Extended Attribute Based Encryption for Private Information Retrieval

Shan Yinan
Department of Computer Science and Engineering
Shanghai Jiao Tong University
Shanghai China
shanyinan@gmail.com

Zhenfu Cao
Department of Computer Science and Engineering
Shanghai Jiao Tong University
Shanghai China
zfcao@cs.sjtu.edu.cn

***Abstract*—Private information retrieval enables the sensitive data to be obtained only if the data authorizers allow the data receivers to access to the data. Sometimes the owners are of a group and there is no need for all members to authorize the receivers. Moreover, the right to authorize could be unequal for different authorizers in the group.**

In this paper, we first proposed a solution providing hierarchical authorization right of different owners of the data with an extension of attribute based encryption. This scheme uses an access structure to describe the hierarchical relations of the authorizers of the data, and also provides privacy for the data and authorizer as well as the security of anti-collusion attack.

In addition, we proposed an improved scheme which allows the authorizers to specify the authorization to certain data instead of providing the access right to all data they are in charge. This scheme is more secure for achieving forward security and more practical.

***Index Terms*—attribute based encryption; information retrieval; hierarchical authorization**

I. Introduction

With the advantage of efficiency and convenience, more and more private information is stored in a third party like database and could be accessed through the internet. However, the authorization for the access to the data is still a big problem requiring great effort in research.

Currently, we use key or password to control the access and many associated schemes about allocating keys for users are proposed [1][2][3]. However, in some scenarios the data is owned by a group of people, (e.g. the data is about financial statistic of a company). It is possible more than one people (manager, vice-manager and employee) who have the right to authorize another person to access to the data. Research on this topic receives much attention in the past. A solution called efficient multi-authorizer accredited symmetrically private information retrieval [5] was proposed, which allowed a threshold of data owner to authorize the data receiver. This scheme used some security definitions from the accredited symmetrically private information retrieval scheme (ASPIR) [4] assuming a setting that the sensitive information of the user is stored in a database and controlled by a party called Sender. Sender is in charge of sending certain data to a party named Receiver.

Also, the authorization right of data owners might vary from different users in practice. (In a company, a chief manager may have the greatest priority to approve a data receiver to access to the data. The data receiver could obtain the data with just a single authorization from the chief manager. While the chief manager is always busy, a data receiver could also ask authorization from other vice-managers and employees. In contrast, the receiver would finally gain the access right if all the two vice-managers allowed or more than 10 employees authorized.)

In this article, we extend attribute based (ABE) encryption and make it applicable to the private information retrieval scenario. In ABE, a user is identified by a certain set of attributes, and ciphertext is encrypted under another set of attributes. When the size of the intersection of these two sets are larger than a predefined threshold the user could decrypt the cipher. The qualified decryptor set is described as an access structure in ABE.

Our Contribution. In our first extended attribute based encryption (EABE) scheme, authorizers could authorize the data receiver separately by signing a signature. The sensitive data is preserved in a database DB and controlled by a third trusted party named sender. Sender will encrypt the required data with the access structure and send the ciphertext to data receiver. Only if the receiver gets enough authorizations which satisfy the access structure can he or she decrypts the ciphertext. Comparing with the works before, this scheme provides a hierarchical authorization system with high efficiency and security. This scheme provides the security of anti-collusion attack and privacy for authorizer, sender and the data. In addition, though ABE provides a hierarchical access rights, no previous work showed how to apply it to a real practice.

To specify the authorization rights towards different data owned by a group of authorizers, we then proposed an improved EABE (IEABE) using the ASPIR [4] scheme. Each authorizer will generate an authorization on a requirement which includes the receiver identity, index of the data and some other policy. The sender will also generate a ciphertext based on the requirement and the access structure. Receiver could retrieve the data from the ciphertext obtained through ASPIR scheme if the access structure is satisfied. Except for the specific authorization function it owns, IEABE is more secure and practical in practice because we don't need to allocate a permanent key for each data receiver during the

978-1-4244-5113-5/09/$25.00

setup course. Receivers are only identified by a global identity. This scheme also provide a useful mechanism for a real-time update system. By adding a time stamp, authorization of the data receiver could be only valid in a period.

