\hat{s}} \delta_3)^s$. Finally, DO sets $CT_W = \langle C_0, C_1, C_2, C_3, C_{\mathcal{R}}, \hat{s} \rangle$. Note that the ciphertext policy W and revocation information $\mathcal{R}$ are implicitly included in ciphertexts.

File Access. Whenever DU with an attribute secret key SK_L wants to access and retrieve an outsourced file, he/she firstly downloads the ciphertext $CT_{\mathcal{F}} = \{CT_0, CT_W\}$ from CSP. Then DU computes $K = \mathsf{Decrypt}(PK, CT_W, SK_L)$ by running the following $\mathsf{Decrypt}$ algorithm, and then retrieves the file $\mathcal{F}$ by symmetric decryption based on K. It is worth noting that DU can successfully recover $\mathcal{F}$ if and only if $L \models W$ and he/she is not revoked.

- $\mathsf{Decrypt}(PK, CT_W, SK_L)$: Suppose $CT_W = \langle C_0, C_1, C_2, C_3, C_{\mathcal{R}}, \hat{s} \rangle$ corresponding to W and $\mathcal{R}$, and $W = \bigwedge_{i \in \mathcal{I}_W} W_i$ with $W_i = v_{i,k_i}$. Then CT_W is decrypted by DU with an attribute secret key $SK_L = \langle sn, sk, \{\overline{\sigma}_i\}_{1 \le i \le n}, d \rangle$ as follows. DU first checks whether $L \models W$ and $sn \notin \mathcal{R}$. If not, the decryption algorithm returns $\perp$. Otherwise, DU checks whether $\hat{e}(g, C_3) = \hat{e}(C_1, \delta_1^{\hat{h}} \delta_2^{\hat{s}} \delta_3)$ and $\hat{e}(g, C_2) = \hat{e}(C_1, X_W)$ or not, where $\hat{h} = \hat{H}(W||C_0||C_1||C_2)$ and $X_W = \prod_{i \in \mathcal{I}_W} X_{i,k_i}$. If one of the two equations does not hold, return $\perp$. Otherwise, DU computes $\sigma_W = \prod_{i \in \mathcal{I}_W} \overline{\sigma}_i$ and

$$K_{\mathcal{R}} = \frac{\hat{e}\left(g_{sn}, C_{\mathcal{R}}\right)}{\hat{e}\left(d \cdot \prod_{i \in \mathcal{I}_m - \mathcal{R}}^{i \neq sn} g_{m+1-i+sn}, C_1\right)}.$$

Finally, the message is recovered as $M = K = \frac{C_0}{\hat{e}(\sigma_W, C_1)\hat{e}(H_1(sk), C_2) K_{\mathcal{R}}}$.

The process of outsourcing and access is shown in Figure 2.

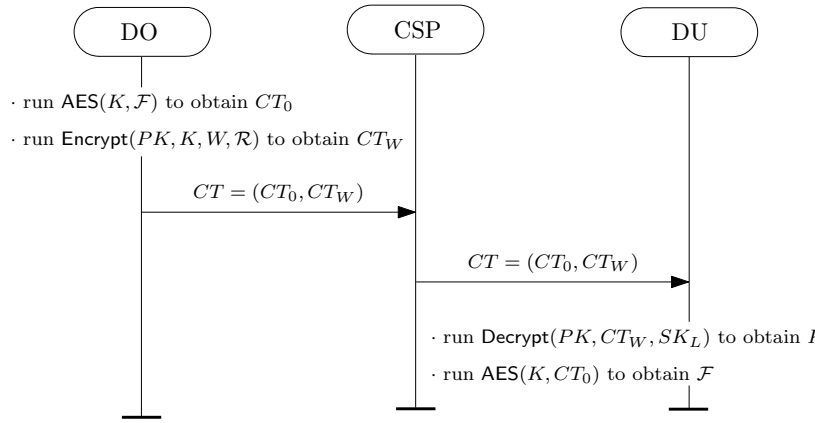


Figure 2. The process of outsourcing and access

7 ANALYSIS OF OUR ACCESS CONTROL SYSTEM

7.1 Correctness

If $L \models W$ and the user associated with sn is not revoked, the ciphertext can be successfully decrypted. Notice that $v = g^{\beta}$ and $d = g_{sn}^{\beta}$, we have

$$K_{\mathcal{R}} = \frac{\hat{e}\left(g_{sn}, C_{\mathcal{R}}\right)}{\hat{e}\left(d \cdot \prod_{i \in \mathcal{I}_m - \mathcal{R}_W}^{i \neq sn} g_{m+1-i+sn}, C_1\right)} = \frac{\hat{e}\left(g_{sn}, \left(v \cdot \prod_{i \in \mathcal{I}_m - \mathcal{R}_W} g_{m+1-i}\right)^s\right)}{\hat{e}\left(g_{sn}^{\beta} \cdot \prod_{i \in \mathcal{I}_m - \mathcal{R}_W}^{i \neq sn} g_{m+1-i+sn}, g^s\right)}$$

$$= \frac{\hat{e}\left(g, g\right)^{s\alpha^{sn} \sum_{i \in \mathcal{I}_m - \mathcal{R}_W} \alpha^{m+1-i}}}{\hat{e}\left(g, g\right)^{s \sum_{i \in \mathcal{I}_m - \mathcal{R}_W}^{i \neq sn} \alpha^{m+1-i+sn}}} = \hat{e}(g, g)^{\alpha^{m+1} s} = \hat{e}(g_1, g_m)^s.$$

