Unidirectional Proxy Re-Encryption for Access Structure Transformation in Attribute-based Encryption Schemes

Xingbing Fu

School of Computer Science and Engineering, University of Electronic Science and Technology of China
No. 2006, Xiyuan Avenue, West Hi-tech Zone, Chengdu 611731, P. R. China
(Email: uestcfuxb@126.com)

(Received March 10, 2014; revised and accepted June 16, 2014)

Abstract

In Ciphertext Policy Attribute Based Encryption (CP-ABE) scheme, a user's private key is associated with a set of attributes, and the sensitive data are encrypted under an access structure over attributes, only if the users whose attributes satisfy the access structure associated with the ciphertext can decrypt the ciphertext data. However, a limitation of the existing CP-ABE schemes is that it does not support transforming access structure provided that the encrypted data are not decrypted. In this work, we proposed Ciphertext Policy Attribute Based Proxy Re-Encryption (CP-ABPRE) scheme which allows to transform access structure associated with the original ciphertext without decrypting it through an honest and curious proxy such as the cloud storage server that re-encrypts the original ciphertext under another access structure such that only if the users whose attributes satisfy the new access structure can decrypt the re-encrypted ciphertext. Security of the proposed scheme is based on the generic bilinear group model. Performance evaluation shows the proposed scheme is efficient.

Keywords: Access structure transformation, attribute based encryption, bilinear maps, proxy re-encryption, unidirectionality

1 Introduction

Traditional public key encryption scheme is to protect the confidentiality of the sensitive data. Encryption is viewed as a mechanism through which one user can share the sensitive data with another user. The scheme is very suitable for the setting where the data owner specifically knows with whom he wants to share the data in advance. However, in many applications such as cloud storage systems, the data owners may want to share data under some access policy over the target users' attributes or credentials to achieve fine-grained access control. Recent years, the proposed Attribute Based Encryption (ABE) schemes can meet the requirements very well. ABE has the two fundamental forms: Key Policy Attribute Based Encryption (KP-ABE) schemes and Ciphertext Policy Attribute Based Encryption (CP-ABE) schemes. In CP-ABE schemes, ciphertexts are associated with access policies, whereas user keys are associated with attribute sets. For example, in cloud storage systems, after the data owner encrypts the data employing CP-ABE scheme, he uploads the encrypted data to the cloud storage server which is semi-honest, such that any data consumers can download the ciphertext data, only if the data consumers whose attributes satisfy the access structures can decrypt the encrypted data. Neither the cloud server nor the unauthorized data consumers including malicious adversaries can decrypt the encrypted data to obtain plaintext messages.

In contrast with the traditional access control schemes such as mandatory access control, discretionary access control, role-based access control et al., CP-ABE schemes have many advantages in providing data security in distributed environments, especially in cloud storage setting, in that they can specify and enforce complex access policies without online interaction with trusted or/and centralized servers. However, the existing CP-ABE schemes do not support the transformation of the access structure. The decrypt-and-encrypt method to implement such a mechanism is that the encryptor sends his private key to the proxy, renders it decrypt the original ciphertext by using his private key to recover the plaintext message, and then encrypts it under another access structure employing the CP-ABE scheme. The shortcoming of the method is that the proxy can learn his private key and access the sensitive plaintext data. To solve this problem, the data owner may carry out the re-encryption operation as follows: he downloads the ciphertext data into his local disks from the cloud server acting as a proxy, then decrypts them employing his private key, re-encrypts the decrypted plaintext data under another access structure employing

the CP-ABE scheme, and finally uploads his re-encrypted ciphertext data to the cloud server. The shortcomings of this method are that the data owner must be online in each re-encryption stage, and it incurs the great processing and communication overheads at the same time,which is inefficient.

To solve the foregoing problems, ciphertext policy attribute based proxy re-encryption scheme is presented. In the presented scheme, a delegator only needs to calculate the re-encryption key $RK_{\mathbb{A}1\rightarrow\mathbb{A}2}$ employed by a proxy to convert the original ciphertext computed under one access structure $\mathbb{A}1$ into the re-encrypted ciphertext computed under another access structure $\mathbb{A}2$ without decrypting the original ciphertext. Our scheme satisfies collusion resistance where if the two users combine their attributes, they cannot decrypt the ciphertext which they cannot decrypt individually. In the existing PRE scheme, communication model is one-to-one, whereas communication model of our scheme is one-to-many, i.e., a ciphertext is decrypted by many users whose attributes satisfy the access structure associated with the ciphertext. Our scheme is very suitable for dynamic setting such as cloud storage system in which the access structures are transformed frequently.

The remainder of our paper is organized as follows: in Section 2 we discuss related works. We introduce preliminaries in Section 3. We present scheme definition and security game in Section 4. We discuss the scheme construction in Section 5. Security proof is given in Section 6. The performance of our scheme is evaluated in Section 7. We conclude and specify the future work in Section 8.

