Blind Expressive Ciphertext Policy Attribute Based Encryption for Fine Grained Access Control on the Encrypted Data

Xingbing Fu[1], Shengke Zeng[2], and Fagen Li[1]
(Corresponding author: Xingbing Fu)
School of Computer Science and Engineering, University of Electronic Science and Technology of China[1]
No.2006, Xiyuan Avenue, West Hi-tech Zone, Chengdu, 611731, P.R.China
(Email: fuxbuestc@126.com)
School of Mathematics and Computer Engineering, Xihua University[2]
Chengdu, Sichuan, China
(Received February 1, 2015; revised and accepted May 1 & May 15, 2015)

Abstract

Oblivious transfer with access control is a protocol where data in the database server are protected with access control policies and users with credentials satisfying the access policies are allowed to access them, whereas the database server learns nothing about the data accessed by users or about her credentials.Our scheme has the advantages as follows: First, our scheme maintains the privacy property of oblivious transfer and offers access control mechanism. Second, it allows the expressive access control polices that directly supports **AND**, **OR** and **Threshold** gates. Third, the communication complexity in our scheme is constant in the numbers of records which have been accessed. Fourth, our scheme is constructed in prime order bilinear group.

Keywords: Access control, bilinear maps, ciphertext policy attribute based encryption, linear secret sharing, oblivious transfer, standard model

1 Introduction

With the advent of cloud computing, more and more organizations plan to adopt the cloud computing service. However, the concerns for the security and privacy make them hesitate to adopt this service. While the encryption techniques can be employed to protect the outsourced data, the cloud service providers can still collect the sensitive information on who accesses the outsourced data, and how she accesses them. To address the problem, researchers proposed to employ the oblivious transfer (OT, for short) [7] primitive to preserve the users privacy. However, oblivious transfer in its basic form has no access control functionality, that is, the users can obtain any files chosen by them without any restrictions. To distinguish the authorized users from the unauthorized users, access control mechanisms are introduced in such a way that only the authorized users are allowed to access data, whereas the unauthorized users cannot. However, traditional access control mechanisms assume the items being requested are knowledgeable.

To preserve the users' privacy and let access control mechanism be enforced by the service provider (database), researchers proposed oblivious transfer with access control mechanism which, for each record of the database, defines an access control policy that determines the attributes, roles and rights which the user needs to possess to access this record. To meet the requirements for the maximal amount of privacy, this mechanism should provide guarantees as follows:

1) The record can be accessed by only the authorized users.
2) Which record the user has accessed is not learned by the database provider.
3) The database provider does not learn which attributes the user possesses when the database is accessed by her.
4) Access control mechanism should be flexible enough to enforce different expressive access control policies.

An encryption scheme is employed to securely share data among users. The symmetric cryptography and traditional public key cryptography are suitable for the setting in which a user securely share data with another user that is known to her in advance, that is, the communication model is one-to-one.Furthermore,access to the encrypted data is all or nothing-a user is either able to decrypt and obtain the entire plaintext or she does not learn anything 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 cryptosystem is insufficient. For instance, the data provider may want to share data according to some policy based on the recipient's credentials or attributes and only the data users satisfying the policy can decrypt. The traditional public key cryptosystem cannot handle such tasks.

Sahai and Waters [17] first proposed the Attribute Based Encryption (ABE) scheme to handle the aforementioned problem. In their scheme, the private keys and ciphertexts are associated with attribute sets, and a private key can decrypt a ciphertext iff there exists a match between the attributes of the private key and those of the ciphertext. Decryption is enabled only if at least d attributes overlap between a ciphertext and a private key. Their scheme is useful for error-tolerant encryption with biometrics, while their scheme is limited to handling threshold access structure. Since the Attribute Based Encryption scheme is proposed, different ABE schemes and their applications [15, 12, 6] are presented in terms of flexibility, efficiency, and security. Existing ABE schemes are classified as Key Policy ABE (KP-ABE) schemes [10, 16] and Ciphertext Policy ABE (CP-ABE) schemes [2]. In KP-ABE schemes, keys are associated with access policies, and ciphertexts are identified with attribute sets.Iff the keys associated with access policies 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 satisfying the access policy associated with the ciphertext are able to decrypt it.

In the `CP-ABE` schemes, the data are protected with access polices, and only those users whose attributes satisfy the access policies are able to decrypt to access them.BSW scheme [2] are the first to implement CP-ABE scheme which is expressive and efficient attribute based encryption scheme. However,security proof of their scheme are based on the generic group model which assumes that an adversary needs to access an oracle to perform any group operations. To achieve ciphertext policy attribute based encryption scheme in the standard model, work has been done as follows: Cheung and Newport [5] proposed a CP-ABE scheme which construct a policy with an **AND** gate under the bilinear Diffie-Hellman assumptions.However, their scheme requires that the number of system attributes be fixed at setup and the access structure of their scheme only support an **AND** gate. These two drawbacks make it less expressive. To enhance the expressiveness, Goyal, Jain, Pandey, and Sahai [9] proposed Bounded CP-ABE scheme in the standard model. However, the encryption and decryption complexity blows up by an $n^{3.42}$ factor in the worst case, which limits its usefulness in practice.Lewko et al. [13] proposed a CP-ABE scheme in the standard model which is expressive, and adaptively secure. However, their scheme is based on composite order bilinear group which incurs some efficiency loss and assumption is non-standard assumption.To overcome this problem, Waters [19] present a CP-ABE scheme which is both expressive and is proven secure under a standard assumption in the standard model.Our scheme builds on this scheme.

We propose blind expressive ciphertext policy attribute based encryption scheme to achieve fine grained access control over the encrypted data. Our scheme has the advantages as follows: First, our scheme maintains the privacy property of oblivious transfer and offers access control mechanism.Second,it allows the expressive access control polices that directly supports **AND**, **OR** and **Threshold** gates.Third, the communication complexity in our scheme is constant in the numbers of records which have been accessed.Fourth, our scheme is constructed in prime order bilinear group.

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 game and Blind CP-ABE scheme in Section 4. We present the scheme construction in Section 5. Blind Private Key Generation Protocol is presented Section 6. We propose fully simulatable oblivious transfer with fine grained access control in Section 7. The performance of our scheme is evaluated in Section 8. We conclude and specify the future work in Section 9.