Suppose the indexes satisfy $L_i = v_{i,k_i}$, then

$$\frac{C_0}{\hat{e}(\sigma_W, C_1)\hat{e}(H_1(sk), C_2) K_{\mathcal{R}}} = \frac{M Y_W^s \hat{e}(g_1, g_m)^s}{\hat{e}\left(\sigma_W, g^s\right) \hat{e}\left(H_1(sk), X_W^s\right) K_{\mathcal{R}}}$$

$$= \frac{M(\prod_{i \in \mathcal{I}_W} \overline{Y}_i)^s}{\hat{e}\left(\prod_{i \in \mathcal{I}_W} \overline{\sigma}_i, g^s\right) \hat{e}\left(H_1(sk), \left(\prod_{i \in W} \overline{X}_i\right)^s\right)}$$

$$= \frac{M\left(\prod_{i \in \mathcal{I}_W} \hat{e}(g, g)^{H_0(y||i||k_i)}\right)^s}{\hat{e}\left(\prod_{i \in \mathcal{I}_W} g^{H_0(y||i||k_i)} H_1(sk)^{H_0(x||i||k_i)}, g^s\right) \hat{e}\left(H_1(sk), \left(\prod_{i \in \mathcal{I}_W} g^{-H_0(x||i||k_i)}\right)^s\right)}$$

$$= M.$$

7.2 Security Analysis

We only need to prove the building block CP-ABE scheme is semantically-secure, which is demonstrated in Theorem 1.

Theorem 1. Assume that $\mathcal{A}$ makes at most q_{H_1} queries to the random oracle H_1, at most q_K queries to the key generation oracle, and at most q_D queries to the decryption oracle. If the decision (τ, ϵ, m)-BDHE assumption holds in $\mathbb{G}$, then the proposed scheme is (τ', ϵ', m)-secure, where $\tau' = \tau + \mathcal{O}(q_{H_1} + mq_K + q_D + N)\tau_1 + \mathcal{O}(q_D + N)\tau_2 + \mathcal{O}(q_D)\tau_p$ with $N = \sum_{i=1}^{n} n_i$, and $\epsilon' = \epsilon - \frac{q_D}{p}$. Here, τ_1 and τ_2 denotes the time complexity to compute an exponentiation in $\mathbb{G}$ and $\mathbb{G}_T$, respectively. τ_p represents the time complexity of a pairing operation.

Proof. Suppose that there exists a τ-time adversary $\mathcal{A}$, which breaks the proposed scheme with $\mathrm{Adv}_{\mathrm{CP-ABE}}^{\mathrm{IND-sCP-CCA2}}(\mathcal{A}) \geq \epsilon$. We build a simulator $\mathcal{S}$ that has advantage ϵ in solving the decision m-BDHE problem in $\mathbb{G}$. $\mathcal{S}$ takes as input a random decision m-BDHE challenge $(g, h, \overrightarrow{y}_{g,\alpha,m}, Z)$, where $\overrightarrow{y}_{g,\alpha,m} = (g_1, g_2, \cdots, g_m, g_{m+2}, \cdots, g_{2m})$ and Z is either $\hat{e}(g_{m+1}, h)$ or a random element in $\mathbb{G}_T$. The simulator $\mathcal{S}$ plays the role of the challenger in the IND-sCP-CCA2 game, and interacts with $\mathcal{A}$ as follows.

Init. The simulator $\mathcal{S}$ receives a challenge access structure $W^* = \bigwedge_{i \in \mathcal{I}_{W^*}} W_i$ and a revocation information set $\mathcal{R}^*$ specified by the adversary $\mathcal{A}$, where $\mathcal{I}_{W^*} = \{i_1, i_2, \cdots, i_w\}$ with $\omega \leq n$ represents the attribute index set specified in W^*. During the game, $\mathcal{A}$ will consult $\mathcal{S}$ for answers to the random oracles H_0, H_1 and $\hat{H}$. Roughly speaking, these answers are randomly generated, but to maintain the consistency and to avoid collisions, $\mathcal{S}$ keeps three tables $\mathcal{L}_1$, $\mathcal{L}_2$ and $\hat{\mathcal{L}}$ to store the answers used.

Setup. $\mathcal{S}$ needs to generate a system public key PK. $\mathcal{S}$ firstly chooses $j^* \in_R \{1, 2, \cdots, w\}$ and $x, x', y, y' \in_R \mathbb{Z}_p^*$. Then, it does the following:

1. If $i_j \in \mathcal{I}_{W^*} - \{i_{j^*}\}$, suppose $W_{i_j} = v_{i_j, k_{i_j}}$, then $\mathcal{S}$ computes

$$\left(X_{i_j,k_{i_j}}, Y_{i_j,k_{i_j}}\right) = \left(g^{-H_0(x||i_j||k_{i_j})} g_{m+1-i_j}^{-1}, \hat{e}(g,g)^{H_0(y||i_j||k_{i_j})}\right).$$

   Also, for $k \neq k_{i_j}$, $\mathcal{S}$ computes

$$\left(X_{i_j,k}, Y_{i_j,k}\right) = \left(g^{-H_0(x'||i_j||k)}, \hat{e}(g,g)^{H_0(y'||i_j||k)}\right).$$

2. For i_{j^*}, suppose $W_{i_{j^*}} = v_{i_{j^*}, k_{i_{j^*}}}$, then $\mathcal{S}$ computes

$$\left(X_{i_{j^*},k_{i_{j^*}}}, Y_{i_{j^*},k_{i_{j^*}}}\right)$$

$$= \left(g^{-H_0(x||i_{j^*}||k_{i_{j^*}})} \prod_{t \in \mathcal{I}_{W^*} - \{i_{j^*}\}} g_{m+1-t}, \hat{e}(g,g)^{H_0(y||i_{j^*}||k_{i_{j^*}})} \hat{e}(g,g)^{\alpha^{m+1}}\right).$$

Also, for $k \neq k_{i_{j^*}}$, $\mathcal{S}$ computes

$$\left(X_{i_{j^*},k}, Y_{i_{j^*},k}\right) = \left(g^{-H_0(x'||i_{j^*}||k)}, \hat{e}(g,g)^{H_0(y'||i_{j^*}||k)}\right).$$