2 Related Works

Sahai and Waters [16] proposed the first attribute based encryption scheme as a new means for access control of the encrypted data. One shortcoming of the scheme is that its initial construction is limited to handling formulas comprising one threshold gate, which makes it less expressive. Goyal et al. [11] greatly enhanced the expressiveness of attribute based encryption scheme where users' keys are associated with access policies, whereas ciphertexts are associated with attribute sets. The drawback of their schemes is that the encryptor does not exert any control over who can access the data which she encrypts, except for her choice of attribute set of the data to be encrypted. Bethencourt et al. [4] proposed the construction of ciphertext policy attribute based encryption scheme where private keys are associated with a set of attributes, and ciphertexts are associated with access policies over attributes. Decryption is enabled if and only if the user's attribute set satisfies the access policy associated with the ciphertext. With the advent of cloud computing, more and more sensitive data will be outsourced to cloud storage server to be stored in the encrypted form. In order to realize fine-grained access control over the encrypted data, attribute based encryption schemes are applied to cloud storage setting where there exist a large number of different types of users who are authorized to read different data. Lee et al. [14] surveyed on attribute-based encryption schemes of access control in cloud environments. However, these schemes are focused on the attribute revocation, not on access structure transformation.

Blaze et al. [5] presented the first bidirectional chosen plaintext attack (CPA) secure scheme where the proxy is prevented from seeing the plaintext information and private keys, and the re-encryption algorithm is bidirectional, which may be undesirable in scenarios where trust relationships are asymmetric and leaving the construction of a unidirectional scheme as an open problem. Ateniese et al. [1, 2] proposed a first unidirectional CPA-secure scheme based on bilinear maps whose re-encryption algorithm is single-hop. Their schemes achieved the master key security in that the proxy and the delegatee cannot collude to reveal the delegator's private key. Both schemes whose re-encryption algorithms are deterministic are only CPA-secure ones, which are insufficient to guarantee security in general protocol settings. Canetti et al. [8] proposed the proxy re-encryption scheme with chosen ciphertext secure, where ciphertexts remain indistinguishable even though the adversary can access the re-encryption oracle and the decryption oracle. The drawback of their scheme is that their construction is bidirectional. Dodis et al. [13] presented the unidirectional proxy encryption where the private key generator delegates decryption rights for all identities in the system. However, their scheme has the serious security vulnerabilities: collusion between the proxy and the delegatee incurs a system-wide compromise, rendering the colluders reconstruct the master secret of IBE. Boneh et al. [7] proposed the Identity-Based Proxy Re-Encryption scheme where the private key generator carries out all delegations, such that users cannot perform non-interactive delegations, and every delegation involves a costly online request to the PKG. Green et al. [12] proposed a unidirectional identity-based proxy re-encryption with chosen ciphertext attack secure. Their security is based on the random oracle model. The recipient of a re-encrypted ciphertext needs to know who the original receiver is, such that he can decrypt the re-encrypted ciphertext. These papers are based on the traditional public key encryption schemes whose communication models are one-to-one.

Yu et al. [18] proposed attribute based data sharing employing proxy re-encryption techniques for fine-grained attribute revocation. Liang et al. [15] presented a ciphertext policy attribute based proxy re-encryption scheme. Chung et al. [10] surveyed two various access policy attribute-based proxy re-encryption schemes and analyzed these schemes.These schemes are based on the CN CP-ABE scheme [9], so that they have the same drawbacks as it: they only supports AND Boolean operator as access policies, the number of system attributes is fixed in setup and the ciphertext size and encryption and decryption time increase linearly in the total number of attributes in the system, which makes them less expressive.

3 Preliminaries

3.1 Bilinear Map

Let $\mathbb{G}_0$ and $\mathbb{G}_1$ be two cyclic groups of prime order p, and g, h are a generator of $\mathbb{G}_0$, respectively. e is a bilinear map $e : \mathbb{G}_0 \times \mathbb{G}_0 \to \mathbb{G}_1$, which has the following properties:

Bilinearity. For any $a, b \in \mathbb{Z}_p$, $e(g^a, h^b) = e(g, h)^{ab}$.

Nondegenerate. $e(g, g) \neq 1_{\mathbb{G}_1}$, $e(g, g)$ is a generator of $\mathbb{G}_1$.

If the group operation on $\mathbb{G}_0$ and the bilinear map $e : \mathbb{G}_0 \times \mathbb{G}_0 \to \mathbb{G}_1$ are efficiently computable, then $\mathbb{G}_0$ is a bilinear group. Our scheme employs the symmetric bilinear map which has the following properties: $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$.

3.2 Benaloh and Leichter Secret Sharing Scheme

Benaloh and Leichter secret sharing scheme [3] shares the secret $s \in \mathbb{Z}_p^*$ as follows: convert an access structure $\mathbb{A}$ into an access policy tree $\mathbb{T}$, and assign the root node of $\mathbb{T}$ the value s. For every other internal node, the following are recursively performed: if the operator is $\wedge$, assign every child node a random $s_j \in \mathbb{Z}_p^* (j = 1, 2, \cdots, n-1)$ except the last one, and assign the last child one

$$s_n = (s - \sum_{j=1}^{n-1} s_j) \bmod p,$$

if the operator is $\vee$, assign every child node the value s.

