Information **2015**, *6*, 481-493; doi:10.3390/info6030481

OPEN ACCESS

information

ISSN 2078-2489

www.mdpi.com/journal/information

Article

Black Box Traceable Ciphertext Policy Attribute-Based Encryption Scheme

Xingbing Fu [1,*], Xuyun Nie [1] and Fagen Li [2]

[1] School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, 610054, China; E-Mail: xynie@uestc.edu.cn

[2] School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, 611731, China; E-Mail: fagenli@uestc.edu.cn

* Author to whom correspondence should be addressed; E-Mail: fuxbuestc@126.com;
Tel.: +86-28-8320-1203.

Academic Editor: Willy Susilo

Received: 9 June 2015 / Accepted: 5 August 2015 / Published: 14 August 2015

Abstract: In the existing attribute-based encryption (ABE) scheme, the authority (*i.e.*, private key generator (PKG)) is able to calculate and issue any user's private key, which makes it completely trusted, which severely influences the applications of the ABE scheme. To mitigate this problem, we propose the black box traceable ciphertext policy attribute-based encryption (T-CP-ABE) scheme in which if the PKG re-distributes the users' private keys for malicious uses, it might be caught and sued. We provide a construction to realize the T-CP-ABE scheme in a black box model. Our scheme is based on the decisional bilinear Diffie-Hellman (DBDH) assumption in the standard model. In our scheme, we employ a pair (ID, S) to identify a user, where ID denotes the identity of a user and S denotes the attribute set associated with her.

Keywords: black box; CP-ABE; oblivious transfer; private key generator; tracing

1. Introduction

With the advent of cloud computing, more and more data and computations will be migrated to the cloud. Storing the data in the cloud has advantages as follows: individuals can reliably store the data and can easily and conveniently access the data; and organizations can save costs. However, when the data are stored remotely, acute concerns for security and privacy are raised. That is to say the sensitive data, such as financial and medical records, are out of the owners' control and may be accessed by untrusted parties. A traditional public key cryptosystem cannot be employed to protect the data well, since they have drawbacks as follows: (1) they only provide coarse-grained access to encrypted data decrypted only by a single secret key; (2) access to the encrypted data is all or nothing; one can either decrypt to recover the entire ciphertext or learns nothing from the plaintext, except for its length. In the cloud computing system, the data owner may share the data with groups of data consumers based on their attributes or credentials, and only the data consumers whose attributes satisfy the access policy can decrypt. The traditional public key cryptosystem cannot address these problems [1,2].

To address these problems, Sahai *et al.* [3] first presented the attribute-based encryption (ABE) scheme enforcing fine-grained access control over the ciphertexts. In their scheme, a ciphertext and a private key are associated with descriptive attribute sets. Decryption will succeed if and only if there exist at least d attributes overlapping them. Their scheme is suitable for error-tolerant encryption. However, one drawback of their scheme is that this construction is only able to address formulae comprising one threshold gate. To enhance the expressiveness, Goyal *et al.* [4] presented the key policy attribute-based encryption (KP-ABE) scheme in which ciphertexts are associated with attribute sets and the private keys are associated with access structures. While they proposed the CP-ABE scheme, they did not implement it. Bethencourt *et al.* [5] first implemented the CP-ABE scheme. In their scheme, attribute sets are employed to identify the private keys, and ciphertexts are associated with access structures. The ciphertexts are decrypted by the private keys iff the access structures are satisfied by the attribute sets. However, they proved security in the generic group model. To achieve CP-ABE schemes in the standard model, work has been done as follows: Cheung *et al.* [6] presented a CP-ABE scheme constructed under a policy with an AND gate. However, their scheme requires that the number of system attributes be fixed at setup, and the access structure of their scheme only supports an AND gate. These two drawbacks make it less expressive. To enhance the expressiveness, Goyal *et al.* [7] proposed the bounded CP-ABE scheme. However, the encryption and decryption cost blows up greatly, which influences its application in practice. Lewko *et al.* [8] presented a CP-ABE scheme that is expressive and adaptively secure. However, their scheme is based on a composite order bilinear group, which incurs some efficiency loss, and the assumption is a non-standard strong assumption. Waters [9] proposed an expressive, efficient and provable secure CP-ABE scheme in the standard model and achieves the same performance and functionality as the scheme of [5]. Researchers applied CP-ABE schemes to a cloud storage system, social networks, *etc*.

In a CP-ABE scheme, a private key for a user's attributes is not able to be generated by herself. Hence, there exists a trusted party, named the authority, *i.e.*, the private key generator (PKG), which sets up the system. To get a private key from the PKG, a user with some attributes will go to a PKG to get the private key associated with her attributes. During this process, she needs to prove to the PKG that these attributes are entitled to her. Then, the private key is generated and passed on to her by the PKG. Since the authority possesses the master secret of the scheme, it is capable of calculating the private key associated with the users' arbitrary attributes, and it is able to decrypt any ciphertexts encrypted to any users; it has to be absolutely trusted. If the authority engages in malicious activities, it will not be caught and sued. Thus, it is required that the trust in the authority should be reduced in a CP-ABE scheme.

