International Journal of Future Generation Communication and Networking
Vol. 9, No. 1 (2016), pp. 285-302
http://dx.doi.org/10.14257/ijfgcn.2016.9.1.25

Oblivious Transfer with Fine Grained Access Control from Ciphertext Policy Attribute Based Encryption in the Standard Model

Xingbing Fu[1], Fagen Li[1] and Shengke Zeng[2]

[1] *School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan, P.R.China*
[2] *School of Mathematics and Computer Engineering, Xihua University, Chengdu, Sichuan, P.R.China*
Corresponding author: Xingbing Fu,
E-mail: uestcfuxb@126.com

Abstract

In this work, an oblivious transfer with complex access control scheme that is constructed based on ciphertext policy attribute based encryption (CP-ABE) scheme is proposed. In this scheme, the database server can enforce fine grained access control for each record where the authorized user is allowed to access, but the unauthorized user cannot, whereas it learns neither which record a user accesses, nor which attributes a user has. This scheme has the advantages as follows: First, it allows the expressive access control policies where access structures are based on linear secret sharing scheme that directly supports AND, OR and Threshold gates. Second, the communication complexity in this scheme is constant in the numbers of records which have been accessed. Third, this scheme is constructed in prime order bilinear group. Fourth, this scheme is secure in the standard model. To the best of our knowledge, this scheme is the first to obtain these features simultaneously.

***Keywords**: Access Control, Ciphertext Policy Attribute Based Encryption, Encrypted Database, Oblivious Transfer, Privacy, Standard Model*

1. Introduction

Electronic transactions such as accessing medical records or financial data require that access to these resources should be protected and the information which datum item is accessed is sensitive. Hence, it is necessary that these transactions should be protected, such that the following requirements are met: (1). The privacy of users is preserved, that is to say, the service provider is oblivious to which user accesses which datum item;(2). The service provider ensures that the only users who possess the sufficient attributes are authorized to access the data. With the advent of cloud computing, outsourcing sensitive information to cloud makes these requirements more compelling. To preserve the users' privacy and let the service provider (database) enforce access control mechanism, cryptographers proposed oblivious transfer with access control to solve the aforementioned requirements.

To enable one to securely share data over an insecure network, encryption techniques are employed. In the symmetric cryptography setting, if the two users communicate the sensitive data, they need to hold the same secret key. It is acceptable for some small organizations. With the advent of Internet, the above solution becomes infeasible. To solve the key distribution problems in the symmetric cryptosystem, Diffie and Hellman proposed the public key cryptosystem in which any two parties can securely share the sensitive data without having a mutually held secret key. The symmetric cryptosystem

ISSN: 2233-7857 IJFGCN

and the traditional public key cryptosystem both have the drawbacks as follows: (1) Encryption is a mechanism to send a message to a single recipient possessing a secret key, communication model is one-to-one. (2)Access to the encrypted data is all or nothing-a user is either able to decrypt and obtain the entire plaintext or he learns nothing at all about the plaintext except for its length. With the advent of cloud computing, where there exist a large number of users, the traditional public key cryptosystem is insufficient. For instance, the data owner may want to share the sensitive data under some policy based on the recipient's credentials or attributes, such that only the users satisfying the policy can decrypt. The traditional public key cryptosystem cannot handle such tasks.

Sahai A. and Waters B. (2005) [1] first proposed the Attribute Based Encryption (ABE) scheme to handle the aforementioned problem. Since the Attribute Based Encryption scheme is proposed, different ABE schemes are presented in terms of flexibility, efficiency, and security. Existing ABE schemes are classified as Key Policy ABE (KP-ABE) schemes [2-3] and Ciphertext Policy ABE (CP-ABE) schemes [4-5]. In KP-ABE schemes, keys are associated with access policies, and ciphertexts are identified with attribute sets. If and only if the keys associated with access policies which are satisfied by the attributes associated with the ciphertexts are able to decrypt the ciphertexts. In CP-ABE schemes, access policies are associated with the ciphertexts and keys are associated with attributes. If and only if keys associated with attributes that satisfy the access policy associated with the ciphertext are able to decrypt it. In all of CP-ABE schemes known so far, only a CP-ABE scheme due to Waters B. [6] is both expressive and is proven secure under a standard assumption in the standard model in prime order bilinear group. Our scheme builds on this scheme.

Our contribution. In this work, we combine expressive ciphertext policy attribute based encryption scheme with oblivious transfer scheme to achieve complex access control over the encrypted records of the database and users' privacy preserving. To the best of our knowledge, we are the first to achieve the four advantages simultaneously as follows: first, it allows the expressive access control policies that directly supports AND, OR and Threshold gates. Second, the communication complexity in our scheme is constant in the numbers of records which have been accessed. Third, our scheme is based on prime order bilinear group. Fourth, our construction is secure in the standard model.

Organization. The remainders of our paper are organized as follows: We discuss related work in section 2. We introduce preliminaries in section 3. We present scheme definition, security model in section 4. We present the construction of scheme in section 5. Security is proved in section 6. Performance is evaluated in section 7. We conclude and specify the future work in section 8.

2. Related Work

Coully S. [7-8] are the first to propose oblivious transfer with access control using state graphs where the users obtain credentials which bind them to a particular state in the graph. Their scheme enforces access control by limiting the possible transitions between states. This scheme has the following advantages: (1). It is suitable for different oblivious transfer schemes; 2.The access control policies are allowed to be changed on condition that the database is not changed. However, their scheme has the drawbacks as follows: (1).Each time the database is accessed by a user, a new credential must be obtained by the user. (2).This scheme cannot efficiently express a large class of access control policies based on state graphs. Camenisch J. [9] proposed an oblivious transfer with access control where each user can obtain a credential which certifies whether the user has some attributes employed to describe each record of data, and a user can access the record if and only if the user has these attributes, which makes access policies only support AND logical gate. To support access policy in disjunctive form, the database server needs to replicate the record, which makes the size of database increased. Additionally, to directly support access policy in disjunctive form, Zhang [10] proposed oblivious transfer with access control that realizes disjunction without duplication. Their scheme builds on adaptively secure attribute based encryption scheme presented by Lewko A. [11]. Unfortunately, their scheme [11] is based on composite order bilinear group resulting in some efficiency loss, and the security of their scheme [11] is based on the generic group model. Zhang [10]' scheme inherits the same limitation as Lewko A. [11]' scheme. Moreover, their scheme [10] does not carry out key validity check and ciphertext validity check. If the issuer and the database are malicious, the two users who have the same attributes may decrypt the same ciphertext to the different plaintexts, which violates anonymity of the users.

3. Preliminaries

3.1. Bilinear Map

Let $\mathbf{G}$ and $\mathbf{G}_{\mathrm{T}}$ be two cyclic groups of prime order p, and g, h are a generator of $\mathbf{G}$ respectively. e is a bilinear map $e:\mathbf{G}\times\mathbf{G}\rightarrow\mathbf{G}_{\mathrm{T}}$ 1,which has the following properties:

Bilinearity: for any $a,b\in\mathbf{Z}_p$ $e(g^a,h^b)=e(g,h)^{ab}$ .Nondegenerate: $e(g,g)\neq 1_{\mathbf{G}_{\mathrm{T}}}$, $e(g,g)$ is a generator of $\mathbf{G}_{\mathrm{T}}$ .If the group operation on $\mathbf{G}$ and on the bilinear map $e:\mathbf{G}\times\mathbf{G}\rightarrow\mathbf{G}_{\mathrm{T}}$]are efficiently computable, then $\mathbf{G}$ is a bilinear group. Our scheme employs the symmetric bilinear map that has the following properties:

$$e(g^a,h^b)=e(g,h)^{ab}=e(g^b,h^a)$$

3.2. Access Structure

Access Structure (Beimel A.) [12]. Let S denote the attribute universe. An access structure on S is a collection $\mathbf{A}$ of non-empty subsets of attributes, i.e. $\mathbf{A}\subseteq 2^{\mathrm{S}}\setminus\{\}$ .The sets in $\mathbf{A}$ are called the authorized sets, and the sets not in $\mathbf{A}$ are called the unauthorized sets. Specifically, an access structure is called monotone if $\forall B,C$: if $B\in\mathbf{A}$ and $B\subseteq C$, then $C\in\mathbf{A}$. In our scheme, we only deal with monotone access structure.