A. Related works

Sahai and Waters [8] firstly proposed a preliminary attribute based encryption (ABE) scheme called fuzzy identity based encryption scheme in 2005. Goyal, Pandey, Sahai and Waters [6] further defined the concept of ABE in two complimentary forms: key-policy ABE (KPABE) and ciphertext-policy ABE (CPABE). While in KPABE attributes are associated with a formula to describe the access structure, in CPABE ciphertext is related to the formula. In addition, Goyal et. al. [6] provided a construction for KPABE, which allows keys to be expressed by any monotonic formula over encrypted data. After that, Bethencourt, Sahai, and Waters [9] firstly gave a scheme for CPABE, which was expressive and efficient. Later, Waters [10] provided a CPABE in standard model with the use of linear secret sharing scheme (LSSS) which is also expressive and efficient. A multi-authority ABE was proposed by Chase [11] in 2007. A multi-authority ABE allows more than one authority to allocate the secret keys for attributes. The authentications of attributes of uncorrupted authorities remain secure if at least one attribute authority remain uncorrupted.

ASPIR [4] defined a setting for data sender and receiver such that the following three security requirements are satisfied:

1) Privacy for the data: the Receiver can retrieve a data record only if he has a valid authorization to do so from the record owner.
2) Privacy for the Receiver: the Sender is convinced that the Receiver's query is authorized by the owner of the target DB record.
3) Privacy for the Sender: the Receiver cannot retrieve information about more than one record in each query.

On the base of the work of ASPIR Mohamed Layouni, Maki Yoshida, and Shingo Okamura [5] further proposed an efficient multi-authorizer ASPIR construction which allows a threshold of data owner to authorize the receiver.

B. Organization

In the next section, we would provide some preliminary and definitions. In the subsequent section, we will provide the extended attribute based encryption scheme and the improved scheme with details. After that, security and privacy evaluation will be given. Performance analysis is in the fifth section. Some conclusions will be given at the end.

II. Preliminary

The hierarchical rights of the authorizers are described as an access structure which is adapted in the CPABE [10], we will first give a definition of the access structure in the following part.

The two schemes we present use a paring-based short signature scheme [13] and linear secret sharing scheme (LSSS) [12]. The signature scheme relies on the hardness of Bilinear Diffie-Hellman Problem (BDH). We will introduce the bilinear maps, LSSS, BDH, and describe building blocks for the extended attributed based encryption for private information retrieval scheme and the improved one.

A. Access structure

Definition 1 (Access Structure). Let $\mathcal{A} = \{A_1, A_2, ..., A_n\}$ be a set of parties. A collection $\Gamma \subseteq 2^{\mathcal{A}}$ is monotone if for all $B, C \subseteq \mathcal{A}$, if $B \in \Gamma$ and $B \subseteq C$ then $C \in \Gamma$. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) Γ of non-empty subset of $\mathcal{A}$. The sets in Γ are called the authorized sets, and the sets not in Γ are called the unauthorized sets.

In an ABE, the attributes take the roles of the parties, while in our scheme the authorizers take these roles.

B. Linear Secret Sharing Schemes

Definition 2 (Linear Secret-Sharing Scheme (LSSS)). A secret-sharing scheme Π over a set of parities $\mathcal{A}$ is called linear (over Z_p) if the following conditions holds.

1) The shares for each party form a vector over Z_p.
2) There exists a matrix M called the share-generating matrix for Π. The matrix M has l rows and w columns. For all $i = 1, \ldots, l$, the ith row of M we let the function defined the party labeling row i as $\rho(i)$. When we consider the column vector $v = (s, r_2, ..., r_w)$, where $s \in Z_p$ is the secret to be shared, and $r_2, ...r_w \in Z_p$ are randomly chosen, then Mv is the vector of l shares of the secret s according to Π. The share $(Mv)_i$ belongs to party $\rho(i)$.

It is shown in [12] that every linear secret sharing-scheme according to the above definition also enjoys the linear reconstruction property, defined as follows: suppose that Π is an LSSS for the access structure Γ. Let $\mathcal{A}' \in \Gamma$ be any authorized set, and let $I \subset \{1, 2, \ldots, l\}$ be defined as $I = \{i | \rho(i) \in \mathcal{A}'\}$ then, there exist constants $\{\omega_i \in Z_p\}_{i \in I}$ such that, if $\{\lambda_i\}$ are valid shares of any secret s according to Π, then $\sum_{i \in I} \omega_i \lambda_i = s$. Furthermore, it is shown in [12] that these constants $\{\omega_i\}$ can be found in time polynomial in the size of the share-generating matrix M.