3. If $i_j \notin \mathcal{I}_{W^*}$, for $1 \leq k_{i_j} \leq n_{i_j}$, $\mathcal{S}$ computes

$$\left(X_{i_j,k_{i_j}}, Y_{i_j,k_{i_j}}\right) = \left(g^{-H_0(x||i_j||k_{i_j})}, \hat{e}(g,g)^{H_0(y||i_j||k_{i_j})}\right).$$

Furthermore, $\mathcal{S}$ chooses $\varphi_1, \varphi_2, \varphi_3, \phi_2, \phi_3 \in_R \mathbb{Z}_p^*$, and computes $\delta_1 = g_1 g^{\varphi_1}$, $\delta_2 = g_1^{\phi_2} g^{\varphi_2}$, $\delta_3 = g_1^{\phi_3} g^{\varphi_3}$. Note that $\delta_1, \delta_2, \delta_3$ are distributed randomly. Also, $\mathcal{S}$ chooses $\beta \in \mathbb{Z}_p^*$, and sets $v = g^{\beta}\left(\prod_{j \in U^*} g_{m+1-j}\right)^{-1}$, where $U^* \subseteq \mathcal{R}_{W^*}$ denotes the target set of involved users to be challenged by $\mathcal{A}$ when revocation events occur. Finally, $\mathcal{S}$ sends $PK = \langle g, \{X_{i,k_i}, Y_{i,k_i}\}_{1 \leq i \leq n, 1 \leq k_i \leq n_i}, \{g_i\}_{1 \leq i \leq 2m, i \neq m+1}, v, \delta_1, \delta_2, \delta_3 \rangle$ to $\mathcal{A}$.

Phase 1. The adversary $\mathcal{A}$ makes the following queries.

- **Hash Oracle** $\mathcal{O}_{H_0}$ and $\mathcal{O}_{\hat{H}}$ are answered in a trivial way.
- **Hash Oracle** $\mathcal{O}_{H_1}(sk)$: We consider there is not an item containing sk in $\mathcal{L}_1$. If sk corresponds to an attribute list L in the key generation oracle, $\mathcal{S}$ adds the entry $\langle sk, g_{i_j} g^z \rangle$ to $\mathcal{L}_1$ and returns $g_{i_j} g^z$, where $z \in_R \mathbb{Z}_p^*$ and i_j is associated with L and satisfies $L_{i_j} \notin W_{i_j}$. Otherwise, $\mathcal{S}$ randomly chooses $i_j \in_R \{1, 2, \cdots, n\}$, $z \in_R \mathbb{Z}_p^*$, adds the entry $\langle sk, g_{i_j} g^z \rangle$ to $\mathcal{L}_1$ and returns $g_{i_j} g^z$.
- **KeyGen Oracle** $\mathcal{O}_{KeyGen}(L)$: Suppose $\mathcal{A}$ summits an attribute list L in a secret key query. If $L \not\models W^*$, there must exist $i_j \in \mathcal{I}_{W^*}$ such that $L_{i_j} \notin W_{i_j}$. Without loss of generality, assume $L_{i_j} = v_{i_j,\widehat{k}_{i_j}}$ and $W_{i_j} = v_{i_j,k_{i_j}}$. $\mathcal{S}$ chooses $sk \in_R \mathbb{Z}_p^*$. Also, $\mathcal{S}$ computes $\overline{\sigma}_{i_j} = \sigma_{i_j,\widehat{k}_{i_j}} = g^{H_0(y'||i_j||\widehat{k}_{i_j})}(g_{i_j} g^z)^{H_0(x'||i_j||\widehat{k}_{i_j})}$. For $t \neq i_j$, $\mathcal{S}$ chooses $z \in_R \mathbb{Z}_p^*$ and computes $\overline{\sigma}_t$ as follows:

  Case 1. If $t \in \mathcal{I}_{W^*} - \{i_{j^*}\}$, suppose $L_t = v_{t,k_t}$, $\mathcal{S}$ computes

  $$\overline{\sigma}_t = \sigma_{t,k_t} = g^{H_0(y||t||k_t)}(g_{i_j})^{H_0(x||t||k_t)} g_{m+1-t+i_j}(\overline{X}_t)^{-z}.$$

  Case 2. If $t = i_{j^*}$, suppose $L_{i_{j^*}} = v_{i_{j^*},k_{i_{j^*}}}$, $\mathcal{S}$ computes $\overline{\sigma}_{i_{j^*}}$ as

  $$\begin{aligned}\overline{\sigma}_{i_{j^*}} &= \sigma_{i_{j^*},k_{i_{j^*}}} \\ &= g^{H_0(y||i_{j^*}||k_{i_{j^*}})}(g_{i_j})^{H_0(x||i_{j^*}||k_{i_{j^*}})}\left(\prod_{k \in \mathcal{I}_{W^*} - \{i_{j^*}, i_j\}} g^{-1}_{m+1-k+i_j}\right)(\overline{X}_{i_{j^*}})^{-z}.\end{aligned}$$

  Case 3. If $t \notin \mathcal{I}_{W^*}$, suppose $L_t = v_{t,k_t}$, $\mathcal{S}$ computes

  $$\overline{\sigma}_t = \sigma_{t,k_t} = g^{H_0(y||t||k_t)}(g_{i_j} g^z)^{H_0(x||t||k_t)}.$$

Subsequently, $\mathcal{S}$ computes $d = g_{sn}^{\beta} \prod_{j \in U^*} g_{m+1-j+sn}^{-1}$.