That is to say, there still exists the key escrow problems in the CP-ABE scheme. Due to the inherent key escrow problem, the CP-ABE scheme is restricted to be used in the small and closed groups, where there exists a central trusted authority. If this problem is not solved well, it will influence the adoption of the CP-ABE scheme.

Our contributions: We formalize the conception of the black box traceable ciphertext policy attribute-based encryption scheme and propose its construction. This construction builds on the ciphertext policy attribute-based encryption scheme presented by [9]. In this scheme, a secure private key generation protocol is constructed. A new security proof is presented to show that this scheme is a traceable (T)-CP-ABE scheme, which handles black box decoders. In this T-CP-ABE scheme, the authority will access decryption oracles, and a judge will decide whether the decoder box is created by the malicious authority or the malicious user.

Organization: The remainder of our paper is organized as follows. Preliminaries are presented in Section 2. The scheme definition and the definition of the security game are presented in Section 3. The scheme construction is presented in Section 4. Security is proven in Section 5. Related works are discussed in Section 6. We make a conclusion and specify future work in Section 7.

2. Preliminaries

2.1. Bilinear Map

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two cyclic groups whose orders are prime order p, respectively. g, u are a generator of $\mathbb{G}$, respectively. e is a bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, which has 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 operations on $\mathbb{G}$ and on the bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ are efficiently computable, then $\mathbb{G}$ is a bilinear group. In our scheme, the symmetric bilinear map is employed, such that: $e(g^a, u^b) = e(g, u)^{ab} = e(g^b, u^a)$.

2.2. Access Structure

Let $\mathbb{S}$ be the universe of attributes. An access structure [10] 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 the monotone access structure is handled.

2.3. Linear Secret Sharing Scheme

A secret sharing scheme [10] 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 c columns for Π. For any $i = 1, \cdots, h$, let the function φ defined the attribute that labels the i-th row as $\varphi(i)$. 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 picked at random, then $M\overrightarrow{v}$ is the vector of h shares of the secret s based on Π. The share $(M\overrightarrow{v})_i$ belongs to the attribute $\varphi(i)$.

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

2.4. Complexity Assumptions

Decisional bilinear Diffie-Hellman (DBDH): Let $\mathcal{G}(1^\kappa) \rightarrow (p, g, \mathbb{G}, \mathbb{G}_T, e)$. Pick $\xi, \varpi, \rho, d \in \mathbb{Z}_p$ uniformly at random. No probabilistic polynomial time (PPT) attackers $\mathcal{A}$ are able to distinguish the tuple $(A = g^\xi, B = g^\varpi, C = g^\rho, D = e(g, g)^{\xi\varpi\rho})$ from the tuple $(A = g^\xi, B = g^\varpi, C = g^\rho$, $D = e(g, g)^d)$ with non-negligible advantages.

2.5. Fully Simulatable k*-out-of-*N *Oblivious Transfer*

A k-out-of-N oblivious transfer protocol makes a recipient pick and receive exactly k of the N messages from the sender, such that the remaining messages are hidden from the recipient and the choices of the recipient are hidden from the sender. We employ fully-simulatable oblivious transfer [11].

2.6. Ciphertext Policy Attribute-Based Encryption

Waters [9] proposed the ciphertext policy attribute-based encryption (CP-ABE) scheme, which is expressive, efficient and provably secure. In this scheme, ciphertexts are associated with access structures, and private keys are associated with attribute sets. They proposed a CP-ABE scheme, which is proven secure in the DBDH assumption in the standard model. Our scheme in part builds on this scheme.

3. Syntax and Definition of Security

3.1. Our Scheme Definition

Definition 1. *A traceable ciphertext policy attribute-based encryption (T-CP-ABE) scheme comprises five components.*

Setup$(1^k) \rightarrow (\mathtt{MSK}, \mathtt{PP})$: *The **Setup** algorithm takes in a security parameter* κ*, and it returns a master secret key* $\mathtt{MSK}$ *and the public parameters* $\mathtt{PP}$*.*

PriKeyGen$(\mathtt{PP}, \mathtt{MSK}, \mathtt{ID}, S)(\rightarrow)K_{ID,S}$: *This is a private key generation algorithm, which takes in* $\mathtt{PP}$,$\mathtt{MSK}$*,* S *and* $\mathtt{ID}$ *employed to trace back to the corresponding owner and the* $\mathtt{Authority}$ *engages in an oblivious transfer protocol with a user* $\mathtt{U}$*, where* S *is an attribute set belonging to the user* $\mathtt{U}$*. At the end,* $\mathtt{U}$ *receives a private key for her* $\mathtt{ID}$ *and her attribute set* S*,* $K_{(ID,S)}$*. The notation* $(\rightarrow)$ *denotes the fact that the authority may not exactly know which key the user has received.*