4 Definition

4.1 Our Scheme Definition

Definition 1. *Ciphertext Policy Attribute Based Proxy Re-Encryption (CP-ABPRE) scheme comprises the six algorithms as follows:*

Setup$(1^k) \to (MS, \mathbb{PP})$: *The Setup algorithm is run by the trusted authority. It takes a security parameter κ as input. It outputs a master secret MS employed to generate the users' private keys and the public parameters $\mathbb{PP}$ defining system attribute sets $\mathbb{S}$ which are employed by all parties in the scheme.*

Encrypt $(\mathbb{PP}, \mathbb{A}1, m) \to CT_{\mathbb{A}1}$: *The Encryption algorithm is run by the sender. It takes as inputs the public parameters $\mathbb{PP}$, the plaintext message m and the access structure $\mathbb{A}1$ over a set of attributes specifying which users are able to decrypt to recover the plaintext message. It outputs the original ciphertext $CT_{\mathbb{A}1}$ associated with access structure $\mathbb{A}1$.*

PriKeyGen$(MS, S) \to PriKey_S$: *The Private Key Generation algorithm is run by the trusted authority. It takes as inputs the master secret MS, and the attribute set of user $S \subseteq \mathbb{S}$. It outputs the private key of user $PriKey_S$ associated with the attribute set of user S.*

ReKeyGen$(\mathbb{PP}, \mathbb{A}1, \mathbb{A}2, PriKey_S) \to RK_{\mathbb{A}1 \to \mathbb{A}2}$: *The Re-Encryption Key Generation algorithm is run by the delegator. It takes as inputs the public parameters $\mathbb{PP}$, the access structures $\mathbb{A}1$ and $\mathbb{A}2$, and the private key $PriKey_S$. It outputs a unidirectional re-encryption key $RK_{\mathbb{A}1 \to \mathbb{A}2}$ which is employed by the proxy to re-encrypt the original cihpertext $CT_{\mathbb{A}1}$ if the attribute set associated with $PriKey_S$ satisfies access structure $\mathbb{A}1$, else it returns NULL.*

ReEncrypt$(\mathbb{PP}, \mathrm{CT}_{\mathbb{A}1}, RK_{\mathbb{A}1 \to \mathbb{A}2}) \to CT_{\mathbb{A}2}$: *The Re-Encryption algorithm is run by the proxy. It takes as inputs the public parameters $\mathbb{PP}$, the ciphertext $CT_{\mathbb{A}1}$ and the re-encryption key $RK_{\mathbb{A}1 \to \mathbb{A}2}$. It outputs the re-encrypted ciphertext $CT_{\mathbb{A}2}$ associated with the access structure $\mathbb{A}2$.*

Decrypt$(CT_{\mathbb{A}k}, PriKey_S) \to m (k = 1, 2)$: The Decryption algorithm is run by the decryptor who is either a delegator or a delegatee. It takes as inputs the $CT_{\mathbb{A}k}$ and the private key $PriKey_S$. It outputs the plaintext message m if attribute set S satisfies the access structures $\mathbb{A}_k$ $(k = 1, 2)$, else it returns NULL.

Correctness: A CPAB-PRE scheme is correct when for all security parameters κ, all messages m, all sets of attributes S, access structures with $\mathbb{A}_k$ $(k = 1, 2)$ with $S \in \mathbb{A}_k$, all master secrets MS and public parameters $\mathbb{PP}$ output by Setup algorithm, all private keys $PriKey_S$ output by PriKeyGen algorithm, all original ciphertexts $CT_{\mathbb{A}1}$ output by Encryption algorithm, all re-encryption keys $RK_{\mathbb{A}1 \to \mathbb{A}2}$ output by ReKeyGen algorithm, all re-encrypted ciphertexts $CT_{\mathbb{A}2}$ output by Re-Encryption algorithm, if a set of attributes S satisfies access structure either $\mathbb{A}1$ or $\mathbb{A}2$,the following propositions hold: Decrypt$(CT_{\mathbb{A}1}, PriKey_s) = m$, Decrypt$(PriKey_s, \mathrm{ReEncrypt}(\mathbb{PP}, CT_{\mathbb{A}1}, RK_{\mathbb{A}1 \to \mathbb{A}2})) = m$.

4.2 Security Model for Ciphertext Policy Attribute Based Proxy Re-Encryption (CPAB-PRE) Scheme

We describe a security model for CPAB-PRE scheme using a security game between a challenger and an adversary as follows:

Setup. The challenger runs the Setup algorithm which generates $(MS, \mathbb{PP})$ and gives the adversary $\mathbb{PP}$.

Phase 1. The adversary issues a polynomial number of key queries: Private key generation oracle $\mathbb{O}_{Prikey}(S)$: on input any set of attributes S, the challenger runs PriKeyGen$(MS, S) \to PriKey_s$, and returns $PriKey_s$ to the adversary.

Re-encryption key generation oracle $\mathbb{O}_{rk}(\mathbb{A}1, \mathbb{A}2)$: on input an access structure $\mathbb{A}1$ and a new access structure $\mathbb{A}2$, the challenger returns $RK_{\mathbb{A}1\to\mathbb{A}2} \leftarrow \text{ReKeyGen}(\mathbb{PP}, \mathbb{A}1, \mathbb{A}2, PriKey_S)$ to the adversary, where $PriKey_S \leftarrow \text{PriKeyGen}(MS, S)$.