C. Bilinear Maps

Definition 3 (Bilinear Maps). Let G and G_T be two multiplicative cyclic groups of prime order p. Let g be a generator of G and e be a bilinear map, $e : G \times G \rightarrow G_T$. The bilinear map e has the following properties:

1) Bilinearity: for all $u, v \in G$ and $a, b \in Z_p$, we have $e(u^a, v^b) = e(u, v)^{ab}$.
2) Non-degeneracy: $e(g, g) \neq 1$.

D. Decisional Bilinear Diffie-Hellman Assumption

We define the decisional Bilinear Diffie-Hellman problem as follows. A challenger chooses a group G of prime order p according to the security parameter. Let $a, b, s \in Z_p$ be chosen at random and g be a generator of G. When given (g, g^a, g^b, g^s) the adversary must distinguish a valid tuple

$e(g,g)^{abs} \in G_T$ from a random element R in G_T.

An algorithm B that outputs $z \in \{0,1\}$ has advantage ϵ in solving decisional BDH in G if

$$|Pr[\mathsf{B}(g, g^a, g^b, g^s, T = e(g,g)^{abs}) = 0] - Pr[\mathsf{B}(g, g^a, g^b, g^s, T = R) = 0]| \geq \epsilon.$$

Definition 4 (The Decisional BDH Assumption). We say that the decisional BDH assumption holds if no polynomial time algorithm has a non-negligible advantage in solving the decisional BDH problem.

E. participants in our scheme

EABE and IEABE involve the initializer, a sender, a receiver, and authorizers, denoted by I, S, R and $\mathcal{A} = \{A_1, A_2, \ldots, A_n\}$ respectively. I generates a common parameter PK and then publishes PK authentically. S has a data d which should be authorized by an authorized set $\mathcal{A}'$ in an access structure Γ. A_i generates their private/public key pair to sign message. In EABE, the ciphertext is generated according to the access structure. The authorization from A_i generated according to the identity of R. While in IEABE S and/or R choose a message m to be signed as a proof of authorization. Then S encrypts d based on m and Γ, and sends its ciphertext $CT_{\Gamma,m}$ to R. R obtains signatures on m from all authorizers in $\mathcal{A}' \in \Gamma$, and then decrypts the ciphertext $CT_{\Gamma,m}$ using the signatures.

F. Extended Attribute Based Encryption for private information retrieval

In this scheme we assume that each receiver R gets a global identity GID, which is unique and distinctive. After the setup of system each receiver R will get a key key_{GID}. Ciphertext is generated under the access structure by sender S and sent to R according to his requirement. R could get authorization signatures from an authorizer set $\mathcal{A}'$. If A' satisfy the Γ, R could decrypt the ciphertext and retrieve the data d.

Definition 5 (Extended Attribute Based Encryption for private information retrieval). An extended attribute based encryption scheme $EABE = (\mathsf{Com}, \mathsf{Init}, \mathsf{KG}, \mathsf{Enc}, \mathsf{Sig}, \mathsf{Ver}, \mathsf{Dec})$ consists of seven algorithms.

- A common parameter generation algorithm, Com. It takes as input a system security parameter 1^k and returns a master key MK and all the common parameter PK needed by users of the scheme, such as choice of groups and hash function.
- An initial algorithm, Init. It takes as a common parameter PK and system master key MK and a GID of the user. It outputs a central key Key_{GID}.
- An authorizer key generation algorithm KG. It takes as input the common parameter PK and outputs a private/public keypair (SK_A, PK_A) that an authorizer use to sign messages. Let (SK_{A_i}, PK_{A_i}) denote a keypair of A_i.
- An encryption algorithm Enc. It takes as input the common parameter PK, an access structure Γ, a set of public keys of authorizers $\{PK_{A_i}\}$ and a data d. It outputs a ciphertext CT_Γ.
- A signing algorithm Sig. It takes as input the common parameter PK, the secret key SK_{A_i} of the authorizer A_i, and a receiver identity GID. It outputs a signature Sig_{GID,A_i}.
- A verification algorithm Ver. It takes as input the common parameter PK, the public key PK_{A_i}, and a signature Sig_{GID,A_i} of the authorizer A_i. It outputs "valid" or "invalid".
- A decryption algorithm Dec. It takes as the input the common parameter PK, a ciphertext CT_Γ which contains an access structure Γ, an authorized set $\mathcal{A}' \in \Gamma$, the public keys $\{PK_{A_i} | A_i \in \mathcal{A}'\}$ of $\mathcal{A}'$, and signatures $\{Sig_{GID,A_i} | A_i \in \mathcal{A}'\}$ on GID by $\mathcal{A}'$. It outputs a data d or the special symbol "$\perp$" which indicates failure.