2 Related Work

Coully et al. [7] presented a scheme based on state graphs where users obtain credentials binding them to a particular state in the graph. This scheme limits the possible transitions between states to enforce access control. Their scheme has the advantages as follows: (1) It can be applied to different oblivious transfer schemes; (2) It permits the access control policies to be changed without changing the database. Unfortunately, their scheme has the two following drawbacks: (1) Each time users access the database, they have to obtain a new credential. (2) This scheme cannot efficiently express a large class of access policies based on state graphs. Camenisch et al. [3] presented an oblivious transfer with access control mechanism in which each user can obtain a credential certifying whether she possesses some attributes used to describe each record of data. A user can access the record as long as she possesses these attributes, which makes access policies only support `AND` condition. To support access policy in disjunctive form, database server needs to duplicate the record, which increases the size of database. To directly support access policy in disjunctive form, Zhang et al. [20] present oblivious transfer with access control which realizes disjunction without duplication.Their scheme builds on fully secure attribute based encryption scheme proposed by Lewko et al. [13]. However, their scheme is based on composite order bilinear group which results in some efficiency loss. Furthermore, their scheme does not perform key sanity check and ciphertext sanity check. In case the issuer and the database are malicious, the two users

which possess the same attributes may decrypt the same encrypted record to different plaintext record, which does not guarantee anonymity of the users.

3 Preliminaries

3.1 Bilinear Map

Let $\mathbb{G}$ and $\mathbb{G}_T$ denote two cyclic groups whose order is prime order p, and g, u are a generator of $\mathbb{G}$, respectively. e is a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ that has the properties as follows:

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

Nondegenerate. $e(g, g) \neq 1_{\mathbb{G}_T}$, $e(g, g)$ is a generator of $\mathbb{G}_T$. If the group operation on $\mathbb{G}$ and on the bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ are efficiently computable, then $\mathbb{G}$ is a bilinear group. Our scheme employs the symmetric bilinear map such that: $e(g^a, u^b) = e(g, u)^{ab} = e(g^b, u^a)$.

3.2 Access Structure

Let $\mathbb{S}$ be the universe of attributes. An access structure [1] on $\mathbb{S}$ is a collection $\mathbb{A}$ of non-empty subsets of attributes, i.e., $\mathbb{A} \subseteq 2^{\mathbb{S}} \setminus \{\}$. We call the sets in $\mathbb{A}$ the authorized attribute sets, and the sets not in $\mathbb{A}$ the unauthorized attribute sets. Specifically, an access structure is monotone if $\forall B, C$: if $B \in \mathbb{A}$ and $B \subseteq C$, then $C \in \mathbb{A}$. In this scheme, only monotone access structure is handled.

3.3 Linear Secret Sharing Scheme

A secret sharing scheme [1, 4, 18] Π over the attribute set is called linear over $\mathbb{Z}_p$ if (1) The shares for each attribute of a secret form a vector over $\mathbb{Z}_p$. (2) There is a matrix M with h rows and n columns for Π. For any $j = 1, \cdots, h$, let the function φ defined the attribute that labels the j^{th} row as $\varphi(j)$. Given the column vector $\overrightarrow{v} = (s, x_2, \cdots, x_n)^T$, in which T is the transpose of the vector $\overrightarrow{v}$, s is the secret that will be shared, and $x_2, \cdots, x_n \in \mathbb{Z}_p$ are uniformly at random picked, then $M\overrightarrow{v}$ is the vector of h shares of the secret s based on Π. The share $(M\overrightarrow{v})_j$ belongs to the attribute $\varphi(j)$.

Let attribute set $S \in \mathbb{A} \wedge S \in \mathbb{S}$ be any authorized attribute set, and let $J = \{j | j \in \{1, \cdots, h\} \wedge \varphi(j) \in S\}$. Then, there exist constants $\{\eta_j \in \mathbb{Z}_p\}_{j \in J}$ such that, if $\{s_j\}_{j \in J}$ are valid shares of a secret s according to Π, then $\Pi_{j \in J} \eta_j s_j = s$.

3.4 Commitment Scheme

A commitment scheme comprises the three algorithms as follows:

Setup $(1^\kappa) \to \mathbb{CP}$**.** This algorithm takes in a security parameter κ, and it outputs the commitment parameters $\mathbb{CP}$.

Commit $(\mathbb{CP}, m) \to (\mathcal{C}, \mathcal{D})$**.** This algorithm takes in the commitment parameters $\mathbb{CP}$ and a message m, and it outputs a pair $(\mathcal{C}, \mathcal{D})$.

Decommit $(\mathbb{CP}, m, \mathcal{C}, \mathcal{D}) \to \{0, 1\}$**.** This algorithm takes in $\mathbb{CP}$, m, $\mathcal{C}$, $\mathcal{D}$, and it outputs 1 if $\mathcal{D}$ opens $\mathcal{C}$ to m, else 0.

We employ the Pedersen commitment scheme [14], where the commitment parameters are a group whose order is prime order p, and random generators $(h_0, \cdots, h_\lambda)$, where λ is a positive integer. In order to commit to the values $(a_1, \cdots, a_\lambda) \in \mathbb{Z}_p^\lambda$, select a random $\varpi \in \mathbb{Z}_p$ and set $\mathcal{C} = h_0^\varpi \prod_{i=1}^{\lambda} h_i^{a_i}$ and $\mathcal{D} = \varpi$.

3.5 Zero Knowledge Proof

We employ definitions from [8]. A pair of algorithms (P, V) which interact with each other is a proof of knowledge (POK) for a relation $R = \{(\gamma, \delta)\} \subseteq \{0,1\}^* \times \{0,1\}^*$, where knowledge error is $\lambda \in [0, 1]$ if (1) For all $(\gamma, \delta) \in R$, $\mathtt{V}(\gamma)$ accepts a conversation with $\mathtt{P}(\delta)$ with probability 1; (2) There is an expected PPT algorithm KE, called the *knowledge extractor*, such that if a cheating prover $\widehat{P}$ has probability ε of convincing V to accept γ, the KE, when given rewindable black box access to $\widehat{P}$, outputs a witness δ for γ with probability $\varepsilon - \lambda$.

A proof system (P, V) is perfect zero-knowledge if there is a PPT algorithm Sim, the *simulator*, such that for any PPT cheating verifier $\widehat{V}$ and for any $(\gamma, \delta) \in R$, the output of $\widehat{V}(\gamma)$ after interacting with $\mathtt{P}(\delta)$ and that of $\mathtt{Sim}^{\widehat{V}(\gamma)}$ are identically distributed.

3.6 Our Scheme Overview

An oblivious transfer with fine grained access control from ciphertext policy attribute based encryption is run between the parties as follows: one credential issuer I, one database DB, and one or many users $\mathtt{U}_1, \cdots, \mathtt{U}_Z$, where Z is a positive integer. DB hosts a database $((m_1, \mathbb{A}_1), \cdots, (m_N, \mathbb{A}_N))$, where $m_l (l = 1, \cdots, N)$ is protected by access structure $\mathbb{A}_l (l = 1, \cdots, N)$. Each access structure $\mathbb{A}_l$ describes the attribute set that a user must possess to access m_l. Each user U possesses attribute set $S_\mathtt{U}$, and she can access messages m_l if and only if her $S_\mathtt{U}$ satisfies access structure $\mathbb{A}_l$. A credential issuer I certifies whether user U possesses attribute set $S_\mathtt{U}$.