- **Decryption Oracle $\mathcal{O}_{Dec}(CT_W)$:** Suppose $\mathcal{A}$ summits $CT_W = \langle C_0, C_1, C_2, C_3, C_{\mathcal{R}}, \hat{s} \rangle$ where $W = \bigwedge_{i \in \mathcal{I}_W} W_i$ with $W_i = v_{i,k_i}$. $\mathcal{S}$ checks whether $\hat{e}(g, C_3) = \hat{e}(C_1, \delta_1^{\hat{h}} \delta_2^{\hat{s}} \delta_3)$ and $\hat{e}(g, C_2) = \hat{e}(C_1, X_W)$ or not, where $\hat{h} = \hat{H}(W || C_0 || C_1 || C_2)$, $X_W = \prod_{i \in \mathcal{I}_W} X_{i,k_i}$. If one of the two equations does not hold, return $\perp$. Furthermore, $\mathcal{S}$ checks if $\hat{h} + \hat{s}\phi_2 + \phi_3 = 0$ holds. If so, $\mathcal{S}$ aborts. Otherwise, $\mathcal{S}$ chooses $sn \in_R \{1, 2, \cdots, m\}$, sets $\gamma = \hat{h} + \hat{s}\phi_2 + \phi_3$, $\hat{C} = C_1^{\hat{h}\varphi_1 + \hat{s}\varphi_2 + \varphi_3}$, and returns

$$\frac{C_0}{\hat{e}\left(\left(\frac{C_3}{\hat{C}}\right)^{\gamma^{-1}}, g_m\right) \cdot \hat{e}(C_1, g)^{y_W} \cdot K_{\mathcal{R}}},$$

where $y_W = \sum_{j=1}^{w} H_0(y || i_j || k_{i_j})$, and

$$K_{\mathcal{R}} = \frac{\hat{e}\left(g_{sn}, C_{\mathcal{R}}\right)}{\hat{e}\left(g_{sn}^{\beta} \cdot \prod_{i \in \mathcal{I}_m - \mathcal{R}}^{i \neq sn} g_{m+1-i+sn}, C_1\right)}.$$

Challenge. $\mathcal{S}$ sets $x_{W^*} = \sum_{j=1}^{\omega} H_0(x || i_j || k_{i_j})$ and $y_{W^*} = \sum_{j=1}^{w} H_0(y || i_j || k_{i_j})$, and defines $\langle X_{W^*}, Y_{W^*} \rangle$ as follows:

$$\begin{cases} X_{W^*} & = \overline{X}_{i_{j^*}} \prod_{t \in \mathcal{I}_{W^*} - \{i_{j^*}\}} \overline{X}_t \\ & = \left(g^{-H_0(x || i_{j^*} || k_{i_{j^*}})} \prod_{t \in \mathcal{I}_{W^*} - \{i_{j^*}\}} g_{m+1-t}\right) \cdot \prod_{t \in \mathcal{I}_{W^*} - \{i_{j^*}\}} g^{-H_0(x || t || k_t)} g_{m+1-t}^{-1} \\ & = g^{-x_{W^*}}, \\ Y_{W^*} & = \overline{Y}_{i_{j^*}} \prod_{t \in \mathcal{I}_{W^*} - \{i_{j^*}\}} \overline{Y}_t \\ & = \hat{e}(g, g)^{H_0(y || i_{j^*} || k_{i_{j^*}})} \hat{e}(g, g)^{\alpha^{m+1}} \cdot \prod_{t \in \mathcal{I}_{W^*} - \{i_{j^*}\}} \hat{e}(g, g)^{H_0(y || t || k_t)} \\ & = \hat{e}(g, g)^{\sum_{j=1}^{w} H_0(y || i_j || k_{i_j}) + \alpha^{m+1}}. \end{cases}$$

Suppose $\mathcal{A}$ summits two messages M_0 and M_1 of equal length. $\mathcal{S}$ chooses $b \in_R \{0, 1\}$, and computes $C_0^* = M_b Z^2 \hat{e}(g, h)^{y_{W^*}}$, $C_1^* = h$, and $C_2^* = h^{-x_{W^*}}$. Then $\mathcal{S}$ sets $\hat{h}^* = \hat{H}(W^* || C_0^* || C_1^* || C_2^*)$, $\hat{s}^* = \frac{-(\hat{h}^* + \phi_3)}{\phi_2}$, and computes $C_3^* = h^{\hat{h}^* \varphi_1 + \hat{s}^* \varphi_2 + \varphi_3}$ and

$$\begin{aligned} C_{\mathcal{R}^*} = h^{\beta} &= \left(g^{\beta} \left(\prod_{j \in U^*} g_{m+1-j}\right)^{-1} \left(\prod_{j \in U^*} g_{m+1-j}\right)\right)^{s} \\ &= \left(v \cdot \prod_{j \in U^*} g_{m+1-j}\right)^{s}. \end{aligned}$$

It is noted that $CT_{W^*} = \langle C_0^*, C_1^*, C_2^*, C_3^*, C_{\mathcal{R}^*}, \hat{s}^* \rangle$ is a valid encryption of M_b whenever $Z = \hat{e}(g_{m+1}, h)$. On the other hand, when Z is a random element in $\mathbb{G}_T$, CT_{W^*} is independent of b in the adversary's view.

Phase 2. Similar to **Phase 1** with a restriction that $\mathcal{A}$ cannot query $\mathcal{O}_{Dec}(\cdot)$ on the challenge ciphertext CT_{W^*}.

Guess. $\mathcal{A}$ outputs a guess bit b' of b. If $b' = b$, $\mathcal{S}$ outputs 1 in the decision m-BDHE game to guess that $Z = \hat{e}(g_{m+1}, h)$. Otherwise, it outputs 0 to indicate that Z is a random element in $\mathbb{G}_T$. We note that $\mathcal{S}$ will abort in decryption queries if $\hat{h} + \hat{s}\phi_2 + \phi_3 = 0$ holds. However, since the values ϕ_2 and ϕ_3 are respectively hidden by blinding factors φ_2 and φ_3, $\mathcal{A}$ could not obtain any information on ϕ_2 and ϕ_3 from decryption queries, and hence the probability that $\hat{h} + \hat{s}\phi_2 + \phi_3 = 0$ occurs is at most $\frac{1}{p}$. Therefore, if $Z = \hat{e}(g_{m+1}, h)$, then CT_{W^*} is a valid ciphertext and we have

$$\begin{aligned}\Pr\left[\mathcal{S}(g, h, \overrightarrow{y}_{g,\alpha,m}, \hat{e}(g_{m+1}, h)) = 1\right] &= \frac{1}{2} + \mathrm{Adv}_{\mathrm{CP-ABE}}^{\mathrm{IND-sCP-CCA2}}(\mathcal{A}) - \frac{q_D}{p} \\ &\geq \frac{1}{2} + \epsilon - \frac{q_D}{p}.\end{aligned}$$

If Z is a random element in $\mathbb{G}_T$, the message M_b is completely hidden from $\mathcal{A}$, and we have $\Pr[\mathcal{S}(g, h, \overrightarrow{y}_{g,\alpha,m}, Z) = 1] = \frac{1}{2}$.