3.3. Linear Secret Sharing Scheme

A secret sharing scheme $\sum$ over a set of attributes is called linear over $\mathbf{Z}_p$ if 1.The shares for each attribute of a secret $s\in\mathbf{Z}_p$ form a vector over $\mathbf{Z}_p$ .2.There is a matrix M with h rows and d columns named the share generating matrix for $\sum$. For any $i=1,\cdots,h$, we let the function φ defined the attribute labeling row i as $\varphi(i)$. When we consider the column vector $\vec{v}=(s,x_2,\ldots,x_n)^T$, where T is the transpose of the vector, s is the secret to be shared, and $x_2,\ldots,x_n\in\mathbf{Z}_p$ are uniformly at random chosen, then $M\vec{v}$ is the vector of h shares of the secret s according to $\sum$ .The share $(M\vec{v})_i$ belongs to attribute $\varphi(i)$.

Let $S\in\mathbf{A}$ be any authorized set, and let $I=\{i:i\in\{1,\cdots,h\}\wedge\varphi(i)\in S\}$ .Then, there exist constants $\{\eta_i\in\mathbf{Z}_p\}_{i\in I}$ such that, if $\{s_i\}_{i\in I}$ are valid shares of any secret s according to $\sum$, then $\sum_{i\in I}\eta_i s_i=s$. These constants $\{\eta_i\in\mathbf{Z}_p\}_{i\in I}$ can be found in time polynomial in the size of the share generating matrix M . For unauthorized sets, there do not exist no such constants.

3.4. Complexity Assumptions

Definition 3.4.1 l-Strong Diffie-Hellman assumption [13] holds in the bilinear group $\mathbf{G}$ provided that for any **PPT** adversary $\mathbf{A}$, the advantage $Adv_G^{lSDH}(k) = \Pr\{A(g, g^{\alpha}, ..., g^{\alpha^l}) = (j, g^{1/(\alpha+j)})\}$ is negligible in the security parameter κ, in which $g \xleftarrow{\$} \mathrm{G}^*$ and $\alpha, j \xleftarrow{\$} \mathbf{Z}_p$.

Definition 3.4.2 The decisional l-bilinear Diffie-Hellman exponent (l-BDHE) assumption [14] holds in the bilinear group $\mathbf{G}$ and the target group $\mathbf{G}_\mathrm{T}$ provided that for any **PPT** adversary $\mathbf{A}$, the advantage

$$Adv_{\mathbf{G},\mathbf{G}_T}^{lBDHE}(k) = \Pr\{A(g,u,g^{x},...,g^{x^{l-1}},g^{x^{l+1}},...,g^{x^{2l}},e(g,u)^{x^l}) - \Pr\{A(g,u,g^{x},...,g^{x^{l-1}},$$
$$g^{x^{l+1}},...,g^{x^{2l}},H\}) = 1\}$$

is negligible in the security parameter κ, in which $g, u \xleftarrow{\$} \mathrm{G}^*$, $H \xleftarrow{\$} \mathrm{G}_T^*$ and $x \xleftarrow{\$} \mathbf{Z}_p$.

Definition 3.4.3 The l-power decisional Diffie-Hellman (l-PDDH) assumption[15] holds in the bilinear group $\mathbf{G}$ and the target group $\mathbf{G}_\mathrm{T}$ provided that for any **PPT** adversary $\mathbf{A}$, the advantage $Adv_{\mathbf{G},\mathbf{G}_T}^{lPDDH}(k) = \Pr\{A(u,u^x,...,u^{x^l},Z,Z^x,Z^{x^2}...,Z^{x^l}) = 1\} - \Pr\{A(u,u^x,...,u^{x^l},Z,Z_1,Z_2...,Z_l) = 1\}$ is negligible in the security parameter κ, in which $u \xleftarrow{\$} \mathrm{G}^*$, $Z, Z_1, ..., Z_l \xleftarrow{\$} \mathrm{G}_T^*$ and $x \xleftarrow{\$} \mathbf{Z}_p$. l-BDHE assumption implies the l-PDDH assumption.

3.5. Ciphertext Policy Attribute Based Encryption

A CP-ABE scheme comprises the four algorithms as follows:

$ABE.Setup(\kappa, \mathbf{S}) \to (PP, MS)$. The setup algorithm takes in security parameter κ and the universe $\mathbf{S}$ of attributes, and outputs the public parameters PP and a master secret MS.

$ABE.\Pr iKeyGen(PP, MS, S) \to \Pr iKey_S$.The private key generation algorithm takes in the public parameters PP, the master secret MS and the attribute set S, and outputs a private key $\Pr iKey_S$.

$ABE.Encrypt(PP, m, \mathbf{A}) \to CT_{\mathbf{A}}$. The encryption algorithm takes in the public parameters PP, a message m and an access structure $\mathbf{A}$ over $\mathbf{S}$, and outputs a ciphertext $CT_{\mathbf{A}}$.

$ABE.Decrypt(PP, \Pr iKey_S, CT_{\mathbf{A}}) \to m$. The decryption algorithm takes in the public parameters PP, a private key $\Pr iKey_S$ and a ciphertext $CT_{\mathbf{A}}$. If the attribute set S associated with the $\Pr iKey_S$ satisfies the access structure $\mathbf{A}$ associated with a ciphertext $CT_{\mathbf{A}}$, then the decryption algorithm will decrypt $CT_{\mathbf{A}}$ to recover the message m, else returns the error symbol $\perp$.

Security Definition of CP-ABE.

Setup. The challenger runs the $ABE.Setup$ setup algorithm to generate the public parameters PP which is given to the adversary.

Phase 1.The adversary makes repeated queries for private keys associated with attribute sets $S_1,...,S_{q_1}$.

Challenge. The adversary submits two messages m_0 and m_1 with $|m_0|=|m_1|$, where $||$ denotes the message length. Furthermore, it submits a challenge access structure $\mathbf{A}^*$ with the restriction with none of the attribute sets $S_1,...,S_{q_1}$ from

Phase 1 satisfy the challenge access structure $\mathbf{A}^*$.The challenger tosses a random coin $\beta \in \{0,1\}$ and encrypts m_β under $\mathbf{A}^*$ to obtain the resulting ciphertext $CT^*_{\mathbf{A}} = ABE.Encrypt(PP, m_\beta, \mathbf{A}^*)$ which is passed on to the adversary.

Phase 2. Phase 1 is repeated except that the challenge access structure $\mathbf{A}^*$ is satisfied by none of the attribute sets $S_{q_1+1},...,S_q$.

Guess. The adversary outputs a guess of β' for β.

The advantage of an adversary $\mathbf{A}$ in this game is defined as $\Pr\{\beta'=\beta\}-\frac{1}{2}$.

The model is secure against chosen ciphertext attacks by allowing for decryption oracles in phase 1 and phase 2.

Definition 3.5.1. A CP-ABE scheme is secure if no PPT adversary has non-negligible advantage in the aforementioned game.

3.6. Zero Knowledge Proofs

In a zero-knowledge proof of knowledge, a prover proves a statement to a verifier without revealing anything about the statement other than its veracity. We employ the notation introduced by Cramer R. et.al. [16]. For example, $POK\{(\gamma,\lambda,\tau): y = g^\gamma u^\lambda \wedge y = \overset{\gamma}{g}\ \overset{\tau}{u}\}$ denotes a "zero knowledge Proof of Knowledge of integers γ,λ,τ such that $y = g^\gamma u^\lambda$ and $y = \overset{\gamma}{g}\ \overset{\tau}{u}$ holds, in which g and u are a generator of the group G, respectively, and g and u are a generator of the group G,respectively. Variables in the parenthesis denote which knowledge is proven about, whereas all other values are known to the verifier.

3.7. Fully Simulatable Oblivious Transfer

We employ the fully simulatable adaptive oblivious transfer protocol due to Camenisch J. et.al. [15] , in which a sender possesses N messages, of which a recipient can adaptively pick to receive k one after the other, such that the sender learns nothing about the recipient's choices, and the receiver only learns about the k requested messages, whereas the remaining messages are hidden from the recipient.

4. Definitions

4.1. Scheme Overview

An oblivious transfer protocol with complex access control from ciphertext policy attribute based encryption is run between an issuer that sets up the system and generates the private keys of users; one database that hosts the list of records, generates the encrypted records by employing CP-ABE schemes and allows users to access the records which they are entitled to access; and users that anonymously fetch records that are entitled to access.

4.2. Scheme Definition

An adaptive oblivious transfer with complex access control from ciphertext policy attribute based encryption (OTAC-ABE) comprises the algorithms as follows:

$IssuerSetup(1^{\kappa}, \mathrm{S}) \rightarrow (PP, MS)$: The issuer runs this algorithm which takes in the security parameter 1^{κ} and the universe S of attributes and outputs a public parameter PP and MS.