The proposed scheme divides the interaction between parties into three phases as follows: A credential issuing phase, an initialization phase, and a transfer phase. In the credential issuing phase, a user U asks I to certify she has the attribute set $S_\mathtt{U}$. If certification succeeds, I issues U a credential on attributes $S_\mathtt{U}$. In the initialization phase, DB encrypts messages $m_l (l = 1, \cdots, N)$ under the corresponding access structure $\mathbb{A}_l (l = 1, \cdots, N)$, sends ciphertext $(C_1, \cdots, C_N)$ to each user U. In the transfer phase, the user U proves in zero-knowledge proof possession of a credential on her attribute set $S_\mathtt{U}$ to DB, and gets a

private key $PriKey_{S_{\mathtt{U}}}$ associated to her attribute set $S_{\mathtt{U}}$ from DB. If her $S_{\mathtt{U}}$ satisfies access structure $\mathbb{A}_l$, she can decrypt all the ciphertexts $C_l(l = 1, \cdots, N)$ to recover plaintext messages $m_l(l = 1, \cdots, N)$.

DB employs a ciphertext policy attribute based encryption scheme [19] to encrypt plaintext messages $(m_l)(l = 1, \cdots, N)$ under the corresponding access structure $\mathbb{A}_l(l = 1, \cdots, N)$. In a CP-ABE scheme, a ciphertext C is associated with access structure $\mathbb{A}$, whereas a private key $PriKey_S$ is associated with the user's attribute set S. If the attribute set S satisfies the access structure $\mathbb{A}$, then the private key $PriKey_S$ can decrypt the ciphertext C to recover plaintext message m.

In the transfer phase, the user U who possesses attribute set $S_{\mathtt{U}}$ can obtain a private key $PriKey_S$ of the CP-ABE scheme from the database DB. In traditional CP-ABE schemes, the Private Key Generator (PKG, for short) needs to learn the attribute set $S_{\mathtt{U}}$ to calculate a private key. Whereas the privacy properties in our scheme require the database acting as PKG should not learn the attribute set $S_{\mathtt{U}}$. Furthermore, DB assures that the user U only obtains the private keys associated with the attribute set $S_{\mathtt{U}}$. To handle these problems, we propose the expressive CP-ABE scheme with a blind key generation, where the user U proves in zero-knowledge proof possession of a credential on her attributes $S_{\mathtt{U}}$ to DB, and then she obtains a private key associated with $S_{\mathtt{U}}$ in a blind manner, such that DB does not learn $S_{\mathtt{U}}$.

We require authenticated communication between a user U and the issuer I, whereas communication between DB and U should be anonymous.

3.7 Credential Signature Scheme

The signature scheme comprises the following algorithms:

1) KeyGen (1^{κ}). The key generation algorithm takes in a security parameter κ, and outputs a keypair (sk, vk).

2) Sign $(sk, m_1, \cdots, m_N)$.The signing algorithm takes in a private signing key sk and one or more messages $m_1, \cdots, m_N$, and outputs the signature α.

3) Verify $(vk, \alpha, m_1, \cdots, m_N)$. The verification algorithm takes in a signature,messages(s) pair$(\alpha,(m_1, \cdots, m_N))$ and verification key vk, and outputs 1 if the signature verification is valid, 0 otherwise.

We extend a signature scheme with two protocols to achieve a credential scheme.First, a user U and a credential issuer I engage in an issuing protocol Issue by means of which U obtains a signature from I on a committed message $\mathcal{C}_{m_l}$ = Commit $(\mathbb{CP}, m_l,$ Decommit$)$, where $l = 1, \cdots, N$. Second, a protocol Show allows U to prove possession of a signature by I on a committed messages $\mathcal{C}_{m_l}$ to a verifier. To prevent users from colluding their credentials and to securely realize any credential scheme, we employ an ideal functionality $\mathtt{F}_{credential}$ as follows:

* On receiving (issue, att) from $\mathtt{U}_z(z = 1, \cdots, Z)$, where Z is a positive integer, and $att \in \mathbb{S}$, where $\mathbb{S}$ is the universe of attributes, it sends (issue, U, att) to I that sends back a bit β. If $\beta = 1$, then att is added to $S_{\mathtt{U}_z}$, and β is sent to $\mathtt{U}_z$; else β is simply sent to $\mathtt{U}_z$.

* On receiving (Show, $S^{\star}$) from $\mathtt{U}_z$, in which the cardinality of attribute set $S^{\star}$ is q, where q is a positive integer, if $S^{\star} \subseteq S_{\mathtt{U}}$, (verify, valid, q) is sent to $\mathtt{U}_z$ and to the verifier; else, (verify, invalid, q) is sent to $\mathtt{U}_z$ and to the verifier.

3.8 k-out-of-N Oblivious Transfer

An oblivious transfer scheme [3, 11] comprises four algorithms ($\mathtt{S}_I$, $\mathtt{R}_I$, $\mathtt{S}_T$, $\mathtt{R}_T$). In the initialization phase, an interactive protocol is run by the sender and the receiver. A state value S_0 is obtained by the sender via running $\mathtt{S}_I$ $(m_1, \cdots, m_N)$, and a state value R_0 is obtained by the receiver via running $\mathtt{R}_I$. Then, during the transfer phase, the sender and receiver interactively conduct $\mathtt{S}_T$, $\mathtt{R}_T$, respectively, k times as follows:

1) In the adaptive $\mathtt{OT}^N_{k\times 1}$ case, where $1 \leq l \leq k$, the l^{th} transfer proceeds as follows: the state value S_l is obtained by the sender via running $\mathtt{S}_T(S_{l-1})$, and the receiver runs $\mathtt{R}_T(R_{l-1}, \sigma_l)$ in which $1 \leq \sigma_l \leq N$ is the index of the message to be received. The receiver obtains state information R_l and the message $m^*_{\sigma_l}$ or $\perp$ which indicates protocol failure.

2) In the non-adaptive $\mathtt{OT}^N_k$ case, the parties conduct the protocol as in the aforementioned case. However, for each round $l < k$,the algorithm $\mathtt{R}_T(R_{l-1}, \sigma_l)$ does not return a message. At the end of the k^{th} transfer, $\mathtt{R}_T(R_{k-1}, \sigma_k)$ returns the messages $(m^*_{\sigma_1}, \cdots, m^*_{\sigma_N})$ in which for $l = 1, \cdots, N$, each $m^*_{\sigma_l}$ is a valid message or the symbol $\perp$ which indicates protocol failure. Our scheme employs k-out-of-N oblivious transfer realizing the ideal functionality $\mathtt{F}_{OT}$. The functionality $\mathtt{F}_{OT}$ performs as follows:

   * On receiving (Initialize, $(m_l, \mathbb{A}_l)_{l=1,\cdots,N}$) from DB, it sets DB $\leftarrow (m_l, \mathbb{A}_l)_{l=1,\cdots,N}$.