Encrypt$(\mathtt{PP}, \mathtt{ID}, \mathbb{A}, m) \rightarrow \mathtt{CT}_{\mathtt{ID},\mathbb{A}}$: *The **Encrypt** algorithm takes in the public parameters* $\mathtt{PP}$*, the identity* $\mathtt{ID}$*, access structure* $\mathbb{A}$ *and a message* $\mathtt{m}$ *and it returns a ciphertext* $\mathtt{CT}_{\mathtt{ID},\mathbb{A}}$*.*

Decrypt$(\mathtt{PP}, \mathtt{CT}_{\mathtt{ID},\mathbb{A}}, K_{ID,S}) \rightarrow m$: *The **Decrypt** algorithm takes in the public parameters* $\mathtt{PP}$*, the ciphertext* $\mathtt{CT}_{\mathtt{ID},\mathbb{A}}$ *and a private key* $K_{ID,S}$*. It returns a plaintext message* m *if the identity of the private key matches that of the ciphertext and the attribute set* S *satisfies the access structure* $\mathbb{A}$*, else it returns an error symbol* $\perp$*.*

Definition 2. *(ε **Useful Decoder Box**) A **PPT** algorithm $\mathcal{D}$ is a ε **Useful Decoder Box** for the identity $\texttt{ID}$, where ε is non-negligible, if $Pr[\mathcal{D}(\textbf{\textit{Encrypt}}(\texttt{PP}, \texttt{ID}, \mathbb{A}, m)) = m] > \varepsilon$.*

Trace$^{\mathcal{D}}(\texttt{PP}, \texttt{ID}, K_{ID,S}, \varepsilon) \rightarrow \{\texttt{User}, \texttt{Authority}\}$*: The **Trace** algorithm takes in the identity $\texttt{ID}$, the public parameters $\texttt{PP}$, a well-formed private key $K_{ID,S}$, a parameter ε and has black box access to a ε useful decoder box $\mathcal{D}$. It outputs $\texttt{User}$ or $\texttt{Authority}$.*

The tracing algorithm allows an honest user to present her private key and a captured decoder box to a judge to incriminate the misfeasance of $\texttt{Authority}$; furthermore, the tracing algorithm hinders a dishonest user from falsely incriminating that the $\texttt{Authority}$ has created the decoder box.

3.2. Definition of Security

A secure black box traceable ciphertext policy attribute-based encryption (T-CP-ABE) scheme holds if the following three requirements are met: (1) it satisfies **IND-ID-CCA** security; (2) if the $\texttt{Authority}$ created a decoder box $\mathcal{D}$, the tracing algorithm should incriminate the $\texttt{Authority}$; (3) if the colluding users created the decoder box $\mathcal{D}$, it should incriminate these users. We capture the security conditions in the three games as follows:

Definition 3. ***(IND-ID-Chosen Plaintext Attacks (CPA) Security Game)** A T-CP-ABE scheme is **IND-ID-CPA** secure if no **PPT** attacker $\mathcal{A}$ has non-negligible advantages in this game:*

***Setup:** The challenger runs the **Setup** algorithm generating $\texttt{MSK}$ and $\texttt{PP}$ given to the attacker $\mathcal{A}$.*

***Query Phase 1:** The attacker $\mathcal{A}$ runs the interactive **PriKeyGen** protocol with the challenger for adaptively-picked identities $\texttt{ID}_i$ and attribute sets S_i, where $i \in \{1, \cdots, q\}$, and receives the corresponding private keys K_{ID_i,S_i}.*

***Challenge:** The attacker $\mathcal{A}$ submits two plaintext messages m_0 and m_1, which are of equal length, challenge identity $\texttt{ID}^\star$ and a challenge access structure $\mathbb{A}^\star$, except that $\texttt{ID}^\star$ should not be equal to any of the identities queried in **Query Phase 1**, and the access structure $\mathbb{A}^\star$ is satisfied by none of the attribute sets S_i where $i \in \{1, \cdots, q\}$ in **Query Phase 1**. The challenger flips a fair binary coin $\beta \in \{0, 1\}$ and encrypts m_β with $\texttt{ID}^\star$ and $\mathbb{A}^\star$. The resulting ciphertext $\texttt{CT} = \textbf{\textit{Encrypt}}(PP, ID^\star, \mathbb{A}^\star, m_\beta)$ is passed on to the attacker $\mathcal{A}$.*