$Issue$: A user engages in the **Issue** protocol with the issuer to generate credentials $Cred_S$ for attribute sets S .The common inputs are the issuer's public parameter PP and the attribute sets S . The issuer's input is her master secret MS . At the end of the protocol, the user obtains the private key as the access credentials

$$Cred_S = \Pr iKey_S = ABE.\Pr iKeyGen(PP, MS, S).$$

$ABE.\Pr iKeySanityCheck(PP, \Pr iKey_S) \rightarrow \{Valid, Invalid\}$: The user runs this algorithm to test whether $\Pr iKey_S$ is valid. It takes in public parameter PP and $\Pr iKey_S$, and outputs $Valid$ or $Invalid$.

$DataBaseSetup(PP, DB = (R_j, \mathbf{A}_j)_{j=1,...,n}) \rightarrow ((PK_{DB}, ER_1, ..., ER_n), (\Pr iKey_{DB}))$: The $DataBaseSetup$ algorithm is run by the database server to initiate a database which contains records R_j protected by access structure $\mathbf{A}_j (j = 1,...,n)$, respectively. This algorithm generates a public key PK_{DB} and the encrypted records $ER_j (j = 1,...,n)$, which is available to all users. The database server keeps the private key $\Pr iKey_{DB}$ for itself.

$ABE.CiphertextSanityCheck(PP, CT) \rightarrow \{Valid, Invalid\}$: The user runs this algorithm to test whether CT is valid. It takes in public parameter PP and CT , and outputs $Valid$ or $Invalid$. If $ABE.\Pr iKeySanityCheck$ and $ABE.CiphertextSanityCheck$ pass, ABE scheme is called the committing ABE scheme that ensures that if the two users possess the same attributes, then they can decrypt the same ciphertext to the same plaintext.

$Transfer$: A user engages in a Transfer protocol with the database server when a user wishes to access a record in the database. The issuer's PP and PK_{DB} of database are common inputs. The user's input is choice index $\sigma \in \{1,...,n\}$ and the credentials $Cred_S$. The private input of the database is $\Pr iKey_{DB}$. At the end of the protocol, the user obtains the record R_σ if the protocol is successfully executed, else an error symbol $\perp$ is returned.

4.3. Definition of Security

Security of an OTAC-ABE protocol is defined through indistinguishability of a real world and an ideal world experiment (Canetti. R.[17]). In the real world, there exist many players running some cryptographic protocols with each other, an adversary A including the dishonest players controlling some of the players, and an environment $\mathbf{E}$ providing the inputs to the honest players, receiving their outputs and interacting with the adversary arbitrary.

In the ideal world, there exist the same players which do not run cryptographic protocols but send their inputs to and receive their outputs from an ideal fully-trusted party $\mathbf{T}$ that applies the functionality that the cryptographic protocols can realize, an adversary including the dishonest players, and an environment $\mathbf{E}$ providing the inputs to, receiving the outputs from the honest players, and interacting arbitrarily with the adversary.

Cryptographic protocol set can securely implement a functionality if for every environment $\mathbf{E}$ and for every real world adversary A there exists an ideal world simulator A^* which controls the same parties in the ideal world as A does in the real world in such a way that the environment is not able to distinguish whether it is run in the real world interacting with A or whether it is run in the ideal world interacting with the simulator A^*.

Real world. Only can the users return the result to the environment $\mathbf{E}$, whereas the issuer and the database output nothing to the environment $\mathbf{E}$.

1. The issuer runs the $IssuerSetup(1^{\kappa}, \mathrm{S})$ to generate (PP, MS) and publishes PP.
2. The environment $\mathbf{E}$ sends the database $DBase$ a message $(Initializedatabase, DB = (R_j, A_j)_{j=1,...,n})$. To encrypt DB , $DBase$ runs $DataBaseSetup(PP, DB = (R_j, \mathbf{A}_j)_{j=1,...,n}) \to ((PK_{DB}, ER_1, ..., ER_n), (\mathrm{Pr}\, iKey_{DB}))$, and sends the encrypted database $(PK_{DB}, (ER_1, ..., ER_n))$ to user $U_c (c = 1, ..., C, C \in \mathbf{N})$.
3. The user U_c engages in an **Issue** protocol with the issuer I when $\mathbf{E}$ sends a message $(issue, S)$ to user U_c. At the end of the protocol, U_c obtains the credential $Cred_S$ for attribute set S . U_c sends back a bit β to the environment indicating this protocol succeeded $\beta = 1$ or failed $\beta = 0$ .If $\beta = 1$, the user U_c will obtain credentials $Cred_S$ for S .
4. The user U_c checks whether he has the credentials $Cred_S$ for attribute set S satisfying the access structure $\mathbf{A}$ when $\mathbf{E}$ sends a message $(transfer, \sigma)$. If so, he engages in a **Transfer** protocol with the database. If this protocol succeeded, he sends back R_σ to $\mathbf{E}$. If it failed, he sends back $\perp$ to the environment.

Ideal World. Here all participants communicate via a trusted party $\mathbf{T}$ implementing the functionality of OTAC-ABE protocol. The ideal world users U_c^*, issuer I^* and database $Dbase^*$ relay inputs and outputs between the trusted party $\mathbf{T}$ and the environment $\mathbf{E}$. $\mathbf{T}$ maintains a set of attributes S_c that is initially empty for each user U_c^* and sets $DB \leftarrow \perp$.

1. When $\mathbf{T}$ receives $(issue, S)$ from U_c^*, it sends $(issue, U_c^*, S)$ to I^* that returns a bit β. If $\beta = 1$, then adds S to $S_{U_c^{'}}$ and sends β to U_c^*, else sends β to U_c^*.
2. When $\mathbf{T}$ receives $(Initializedatabase, DB = (R_j, A_j)_{j=1,...,n})$ from U_c^* , $\mathbf{T}$ sets $DB = (R_j, \mathbf{A}_j)_{j=1,...,n}$.
3. When $\mathbf{T}$ receives $(transfer, \sigma)$ from $U_c^{'}$, if $DB \neq \perp$, it sends **transfer** to $Dbase^*$ that returns a bit β. If $\beta = 1$ and $\mathbf{T}$ checks whether $\sigma \in [1, ..., n]$

and $S_{U_c^*}$ satisfies the access structure $\mathbf{A}_\sigma$. If so, $\mathbf{T}$ sends the user U_c^* the record R_σ, else it returns $\perp$ to U_c^*.

5. Construction

In this construction, a ciphertext policy attribute based encryption scheme is combined with simulatable adaptive oblivious transfer to achieve oblivious transfer with fine grained access control in the standard model. We employ hybrid encryption to design a new ciphertext policy attribute based encryption scheme that supports the same expressive access structure as the original CP-ABE scheme. This scheme is implemented via combining the underlying CP-ABE scheme with data encapsulation mechanism (DEM) (Herranz, J..[18]). We employ this new CP-ABE scheme combined with simulatable adaptive oblivious transfer to achieve oblivious transfer with fine grained access control in the standard model. Our construction is as follows:

$IssuerSetup(1^\kappa, \mathrm{S}) \to (PP, MS)$: On input the security parameter 1^κ and the universe of system attributes S, the issuer runs $ABE.Setup$ algorithm to generate a bilinear group $\mathbf{G}$ of prime order p with a generator g, a bilinear map $e: \mathbf{G} \times \mathbf{G} \to \mathbf{G}_\mathrm{T}$ 1 and random exponents $\mu, \theta, t_k \in \mathbf{Z}_p (1 \le k \le |\mathrm{S}|)$,and sets $T_k = g^{t_k} (1 \le k \le |\mathrm{S}|)$. The public parameter PP is published as $PP = (g, e(g,g)^\mu, g^\theta, \{T_k = g^{t_k} (1 \le k \le |\mathrm{S}|)\})$. The master secret MS is $MS = g^\mu$.