   * On receiving (transfer, $\sigma_1, \cdots, \sigma_k$) from $\mathtt{U}_z$, it proceeds as follows: It sends (receive, k) to DB. If DB is honest, $\mathtt{F}_{OT}$ sets $\{\beta_l = 1\}^k_{l=1}$, else, DB sends back (transfer, $\{\beta_l\}^k_{l=1}$). For $l = 1$ to k, if $\beta_l = 1$, $\mathtt{F}_{OT}$ sets $m^*_{\sigma_l} = m_{\sigma_l}$; else $\mathtt{F}_{OT}$ sends back $\perp$. $\mathtt{F}_{OT}$ returns (transfer, $m^*_{\sigma_1}, \cdots, m^*_{\sigma_k}$) to $\mathtt{U}_z$.

4 Blind Expressive Ciphertext Policy Attribute Based Encryption

4.1 Scheme Definition

Definition 1. *Ciphertext Policy Attribute Based Encryption (CP-ABE) scheme [19] comprises the four algorithms as follows:*

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

$ABE.Encrypt(PP, \mathbb{A}, m) \rightarrow \mathbf{CT}_{\mathbb{A}}$. It takes in the public parameters PP, the plaintext message m and the access structure $\mathbb{A}$ over a set of attributes specifying which users are able to decrypt to recover the plaintext message. It outputs the ciphertext $CT_{\mathbb{A}}$ associated with access structure $\mathbb{A}$.

$ABE.PriKeyGen(MS, S) \rightarrow PriKey_S$. It takes in 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.

$ABE.Decrypt(CT_{\mathbb{A}}, PriKey_S) \rightarrow M$. It takes in the $CT_{\mathbb{A}}$ and the private key $PriKey_S$. It outputs the plaintext message m if attribute set S satisfies the access structures $\mathbb{A}$, else it returns $\perp$.

Correctness. *A CP-ABE scheme is correct when for all security parameters κ, all messages m, all sets of attributes S, access structures $\mathbb{A}$, all master secrets MS and public parameters PP output by ABE.Setup algorithm, all private keys $PriKey_S$ output by ABE.PriKeyGen algorithm, all ciphertexts $CT_{\mathbb{A}}$ output by ABE.Encrypt algorithm, if a set of attributes S satisfies access structure $\mathbb{A}$, the following proposition holds: $ABE.Decrypt(ABE.Encrypt(PP, \mathbb{A}, m), PriKey_s) = m$.*

4.2 Security Model for Ciphertext Policy Attribute Based Encryption Scheme

We describe a security model for CP-ABE scheme using a security game between a challenger and an attacker as follows:

Setup. The challenger runs the *ABE.Setup* algorithm which generates (MS, PP) and gives the attacker PP.

Phase 1. The attacker makes repeated private keys associated with attribute sets $S_1, \cdots, S_{Q_1}$, respectively.

Challenge. The attacker submits two plaintext messages m_0 and m_1 with $|m_0| = |m_1|$ and a challenge access structure $\mathbb{A}^*$ to the challenger with the restriction that none of the attribute sets $S_1, \cdots, S_{Q_1}$ from **Phase 1** satisfy the access structure $\mathbb{A}^*$. The challenger flips a random coin β, and encrypts m_β under $\mathbb{A}^*$. The resulting ciphertext $\mathtt{CT}^*$ is given to the attacker.

Phase 2. Phase 1 is repeated with the restriction that none of the attribute sets $S_{Q_1+1}, \cdots, S_Q$ satisfy the access structure $\mathbb{A}^*$ in the challenge phase.

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

Definition 2. *A CP-ABE scheme is secure against chosen plaintext attacks (CPA) if no probabilistic polynomial time attackers have non-negligible advantage in the aforementioned game, where the advantage is defined as $|Pr[\beta^* = \beta] - \frac{1}{2}|$.*

4.3 Blind Expressive Ciphertext Policy Attribute Based Encryption with Fine Grained Access Control

In the proposed oblivious transfer with fine grained access control (**AC-OT**) scheme, the database DB acts as `PKG`. When a user U who possesses attribute set $S_{\mathtt{U}}$ makes a request for DB, DB will check whether U possesses the credential of $S_{\mathtt{U}}$, if so, calculates $PriKey_{S_{\mathtt{U}}}$.

In traditional `CP-ABE` scheme due to [19], when a user U asks a private key associated with her attribute set $S_{\mathtt{U}}$, `PKG` will learn $S_{\mathtt{U}}$ to check whether U possesses the attributes $S_{\mathtt{U}}$, and calculate the private key $PriKey_{S_{\mathtt{U}}}$ by running $ABE.PriKeyGen$ algorithm. Whereas, in the proposed scheme, DB will accomplish the tasks without learning $S_{\mathtt{U}}$. To handle the problem, we extend traditional `CP-ABE` scheme with a blind private key generation protocol $ABE.BlindPriKeyGen$.

Definition 3. *If the underlying `CP-ABE` scheme (ABE.Setup, ABE.PriKeyGen, ABE.Encrypt, ASE.Decrypt) is secure and ABE.BlindPriKeyGen can be securely realized, then a blind `CP-ABE` scheme (ABE.Setup, ABE.BlindPriKeyGen, ABE.Encrypt, ABE.Decrypt) is secure.*

4.4 Additional Properties for a Blind CP-ABE Scheme

We employ blind `CP-ABE` scheme as a tool for constructing oblivious transfer with fine-grained access control.

Efficient POK for master secret. Our `AC-OT` constructions require an efficient zero-knowledge proof of knowledge protocol for the statement $\mathtt{POK}\{(msk) : (PP, msk) \in Setup(1^\kappa)\}$.

Committing CP-ABE scheme. To construct AC-OT protocols, we require our blind CP-ABE scheme should be committing.

The committing property requires that, given a ciphertext CT associated with an access structure $\mathbb{A}$, two different private keys associated with two different attribute sets satisfying $\mathbb{A}$ will yield a same plaintext message when the ciphertext CT is decrypted, which prevents a malicious database DB from calculating *mal-formed* ciphertexts, which makes the anonymity of the user be guaranteed. Two algorithms are defined as follows:

ABE.KeySanityCheck. This is a private key sanity check algorithm. It takes in public parameters PP, attribute set S, and private key $PriKey_S$ associated with S, and it outputs `Valid` if checks pass, else `Invalid`.

ABE.CiphertextSanityCheck. This is a ciphertext sanity check algorithm. It takes in public parameters PP and the ciphertext CT, and it outputs `Valid` if PP and the ciphertext CT are honestly generated, else `Invalid`.