Challenge. The adversary submits two plaintext messages m_0, m_1 of equal length and the challenge access structure $\mathbb{A}^*$ to the challenger, with the restriction that the adversary should not select a challenge access structure $\mathbb{A}^*$ if it has performed the queries in Phase 1 as follows: $\text{PriKeyGen}(S)$ queries such that the set of attributes S satisfies the challenge access structure $\mathbb{A}^*$ or any derivative challenge access structures. $\text{ReKeyGen}(\mathbb{PP}, \mathbb{A}1, \mathbb{A}2, PriKey_S)$ queries if the adversary has beforehand issued $PriKey_S$ queries such that a set of attributes S satisfies $\mathbb{A}2$ and $\mathbb{A}1$ is a derivative challenge access structure. The challenger flips a fairy binary coin $\beta \in \{0, 1\}$, and encrypts m_β under $\mathbb{A}^*$ as the challenge ciphertext $CT^* = \text{Encrypt}(\mathbb{PP}, \mathbb{A}^*, m_\beta)$ which is given to the adversary.

Phase 2. Phase 1 is repeated with the same restriction as the challenge phase.

Guess. The adversary outputs a guess $\beta' \in \{0, 1\}$ of β, if $\beta' = \beta$, the adversary wins.

Definition 2. *A CPAB-PRE scheme is secure against chosen plaintext attacks (CPA) if no probabilistic polynomial time adversaries have non-negligible advantage in the aforementioned game, where the advantage is defined as*

$$|Pr[\beta' = \beta] - \frac{1}{2}|.$$

5 Scheme Construction

5.1 Our Scheme Construction

This construction comprises the algorithms as follows:

Setup$(1^\kappa) \to (\mathbf{MS}, \mathbb{PP})$**:** The setup algorithm calls the group generator algorithm $\mathbb{G}(1^\kappa)$ and obtains the descriptions of the two groups and the bilinear map $D = (p, \mathbb{G}_0, \mathbb{G}_1, g, e)$, in which p is the prime order of the cyclic groups $\mathbb{G}_0$ and $\mathbb{G}_1$, g is a generator of $\mathbb{G}_0$ and e is a bilinear map. The trusted authority generates the universe of system attributes $\mathbb{S} = \{att_1, att_2, \cdots, att_n\}$, where n is a positive integer. It selects the random exponents $t_1, t_2, \cdots, t_n, \mu \in \mathbb{Z}_p^*$. For each attribute $att_i \in S(1 \le i \le n)$, it selects a corresponding $t_i \in \mathbb{Z}_p^*$, and sets $T_i = g^{t_i}(1 \le i \le n)$. It employs a cryptographic hash function $H : \mathbb{G}_1 \to \mathbb{G}_0$ which hashes the elements of $\mathbb{G}_1$ into the elements of $\mathbb{G}_0$. The public parameters are published as: $\mathbb{PP} = (D, e(g, g)^\mu, \{T_i\}_{1\le i\le n}, H)$, where $e(g, g)^\mu$ can be pre-computed. The master secret is $MS = (\mu, \{t_i\}_{1\le i\le n})$.

Encrypt$(\mathbb{PP}, \mathbb{A}1, m) \to CT_{\mathbb{A}1}$**:** The encryption algorithm encrypts a message $m \in \mathbb{G}_1$ under the access structure $\mathbb{A}1$. It selects a random value $s \in \mathbb{Z}_p^*$, and then assigns attributes in the access structure $\mathbb{A}1$ values s_j $(1 \le j \le n)$, where values s_j $(1 \le j \le n)$ are shares of secret s which are generated based on the aforementioned Benaloh and Leichter secret sharing scheme. The resulting ciphertext is constructed and calculated as follows:

$$\begin{aligned} CT_{\mathbb{A}1} &= (\mathbb{A}1, E_b = g^s, E_2 = m \cdot e(g, g)^{\mu s}, \\ &\quad \{E_{3,i,j} = g^{t_i s_j}\}_{att_{i,j}\in\mathbb{A}1}). \end{aligned}$$

PriKeyGen$(MS, S) \to PriKey_S$**:** The private key generation algorithm takes in the master secret MS and the attribute set of the user $S \subseteq \mathbb{S}$. For every user, it selects a random $r \in \mathbb{Z}_p^*$ employed to prevent collusion attacks through which the different users can pool their attributes to decrypt the ciphertext that they cannot decrypt individually and calculates the private key $PriKey_S$ as follows: $PriKey_S = (K_b = g^{\mu+r}, K_{2,i} = \{g^{rt_i^{-1}}\}_{att_i\in S})$.