$DataBaseSetup(PP, DB = (R_j, \mathbf{A}_j)_{j=1,\ldots,n}) \to ((PK_{DB}, ER_1, \ldots, ER_n), (\mathrm{Pr}\,iKey_{DB}))$:

The database employs the bilinear group generator to create a bilinear map $\overset{\frown}{e}: \mathbf{G} \times \mathbf{G} \to \mathbf{G}_T$, where $\mathbf{G}$ and $\mathbf{G}_T$ are of the same prime order p , and $\mathbf{G}$ and $\mathbf{G}_T$ may not be identical to $\mathbf{G}$ and $\mathbf{G}_\mathrm{T}$, respectively . It picks u, f at random from $\mathbf{G}$ and picks $\alpha \in \mathbf{Z}_p$ at random. It computes $F = \overset{\frown}{e}(u, f)$ and $y = u^\alpha$ .For each $j = 1, \ldots, n$, $DataBaseSetup$ algorithm computes $C_j = (A_j, B_j)$,in which $A_j = u^{1/(\alpha + j)}$,and $B_j = \overset{\frown}{e}(A_j, f) R_j$. It sets the private key $\mathrm{Pr}\,iKey_{DB} = (f, \alpha)$ and publishes

$$PK_{DB} = (\overset{\frown}{e}, \mathbf{G}, \mathbf{G}_T, p, u, y, F).$$

For each $j = 1, \ldots, n$, it parses the access structure $\mathbf{A}_j (j = 1, \ldots, n)$ as $A_j = (M_j, \varphi_j)$, in which M_j is an $h \times d$ matrix , φ_j is a map that associates rows of M_j to attributes, where φ_j is limited to an injective function, i.e., an attribute is associated with at most one row of M_j. It picks content key K_j from $\mathbf{G}_T$ at random and a random vector $\overrightarrow{v_j} = (s_j, x_{j,2}, \ldots, x_{j,n})^T \in \mathbf{Z}_p^n$ that is employed to share the secret encryption expenent s_j . For $i = 1, \ldots, h$, it computes $s_{j,i} = M_{j,i} \overrightarrow{v_j}$, where $s_{j,i}$ is the shares of s_j and $M_{j,i}$ is the vector corresponding to the i^{th} row of M_j . It computes $D_{j,1} = ((M_j, \varphi_j(i)), E_j = K_j \square e(g,g)^{\mu s_j}, E_{j,b} = g^{s_j}, E_{j,i} = g^{\theta s_{j,i}} T_{\varphi_j(i)}^{-s_j})$ and $D_{j,2} = DEM.Encrpt(K_j, A_j \| B_j)$.

The database server publishes $(ER_j)_{j=1,\ldots,n} = (D_j = (D_{j,1}, D_{j,2}), \mathbf{A}_j)_{j=1,\ldots,n}$.

Issue: To make database queries, a user wants to obtain the credentials for the attribute set satisfying the access structure $\mathbf{A}_j (j=1,...,n)$. Hence, the **Issue** protocol is run between the user and the issuer as displayed in Figure 1. The flag f_I that is initially equal to 0 is sent to the issuer by the user. If f_I is equal to 0, then the issuer sends the user a proof of knowledge $POK\{(\mu): e(g,g)^{\mu}\}$. $f_I = 1$ is updated by the user who sends the attribute set S to the issuer.The issuer picks a random $r_j \in \mathbf{Z}_p$, and creates the private key as follows:

$$\Pr iKey_S = (K_{j,b,1} = g^{\mu} g^{\theta r_j}, K_{j,b,2} = g^{r_j}, \{K_{j,x} = g^{r_j t_x}\}_{x\in S}).$$

It outputs the private key $\Pr iKey_S$ as credentials which are sent to the user.

$ABE.\Pr iKeySanityCheck(PP, \Pr iKey_S) \to \{Valid, Invalid\}$: The user runs this algorithm to test whether $\Pr iKey_S$ is valid as follows:

$$e(K_{j,b,1}, g) = e(g^{\mu} g^{\theta r_j}, g) = e(g^{\mu}, g) e(g^{\theta r_j}, g) = e(g,g)^{\mu} e(g^{\theta}, g^{r_j}) = e(g,g)^{\mu} e(g^{\theta}, K_{j,b,2})$$

$$\forall x \in S, e(K_{j,x}, g) = e(T_x, K_{j,b,2}).$$

If the aforementioned checks pass, the $ABE.\Pr iKeySanityCheck$ algorithm outputs $Valid$, else outputs $Invalid$.

$ABE.CiphertextSanityCheck(PP, D_{j,1}) \to \{Valid, Invalid\}$: The user runs this algorithm to test whether $D_{j,1}$ is valid as follows:

If the attribute set S satisfies the access structure $\mathbf{A}_j (j=1,...,n)$, and let $\{\eta_{j,i} \in \mathbf{Z}_p\}_{\varphi_j(i)\in S}$ be constant set, then $\sum_{\varphi_j(i)\in S} \eta_{j,i} s_{j,i} = s_j$.

$$\prod_{\varphi_j(i)\in S} e(E_{j,i}, g)^{\eta_{j,i}} = \prod_{\varphi_j(i)\in S} e(g^{\theta s_{j,i}} T_{\varphi_j(i)}^{-s_j}, g)^{\eta_{j,i}} = e(g^{\theta \sum_{\varphi_j(i)\in S} \eta_{j,i} s_{j,i}}, g) \prod_{\varphi_j(i)\in S} e(T_{\varphi_j(i)}^{-s_j}, g)^{\eta_{j,i}}$$

$$= e(g^{\theta s_j}, g) \prod_{\varphi_j(i)\in S} e(T_{\varphi_j(i)}^{-1}, g^{s_j})^{\eta_{j,i}} = e(g^{\theta}, g^{s_j}) \prod_{\varphi_j(i)\in S} e(T_{\varphi_j(i)}^{-1}, g^{s_j})^{\eta_{j,i}}$$

$$= e(g^{\theta}, E_{j,b}) \prod_{\varphi_j(i)\in S} e(T_{\varphi_j(i)}^{-1}, E_{j,b})^{\eta_{j,i}}$$

If the aforementioned checks pass, the $ABE.CiphertextSanityCheck$ algorithm outputs $Valid$, else outputs $Invalid$.

Transfer: The user employs the $ABE.Decrpt$ algorithm to compute

$$E_j / ((E_{j,b}, K_{j,b,1}) / (\prod_{\varphi_j(i)\in S} e(E_{j,i}, K_{j,b,2}) e(E_{j,b}, K_{j,\varphi_j(i)}))^{\eta_{j,i}})$$

$$= K_j \square e(g,g)^{\mu s_j} / ((e(g,g)^{\mu s_j} e(g,g)^{\theta s_j r_j} / \prod_{\varphi_j(i)} e(g,g)^{\theta r_j s_{j,i} \eta_{j,i}}))$$

$$= K_j \square e(g,g)^{\mu s_j} / e(g,g)^{\mu s_j} = K_j$$

Then it computes $(A_{\sigma}, B_{\sigma}) = DEM.Decrypt(K_j, D_{j,2})$.

The user engages in a **Transfer** protocol with the database server when he hopes to access a record in the database as depicted in Figure 2. The user picks $\omega \in \mathbf{Z}_p$ at random and computes $W = A_{\sigma}^{\omega}$. The user sends the database server W, together with a zero knowledge proof of knowledge $POK\{(\sigma,\omega):\hat{e}(W,y)=\hat{e}(W,u)^{-\sigma}\hat{e}(u,u)^{\omega}\}$ .If the database server accepts the proof, and computes $V=\hat{e}(f,W)$. The database server sends the user F , together with a zero knowledge proof of knowledge $POK\{(f):F=\hat{e}(u,f)\wedge V=\hat{e}(f,W)\}$.The user obtains $R_{\sigma}=B_{\sigma}/V^{1/\omega}$.