Therefore, the simulator $\mathcal{S}$ has at least a non-negligible advantage $\epsilon - \frac{q_D}{p}$ in solving the decision m-BDHE problem in $\mathbb{G}$ within time τ. It easily follows that the time complexity of $\mathcal{S}$ is

$$\tau' = \tau + \mathcal{O}\left(q_{H_1} + mq_K + q_D + \sum_{i=1}^{n} n_i\right)\tau_1 + \mathcal{O}\left(q_D + \sum_{i=1}^{n} n_i\right)\tau_2 + \mathcal{O}(q_D)\tau_p.$$

□

7.3 Performance Analysis

In this section, we analyze and compare the performance of the proposed scheme with the previous CP-ABE schemes from the aspects of security and efficiency. Table 1 shows the performance comparison in terms of the size of ciphertext (CT) and the system public key (PK) size, the computation overheads of encryption and decryption, the expressiveness of access policy, and the revocation mechanism. For simplicity, we use **e** and **p** to represent an exponentiation operation and a pairing operation, respectively. Let n be the total number of attributes in universe, s be the number of attributes the user has to hold in order to match the access policy, t be the number of attributes associated with the user's secret key, s_m and t_m be the maximum size allowed for s and t, m be the maximum number of users in the system, r be the number of revocation events, and N be the total number of attribute values

in the system. We denote the bit length of an element in a group $\mathbb{G}$ by $|\mathbb{G}|$. In addition, IAR and DUR respectively represent "Indirect Attribute Revocation" and "Direct User Revocation".

Schemes	Parameter Size		Computation Cost		Policy	Revocation
	CT	PK	Encryption	Decryption		
HSM [12]	$2\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$(n+4)\|\mathbb{G}\|$	3 **e**	2 **p**	Type 1[†]	×
EM [13]	$2\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$(N+2)\|\mathbb{G}\|+\|\mathbb{G}_T\|$	3 **e**	2 **p**	Type 2[‡]	×
CZF1 [14]	$2\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$2n\|\mathbb{G}\|+2n\|\mathbb{G}_T\|$	3 **e**	2 **p**	Type 3[§]	×
CZF2 [14]	$3\|\mathbb{G}\|+\|\mathbb{G}_T\|+\|\mathbb{Z}_p^*\|$	$(2n+3)\|\mathbb{G}\|+2n\|\mathbb{G}_T\|$	6 **e**	6 **p**+2 **e**	Type 3	×
YWR [29]	$(n+1)\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$(3n+1)\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$(s+2)$**e**	$(n+1)$**p**	Type 3	IAR
AI1 [31]	$(s+2)\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$(s_m+t_m+2m+1)\|\mathbb{G}\|$	$(2s+3)$ **e**+1 **p**	$(2s+m+1)$ **p**	Type 4[♯]	DUR
AI2 [31]	$(s+2r+1)\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$(s_m+t_m+7)\|\mathbb{G}_T\|$	$(2s+2r+2)$ **e**	$(2s+2r+1)$ **p**	Type 4	DUR
Ours	$4\|\mathbb{G}\|+\|\mathbb{G}_T\|+\|\mathbb{Z}_p^*\|$	$(N+2m+4)\|\mathbb{G}\|+N\|\mathbb{G}_T\|$	8 **e**	8 **p**+2 **e**	Type 5[¶]	DUR

[†] AND-gate policy supporting single positive value without wildcards.
[‡] AND-gate policy supporting multiple values without wildcards.
[§] AND-gate policy supporting positive and negative values with wildcards.
[♯] Access structures based on linear secret sharing.
[¶] AND-gate policy supporting multiple values with wildcards.

Table 1. Performance comparison of CP-ABE schemes

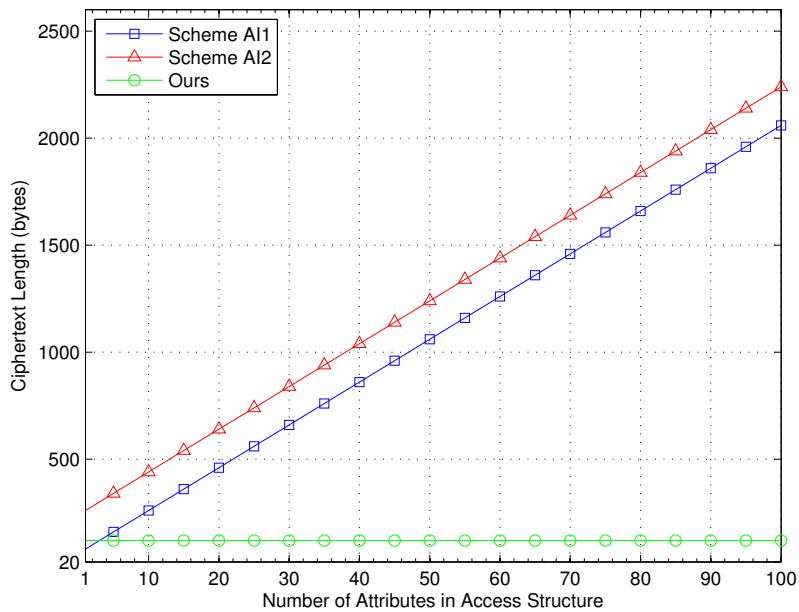


Figure 3. Comparison of ciphertext length

From Table 1, we know that the CP-ABE schemes [12, 13, 14] and the proposed scheme have small and constant computation cost. Although enjoying constant computation cost, the schemes [12, 13, 14] fail to support revocation mechanisms.