ReKeyGen$(\mathbb{PP}, \mathbb{A}1, \mathbb{A}2, PriKey_s) \to RK_{\mathbb{A}1\to\mathbb{A}2}$**:** The Re-Encryption Key Generation algorithm produces a unidirectional re-encryption key $RK_{\mathbb{A}1\to\mathbb{A}2}$ employed by the proxy to convert the original ciphertext $CT_{\mathbb{A}1}$ computed under the access structure $\mathbb{A}1$ into the re-encrypted ciphertext $CT_{\mathbb{A}2}$ computed under the access structure $\mathbb{A}2$.Let $S' \subseteq S$ be the minimal set of attributes satisfying the access structure $\mathbb{A}1$. It selects random $\omega, \lambda \in \mathbb{Z}_p^*$, and calculates the re-encryption key $RK_{\mathbb{A}1\to\mathbb{A}2}$ as follows:

$$RK_{\mathbb{A}1\to\mathbb{A}2} = (K_b^*, K_{2,i}^*, K_3^*),$$

where

$$\begin{aligned} K_b^* &= K_b \cdot g^{-\omega} = g^{\mu+r-\omega}, \\ K_{2,i}^* &= \{K_{2,i}\}_{att_i\in S'}, \\ K_3^* &= (K_{3,1}^*, K_{3,2}^*, K_{3,i,j}^*) = \text{Encrypt}(\mathbb{PP}, \mathbb{A}2, g^\omega). \end{aligned}$$

$Encrypt(\mathbb{PP}, \mathbb{A}2, g^\omega)$ is performed as follows in the similar way as $\text{Encrypt}(\mathbb{PP}, \mathbb{A}1, m)$ in the Encryption phase:

$$\begin{aligned} K_{3,1}^* &= g^\lambda, \\ K_{3,2}^* &= g^\omega \cdot H(e(g, g)^{\mu\lambda}), \\ K_{3,i,j}^* &= \{g^{t_i\lambda_j}\}_{att_{i,j}\in\mathbb{A}2}. \end{aligned}$$

Likewise, where $\lambda_j(1 \le j \le n)$ values are shares of secret λ which are generated based on the aforementioned BL secret sharing scheme.

ReEncrypt$(\mathbb{PP}, \boldsymbol{CT}_{\mathbb{A}1}, RK_{\mathbb{A}1\to\mathbb{A}2}) \to CT_{\mathbb{A}2}$**:** The re-encryption algorithm calculates the components as follows:

Step 1. For each attribute $att_i \in S'$, it calculates

$$\begin{aligned} B_1 &= \prod_{att_i \in S'} e(E_{3,i,j}, K^*_{2,i}) \\ &= \prod_{att_i \in S'} e(g^{t_i s_j}, g^{r t_i^{-1}}) \\ &= \prod_{att_i \in S'} e(g^{s_j}, g^r) = e(g,g)^{rs}. \end{aligned}$$

Step 2. It calculates

$$\begin{aligned} B_2 &= e(E_b, K^*_b)/B_1 = e(g^s, g^{\mu+r-\omega})/e(g,g)^{rs} \\ &= e(g^s, g^{\mu+r}) \cdot e(g^s, g^{-\omega})/e(g,g)^{rs} \\ &= e(g^s, g^{\mu-\omega}). \end{aligned}$$

Step 3. It calculates

$$\begin{aligned} E^*_2 &= \frac{E_2}{B_2} \\ &= \frac{m \cdot e(g,g)^{\mu s}}{e(g^s, g^{\mu-\omega})} \\ &= \frac{m}{e(g^s, g^{-\omega})} \\ &= m \cdot e(g^s, g^{\omega}). \end{aligned}$$

Step 4. It sets

$$\begin{aligned} E^*_b &= E_b = g^s, \\ E^*_3 &= K^*_3 = (K^*_{3,1}, K^*_{3,2}, K^*_{3,i,j}). \end{aligned}$$

The resulting re-encrypted ciphertext comprises the following components:

$$CT_{\mathbb{A}2} = (\mathbb{A}_2, E^*_b, E^*_2, E^*_3).$$

Decrypt$(CT_{\mathbb{A}k}, PriKey_S) \rightarrow m (k = 1, 2)$**:** The decryption algorithm takes in the ciphertext $CT_{\mathbb{A}k}$ and the private key $PriKey_S$. If the set of attributes S does not satisfy the access structure $\mathbb{A}_k (k = 1, 2)$, the algorithm returns NULL. If the access structure $\mathbb{A}_k (k = 1, 2)$ is satisfied by S and $CT_{\mathbb{A}k}$ is a well-formed ciphertext, then the decryption algorithm performs the steps as follows:

Step 1. It selects the minimal set of attributes $S' \subseteq S$ satisfying the access structure $\mathbb{A}1$, and calculates

$$\begin{aligned} N_1 &= \prod_{att_i \in S'} e(E_{3,i,j}, K_{2,i}) \\ &= \prod_{att_i \in S'} e(g^{t_i s_j}, g^{r t_i^{-1}}) \\ &= \prod_{att_i \in S'} e(g^r, g^{s_j}) = e(g,g)^{rs}. \end{aligned}$$

Step 2. It calculates

$$\begin{aligned} N_2 &= e(E_b, K_b)/N_1 \\ &= e(g^s, g^{\mu+r})/e(g,g)^{rs} \\ &= e(g,g)^{\mu s}. \end{aligned}$$

Step 3. The message m is recovered via calculating

$$\begin{aligned} \frac{E_2}{N_2} &= \frac{m \cdot e(g,g)^{\mu s}}{e(g,g)^{\mu s}} \\ &= m. \end{aligned}$$

If S satisfies the access structure $\mathbb{A}2$, $S' \subseteq S$ be the minimal set of attributes satisfying the access structure $\mathbb{A}2$ and $CT_{\mathbb{A}2}$ is a re-encrypted ciphertext, then the decryption algorithm performs the following steps:

Step 1. For each attribute $att_i \in S'$, it calculates:

$$\begin{aligned} V_1 &= \prod_{att_i \in S'} e(K^*_{3,i,j}, K_{2,i}) \\ &= \prod_{att_i \in S'} e(g^{t_i \lambda_j}, g^{r t_i^{-1}}) \\ &= \prod_{att_i \in S'} e(g^{\lambda_j}, g^r) \\ &= e(g,g)^{r\lambda}. \end{aligned}$$

Step 2. It calculates

$$\begin{aligned} V_2 &= e(K_b, K^*_{3,1})/V_1 \\ &= e(g^{\mu+r}, g^{\lambda})/e(g,g)^{r\lambda} \\ &= e(g,g)^{\mu\lambda}. \end{aligned}$$

Step 3. It calculates

$$\begin{aligned} V_3 &= \frac{K^*_{3,2}}{H(V_2)} \\ &= \frac{g^{\omega} \cdot H(e(g,g)^{\mu\lambda})}{H(V_2)} \\ &= \frac{g^{\omega} \cdot H(e(g,g)^{\mu\lambda})}{H(e(g,g)^{\mu\lambda})} \\ &= g^{\omega}. \end{aligned}$$

Step 4. The message is recovered as follows:

$$\begin{aligned} \frac{E^*_2}{e(E^*_b, V_3)} &= \frac{m \cdot e(g^s, g^{\omega})}{e(g^s, g^{\omega})} \\ &= m. \end{aligned}$$

6 Security Proof

Proof of security is provided in the generic bilinear group model [6, 17] where group elements are encoded as unique random strings. We consider two random encodings φ_0,φ_1 of the additive group $\mathbb{F}_p$ which are injective maps $\varphi_0, \varphi_1 : \mathbb{F}_p \rightarrow \{0,1\}^l$, in which $l > 3\log_2 p$. Let $\mathbb{G}_i = \{\varphi_i(x) : x \in \mathbb{F}_p\}, i = 0, 1$. We are given oracles to calculate the induced group action on $\mathbb{G}_0$ and $\mathbb{G}_1$, and an oracle to calculate a bilinear map

$$e : \mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1.$$

Theorem 1. *Let $\varphi_0, \varphi_1, \mathbb{G}_0, \mathbb{G}_1$ be defined as aforementioned. For any adversary, let q be a bound on the total number of group elements it receives from queries that it makes to the oracles for groups $\mathbb{G}_0$ and $\mathbb{G}_1$, and the bilinear map e, and from its interaction with the CPAB-PRE security game. Then the advantage of the adversary in the CPAB-PRE security game is $\mathbb{O}(q^2/p)$.*

Proof. In the CPAB-PRE security game, the challenge ciphertext has a component that is either $m_0 e(g,g)^{\mu s}$ or $m_1 e(g,g)^{\mu s}$. Instead, we can consider a modified game where ciphertext component E_2 is either $e(g,g)^{\mu s}$ or $e(g,g)^{\sigma}$, in which σ is selected uniformly at random from $\mathbb{F}_p$ and the adversary must decide which the case is. Any adversary who has advantage ε in the CPAB-PRE security game can be converted into another adversary who has advantage at least $\varepsilon/2$ in the modified CPAB-PRE security game.

We will write g^{α} to denote $\varphi_0(\alpha)$ and $e(g,g)^{\eta}$ to denote $\varphi_1(\eta)$, where $\alpha, \eta \in \mathbb{Z}_p$. Each random encoding is associated with a rational function in the variables: $\{\mu, \sigma, s, \{t_i\}_{1\le i\le n}, \lambda, r, \omega\}$, where each variable is a random element selected in the scheme.

In Setup phase, let $g = \varphi_0(1)$, $\{g^{t_i} = \varphi_0(t_i)\}_{1\le i\le n}$,$e(g,g)^{\mu} = \varphi_1(\mu)$. The public parameters are sent to the adversary.

In Phase 1 and Phase 2 of the security game, for Private key generation oracle $\mathbb{O}_{PriKey}(S)$, let

$$\begin{aligned} K_b &= g^{\mu+r} = \varphi_0(\mu+r), \\ K_{2,i} &= \{g^{rt_i^{-1}} = \varphi_0(rt_i^{-1})\}_{att_i\in S}, \end{aligned}$$

for Re-encryption key generation oracle $\mathbb{O}_{rk}(\mathbb{A}1, \mathbb{A}2)$, let

$$\begin{aligned} K_b^* &= K_b \cdot g^{-\omega} = g^{\mu+r-\omega} \\ &= \varphi_0(\mu+r-\omega), \\ K_{2,i}^* &= \{K_{2,i}\}_{att_i\in S'}, \\ (K_{3,1}^*, K_{3,2}^*, K_{3,i,j}^*) &= \text{Encrypt}(\mathbb{PP}, \mathbb{A}2, g^{\omega}) \\ &= (\varphi_0(\lambda), \varphi_0(h), \{\varphi_0(t_i\lambda_j)\}_{att_{i,j}\in\mathbb{A}2}). \end{aligned}$$

These values are given to the adversary.