Correctness. For EABE to be correct, it is required that the following holds: for any receiver id GID, any access structure Γ and any attribute set $\mathcal{A}' \in \Gamma$, if

$$(PK, MK) \leftarrow \mathsf{Com}(1^k)$$

$$Key_{GID} \leftarrow \mathsf{Init}(PK, MK, GID)$$

$$\{(SK_{A_i}, PK_{A_i}) \leftarrow \mathsf{KG}(PK)\}$$

$$\{Sig_{GID,A_i}\} \leftarrow \{\mathsf{Sig}(PK, SK_{A_i}, GID)\}$$

$$\{\text{“}valid\text{”} \leftarrow \mathsf{Ver}(PK, PK_{A_i}, Sig_{GID,A_i})\}$$

$$CT_\Gamma \leftarrow \mathsf{Enc}(PK, \Gamma, \{PK_{A_i}\}, d)$$

then $d \leftarrow \mathsf{Dec}(PK, Key_{GID}, \{Sig_{GID,A_i} | A_i \in \mathcal{A}'\}, CT_\Gamma)$

G. Improved Extended Attribute Based Encryption with ASPIR

In this scheme we use a message m as the requirement of certain data and the distinction part of the authorization, which includes the receiver identity GID, policy setting $Policy$ and data index i, i.e. $m = GID||Policy||i$. $Policy$ includes time stamp or some other system settings. The data receiver generates a ASPIR requirement on m and sends the requirement and $GID||Policy$ to the sender S without the index i. According to the ASPIR scheme, receiver R could obtain a ciphertext of the data d on the requirement m without letting S know the index i. The ciphertext $C_{\Gamma,m}$ is encrypted under the access structure Γ. Authorization is the signature $Sig_{A_i,m}$ from the authorizer A_i on the m. Only if $\{A_i |$ R get $Sig_{A_i,m}\}$ satisfy the access structure Γ could R decrypt the ciphertext.

Definition 6 (Improved Extended Attribute Based Encryption with ASPIR). An improved extended attribute based encryption scheme $IEABE = (\mathsf{Com}, \mathsf{KG}, \mathsf{Enc}, \mathsf{Sig}, \mathsf{Ver}, \mathsf{Dec})$ consists of six algorithms. Comparing with the EABE scheme there are some differences as follow. The output of Com is just a common parameter PK. Enc,Dec, Ver and sig algorithms all have an additional input, the requirement message m.

Correctness. For IEABE to be correct, it is required that the following holds: for any requirement message m =

$GID||Policy||i$, any access structure Γ and any attribute set $\mathcal{A}' \in \Gamma$, if $\mathcal{A}'$ satisfy Γ.

$$(PK) \leftarrow \mathsf{Com}(1^k)$$

$$\{(SK_{A_i}, PK_{A_i}) \leftarrow \mathsf{KG}(PK)\}$$

$$\{Sig_{A_i,m} \leftarrow \mathsf{Sig}(PK, SK_{A_i}, m)\}$$

$$\{\text{“}valid\text{''} \leftarrow \mathsf{Ver}(PK, PK_{A_i}, Sig_{GID,A_i})\}$$

$$CT_{\Gamma,m} \leftarrow \mathsf{Enc}(PK, \{PK_{A_i}\}, d, m, \Gamma)$$

then $d \leftarrow \mathsf{Dec}(PK, \{Sig_{A_i,m} | A_i \in \mathcal{A}'\}, CT_{\Gamma,m})$

III. Construction

In this section we give the constructions of EABE and IEABE as follows.