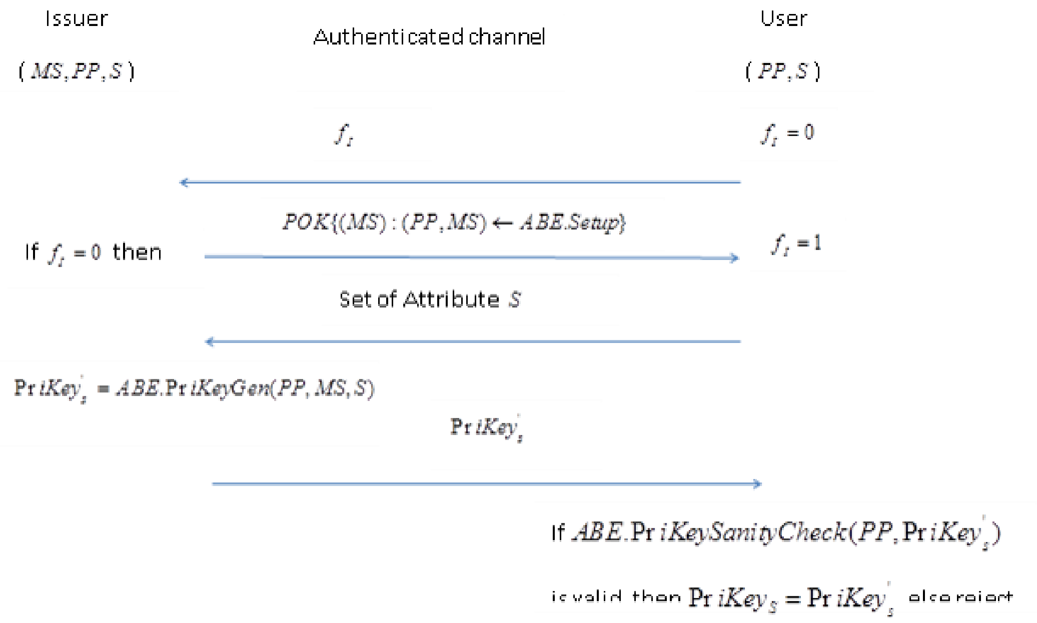
Issuer
Authenticated channel
User
(MS, PP, S)
(PP, S)
f_I
$f_I = 0$
$POK\{(MS):(PP,MS)\leftarrow ABE.Setup\}$
If $f_I = 0$ then
$f_I = 1$
Set of Attribute S
$\Pr iKey_S' = ABE.\Pr iKeyGen(PP, MS, S)$
$\Pr iKey_S'$
If $ABE.\Pr iKeySanityCheck(PP, \Pr iKey_S')$
is valid then $\Pr iKey_S = \Pr iKey_S'$ else reject

Figure 1. Issuer Protocol

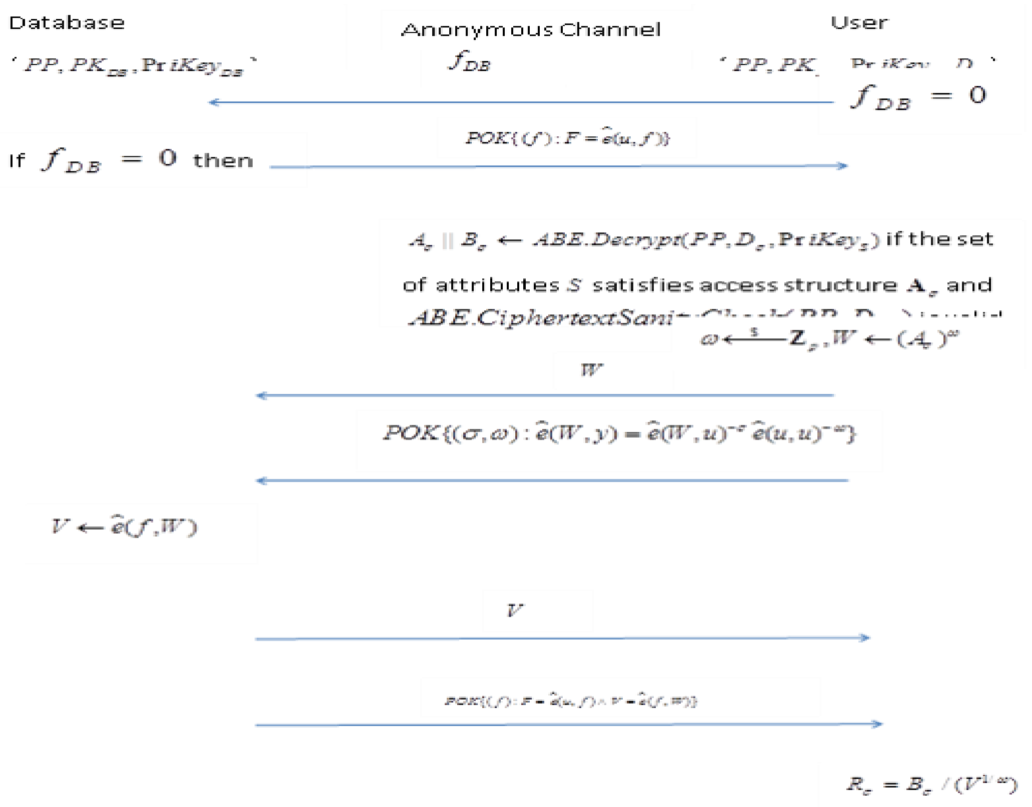
Database
Anonymous Channel
User
($PP, PK_{DB}, \Pr iKey_{DB}$)
f_{DB}
(PP, PK
$\Pr iKey$ D)
$f_{DB} = 0$
$POK\{(f):F=\hat{e}(u,f)\}$
If $f_{DB} = 0$ then
$A_{\sigma} \| B_{\sigma} \leftarrow ABE.Decrypt(PP, D_{\sigma}, \Pr iKey_S)$ if the set
of attributes S satisfies access structure $\mathbf{A}_{\sigma}$ and
$ABE.CiphertextSani$
$\omega \xleftarrow{\$} \mathbf{Z}_p, W \leftarrow (A_{\sigma})^{\omega}$
W
$POK\{(\sigma,\omega):\hat{e}(W,y)=\hat{e}(W,u)^{-\sigma}\hat{e}(u,u)^{-\omega}\}$
$V \leftarrow \hat{e}(f,W)$
V
$POK\{(f):F=\hat{e}(u,f)\wedge V=\hat{e}(f,W)\}$
$R_{\sigma} = B_{\sigma}/(V^{1/\omega})$

Figure 2. Transfer Protocol

6. Proof of Security

We analyze the security of the proposed protocol via proving indistinguishability between adversary actions in the real world and in the ideal world. Given a real world attacker A, an ideal-world attacker A^* is constructed in such a way that no environment $\mathbf{E}$ can distinguish whether it is interacting with A or A^*. We organize the proof in the following lemmas based on which parties are corrupted. The cases are not considered as follows: all parties are honest or dishonest, and the issuer is the only honest or dishonest party, since they have no real practical interest. For the remaining each case, we define a sequence of hybrid games Game-0,…, Game-N to prove the indistinguishability between the real and ideal worlds. In each game we define a simulator $Sim_c(c=0,...,n)$ which runs A as a subroutine and that provides the entire view of the environment. $Hybrid_{\mathbf{E},Sim_c}$ is defined as the probability that $\mathbf{E}$ outputs 1 when run in the world provided by Sim_c. We can construct the games such that it holds that $Hybrid_{\mathbf{E},Sim_0}(\kappa)=\mathrm{Re}\,al_{\mathbf{E},Sim_0}(\kappa)$ and $Hybrid_{\mathbf{E},Sim_n}(\kappa)=Ideal_{\mathbf{E},Sim_n}(\kappa)$. An upper bound for $\mathrm{Re}\,al_{\mathbf{E},A}(\kappa)-Ideal_{\mathbf{E},A^*}(\kappa)$ can be obtained by summing $Hybrid_{\mathbf{E},Sim_c}(\kappa)-Hybrid_{\mathbf{E},Sim_{c+1}}(\kappa)$ for $(c=0,...,n)$. $\nu_n(k)$ denotes a negligible function in k.

Theorem 1. The OTAC-ABE protocol described in section 5 securely implements the OTAC-ABE functionality under the security of the CP-ABE scheme, and if the $(n+1)BDHE$ assumption holds in $\mathbf{G}$ and $\mathbf{G}_T$ holds and $(n+1)SDH$ assumption holds in $\mathbf{G}$.

This theorem is proved via the four lemmas as follows:

Lemma 1. For any an environment $\mathbf{E}$ and any an attacker A which corrupts the database and the issuer, there exists an ideal world attacker A^* such that $\mathrm{Re}\,al_{\mathbf{E},A}(\kappa)-Ideal_{\mathbf{E},A^*}(\kappa)$ is negligible.

Proof. **Game-1:** This game is identical to **Game-0,** except that the knowledge extractor is employed to extract MS from the proof of knowledge $POK\{(MS):(PP,MS)\leftarrow ABE.Setup(1^{\kappa})\}$. Since the extraction event succeeds with all but negligible probability, it holds that $Hybrid_{\mathbf{E},Sim_0}(\kappa)-Hybrid_{\mathbf{E},Sim_1}(\kappa)\le\nu_1(\kappa)$.

Game-2: This game is identical to **Game-1,** except that all ill-formed ciphertexts checked via running $ABE.CiphertextValidityCheck$ must be rejected. The committing property of the CP-ABE scheme ensure that the same ciphertext will be decrypted to the same plaintext by employing any valid private keys if $ABE.CiphertextValidityCheck$ is valid. Hence, $Hybrid_{\mathbf{E},Sim_1}(\kappa)-Hybrid_{\mathbf{E},Sim_2}(\kappa)=0$.