In the Challenge phase, for the Encryption oracle, when the adversary submits two challenge plaintext messages $m_0, m_1 \in \mathbb{G}_1$ and the challenge access structure $\mathbb{A}^*$, let

$$\begin{aligned} E_b &= g^s = \varphi_0(s), E_2 = e(g,g)^{\sigma} = \varphi_1(\sigma), \\ \{E_{3,i,j} &= g^{t_i t_j}\}_{att_{i,j}\in\mathbb{A}^*} = \{\varphi_0(t_i s_j)\}_{att_{i,j}\in\mathbb{A}^*}. \end{aligned}$$

These values are passed on to the adversary.

We will show the adversary cannot distinguish with non-negligible advantage the simulation of the modified game in which the challenge ciphertext is $E_2 = e(g,g)^{\sigma}$, from the simulation of the real game in which the challenge ciphertext is $E_2 = e(g,g)^{\mu s}$. Firstly, the adversary's view is given if the challenge ciphertext is $\varphi_1(\sigma)$, and the adversary's view can change if an unexpected collision occurs due to the random choices of these variables $\{\mu, \sigma, s, \{t_i\}_{1\le i\le n}, \lambda, r, \omega\}$. For any two distinct queries, the probability that any such collision happens is at most $\mathbb{O}(q^2/p)$. Secondly, what the adversary's view would have been if we had set $\varphi_1(\mu s)$. The adversary cannot obtain a query polynomial of the form μs, so such a collision cannot occur. In Table 1, we list possible queries into $\mathbb{G}_1$ based on the bilinear map and the group elements passed on to the adversary in the simulation.

Table 1: Possible query types from the adversary

$(\mu+r)t_is_j$	$(\mu+r)s$	rs_j	$\mu s+rs-rs_j$
rst_i^{-1}	$(\mu+r)\lambda$	$(\mu+r)h$	$(\mu+r)t_i\lambda_j$
$r\lambda t_i^{-1}$	$rt_i^{-1}h$	$r\lambda_j$	$(\mu+r-\omega)t_is_j$
$(\mu+r-\omega)s$	λs	$\lambda_j t_i^2 s_j$	$\lambda_j t_i s$
hs	ht_is_j	$\lambda t_i s_j$	

As seen from Table 1, the adversary can pair t_is_j with rt_i^{-1}, and $\mu+r$ with s, and then make the latter subtract the former to obtain $(\mu+r)s - \sum_{att_{i,j}\in S} rs_j$. In order to obtain μs, the adversary must make polynomial requests to cancel rs. The adversary has to pair t_is_j with rt_i^{-1} to get rs. As you can see from Table 1, the adversary has to construct a query polynomial of the form: $\mu s + rs - \sum_{att_j\in s} rs_j$. Whereas the adversary cannot construct a query polynomial of the form μs if he does not possess a private key associated with the set of attributes satisfying the access structure. There has to be one rs_j missing, in that even if the adversary has one ciphertext component $g^{t_is_j}$, he has not a private key component $g^{rt_i^{-1}}$ to pair. Therefore he is not able to reconstruct rs, as a result he cannot cancel the second term and the third term to get μs. From the foregoing analysis, we can draw a conclusion that the adversary cannot make a polynomial query of the form μs. □

7 Performance Analysis

7.1 Properties Comparison

As seen from Table 2, the distinguished property of our scheme is that the communication model of our scheme is one-to-many, i.e., a ciphertext is decrypted by many users whose attributes satisfy the access structure associated with the ciphertext, whereas the traditional proxy re-encryption schemes based on the traditional public key encryption schemes or identity based encryption schemes are one-to-one, i.e., a ciphertext is only decrypted by a private key.

7.2 Performance Evaluation

As illustrated in Table 3, where $x\mathbb{G}_0$, $y\mathbb{G}_1$, zC_e,kH and $||$ denote x exponentiations in $\mathbb{G}_0$, y exponentiations in $\mathbb{G}_1$, z times bilinear maps, k times hash, and the cardinality of the set, respectively, our scheme supports

Table 2: Property comparison of PRE schemes

References	Unidirectional	Hops	CCA security	Collusion Resistance	Non-interactive	Non-transitive	Key Optimal	Communication Model
BBS Scheme [5]	No	Multi-Hop	No	No	No	No	Yes	One-to-one
AFGH Scheme [1, 2]	Yes	Single-Hop	No	Yes	Yes	Yes	Yes	One-to-one
CH Scheme [8]	No	Multi-Hop	Yes	No	Yes	Yes	Yes	One-to-one
GA Scheme [12]	Yes	Multi-Hop	Yes	Yes	Yes	Yes	Yes	One-to-one
Our Scheme	Yes	Single-Hop	No	Yes	Yes	Yes	Yes	One-to-many

the transformation of access structure, whereas BSW scheme does not support it; furthermore, our scheme has better performances on Private Key Generation, Encryption, and Decryption operations than those of BSW scheme. Performances on Re-Encryption Key Generation, Re-Encryption, and Decryption for the Re-Encrypted Ciphertext operations are analyzed.