A. EABE

$\mathsf{Com}(1^K)$. The common parameter generation algorithm chooses a bilinear group G of prime order p and a generator g and chooses $\alpha, a \in Z_p$ randomly. It also chooses a hash function $H(x) : \{0,1\}^* \rightarrow G$. The common parameter is published as

$$PK = \big(g, e(g,g)^{\alpha}, g^a, H, e, G, G_T\big).$$

$$MK = \big(g^{\alpha}, a\big)$$

$\mathsf{Init}(MK, GID)$. The algorithm generates the key for user GID as :

$$Key_{GID} = g^{\alpha} H(GID)^a$$

$\mathsf{KG}(PK)$. The key generation algorithm randomly chooses $SK_{A_i} = t_i \in Z_p$ and calculate $PK_{A_i} = g^{t_i}$ and then publish the public key authentically.

$\mathsf{Enc}(PK, \Gamma, \{PK_{A_i}\}, d)$. Let Γ be an LSSS access structure (M, ρ). The function ρ associates rows of M to authorizers. In this construction, ρ is limited to be an injective function. Let M be an $l \times n$ matrix. The algorithm first chooses a random vector $\overrightarrow{v} = (s, y_2, ..., y_n) \in Z_p^n$. For $i = 1$ to l it calculates $\lambda_i = \overrightarrow{v} \cdot M_i$ where M_i is the vector corresponding to the ith row of M. The algorithm also chooses a random $t_0 \in Z_p$. The ciphertext is published as

$$CT_{\Gamma} = \big(C = d \cdot e(g,g)^{\alpha s}, C' = g^s,$$

$$C_1 = g^{a\lambda_1} g^{-t_1 s}, ...C_l = g^{a\lambda_l} g^{-t_l s}\big),$$

$\mathsf{Sig}(PK, SK_{A_i}, GID)$. The signature in represent of the authentication is generated:

$$Sig_{GID,A_i} = H(GID)^{t_i}$$

$\mathsf{Dec}(PK, CT_{\Gamma}, \{Sig_{GID,A_i} | A_i \in \mathcal{A}'\}, Key_{GID})$. Suppose $\mathcal{A}' \in \Gamma$ and $I = \{i : \rho(i) \in \mathcal{A}'\} = \{1, 2, \ldots, l\}$. According to the LSSS scheme [12], $\{\omega_i | i \in I\}$ can be calculated within polynomial time which satisfy $\sum_{i \in I} \lambda_i \omega_i = s$. The decryption algorithm computes

$$\frac{e(C', Key_{GID})}{\Pi_{i \in I}(e(C_i, H(GID)) e(Sig_{GID,A_i}, C'))^{\omega_i}} = e(g,g)^{\alpha s}$$

Then the algorithm obtains the data d by

$$d = C / e(g,g)^{\alpha s}$$

B. IEABE

$\mathsf{Com}(1^K)$. The common parameter generation algorithm chooses a bilinear group G of prime order p and a generator g and choose $a \in Z_p$ randomly. It also chooses a hash function $H(x) : \{0,1\}^* \rightarrow G$. The common parameter is published as

$$PK = \big(g, g^a, H, e, G, G_T\big).$$

$\mathsf{KG}(PK)$. The key generation algorithm randomly chooses $SK_{A_i} = t_i \in Z_p$ and calculate $PK_{A_i} = g^{t_i}$ and then publish the public key authentically.

$\mathsf{Enc}(PK, \Gamma, m, d)$. Let Γ be an LSSS access structure (M, ρ). The function ρ associates rows of M to authorizers. In this construction, ρ is limited to be an injective function. Let M be an $l \times n$ matrix. The algorithm first chooses a random vector $\overrightarrow{v} = (s, y_2, ..., y_n) \in Z_p^n$. For $i = 1$ to l it calculates $\lambda_i = \overrightarrow{v} \cdot M_i$ where M_i is the vector corresponding to the ith row of M. The algorithm also chooses a random $t_0 \in Z_p$. The ciphertext is published as

$$CT_{\Gamma,m} = \big(C = d \cdot e(g, H(m))^{as}, C' = g^s,$$

$$C_1 = e(g^{a\lambda_1} g^{-t_1 s}, H(m)), ...C_l = e(g^{a\lambda_l} g^{-t_l s}, H(m))\big),$$

$\mathsf{Sig}(PK, SK_{A_i}, GID)$. The signature in represent of the authentication is generated:

$$Sig_{A_i,m} = H(m)^{t_i}$$

$\mathsf{Ver}(PK, m, Sig_{A_i,m}, PK_{A_i})$. The verification algorithm checks whether the following equation holds: $e(Sig_{A_i,m}, g) = (H(m), PK_{A_i})$, and outputs “valid” if it holds and otherwise “invalid”.