Game-3: This game is identical to **Game-2,** except that at the first transfer query dictated by $\mathbf{E}$, the simulator Sim_3 runs the extractor for the proof of knowledge $POK\{(f):F=\widehat{e}(u,f)\}$ to extract the element f from the attacker A such that $F=\widehat{e}(u,f)$. Sim_3 will return $\perp$ to $\mathbf{E}$ if the extractor fails. Otherwise, it runs A interacting with the honest user. Under the knowledge error of the proof of knowledge, it holds that

$$Hybrid_{\mathbf{E},Sim_2}(\kappa) - Hybrid_{\mathbf{E},Sim3}(\kappa) \le \nu_3(\kappa).$$

Game-4: This game is identical to **Game-3,** except that during each transfer phase it lets the user query a record picked at random if the user possesses the private keys associated with the attribute sets satisfying the access structure. Under the perfect zero knowledge of the proof of knowledge of $POK\{(\sigma,W): \hat{e}(W,y) = \hat{e}(W,u)^{-\sigma}\hat{e}(u,u)^{\omega}\}$, it holds that $Hybrid_{\mathbf{E},Sim_3}(\kappa) - Hybrid_{\mathbf{E},Sim_4}(\kappa) = 0$.

According to the real world attacker A, an ideal world attacker A^* acting as the database and the issuer simultaneously and incorporating all steps from **Game-4** can be constructed. All messages are relayed between $\mathbf{E}$ and A by the attacker A^*. A^* runs A to obtain the issuer's public key PP and the encrypted database $ER_j(j=1,...,n)$. A^* acting as the user conducts the **issue** protocol with A when A^* receives (**issue,**U^***,** S) from $\mathbf{T}$. If the output of $KeyValidityCheck$ is valid, A^* sends $\beta = 1$ back to $\mathbf{T}$, else it sends $\beta = 0$ back to $\mathbf{T}$. When A^* receives a message **Transfer** from $\mathbf{T}$ for the first time, it runs the extractor of $POK\{(f): F = \hat{e}(u,f)\}$ to extract f from A. A^* employs the private key $\Pr iKey_S$ to decrypt $ER_j(j=1,...,n)$ to obtain $A_j \| B_j$, in which $B_j = \hat{e}(f, A_j)R_j$, A^* computes $R_j = B_j / \hat{e}(f, A_j)(j=1,...,n)$ and sends $\left(\text{InitializeDB}, R_j, \mathbf{A}_j\right)_{j=1,...,n}$ to $\mathbf{T}$. A^* simulates an honest user querying for record R picked at random with the access structure satisfied by the attribute set S. If the transfer query succeeds, A^* returns $\beta = 1$ to $\mathbf{T}$; if not, it returns $\beta = 0$ to $\mathbf{T}$. The remaining transfers are treated in the same way.

As you can see, A^* provides A with exactly the same environment as Sim_4. Hence, it holds that $Ideal_{\mathbf{E},A^*}(\kappa) = Hybrid_{\mathbf{E},Sim_4}(\kappa)$.

By summation, it holds that $\operatorname{Re}al_{\mathbf{E},A}(\kappa) - Ideal_{\mathbf{E},A^*}(\kappa) \le \nu_4(\kappa)$.

Lemma 2. For any an environment $\mathbf{E}$ and any an attacker A which only corrupts the database, there exists an ideal world attacker A^* such that $\operatorname{Re}al_{\mathbf{E},A}(\kappa) - Ideal_{\mathbf{E},A^*}(\kappa)$ is negligible.

Proof. **Game-1:** This game is identical to **Game-0,** except that at the first transfer query dictated by $\mathbf{E}$, the simulator Sim_3 runs the extractor for the proof of knowledge $POK\{(f): F = \hat{e}(u,f)\}$ to extract the element f from the attacker A such that $F = \hat{e}(u,f)$. Sim_1 will return $\perp$ to $\mathbf{E}$ if the extractor fails. Otherwise, it runs A interacting with the honest user. Under the knowledge error of the proof of knowledge, it holds that

$$Hybrid_{\mathbf{E},Sim_0}(\kappa) - Hybrid_{\mathbf{E},Sim_1}(\kappa) \le \nu_1(\kappa).$$

Game-2: This game is identical to **Game-1,** except that during each transfer phase it lets the user query a record picked at random if the user possesses the private keys associated with the attribute sets satisfying the access structure. Under the perfect zero knowledge of the proof of knowledge of $POK\{(\sigma,W): \hat{e}(W,y) = \hat{e}(W,u)^{-\sigma}\hat{e}(u,u)^{\omega}\}$, it holds that $Hybrid_{\mathbf{E},Sim_1}(\kappa) - Hybrid_{\mathbf{E},Sim_2}(\kappa) = 0$.

According to the real world attacker A, an ideal world attacker A^* only acting as the database and incorporating all steps from **Game-2** can be constructed. All messages are relayed between $\mathbf{E}$ and A by the attacker A^*. A^* runs A to obtain the issuer's public key PP and the encrypted database $ER_j(j=1,...,n)$. When A^* receives a message **Transfer** from $\mathbf{T}$ for the first time, it runs the extractor of $POK\{(f): F=\hat{e}(u,f)\}$ to extract f from A. A^* employs the private key $\Pr iKey_S$ to decrypt $ER_j(j=1,...,n)$ to obtain $A_j \| B_j$, in which $B_j=\hat{e}(f,A_j)R_j$, A^* computes $R_j=B_j/\hat{e}(f,A_j)(j=1,...,n)$ and sends $\left(\text{InitializeDB}, R_j, \mathbf{A}_j\right)_{j=1,...,n}$ to $\mathbf{T}$. A^* simulates an honest user querying for record R picked at random with the access structure satisfied by the attribute set S. If the transfer query succeeds, A^* returns $\beta=1$ to $\mathbf{T}$; if not, it returns $\beta=0$ to $\mathbf{T}$. The remaining transfers are treated in the same way.

As you can see, A^* provides A with exactly the same environment as Sim_2. Hence, it holds that $Ideal_{\mathbf{E},A^*}(\kappa)=Hybrid_{\mathbf{E},Sim_2}(\kappa)$.

By summation, it holds that $\mathrm{Re}\,al_{\mathbf{E},A}(\kappa)-Ideal_{\mathbf{E},A^*}(\kappa)\le \nu_2(\kappa)$.

Lemma 3. For any an environment $\mathbf{E}$ and any an attacker A which corrupts some of the users, there exists an ideal world attacker A^* such that $\mathrm{Re}\,al_{\mathbf{E},A}(\kappa)-Ideal_{\mathbf{E},A^*}(\kappa)$ is negligible.

Proof. To prevent the users from colluding their attributes, multiple users are considered.

Game-1: This game is identical to **Game-0,** except that a simulatable proof is employed to replace the proof of knowledge $POK\{(MS):(PP,MS)\leftarrow ABE.Setup(1^\kappa)\}$. According to the zero knowledge property of the proof system, it holds that $Hybrid_{\mathbf{E},Sim_0}(\kappa)-Hybrid_{\mathbf{E},Sim_1}(\kappa)\le \nu_1(\kappa)$.

Game-2: This game is identical to **Game-1,** except that at each transfer query, A queries a record R_σ from the database server in behalf of some user. A submits W, together with zero knowledge of proof of knowledge $POK\{(\sigma,\omega):\hat{e}(W,y)=\hat{e}(W,u)^{-\sigma}\hat{e}(u,u)^{\omega}\}$. If the extractor fails, then Sim_2 outputs $\perp$ to $\mathbf{E}$; else, it continues to run A interacting with the honest database server. Under the zero knowledge of the proof of knowledge, it holds that $Hybrid_{\mathbf{E},Sim_1}(\kappa)-Hybrid_{\mathbf{E},Sim_2}(\kappa)\le \nu_2(\kappa)$.

Game-3: This game is identical to **Game-2,** except that ω,σ have been extracted, Sim_3 calculates $A_\sigma=W^{1/\omega}$. If A has never queried the private key associated with the set of attributes S which satisfies $\mathbf{A}_\sigma$ and $A_\sigma=A_\sigma$, Sim_3 outputs $\perp$ to $\mathbf{E}$. If the underlying CP-ABE scheme is selectively secure and the $(n+1)SDH$ assumption holds. It holds that $Hybrid_{\mathbf{E},Sim_2}(\kappa)-Hybrid_{\mathbf{E},Sim_3}(\kappa)\le \nu_3(\kappa)$.