8 Conclusions

In this work, for the settings such as cloud storage system where the access structures are frequently changed, we proposed a ciphertext policy attribute based proxy re-encryption scheme which delegates the proxy to transform the access structure associated with the original ciphertext without decrypting it. However, in our scheme, suppose there exists a single trusted authority, which may bring about a single point of failure. A user may possess attributes issued from multiple authorities and the data owner may share the data with users administered by different authorities. In order to enhance robustness, we will design multi authority CPAB-PRE scheme to transform the access structure associated with the ciphertext. The PRE algorithm in our scheme is only CPA-secure, and CPA security is often insufficient to guarantee security in general protocol settings.So we will address the problem of achieving CPAB-PRE scheme which is secure in arbitrary protocol settings, i.e., CCA secure.

Acknowledgments

The author gratefully acknowledges the anonymous reviewers for their valuable comments.

References

[1] Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in *the 12th Annual Network and Distributed System Security Symposium*, pp. 176–180, 2005.

[2] Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM TISSEC*, vol. 9, no. 1, pp. 1–30, 2006.

[3] Josh Benaloh and Jerry Leichter, "Generalized secret sharing and monotone functions," in *Advances in Cryptology - CRYPTO,vol. 403 of LNCS*, p. 27C36, Springer, 1988.

[4] John Bethencourt, Amit Sahai, and Brent Waters, "Ciphertext-policy attribute-based encryption," in *IEEE Symposium on Security and Privacy*, pp. 321 – 334, 2007.

[5] Matt Blaze, Gerrit Bleumer, and Martin Strauss, "Divertible protocols and atomic proxy cryptography," in *Proceedings of Eurocrypt 98*, vol. 1403, pp. 176–180, 1998.

[6] Dan Boneh, Xavier Boyen, and Eu-Jin Goh, "Hierarchical identity based encryption with constant size ciphertext," in *R.Cramer, editor, EUROCRYPT, vol. 3494 of Lecture Notes in Computer Science*, pp. 440–456, Springer, 2005.

[7] Dan Boneh, Eu-Jin Goh, and Toshihiko Matsuo, "Proposal for p1363.3 proxy re-encryption," in *http://grouper.ieee.org/groups/1363/IBC/submissions/NTTDataProposal-for-P1363*, September 2006.

[8] Ran Canetti and Susan Hohenberger, "Chosen-ciphertext secure proxy e-encryption," in *ACM CCS07*, pp. 185–194, New York, 2007.

[9] Ling Cheung and Calvin C. Newport, "Provably secure ciphertext policy abe," in *ACM Conference on Computer and Communications Security*, pp. 456–465, 2007.

Table 3: Performance comparison of our scheme with BSW scheme

References	**Private Key Generation**	**Encryption**	**Re-Encryption Key Generation**	**Re-Encryption**	**Decryption (Original Ciphertext)**	**Decryption (Re-Encrypted Ciphertext)**
BSW Scheme [4]	$(2\|S\|+1)\mathbb{G}_0$	$(2\|\mathbb{A}_1\|+1)\mathbb{G}_0+1\mathbb{G}_1$	Not Supported	Not Supported	$\|S'\|\mathbb{G}_1+2\|S'\|C_e$	Not Supported
Our Scheme	$(\|S\|+1)\mathbb{G}_0$	$(\|\mathbb{A}_1\|+1)\mathbb{G}_0+1\mathbb{G}_1$	$(\|\mathbb{A}_2\|+3)\mathbb{G}_0+1\mathbb{G}_1+1H$	$(\|S'\|+1)C_e$	$(\|S'\|+1)C_e$	$(\|S'\|+1)C_e+1H$

[10] Pei-Shan Chung, Chi-Wei Liu, and Min-Shiang Hwang, "A study of attribute-based proxy re-encryption scheme in cloud environments," *International Journal of Network Security*, vol. 16, no. 1, pp. 1–13, Jan. 2014.

[11] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM conference on Computer and communications security*, pp. 89 – 98, 2006.

[12] Matthew Green and Giuseppe Ateniese, "Identity-based proxy re-encryption," in *ACNS0, LNCS 4521*, pp. 288–306, New York:Springer, 2007.

[13] Anca Ivan and Yevgeniy Dodis, "Proxy cryptography revisited," in *the 10th Annual Network and Distributed System Security Symposium (NDSS03)*.

[14] Cheng-Chi Lee, Pei-Shan Chung, and Min-Shiang Hwang, "A survey on attribute-based encryption schemes of access control in cloud environments," *International Journal of Network Security*, vol. 15, no. 4, pp. 231 – 240, July 2013.

[15] Xiaohui Liang, Zhenfu Cao, Huang Lin, and Jun Shao, "Attribute based proxy re-encryption with delegating capabilities," in *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, pp. 276 – 286, 2009.

[16] Amit Sahai and Brent Waters, "Fuzzy identity based encryption," in *Advances in Cryptology (Eurocrypt)*, vol. 3494 of LNCS, pp. 457 – 473. Springer, 2005.

[17] Victor Shoup, "Lower bounds for discrete logarithms and related problems," in *EUROCRYPT*, pp. 256–266, 1997.

[18] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou, "Attribute based data sharing with attribute revocation," in *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, pp. 261–270, 2010.

Xingbing Fu is a lecturer, he received his M.S. degree from Southwest University in 2007. He is currently a PhD Candidate in the School of Computer Science and Engineering, University of Electronic Science and Technology of China. His research interests are information security, cloud computing, cryptography and artificial intelligence.