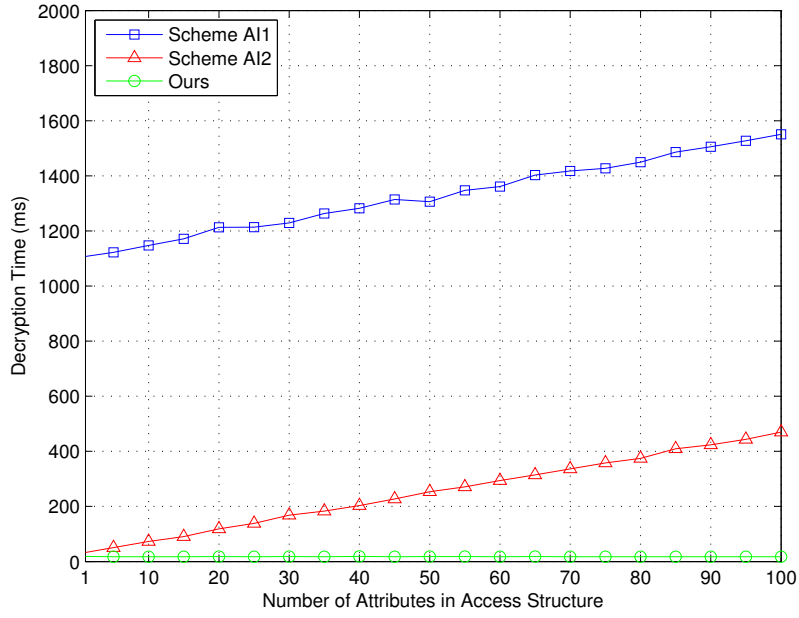


Figure 4. Comparison of decryption cost

Also, the access policies in [12] only support single attribute value. Furthermore, the scheme [29] supports indirect attribute revocation, and only the schemes [31] and the proposed scheme enjoy direct user revocation. However, the schemes [29, 31] suffer an efficiency drawback that the encryption and decryption cost is not constant in terms of the the number of $\mathbf{e}$ or $\mathbf{p}$.

Based on the above analysis, we further compare schemes in [31] denoted as AI1, AI2 and ours with respect to the ciphertext length in Figure 3. As for the ciphertext length comparison, we set $|\mathbb{G}_0| = |\mathbb{G}_T| = 160$ bits and the number of revocation events as $r = 5$. Note that the ciphertext length of the scheme AI2 is linearly proportional to r. Both the ciphertext length of AI1 and AI2 linearly increases with s. On the other hand, we do simulation experiments based on the Stanford Pairing-Based Crypto (PBC) library [37] and a Linux machine with 3.30 GHz $\times$ 8 Intel Xeon(R) E3-1230 CPU and 7.5 GB of RAM. The simulation results are shown in Figure 4. In the simulation, the maximum number of users in the system is set as $m = 500$. In order to precisely evaluate the decryption cost, a total of 100 distinct access policies are generated, where each attribute has a positive occurrence. For each access policy, the experiment is repeated for 30 times and the final result is an average value. It is noted that both the decryption cost of the scheme AI1 and AI2 linearly increases with the number of columns in access policies,

and the proposed scheme enjoys small and constant decryption cost. Generally, we argue that the proposed ABE scheme is more suitable for access control in cloud computing.

8 CONCLUSION

In this paper, we propose an efficient data access control system in cloud computing. The main building block is a new CP-ABE scheme, which enjoys constant computation cost and direct user revocation. The proposed access system is proven secure in the random oracle model, and it can efficiently support AND-policy with multiple attribute values and wildcards. Extensive performance comparisons indicate that the proposed solution is extremely suitable for resource-constrained applications.

Acknowledgements

We are grateful to the anonymous referees for their invaluable suggestions. This work is supported by National Key R & D Program of China (No. 2017YFB0802000), National Natural Science Foundation of China (No. 61772418, 61402366), Yinghui Zhang is supported by New Star Team of Xi'an University of Posts and Telecommunications.

REFERENCES

[1] Sahai, A.—Waters, B.: Fuzzy Identity-Based Encryption. In: Cramer, R. (Ed.): Advances in Cryptology – EUROCRYPT 2005. Springer, Lecture Notes in Computer Science, Vol. 3494, 2005, pp. 457–473, doi: 10.1007/11426639_27.

[2] Goyal, V.—Pandey, O.—Sahai, A.—Waters, B.: Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06), ACM, 2006, pp. 89–98, doi: 10.1145/1180405.1180418.

[3] Bethencourt, J.—Sahai, A.—Waters, B.: Ciphertext-Policy Attribute-Based Encryption. Proceedings of Symposium on Security and Privacy (SP '07), IEEE, 2007, pp. 321–334, doi: 10.1109/SP.2007.11.

[4] Cheung, L.—Newport, C.: Provably Secure Ciphertext Policy ABE. Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07), ACM, 2007, pp. 456–465, doi: 10.1145/1315245.1315302.

[5] Zhang, X.—Tan, Y.—Liang, C.—Li, Y.—Li, J.: A Covert Channel over VoLTE via Adjusting Silence Periods. IEEE Access, Vol. 6, 2018, pp. 9292–9302, doi: 10.1109/ACCESS.2018.2802783.

[6] Zhang, Y.—Zheng, D.—Chen, X.—Li, J.—Li, H.: Efficient Attribute-Based Data Sharing in Mobile Clouds. Pervasive and Mobile Computing, Vol. 28, 2016, pp. 135–149, doi: 10.1016/j.pmcj.2015.06.009.