If Sim_3 obtains the right $\mathbf{A}_\sigma$ from A in such a way that the private key of CP-ABE scheme is not given to A, then A is employed to break the selective security of the underlying CP-ABE scheme. An attacker B can be constructed to win the break the selective security of the underlying CP-ABE scheme. B acts as the Sim_3 and has black box access to A.

The challenger runs $ABE.Setup(1^{\kappa}, \mathrm{S})$ to generate the public parameters PP which is given to B . B declares $\mathbf{A}_{\sigma}$ to the challenger. B calculates $A_j = u^{1/(\alpha+j)}$ and $B_j = \widehat{e}(f, A_j)R_j, j = 1,...,n$. B picks at random two elements $P_A \in \mathbf{G}$ and $P_B \in \mathbf{G}_T$. B sets $m_0 = A_{\sigma} \| B_{\sigma}$ and $m_1 = P_A \| P_B$. B submits m_0 and m_1. The challenger tosses a fair binary coin β and encrypts m_{β} to obtain the resulting ciphertexts $CT^* = Encrypt(PP, m_{\beta}, \mathbf{A})$ which is given to B . Here, B is no able to query the private key associated with attribute set satisfying the access structure. If A outputs A_{σ}, then B output $\beta' = 0$ as its guess; else output $\beta' = 1$. If $\beta = 0$, CT^* is the resulting ciphertext. This is the same as **Game-3.** If $\beta = 1$ **,** CT^* is the encryption of random $P_A \| P_B$ independent of A_{σ}. A will not output the right A_{σ}; else, A forges a modified BB signature under weak chosen message attack, which happens with a negligible probability under the $(N+1)SDH$ assumption.

Game-4: This game is identical to **Game-3,** except that during each transfer phase, it calculates $V = (B_{\sigma} / R_{\sigma})^{\omega}$ and a simulated proof is employed to replace the proof of knowledge $POK\{(f): F = \widehat{e}(u, f)\}$ since Sim_3 does not require knowledge of f . Under the perfect zero knowledge property of the proof of knowledge, it holds that

$$Hybrid_{\mathbf{E},Sim_3}(\kappa) - Hybrid_{\mathbf{E},Sim4}(\kappa) \le \nu_4(\kappa).$$

Game-5: This game is identical to **Game-4,** except that Sim_5 employs the random elements from **G***T* to replace the values $B_j (j = 1,...,n)$ from **G***T* during **DataBaseSetup** phase. When these changes make an environment $\mathbf{E}$ separate the experiments, an instance of the $(n+1)BDHE$ problem can be solved. If the $(n+1)BDHE$ assumption holds, it holds that $\mathrm{Re}\,al_{\mathbf{E},A}(\kappa) - Ideal_{\mathbf{E},A^*}(\kappa)$ is negligible.

Proof. Given the environment $\mathbf{E}$, if A can distinguish Game-4 from Game-5 with non-negligible advantage, then the attacker B can be employed to solve the $(n+1)PDDH$ problem.

Upon receiving $u, u^{\alpha}, ..., u^{\alpha^{n+1}}, Z_0, Z_1, ..., Z_{n+1}$, B runs $\mathbf{E}$ and A as Sim_4 dictates to create database $DB = (R_j, \mathbf{A}_j)_{j=1,...,n}$. Let $h(\alpha) = \prod_{j=1}^{n}(\alpha + j) = \sum_{j=1}^{n} \delta_j \alpha^j$, and $h_j(\alpha) = h(\alpha)/(\alpha + j) = \sum_{i=0}^{n} \chi_{j,i} \alpha^i$ for $j = 1,...,n$. B calculates $u' = u^{h(\alpha)} = \prod_{j=0}^{n} (u^{\alpha^j})^{\delta_j}, \beta_{DB} = u^{\alpha h(\alpha)} = \prod_{j=0}^{n} (u^{\alpha^{j+1}})^{\delta_j}$. For $j = 1,...,n$, $A_j = u'^{1/(\alpha+j)} = \sum_{i=0}^{n} (u^{\alpha^i})^{\chi_{j,i}}$ and $B_j = \prod_{i=0}^{n-1} (Z_j)^{\chi_{j,i}}$. B feeds $(PK_{DB} = (u', Z_0, \beta_{DB}), (A_1, B_1), ..., (A_n, B_n))$ as the encrypted database to A , and continues running $\mathbf{E}$ and A as under Sim_4. If $\mathbf{E}$ outputs a bit β , then B outputs the same bit β .

If $Z_j = Z_0^{\alpha^j}$, then the database has the same distribution as **Game-4,** whereas if $Z_1, ..., Z_{n+1}$ are random, then the database has the same distribution as **Game-5.** The advantage of B breaking the $(n+1)PDDH$ assumption is the $\mathbf{E}$'s advantage in distinguishing **Game-4** from **Game-5.**

A^* provides A with the same environment as Sim_5, it holds that $Ideal_{\mathbf{E},A^*}(\kappa) = Hybrid_{\mathbf{E},Sim_5}(\kappa)$.

By summation, it holds that $\mathrm{Re}\,al_{\mathbf{E},A}(\kappa) - Ideal_{\mathbf{E},A^*}(\kappa) \le v_5(\kappa)$.

Lemma 4. For any an environment $\mathbf{E}$ and any an attacker A which corrupts the one or more users and the issuer, there exists an ideal world attacker A^* such that $\mathrm{Re}\,al_{\mathbf{E},A}(\kappa) - Ideal_{\mathbf{E},A^*}(\kappa)$ is negligible.

Proof. The setting is simply to restricted to a single corrupted user since the attacker corrupts the issuer and users.

Game-1: This game is identical to **Game-0,** except that at each transfer query instructed by $\mathbf{E}$, Sim_1 runs the knowledge extractor to extract (σ,ω) from the proof of knowledge $POK\{(\sigma,\omega): \widehat{e}(W,y) = \widehat{e}(W,u)^{-\sigma} e(u,u)^{\omega}\}$. Since the extraction event succeeds with all but negligible probability, it holds that $Hybrid_{\mathbf{E},Sim_0}(\kappa) - Hybrid_{\mathbf{E},Sim_1}(\kappa) \le v_1(\kappa)$.

Game-2: This game is identical to **Game-1,** except that the extracted value $\alpha \notin \{1,...,n\}$ or the attribute set S does not satisfy access structure $\mathbf{A}_{\sigma}$ during any transfers. In this case $s = W^{1/\omega}$ is a forged modified BB signature on record $R_{\sigma}^{'}$. If the $(n+1)SDH$ holds assumption, it holds that $Hybrid_{\mathbf{E},Sim_1}(\kappa) - Hybrid_{\mathbf{E},Sim_2}(\kappa) \le v_2(\kappa)$.

Game-3: This game is identical to **Game-2,** except that at the first transfer query dictated by $\mathbf{E}$, the simulator Sim_3 runs the simulated proof of knowledge $POK\{(f): F = \widehat{e}(u,f)\}$ .The value L is calculated as $L = (B_{\sigma}/R_{\sigma})^{\omega}$. A simulated proof is employed to replace the final POK in the transfer phase. Under the perfect zero knowledge property, it holds that

$$Hybrid_{\mathbf{E},Sim_2}(\kappa) - Hybrid_{\mathbf{E},Sim3}(\kappa) = 0.$$

Game-4: This game is identical to **Game-3,** except that Sim_4 employs the random elements from $\mathbf{G}_T$ to replace the values $B_j (j=1,...,n)$ from $\mathbf{G}_T$ during **DataBaseSetup** phase. When these changes make an environment $\mathbf{E}$ separate the experiments, an instance of the $(n+1)BDHE$ problem can be solved. If the $(n+1)BDHE$ assumption holds, it holds that $Hybrid_{\mathbf{E},Sim_3}(\kappa) - Hybrid_{\mathbf{E},Sim_4}(\kappa) \le v_4(\kappa)$.

Proof. According to the real world attacker A, an ideal world attacker A^* acting as the issuer and users can be constructed. After A^* has extracted σ' from A, he queries $\mathbf{T}$. All messages are relayed between $\mathbf{E}$ and A by the attacker A^*. A^* runs A to obtain the issuer's PP and the encrypted database $ER_j (j=1,...,n)$. When A^* receives a message **Transfer** from $\mathbf{T}$ for the first time, it runs the extractor of $POK\{(f): F = \widehat{e}(u,f)\}$ to extract f from A. A^* employs the private key $\mathrm{Pr}\,iKey_S$ to decrypt $ER_j (j=1,...,n)$ to obtain $A_j \| B_j$, in which $B_j = \widehat{e}(f,A_j)R_j$, A^* computes $R_j = B_j / \widehat{e}(f,A_j) (j=1,...,n)$ and sends $\left(\text{InitializeDB}, R_j, \mathbf{A}_j\right)_{j=1,...,n}$ to $\mathbf{T}$. A^* simulates an honest user querying for record R picked at random with the access structure satisfied by the attribute set S. If the transfer query succeeds, A^* returns $\beta = 1$ to $\mathbf{T}$; if not, it returns $\beta = 0$ to $\mathbf{T}$. The remaining transfers are treated in the same way.