Definition 4. *(Committing CP-ABE Scheme.) A (blind) CP-ABE scheme is committing if and only if: (1) It is secure according to Definition 1; (2) Each PPT attacker A has a negligible advantage in κ in the game as follows: First, A outputs public parameters PP, a ciphertext CT associated with access structure $\mathbb{A}$ and two different attribute sets S and S^* satisfying $\mathbb{A}$. If ABE.CiphertextSanityCheck outputs Invalid, then aborts, else the challenger runs the ABE.BlindPriKeyGen protocol with the attacker A twice on input (PP, S) and (PP, S^*) to obtain $PriKey_s$ and $PriKey_s^*$. The challenger runs ABE.KeySanityCheck(PP, S, $PriKey_S$) and ABE.KeySanityCheck(PP, S^*, $PriKey_{S^*}$) and aborts if the output of any of them is Invalid. The attacker A's advantage is defined to be: $|Pr[ABE.Decrypt(CT_{\mathbb{A}}, S, PriKey_S) \neq Pr[ABE.Decrypt(CT_{\mathbb{A}}, S^*, PriKey_{S^*})]|$.*

5 Scheme Construction

Blind expressive ciphertext policy attribute based encryption scheme employed to enforce fine-grained access control on the encrypted data is constructed as follows:

ABE.Setup$(1^k) \rightarrow (MS, PP)$. The setup algorithm calls the group generator algorithm $\mathbb{G}(1^\kappa)$ and obtains the descriptions of the two groups $\mathbb{G}$ and $\mathbb{G}_T$ and the bilinear map $\mathbb{D} = (p, \mathbb{G}, \mathbb{G}_T, g, e)$, in which p is the prime order of the cyclic groups $\mathbb{G}$ and $\mathbb{G}_T$, g is a generator of $\mathbb{G}$ and e is a bilinear map. The universe of system attributes are $\mathbb{S} = \{att_1, att_2, \cdots, att_{|\mathbb{S}|}\}$, where $|\mathbb{S}|$ is the cardinality of the universe $\mathbb{S}$ of system attributes. It selects the random exponents $t_1, t_2, \cdots, t_{|\mathbb{S}|}, \theta, \mu \in \mathbb{Z}_p^*$. For each attribute $att_d \in \mathbb{S}(1 \leq d \leq |\mathbb{S}|)$, it selects a corresponding $t_d \in \mathbb{Z}_p^*$, and sets $T_d = g^{t_d}(1 \leq d \leq |\mathbb{S}|)$. The public parameters are published as: $PP = (\mathbb{D}, g, e(g,g)^\mu, g^\theta, \{T_d\}_{1 \leq d \leq |\mathbb{S}|})$, where $e(g,g)^\mu$ can be pre-computed. The master secret is $MS = g^\mu$.

ABE.Encrypt$(PP, (M, \varphi), m) \rightarrow CT_{(M,\varphi)}$. The encryption algorithm encrypts a message $m \in \mathbb{G}_T$ under the access structure $\mathbb{A} = (M, \varphi)$, employing the public parameters PP. Let access matrix M be an matrix with h rows and n columns. The algorithm selects the column vector $\overrightarrow{v} = (s, x_2, \cdots, x_n)^T \in \mathbb{Z}_p^n$, where T is the transpose of the vector $\overrightarrow{v}$, $x_2, \cdots, x_n$ are uniformly at random chosen and $\overrightarrow{v}$ is employed to share the secret encryption exponent s. For any $j = 1, \cdots, h$, then $s_j = M_j \overrightarrow{v}$ is j^{th} share of the secret s according to Π, where M_j is the vector corresponding to the j^{th} row of M. Furthermore, the algorithm selects random elements $c_j \in \mathbb{Z}_p (j = 1, \cdots, h)$. The resulting ciphertext is constructed and calculated as follows:

$$\begin{aligned} CT_{(M,\varphi)} &= ((M,\varphi), E_b, E, \{E_j, F_j\}_{j=1,\cdots,h}). \\ E_b &= g^s \\ E &= m \cdot e(g,g)^{\mu s} \\ E_j &= g^{\theta s_j} T_{\varphi(j)}^{-c_j} \\ F_j &= g^{c_j}. \end{aligned}$$

PriKeyGen$(MS, S) \rightarrow PriKey_S$. 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:

$$\begin{aligned} PriKey_S &= (K_b, D_b, \{K_d\}_{d \in S}). \\ K_b &= g^{\mu + \theta \cdot r} \\ D_b &= g^r \\ K_d &= T_d^r. \end{aligned}$$

ABE.Decrypt$(CT_{(M,\varphi)}, PriKey_S) \rightarrow m$. The decryption algorithm takes in $\mathrm{CT}_{(M,\varphi)}$ and $PriKey_S$. If attribute set S satisfies the access structure (M, φ), and let $J = \{j : j \in \{1, \cdots, h\} \wedge \varphi(j) \in S\}$. Then, there exist constants $\{\eta_j \in \mathbb{Z}_p\}_{j \in J}$ such that, if $\{s_j\}_{j \in J}$ are valid shares of a secret s according to M, then $\Pi_{j \in J} \eta_j s_j = s$. The decryption algorithm performs as follows:

Step 1. It calculates

$$\begin{aligned} V_1 &= \prod_{j\in J}((e(E_j, D_b)e(F_j, K_{\varphi(j)}))^{\eta_j} \\ &= \prod_{j\in J}(e(g^{\theta s_j}T_{\varphi(j)}^{-c_j}, g^r)e(g^{c_j}, T_{\varphi(j)}^r))^{\eta_j} \\ &= e(g,g)^{\sum_{j\in J}\theta r s_j \eta_j} \\ &= e(g,g)^{\theta r \sum_{j\in J} s_j \eta_j} \\ &= e(g,g)^{\theta rs}. \end{aligned}$$

Step 2. It calculates

$$\begin{aligned} V_2 &= e(E_b, K_b)/V_1 \\ &= e(g^s, g^{\mu+\theta\cdot r})/e(g,g)^{\theta rs} \\ &= e(g,g)^{\mu s}. \end{aligned}$$

Step 3. It calculates

$$\begin{aligned} E/V_2 &= m\cdot e(g,g)^{\mu s}/e(g,g)^{\mu s} \\ &= m. \end{aligned}$$

This scheme is provided with a zero-knowledge proof of knowledge of the statement $POK\{(MS) : (PP, MS) \in Setup(1^\kappa)\}$ that is given by $POK\{(\theta, g^\mu) : g^\theta \wedge e(g, g^\mu)\}$.

We prove that this **CP-ABE** scheme is committing as follows:

ABE.KeySanityCheck$(PP, S, PriKey_S)$**.** Parse $PriKey_S$ as $(K_b, D_b, \{K_d\}_{d\in S})$), and checks whether $e(K_b, g) = e(g^\theta, D_b)\cdot e(g,g)^\mu$ and for any attribute $d \in S$, $e(g, K_d) = e(D_b, T_d)$ holds. If so, it outputs `Valid`, else `Invalid`.