[7] Lin, Q.—Yan, H.—Huang, Z.—Chen, W.—Shen, J.—Tang, Y.: An ID-Based Linearly Homomorphic Signature Scheme and Its Application in Blockchain. IEEE Access, 2018, online, doi: 10.1109/ACCESS.2018.2809426.

[8] Xu, J.—Wei, L.—Zhang, Y.—Wang, A.—Zhou, F.—Gao, C.: Dynamic Fully Homomorphic Encryption-Based Merkle Tree for Lightweight Streaming Authenticated Data Structures. Journal of Network and Computer Applications, Vol. 107, 2018, pp. 113–124, doi: 10.1016/j.jnca.2018.01.014.

[9] Liu, Z.—Huang, Y.—Li, J.—Cheng, X.—Shen, C.: DivORAM: Towards a Practical Oblivious RAM with Variable Block Size. Information Sciences, Vol. 447, 2018, pp. 1–11, doi: 10.1016/j.ins.2018.02.071.

[10] Xie, D.—Lai, X.—Lei, X.—Fan, L.: Cognitive Multiuser Energy Harvesting Decode-and-Forward Relaying System with Direct Links. IEEE Access, Vol. 6, 2018, pp. 5596–5606, doi: 10.1109/ACCESS.2017.2776953.

[11] Lin, Q.—Li, J.—Huang, Z.—Chen, W.—Shen, J.: A Short Linearly Homomorphic Proxy Signature Scheme. IEEE Access, Vol. 6, 2018, pp. 12966–12972, online, doi: 10.1109/ACCESS.2018.2809684.

[12] Han, J.—Susilo, W.—Mu, Y.—Yan, J.: Attribute-Based Oblivious Access Control. The Computer Journal, Vol. 55, 2012, No. 10, pp. 1202–1215, doi: 10.1093/comjnl/bxs061.

[13] Emura, K.—Miyaji, A.—Nomura, A.—Omote, K.—Soshi, M.: A Ciphertext-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length. Proceedings of International Conference on Information Security Practice and Experience (ISPEC '09). Springer, Lecture Notes in Computer Science, Vol. 5451, 2009, pp. 13–23, doi: 10.1007/978-3-642-00843-6_2.

[14] Chen, C.—Zhang, Z.—Feng, D.: Efficient Ciphertext Policy Attribute-Based Encryption with Constant-Size Ciphertext and Constant Computation-Cost. Proceedings of International Conference on Provable Security (ProvSec 2011). Springer, Lecture Notes in Computer Science, Vol. 6980, 2011, pp. 84–101, doi: 10.1007/978-3-642-24316-5_8.

[15] Zhang, Y.—Zheng, D.—Chen, X.—Li, J.—Li, H.: Computationally Efficient Ciphertext-Policy Attribute-Based Encryption with Constant-Size Ciphertexts. Proceedings of International Conference on Provable Security (ProvSec 2014). Springer, Lecture Notes in Computer Science, Vol. 8782, 2011, pp. 259–273, doi: 10.1007/978-3-319-12475-9_18.

[16] Li, J.—Chen, X.—Li, M.—Li, J.—Lee, P.—Lou, W.: Secure Deduplication with Efficient and Reliable Convergent Key Management. IEEE Transactions on Parallel and Distributed Systems, Vol. 25, 2014, No. 6, pp. 1615-1625, doi: 10.1109/TPDS.2013.284.

[17] Chase, M.: Multi-Authority Attribute Based Encryption. Proceedings of Theory of Cryptography Conference (TCC'07). Springer, Lecture Notes in Computer Science, Vol. 4392, 2007, pp. 515–534, doi: 10.1007/978-3-540-70936-7_28.

[18] Lewko, A.—Waters, B.: Decentralizing Attribute-Based Encryption. Advances in Cryptology – EUROCRYPT 2011. Springer, Lecture Notes in Computer Science, Vol. 6632, 2011, pp. 568–588, doi: 10.1007/978-3-642-20465-4_31.

[19] Green, M.—Hohenberger, S.—Waters, B.: Outsourcing the Decryption of ABE Ciphertexts. Proceedings of the 20th USENIX Conference on Security (SEC'11), USENIX Association, 2011, pp. 1–16, http://static.usenix.org/events/sec11/tech/full_papers/Green.pdf.

[20] Li, J.—Huang, X.—Li, J.—Chen, X.—Xiang, Y.: Securely Outsourcing Attribute-Based Encryption with Checkability. IEEE Transactions on Parallel and Distributed Systems, Vol. 25, 2014, No. 8, pp. 2201–2210, doi: 10.1109/TPDS.2013.271.

[21] Li, J.—Chen, X.—Li, J.—Jia, C.—Ma, J.—Lou, W.: Fine-Grained Access Control System Based on Outsourced Attribute-Based Encryption. Proceedings of European Symposium on Research in Computer Security (ESORICS'13). Springer, Lecture Notes in Computer Science, Vol. 8134, 2013, pp. 592–609, doi: 10.1007/978-3-642-40203-6_33.

[22] Katz, J.—Sahai, A.—Waters, B.: Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products. Advances in Cryptology – EUROCRYPT 2008. Springer, Lecture Notes in Computer Science, Vol. 4965, 2008, pp. 146–162, doi: 10.1007/978-3-540-78967-3_9.

[23] Nishide, T.—Yoneyama, K.—Ohta, K.: Attribute-Based Encryption with Partially Hidden Encryptor-Specified Access Structure. Proceedings of International Conference on Applied Cryptography and Network Security (ACNS 2008). Springer, Lecture Notes in Computer Science, Vol. 5037, 2008, pp. 111–129, doi: 10.1007/978-3-540-68914-0_7.

[24] Zhang, Y.—Chen, X.—Li, J.—Wong, D. S.—Li, H.—You, I.: Ensuring Attribute Privacy Protection and Fast Decryption for Outsourced Data Security in Mobile Cloud Computing. Information Sciences, Vol. 379, 2017, pp. 42–61, doi: 10.1016/j.ins.2016.04.015.