As you can see, A^* provides A with exactly the same environment as Sim_4. Hence, it holds that $Ideal_{\mathbf{E},A^*}(\kappa) = Hybrid_{\mathbf{E},Sim_4}(\kappa)$.

By summation, it holds that $\mathrm{Re}\,al_{\mathbf{E},A}(\kappa) - Ideal_{\mathbf{E},A^*}(\kappa) \le v_4(\kappa)$.

7. Performance Analysis

As depicted in Table 1 where *cat* denotes category and || denotes the cardinality of the set: for access policy, CDN scheme [9] supports conjunction, and disjunction via duplication, whereas our scheme and XSF scheme [19] supports conjunction, disjunction and threshold gate directly. For the encrypted record size, given a conjunction normal form $(I_{1,1} \vee \ldots \vee I_{1,y_1}) \wedge \ldots \wedge (I_{1,1} \vee \ldots \vee I_{n,y_n})$,we represent it by employing an access tree whose internal nodes are **OR** gates and **AND** gates, and leaf nodes denote attributes; in our scheme and XSF scheme [19] , the encrypted record size is $\sum_{i=1}^{n} y_i$, whereas, in CDN scheme, the encrypted record size is $\prod_{i=1}^{n} y_i$ due to disjunction via duplication. By directly supporting disjunction, our scheme and XSF scheme [19] greatly reduces the size of encrypted database. For issuing phase, these three schemes have communication complexity linear in the number of attributes possessed by some user. For initialization phase, these three schemes have computation complexity linear in the number n of messages. For transfer phase, our scheme and XSF scheme have communication complexity linear in the cardinality of the universe of attribute, whereas that of CDN scheme is linear in the attribute number possessed by some user; however, in the CDN scheme, user U only obtains a record, whereas our scheme U and XSF scheme obtains all the records which he is authorized to access. It is seen that XSF scheme is identical to our scheme in terms of Access Policy, Encrypted Record Size, Issuing Phase, Initialization Phase, and Transfer Phase, but the security model of our scheme is standard model, whereas the security model of XSF scheme is random oracle model. Hence, when access policies are complex or the number of records authorized to access is larger, our scheme is more efficient than the CDN scheme. Our scheme is stronger than XSF scheme in terms of security.

Table 1. Comparison of Our Scheme with CDN Scheme and XSF Scheme

References	Access Policy	Encrypted Record Size	Issuing Phase	Initialization Phase	Transfer Phase	Security Model
CDN Scheme	conjunction and disjunction via duplication	$\prod_{i=1}^{n} y_i$	$O(\|cat\|)$	$O(n)$	$O(\|cat\|)$	Standard Model
XSF scheme	conjunction, disjunction and threshold	$\sum_{i=1}^{n} y_i$	$O(\|S\|)$	$O(n)$	$O(\|\mathrm{S}\|)$	Random Oracle Model
Our Scheme	conjunction, disjunction	$\sum_{i=1}^{n} y_i$	$O(\|S\|)$	$O(n)$	$O(\|\mathrm{S}\|)$	Standard Model

	and threshold					

8. Conclusion and Future Work

In this work, we propose an oblivious transfer scheme with complex access control from ciphertext policy attribute based encryption in the standard model which greatly enhances expressiveness for access policies, and reduces the size of encrypted database. Furthermore, the communication complexity in the transfer phase of our scheme is constant in the number of records accessed. However, the access policies of our scheme are public. In the future work, we will design a scheme where access policies are hidden to furthermore enhance privacy preserving to meet the highly sensitive requirements such as electronic medical database. Moreover, to further enhance the expressiveness, we plan to combine the attribute based encryption for circuit with oblivious transfer to achieve user privacy and the database access control.

9. Acknowledgements

This work was supported by the National Science Foundation of China (Grant No. 61402376).The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

10. References

[1] A. Sahai and B. Waters, “Fuzzy Identity Based Encryption. *Advances in Cryptology, Eurocrypt 2005”,* vol. 3494, **(2005)**, pp. 457-473.

[2] V. Goyal, O. Pandey, A. Sahai and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data”, *Proceedings of the 13th ACM conference on Computer and communications security,* **(2006)**, pp. 89 - 98.

[3] R. Ostrovsky, A. Sahai and B. Waters, “ Attribute-based encryption with non-monotonic access structures”, ACM Conference on Computer and Communications Security 2007, ACM Press, **(2007)**, pp. 195–203.

[4] J. Bethencourt, A. Sahai and B. Waters, “Ciphertext-Policy Attribute-based Encryption”, IEEE Symposium on Security and Privacy, (**2006)**, pp. 321 - 334.

[5] V. Goyal, A. Jain, O. Pandey and A. Sahai, ”Bounded ciphertext policy attribute-based encryption”, *ICALP 2008,* ***(2008)***.

[6] B. Waters, ”Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization”, PKC 2011, **(2011)**, pp. 371–380.

[7] S. Coully, M. Green and S. Hohenberger, “Controlling access to an oblivious database using stateful anonymous credentials”, *Cryptology ePrint Archive*, Report, 2008/474, **(2008)**.

[8] S. Coully, M. Green and S. Hohenberger, “Access controls for oblivious and anonymous systems”, *ACM Trans. Inf. Syst. Secur,* vol. 14, no. 1, **(2011),** pp. 10.

[9] J. Camenisch, M. Dubovitskaya and G. Neven, “Oblivious Transfer with Access Control”, ACM CCS 2009, New York, **(2009)**, pp. 131–140.

[10] Y. Zhang, M.H. Au, D.S.Wong, Q. Huang, N. Mamoulis, D.W. Cheung and S.M. Yiu, “Oblivious Transfer with Access Control :Realizing Disjunction without Duplication”, *Pairing 2010,* **(2010)**, pp.96-115.

[11] A. Lewko, T. Okamoto, A. Sahai and K. Takashima, “Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption”, *EUROCRYPT 2010,* **(2010)**, pp. 62-91.

[12] A. Beimel, “Secure Schemes for Secret Sharing and Key Distribution”, Israel Institute of Technology, Technion, Haifa, Israel, **(1996)**.

[13] D. Boneh and X. Boyen, “Short signatures without random oracles”, In EUROCRYPT 2004, pp. 56-73.

[14] D. Boneh, C. Gentry and B. Waters, “Collusion resistant broadcast encryption with short ciphertexts and private keys” In CRYPTO 2005, LNCS, Springer, vol. 3621, **(2005)**, pp. 258–275.

[15] J. Camenisch, G. Neven and A. Shelat, “Simulatable adaptive oblivious transfer”, In EUROCRYPT ’07, vol. 4515, **(2007)**, pp. 573–590.

[16] R. Cramer, I. Damgard and D., “Efficient zero-knowledge proofs of knowledge without intractability assumptions”, *PKC 2000: 3rd International Workshop on Theory and Practice in Public Key Cryptography*, vol.1751, **(2003),** pp. 354–372.

[17] R. Canetti, “Universally Composable Security: A New Paradigm for Cryptographic Protocols”, **(2013)**.

[18] J. Herranz, D. Hofheinz and E. Kiltz, “KEM/DEM: Necessary and Sufficient Conditions for Secure Hybrid Encryption, **(2006)**.

[19] F. Xingbing, Z. Shengke and L. Fagen, ”Blind Expressive Ciphertext Policy Attribute Based Encryption for Fine Grained Access Control on the Encrypted Data”, International Journal of Network Security, vol. 17, no. 6, **(2015)**, pp. 661-671.

Authors

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 .

Shengke Zeng is a lecturer at the School of Mathematics and Computer Engineering, Xihua University. She received her Ph.D. degree from University of Electronic Science and Technology of China (UESTC) in 2013. Her research interests include: Cryptography and Network Security.

Fagen Li received the Ph.D. degree in Cryptography from Xidian University, Xi'an, P.R. China in 2007. His research interests include cryptography and network security, especially in signcryption schemes, signature schemes and key agreement protocols.