ABE.CiphertextSanityCheck$(PP, CT_{(M,\varphi)}$**.** Parse $\mathrm{CT}_{(M,\varphi)}$ as $((M,\varphi), E_b = g^s, E = m\cdot e(g,g)^{\mu s}$, $\{E_j = g^{\theta s_j}T_{\varphi(j)}^{-c_j}, F_j = g^{c_j}\}_{j=1,\cdots,h})$. Check whether $\prod_{\varphi(j)\in S} e(E_j, g)^{\eta_j} = \prod_{\varphi(j)\in S} e(F_j, T_{\varphi(j)}^{-1})^{\eta_j}\cdot e(g^\theta, E_b)$ holds. If so, output `Valid`; if not, output `Invalid`.

6 Blind Private Key Generation Protocol

A blind private key generation protocol is employed to extend **CP-ABE** scheme to enforce fine-grained access control on the encrypted data. Assuming database DB and credential issuer `I` operate on a universe $\mathbb{S}$ of attribute. U obtains a credential certifying that U has attribute set S from `I`. U and `I` engage in the credential issuing protocol as follows.

Issue():

1) U obtains $S_U \leftarrow S_U \cup \{att\}$ and sends S_U to I.
2) I checks S_U.
3) I generates a credential for S_U, i.e. $Cred(S_U)$, and sends it to U.
4) U obtains $Cred(S_U)$.

We employ full simulatable k-out-of-N oblivious transfer scheme and the credential scheme.`I` runs KeyGen(1^κ) of the credential scheme to generate $(PriKey_{\mathtt{I}}, PK_{\mathtt{I}})$. DB runs $ABE.Setup(1^k)$ to generate PP, MS. U have both $PK_{\mathtt{I}}$ and PP. A blind private key generation protocol for **CP-ABE** scheme is depicted as follows.

BlindPriKeyGen():

1) U calculates commitments $\{(Com_i, Decom_i) = Commit(i)\}_{i\in S}$ and sends $\{Com_i\}_{i\in S}$ to DB.
2) U proves in zero-knowledge possession of credential $Cred(S_U)$ to DB.
3) If the proof fails, abort.
4) DB runs $PriKeyGen(MS, S) \rightarrow PriKey_S$ to generate $PriKey_S = (K_b = g^{\mu+\theta\cdot r}, D_b = g^r, \{K_d = T_d^r\}_{d\in S})$. DB as a sender and U as a receiver runs a full simulatable k-out-of-N oblivious transfer protocol.
5) U inputs S as selection values.
6) DB inputs commitments $\{com_i\}_{i\in S}$ and $\{K_d\}_{d\in\mathbb{S}}$ as messages to be received.
7) U obtains $\{K_d\}_{d\in S}$.
8) DB returns nothing.
9) DB sends K_b, D_b to U.
10) U sets $PriKey_S = (K_b = g^{\mu+\theta\cdot r}, D_b = g^r, \{K_d = T_d^r\}_{d\in S})$ and calls $ABE.KeySanityCheck(PP, S, PriKey_S)$, if the output is `Valid`, U obtains PriKey_S.

As a result, U obtains a private key associated with S and DB does not learn anything about S.

Theorem 1. *This Blind Private Key Generation protocol can securely realize F_{BPKG}.*

Proof. We define a simulator $\mathtt{Sim}_{BPKG}$ which runs `A` as a subroutine and interacts with $\mathtt{F}_{BPKG}$. Given a real world attacker `A`, we construct an ideal world attacker $\mathtt{A}^*$ such that no environment `E` can distinguish between the real and the ideal world. Security is proved under a secure credential scheme and a secure oblivious transfer scheme. The secure credential scheme implies a simulator $Sim_{Credential}$ which interacts with $\mathtt{F}_{Credential}$ and `E` such that `E` cannot distinguish between the real and the ideal world. The secure oblivious transfer scheme implies a simulator Sim_{OT} which interacts with $\mathtt{F}_{OT}$ and `E` such that `E` cannot distinguish the real world from the ideal world.

The cases are not considered as follows: All parties are honest, all parties are dishonest, the issuer is the only honest party, or the issuer is the only dishonest party, since theses cases have no real practical interest.

For the remaining each case, we define a sequence of games to prove the indistinguishability between the real and ideal worlds. Let $\mathtt{Adv}[\mathbf{Game\ I}]$ denotes the advantage that $\mathtt{E}$ distinguishes between the ensemble of **Game I** and that of the real execution. We consider the four cases as follows. □

Case 1. *When attacker $\mathtt{A}$ corrupts the issuer $\mathtt{I}$ and the database DB, the ensembles $\boldsymbol{REAL}_{A,E}$ and $\boldsymbol{IDEAL}_{A^*,E}$ are computationally indistinguishable provided that the credential scheme is secure and the oblivious transfer scheme is secure.*

Proof. By applying all the changes represented in $Sim_{Credential}$, the environment $\mathtt{E}$ cannot distinguish between the real world and the ideal world provided that the credential scheme is secure. By applying all the changes represented in Sim_{OT}, the environment $\mathtt{E}$ cannot distinguish between the real world and the ideal world, provided that the oblivious transfer scheme is secure. Therefore, this distribution is identical to that of Sim_{BPKG}. □

Case 2. *When attacker $\mathtt{A}$ corrupts the database DB, the ensembles $\boldsymbol{REAL}_{A,E}$ and $\boldsymbol{IDEAL}_{A^*,E}$ are computationally indistinguishable provided that the credential scheme is secure and the oblivious transfer scheme is secure.*

Proof. The proof is similar to that of Case 1. □

Case 3. *When attacker $\mathtt{A}$ corrupts some users, the ensembles $\boldsymbol{REAL}_{A,E}$ and $\boldsymbol{IDEAL}_{A^*,E}$ are computationally indistinguishable, provided that the credential scheme is secure,the oblivious transfer scheme is secure and the commitment scheme is binding.*

Proof. By applying all the changes represented in $Sim_{Credential}$, the environment $\mathtt{E}$ cannot distinguish between the real world and the ideal world, provided that the credential scheme is secure. By applying all the changes represented in Sim_{OT}, the environment $\mathtt{E}$ cannot distinguish between the real world and the ideal world, provided that the oblivious transfer scheme is secure. If the selection values $\sigma_1, \cdots, \sigma_k$ generated by Sim_{OT} is different from attribute sets S generated by Sim_{OT}, it means that $\mathtt{A}$ can de-commit any of the commitments to two different values, which happens with negligible probability since the commitment scheme is binding. Therefore, this distribution is identical to that of Sim_{BPKG}. □

Case 4. *When attacker $\mathtt{A}$ corrupts the issuer $\mathtt{I}$ and some users U, the ensembles $\boldsymbol{REAL}_{A,E}$ and $\boldsymbol{IDEAL}_{A^*,E}$ are computationally indistinguishable provided that the credential scheme is secure, the oblivious transfer scheme is secure and the commitment scheme is binding.*

Proof. The proof is similar to that of Case 3. □

7 Fully Simulatable Oblivious Transfer with Fine Grained Access Control

Definition 5. *(Functionality $F_{SOTFGAC}$) Functionality $F_{SOTFGAC}$ performs as follows:*