$\mathsf{Dec}(PK, CT_{\Gamma,m}, \{PK_{A_i} | A_i \in \mathcal{A}'\}, \{Sig_{GID,A_i} | A_i \in \mathcal{A}'\})$. Suppose $\mathcal{A}' \in \Gamma$ and $I = \{i : \rho(i) \in \mathcal{A}'\} = \{1, 2, \ldots, l\}$. According to the LSSS scheme[12], $\{\omega_i | i \in I\}$ can be calculated within polynomial time which satisfy $\sum_{i \in I} \lambda_i \omega_i = s$. The decryption algorithm computes

$$\Pi_{i \in I}(e(C_i, H(m)) e(Sig_{GID,A_i}, C'))^{\omega_i} = e(g, H(m))^{as}$$

Then the algorithm obtains the data d by

$$d = C / e(g, H(m))^{as}$$

IV. Security and Privacy Evaluation

Definition 7. Security . We define our security on the basis of ASPIR as follows:

1) **Privacy for the data**: the Receiver can retrieve a data record only if he has a valid authorization to do so from the record owner.
2) **Privacy for the Receiver**: the Sender is convinced that the Receiver's query is authorized by the owner of the target DB record and don't know the exact index of the data is.
3) **Privacy for the Sender**: the Receiver cannot retrieve information about more than one record in each query.

4) **Privacy for the authorizer.** During the authorization course, each authorizer don't need to communicate with each other and don't know who gave the signature to the Receiver already. Even if part of the authorizer is corrupted, adversary could not forge authorization from other uncorrupted authorizers.

Theorem 1. In EABE, Privacy for the data, Sender and Authorizer is achieved under BDH assumptions.

Since the Signature used as the authorization is the same with the short signature from weil pairing [13]. The signature cannot be forged in a non-negligible advantage if the BDH assumption holds. During the KG and Sig the authorizer could run the algorithm separately, so the privacy of the authorizer could be guaranteed as the adversary could not get any information concerning with the private key of authorizers even if some of them were corrupted. Therefore, the privacy of authorizer could be reduced to the short signature as well.

For the Privacy of the data, we can reduce our scheme to the semantic security of the CPABE scheme proposed by Waters [10] in the following steps.

Suppose the receiver GID got the key_{GID} and $\{Sig_{GID,A_i}\}$ which $\{A_i|GID$ got the $Sig_{GID,A_i}\}$ does not satisfy the access structure Γ. Set $Sig_{GID,A_i} = H(GID)^{t_i} = H(x_i)^t$, $Key_{GID} = g^{\alpha}H(x)^a = g^{\alpha}g^{at}$, such x_i and t could be proved exist. According to this setting the C_i of ciphertext CT_{Γ} could be set as the $g^{a\lambda}H(x_i)^{-s}$. According to the CPABE [10], this privacy could be proved if the BDH assumption holds.

Since the receiver R must indicate the index i to the Sender S, EABE does not achieve the privacy for the Receiver. However, if the receiver generates a requirement for the data according to the ASPIR scheme this privacy could be achieved too. Since the ciphertext and the signatures in EABE are transmitted in an open network, we sacrifice the privacy for the receiver to achieve a more efficient scheme.

Anti-collusion attack. The EABE is resistant to collusion attack. Since the Authorizer could not forge the signature of others. The receiver could only get signatures from specific authorizers. As the signature is on the GID, more than one receiver cannot join their authorizations together to get a authorized set because during the course

$$\frac{e(C', Key_{GID})}{\Pi_{i\in I}(e(C_i, H(GID))e(Sig_{GID,A_i}, C'))^{\omega_i}}$$

GID is different so $e(g,g)^{\alpha s}$ could not be output through the calculation in collusion attack.

Theorem 2. In IEABE, Privacy for the data, Sender, Receiver and authorizer is fully achieved under BDH assumptions.

The privacy for data, sender and authorizer is the same with EABE. Specifically, the authorization is distinct by the requirement message m in IEABE. For the privacy of the Receiver, an ASPIR query Q_{SPIR} is generated according to the index i and sent together $Policy||GID$ part. The Sender will generate $\{CT_{\Gamma,m_i}\}$, $m_i = GID||Policy||index_i$ for all the data entry in the database and execute the ASPIR scheme and return R_{SPIR} to the R, then R could retrieve the ciphertext he want by executing the ASPIR scheme again. The ASPIR scheme has provided a secure model for the privacy of the receiver.