[25] Zhang, Y.—Chen, X.—Li, J.—Wong, D. S.—Li, H.: Anonymous Attribute-Based Encryption Supporting Efficient Decryption Test. Proceedings of 8th ACM SIGSAC Symposium on Information, Computer and Communications Security (ASIA CCS'13), ACM, 2013, pp. 511–516, doi: 10.1145/2484313.2484381.

[26] Zhang, Y.—Li, J.—Zheng, D.—Chen, X.—Li, H.: Towards Privacy Protection and Malicious Behavior Traceability in Smart Health. Personal and Ubiquitous Computing, Vol. 21, 2017, No. 5, pp. 815–830, doi: 10.1007/s00779-017-1047-8.

[27] Xhafa, F.—Feng, J.—Zhang, Y.—Chen, X.—Li, J.: Privacy-Aware Attribute-Based PHR Sharing with User Accountability in Cloud Computing. The Journal of Supercomputing, Vol. 71, 2015, No. 5, pp. 1607–1619, doi: 10.1007/s11227-014-1253-3.

[28] Zhang, Y.—Li, J.—Zheng, D.—Chen, X.—Li, H.: Accountable Large-Universe Attribute-Based Encryption Supporting Any Monotone Access Structures. Proceedings of Australasian Conference on Information Security and Privacy (ACISP 2016). Springer, Lecture Notes in Computer Science, Vol. 9722, 2016, pp. 509–524, doi: 10.1007/978-3-319-40253-6_31.

[29] Yu, S.—Wang, C.—Ren, K.—Lou, W.: Attribute Based Data Sharing with Attribute Revocation. Proceedings of the 5th ACM Symposium on Information, Com-

puter and Communications Security (ASIA CCS '10), ACM, 2010, pp. 261–270, doi: 10.1145/1755688.1755720.

[30] Yang, K.—Jia, X.—Ren, K.: Attribute-Based Fine-Grained Access Control with Efficient Revocation in Cloud Storage Systems. Proceedings of 8th ACM SIGSAC Symposium on Information, Computer and Communications Security (ASIA CCS '13), ACM, 2013, pp. 523–528, doi: 10.1145/2484313.2484383.

[31] Attrapadung, N.—Imai, H.: Conjunctive Broadcast and Attribute-Based Encryption. Proceedings of International Conference on Pairing-Based Cryptography (Pairing 2009). Springer, Lecture Notes in Computer Science, Vol. 5671, 2009, pp. 248–265, doi: 10.1007/978-3-642-03298-1_16.

[32] Fiat, A.—Naor, M.: Broadcast Encryption. Advances in Cryptology – CRYPTO 1993. Springer, Lecture Notes in Computer Science, Vol. 773, 1994, pp. 480–491, doi: 10.1007/3-540-48329-2_40.

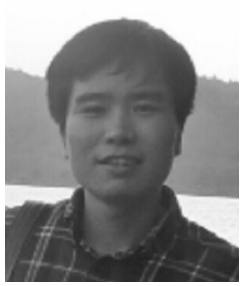
[33] Boneh, D.—Gentry, C.—Waters, B.: Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys. Advances in Cryptology – CRYPTO 2005. Springer, Lecture Notes in Computer Science, Vol. 3621, 2005, pp. 258–275, doi: 10.1007/11535218_16.

[34] Zhang, Y.—Chen, X.—Li, J.—Li, H.—Li, F.: FDR-ABE: Attribute-Based Encryption with Flexible and Direct Revocation. Proceedings of 2013 5th International Conference on Intelligent Networking and Collaborative Systems (INCoS '13), IEEE, 2013, pp. 38–45, doi: 10.1109/INCoS.2013.16.

[35] Li, J.—Zhang, Y.—Chen, X.—Xiang, Y.: Secure Attribute-Based Data Sharing for Resource-Limited Users in Cloud Computing. Computers and Security, Vol. 72, 2018, pp. 1–12, doi: 10.1016/j.cose.2017.08.007.

[36] Zhang, Y.—Li, J.—Chen, X.—Li, H.: Anonymous Attribute-Based Proxy Re-Encryption for Access Control in Cloud Computing. Security and Communication Networks, Vol. 9, 2016, No. 14, pp. 2397—2411, doi: 10.1002/sec.1509.

[37] Lynn, B.: The Stanford Pairing Based Crypto Library. `https://crypto.stanford.edu/pbc/`.



Yinghui Zhang received his Ph.D. degree in cryptography from the Xidian University, China, in 2013. He is Associate Professor at the National Engineering Laboratory for Wireless Security (NELWS), Xi'an University of Posts and Telecommunications. He has published over 50 research articles including ASIACCS, ACISP, IEEE CSE, computer networks, computers & security. His research interests include cloud security, public key cryptography and wireless network security.

Dong Zheng received his Ph.D. degree in communication engineering from the Xidian University, China, in 1999. He is currently Professor at the National Engineering Laboratory for Wireless Security (NELWS), Xi'an University of Posts and Telecommunications. He has published over 100 research articles including CT-RSA, IEEE Transactions on Industrial Electronics, etc. His research interests include cloud computing and public key cryptography.

Rui Guo received his Ph.D. degree from the Department of State Key Laboratory of Networking and Switch Technology, Beijing University of Posts and Telecommunications, China, in 2014. He is currently Lecturer at the National Engineering Laboratory for Wireless Security (NELWS), Xi'an University of Posts and Telecommunications. His present research interests include attribute-based cryptography, cloud computing and blockchain technology.

Qinglan Zhao received her B.Sc. degree from the Shaanxi Normal University, China, in 1999, and her M.Sc. degree from the Northwestern Polytechnical University, China, in 2006. She received her Ph.D. degree from the Shanghai Jiao Tong University, China, in 2017. Since 2014, she has been Associate Professor at the Xi'an University of Post and Telecommunications, China. Her research interests include cryptographic functions and information security.