* *On receiving (`issue`, att) from $\mathtt{U}_z$, in which att $\in \mathbb{S}$, it sends (issue, $\mathtt{U}_z$, att) to $\mathtt{I}$ that sends back a bit β. If $\beta = 1$, then att is added to $S_{\mathtt{U}_z}$, and β is sent to $\mathtt{U}_z$; else β is simply sent to $\mathtt{U}_z$.*
* *On receiving (`initialize`, $(m_l, \mathbb{A}_l)_{l=1,\cdots,N}$) from $\mathtt{DB}$, it sets $DB \leftarrow (m_l, \mathbb{A}_l)_{l=1,\cdots,N}$.*
* *On receiving (`transfer`, S) from $\mathtt{U}_z$, it proceeds as follows: If $DB \neq \perp$, it sends `transfer` to DB that returns a bit β. If $\beta = 0$ or $DB = \perp$, it sends $\perp$ to $\mathtt{U}_z$. If $\beta = 1$ and S satisfies access structures $\mathbb{A}_l$, it sends $(m_1^*, \cdots, m_N^*)$ to $\mathtt{U}_z$.*

7.1 Construction

Our construction employs the blind **CP-ABE** scheme to certify the attributes of users and to enforce fine grained access control. Here, $m_1, \cdots, m_N \in \{0,1\}^n$, and hash functions $H : m \rightarrow \{0,1\}^n$ are modelled as a random oracle. Credential Issuing phase is depicted in Section 6. Initialization phase is depicted as follows:

1) DB_I: Select $(PP, MS) \leftarrow ABE.Setup(1^k)$.
2) DB_I: Select random values $W_l \in \mathbb{G}_T$, and for $l = 1, \cdots, N$ set:
$$\begin{aligned} A_l &= ABE.Encrypt(PP, \mathbb{A}_l, W_l) \\ B_l &= H(W_l) \bigoplus m_l \\ C_l &= (A_l, B_l). \end{aligned}$$
3) DB_I: Execute $PoK\{(MS): (PP, MS) \in ABE.Setup(1^k)\}$.
4) DB_I: Send $\{PP, C_1, \cdots, C_N\}$ to U.
5) U_I: If the proof does not verify, or $ABE.CiphertextSanityCheck$ returns `Invalid`, these ciphertexts are rejected.
6) U_I: $R_0 = (PP, (C_1, \cdots, C_N))$.
7) DB_I: Return $S_0 = (PP, MS)$.

In the l^{th} transfer, `BlindPriKeyGen()` is run, and U obtains PriKey_S. Transfer phase is depicted as follows:

1) U_T: If `BlindPriKeyGen()` fails, then $m_l^* = \perp$.
2) U_T: Else for $l = 1$ to N, U_T checks whether S satisfies the access structure $\mathbb{A}_l$. If so, U runs $W_{\sigma_l} = ABE.Decrypt(PP, A_{\sigma_l}, PriKey_S)$, and obtains the messages $m_{\sigma_l}^* = H(W_{\sigma_l}) \bigoplus B_{\sigma_l}$; otherwise, $m_{\sigma_l}^* = \perp$.

3) U_T: Return $R_l = (R_{l-1}, m^*_{\sigma_l}, S)$.

4) DB_T: Return $S_l = (S_{l-1})$.

The encryption technique employed is secure in the random oracle model.

7.2 Proof of Security

Theorem 2. *$F_{SOTFGAC}$ is securely realized by fully simulatable oblivious transfer with fine grained access control.*

Proof. Given a real world attacker A, we construct an ideal world attacker $\mathtt{A}^*$ such that no environment E can distinguish between the real and the ideal world.The cases are not considered as follows: all parties are honest, all parties are dishonest, the issuer is the only honest party, or the issuer is the only dishonest party, since theses cases have no real practical interest.

For the remaining each case, we define a sequence of games to prove the indistinguishability between the real world and the ideal world. Let Adv[**Game I**] denotes the advantage that E distinguishes between the ensemble of **Game I** and that of the real execution. We define some set of negligible functions in which $\upsilon_n()$ denotes the n^{th} function. We consider the four cases as follows. □

Case 1. *When the real world attacker A corrupts I and DB, the ensembles $\boldsymbol{REAL}_{A,E}$ and $\boldsymbol{IDEAL}_{A^*,E}$ are computationally indistinguishable provided that proofs of knowledge are extractable, the **CP-ABE** is committing and secure is the blind private key generation with access control in the random oracle model.*

Proof.

Game 0. In this game, the dishonest real world DB and I interacts with the real world honest users $\mathtt{U}_z$. Hence, $Adv[Game0] = 0$.

Game 1. This game is the same as Game 0, except that the knowledge extractor is employed to extract MS from the proof of knowledge $\mathtt{POK}\{MS : (PP, MS) \in ABE.Setup(1^k)\}$. Since this extractor succeeds with all but negligible probability, Adv[Game 1] − Adv[Game 0] $\leq \upsilon_1(\kappa)$.

Game 2. This game is the same as Game 1, except that all ill-formed ciphertexts detected by running $ABE.CiphertextSanityCheck$ are rejected. The committing CP-ABE scheme ensures that if a ciphertext is valid via $ABE.CiphertextSanityCheck$, then it decrypts to the same message by employing any valid private key.Hence, Adv[Game 2]−Adv[Game 1] = 0.

Game 3. This game is the same as Game 2, except that it carries out all the changes depicted in $\mathtt{Sim}_{BPKG}$. Since the blind private key generation with fine grained access control is secure, it holds that Adv[Game 3] − Adv[Game 2] $\leq \upsilon_3(\kappa)$.

By summation, it holds that Adv[Game 3]−Adv[Game 0] = Adv[Game 3] is negligible. □

Case 2. *When the real world attacker A corrupts DB, the ensembles $\boldsymbol{REAL}_{A,E}$ and $\boldsymbol{IDEAL}_{A^*,E}$ are computationally indistinguishable provided that secure is the blind private key generation with access control in the random oracle model,proofs of knowledge are extractable, and the **CP-ABE** is committing.*

Proof. This proof is similar to that of Case 1. □

Case 3. *When the real world attacker A corrupts some users $\mathtt{U}_z$, the ensembles $\boldsymbol{REAL}_{A,E}$ and $\boldsymbol{IDEAL}_{A^*,E}$ are computationally indistinguishable provided that secure is the blind private key generation with access control in the random oracle model, proofs of knowledge are zero knowledge, and the **CP-ABE** scheme is secure.*

Proof.

Game 0. In this game, the honest real world DB and I interacts with the real world cheating user U . Hence, $Adv[Game0] = 0$.