Anti-collusion Attack. In IEABE, each authorization is based on a requirement m, which is distinctive in GID, $index$ and $Policy$. Therefore, the scheme also achieved the anti-collusion attack security.

Forward Security. If we set the $Policy$ as a time stamp on the valid period of authorization, then the scheme could also achieve the forward security which guarantee that the authorization could be of a period. This setting is useful in the real world since the sensitive data (daily profit) could be changing all the time. A data receiver could obtain the data of certain period, but not all the time. This function is achieved since the sender S will send an updated data d' according to new time stamp.

V. Performance analysis

Since the pairing operation can be reduced to a single exponentiation of size less than the group order as noted in [14], in this analysis we mainly focus on exponentiation operations of group.

In EABE, the ciphertext is generated once with reference to the access structure. The time of exponentiation operation is $2l + 2$; l is the number of rows of matrix M which is related to the access structure Γ . The authorization algorithm takes 2 times exponentiation operation each time. During the dec algorithm runs, it takes the $3l + 3$ times of calculation. So the total calculation for once success authorization to the data is approximately $7l$ times of exponentiation operation. This linear increasing cost is related to the size of the access structure, which is efficient in real practice. If pre-calculation mechanism is used for calculating the ciphertext, the cost for calculation could be optimized to $5l$ times.

In IEABE, the ciphertext is generated with the size of the database $|DB|$ and the best computation complexity for ASPIR achieved so far is $O(log^2(N))$ which is negligible. The computation cost is $(2|DB|+6)l$ times of exponentiation operation.

VI. Conclusion

This paper proposed two access control protocols EABE and IEABE for private information retrieval based on an extension in attribute based encryption. In EABE, authorizer could authorize the data receiver to retrieve the data belonging to them. While in IEABE, authorizers have more control rights over the data and could authorize the data receiver with specific data he owns instead of providing the access right to all the data. The two schemes are both resist to the collusion attacks and are efficient and practical.

References

[1] Brands, S.: Rethinking Public key Infrastructures and Digital Certificate: Building in Privacy. The MIT Press(2000)

[2] Camenishch, J., Lysyanskaya, A.: Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation. In: Advances in Cryptology-EuroCrypt'01. Volume 2045 of LNCS., Springer Verlag (2002) 93-118
[3] Golle, P., McSherry, F., Mironov, I.: Data collection with self-enforcing privacy. In: ACM Conference on Computer and Communications Security. (2006) 69C78
[4] Layouni,M.: Acredited symmetrically private information retrieval. In Miyaji, A., Kikuchi, H., Rannenberg, K., eds.: IWSEC. Volume 4752 of Lecture Notes in Computer Science., Springer (2007) 262-277
[5] Mohamed Layouni, Maki Yoshida, Shinago Okamura.: Efficient Multi-Authorizer Accredited Symmetrically Private Information Retrieval. Information and Communications Security(Proceedings of the 10th International ICICS Conference, Birmingham, UK, 2008) (UK) 387-393
[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and Communications Security (CCS'06), pages 89-98, 2006.
[7] Dan Boneh, Xavier Boyen, and Eu-Jin Goh. Hierarchical identity based encryption with constant size ciphertext. In EUROCRYPT, pages 440C456, 2005.
[8] A. Sahai and B. Waters. Fuzzy Identity Based Encryption. In Advances in Cryptology - Eurocrypt, volume 3494 of LNCS, pages 457-473. Springer, 2005.
[9] Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy, IEEE Computer Society (2007)321-334
[10] Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy, IEEE Computer Society (2007)321-334
[11] Chase, M.: Multi-authority attribute based encryption. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 515C534. Springer, Heidelberg (2007)
[12] Amos Beimel. Secure Schemes for Secret Sharing and Key Distribution. PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.
[13] D Boneh, B Lynn, H Shacham:Short signatures from the Weil pairing.Journal of Cryptology, 2004 Volume 17, Number 4 297-319
[14] Boyen, X.: A promenade through the new cryptography of bilinear pairings. In: IEEE Information Theory WorkshopłITW 2006, IEEE Press (2006) 19C23