Game 1. This game is the same as Game 0, except that a simulated proof is employed to replace the proof of knowledge $\mathtt{POK}\{MS : (PP, MS) \in ABE.Setup(1^k)\}$. Based on the zero-knowledge property of the zero-knowledge proof, it holds that Adv[Game 1] − Adv[Game 0] $\leq \upsilon_1(\kappa)$.

Game 2. This game is the same as Game 1, except that we employ all the changes presented in $\mathtt{Sim}_{BPKG}$. The secure blind private key generation with access control protocol implies that protocol execution in the real world is indistinguishable from the interaction between $\mathtt{Sim}_{BPKG}$ and $\mathtt{F}_{BPKGAC}$. Hence, Adv[Game 2] − Adv[Game 1] $\leq \upsilon_2(\kappa)$.

Game 3. This game is the same as Game 2, except that random values are employed to replace $B_1, \cdots, B_N$. We construct an algorithm A which breaks the security of the CP-ABE with non-negligible advantage. The challenger of the security game of the CP-ABE gives the public parameters of the CP-ABE to A. For $l = 1$ to N, A selects a random P_0,sets $P_1 = A_l$ and sends (P_0, P_1) to the challenger. The challenger tosses a fairly binary coin β and sends back a challenge ciphertext $A_l = ABE.Encrypt(PP, \mathbb{A}_l, P_\beta)$. A continues the simulation. On receiving a query, if it is not equal to P_0, or P_1 then A returns $\perp$. If it is P_0, A sets $\beta^* = 0$, else, A sets $\beta^* = 1$. A sends β^* to the challenger. The distribution in Game 3 is the same as that of the simulation. Hence, it holds that Adv[Game 3] − Adv[Game 2] $\leq \upsilon_3(\kappa)$.

By summation, it holds that Adv[Game 3]−Adv[Game 0] = Adv[Game 3] is negligible. □

Case 4. *When the real world attacker* $\mathtt{A}$ *corrupts some users* U *and* $\mathtt{I}$*, the ensembles* $\boldsymbol{REAL}_{A,E}$ *and* $\boldsymbol{IDEAL}_{A^*,E}$ *are computationally indistinguishable provided that secure is the blind private key generation with access control in the random oracle model, proofs of knowledge are zero knowledge, and the* ***CP-ABE*** *scheme is secure.*

Proof. The proof of Case 4 is similar with that of Case 3. □

8 Performance Evaluation

As depicted in Table 1 where *cat* denotes *category* and || denotes the cardinality of the set: for access policy, CDN scheme supports conjunction, and disjunction via duplication, whereas our scheme supports conjunction, disjunction and threshold directly. For the encrypted record size, given a conjunction normal form $(I_{1,1} \vee \cdots \vee I_{1,y_1}) \wedge \cdots \wedge (I_{n,1} \vee \cdots \vee I_{n,y_n})$, 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, 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 greatly reduces the size of encrypted database. For credential issuing phase, both schemes have communication complexity linear in the number of attributes possessed by some user. For initialization phase, both schemes have computation complexity linear in the number N of messages. For transfer phase, our scheme have communication complexity linear in the cardinality of the attribute universe, 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 obtains all the records which she is authorized to access. Hence, when fine grained access control needs to be enforced or the number of records authorized to access is larger, our scheme is more efficient than the CDN scheme.

9 Conclusion and Future Work

In this work, we propose an oblivious transfer scheme with fine grained access control from ciphertext policy attribute based encryption 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. In the future work, we will design a scheme where access policies are hidden to furthermore enhance privacy.

10 Acknowledgments

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

References

[1] A. Beimel, *Secure Schemes for Secret Sharing and Key Distribution*, Ph.D Thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[2] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE Symposium on Security and Privacy*, pp. 321–334, 2007.

[3] J. Camenisch, M. Dubovitskaya, and G. Neven, "Oblivious transfer with access control," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, pp. 131–140, 2009.

[4] T. Y. Chang and W. P. Yang M. S. Hwang, "An improved multi-stage secret sharing scheme based on the factorization problem," *Information Technology and Control*, vol. 40, pp. 246–251, 2011.

[5] L. Cheung and C. C. Newport, "Provably secure ciphertext policy ABE," in *ACM Conference on Computer and Communications Security*, pp. 456–465, 2007.

[6] P. S. Chung, C. W. Liu, and M. S. 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.

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

[8] R. Cramer, I. Damgard, and P. D. MacKenzie, "Efficient zero-knowledge proofs of knowledge without intractability assumptions," in *3rd International Workshop on Theory and Practice in Public Key Cryptography (PKC'00)*, LNCS 1751, pp. 354–372, Melbourne, Victoria, Australia, Jan. 2000.

[9] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute-based encryption," in *Proceedings of 35th International Colloquium (ICALP'08)*, pp. 579–591, Reykjavik, Iceland, July 7-11, 2008.

[10] 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*, pp. 89–98, 2006.

[11] M. Green and S. Hohenberger, "Blind identity-based encryption and simulatable oblivious transfer," in *Advances in Cryptology (ASIACRYPT'07)*, LNCS 4833, pp. 265–282, 2007.

[12] C. C. Lee, P. S. Chung, and M. S. 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.

Table 1: Comparison of our scheme with CDN scheme

References	Access Policy	Encrypted Record Size	Credential Issuing Phase	Initialization Phase	Transfer Phase
CDN Scheme [3]	conjunction and disjunction via duplication	$\prod_{i=1}^{n} y_i$	$\mathcal{O}(\|cat\|)$	$\mathcal{O}(N)$	$\mathcal{O}(\|cat\|)$
Our Scheme	conjunction, disjunction and threshold	$\sum_{i=1}^{n} y_i$	$\mathcal{O}(\|S\|)$	$\mathcal{O}(N)$	$\mathcal{O}(\|\mathbb{S}\|)$

[13] A. Lewko, T. Okamoto, A. Sahai, and K. Takashima, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Advances in Cryptology (EUROCRYPT'10)*, LNCS 6110, pp. 62–91, 2010.

[14] T. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Advances in Cryptology (CRYPTO'91)*, LNCS 576, pp. 129–140, Heidelberg, 1991.

[15] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems," in *ACM Conference on Computer and Communications Security*, pp. 99–112, 2006.

[16] A. S. R. Ostrovsky and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *ACM Conference on Computer and Communications Security*, pp. 195–203, 2007.

[17] A. Sahai and B. Waters, "Fuzzy identity based encryption," in *Advances in Cryptology (Eurocrypt'05)*, LNCS 3494, pp. 457–473, 2005.

[18] Subba Rao Y V and Chakravarthy Bhagvati, "CRT based threshold multi secret sharing scheme," *International Journal of Network Security*, vol. 16, no. 4, pp. 249–255, 2014.

[19] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Public Key Cryptography (PKC'11)*, LNCS 6571, pp. 53–70, 2011.

[20] Ye Zhang, M. Ho 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-Based Cryptography (Pairing'10)*, LNCS 6487, pp. 96–115, 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, and cryptography.

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 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.