***Query Phase 2:** Phase 1 is repeated, except that $\texttt{ID}^\star$ should not be equal to any of the identities in $\texttt{ID}_i$, and the access structure $\mathbb{A}^\star$ is satisfied by none of the attribute sets S_i in which $i \in \{q+1, \cdots, Q\}$, where Q is the number of the queries made by the attacker.*

***Guess:** The attacker returns a guess $\beta' \in \{0, 1\}$ of β; if $\beta' = \beta$, the attacker will win.*

Definition 4. *The proposed scheme is secure against chosen plaintext attacks (CPA) if no probabilistic polynomial time adversary has a non-negligible advantage in the aforementioned game, in which the advantage is defined as:*

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

*The above game can be extended to obtain security against chosen ciphertext attacks where decryption oracles are allowed for in **Phase 1** and **Phase 2**. Such a game is called the **IND-ID-CCA** security game.*

Definition 5. ***(Dishonest User Security Game)** In this game, some dishonest users $\texttt{ID}_i$ where $i \in \{1, \cdots, Q\}$ collude to try to create a decoder box framing the $\texttt{Authority}$. The challenger* *and the attacker have the following common inputs: the security parameter κ and another parameter $\varepsilon = 1/poly(\kappa)$. A T-CP-ABE scheme is **Dishonest User** secure if no **PPT** attacker $\mathcal{A}$ has a non-negligible advantage in the following game:*

***Init:** The attacker $\mathcal{A}$ commits to a challenge identity $\mathtt{ID}^\star$ to the challenger.*

***Setup:** The challenger runs the **Setup** algorithm, which generates $\mathtt{MSK}$ and $\mathtt{PP}$ that are given to the attacker $\mathcal{A}$.*

***Private Key Generation Queries:** The attacker $\mathcal{A}$ runs the interactive **PriKeyGen** protocol with the challenger for adaptively-picked identities $\mathtt{ID}_i$ and attribute sets S_i, where $i \in \{1, \cdots, Q\}$, and receives the corresponding private keys $K_{\mathtt{ID}_i, S_i}$.*

***Create Decoder Box:** The attacker $\mathcal{A}$ submits a private key $K_{\mathtt{ID}^*,S}$ and a decoder box $\mathcal{D}$ for the challenge identity $\mathtt{ID}^\star$ declared in the **Init** phase.*

***Tracing Failure:** The tracing algorithm falsely incriminates the $\mathtt{Authority}$,* i.e., ***Trace**$^{\mathcal{D}}(\mathtt{ID}, K_{\mathtt{ID},S}, \varepsilon) = \mathtt{Authority}$. Furthermore, the decoder box $\mathcal{D}$ is ε useful for $\mathtt{ID}$,* i.e., *$Pr[\mathcal{D}($**Encrypt**$(\mathtt{PP}, \mathtt{ID}, \mathbb{A}, m)) = m] > \varepsilon$. If these two conditions hold, the attacker $\mathcal{A}$ will win this game.*

Definition 6. ***(Dishonest Authority Security Game)** In this game, a malicious **Authority** tries to create a decoder box framing the user. Both the challenger and the attacker **Authority** have common inputs as follows: the security parameter κ and another parameter $\varepsilon = 1/poly(\kappa)$. A traceable CP-ABE scheme is **Dishonest Authority** secure if no **PPT** attacker $\mathcal{A}$ has non-negligible advantages in the following game:*

***Setup:** The challenger is given an identity $\mathtt{ID}$ and $\mathtt{PP}$, which are generated by the attacker $\mathcal{A}$ (acting as a malicious **Authority**) and checks whether $\mathtt{ID}$ and $\mathtt{PP}$ are well formed, aborting if these checks fail.*

***PriKeyGen:** The attacker $\mathcal{A}$ and the challenger conduct the private key generation protocol to generate a private key for the identity $\mathtt{ID}$ and the attribute set S. If no party aborts, the private key $K_{\mathtt{ID},S}$ is received by the challenger as output.*

***Decryption Queries:** The attacker $\mathcal{A}$ adaptively makes queries for ciphertexts $\mathtt{CT}_1, \cdots, \mathtt{CT}_Q$ of the challenger, and the challenger responds with the decryption values under $K_{\mathtt{ID},S}$.*

***Create Decoder Box:** The attacker $\mathcal{A}$ returns a decoder box $\mathcal{D}$.*

***Tracing Failure:** The tracing algorithm falsely incriminates the $\mathtt{User}$,* i.e., ***Trace**$^{\mathcal{D}}(\mathtt{ID}, K_{\mathtt{ID},S}, \varepsilon) = \mathtt{User}$. Furthermore, the decoder box $\mathcal{D}$ is ε useful for $\mathtt{ID}$,* i.e., *$Pr[\mathcal{D}($**Encrypt**$(\mathtt{PP}, \mathtt{ID}, \mathbb{A}, m)) = m] > \varepsilon$. If these two conditions hold, the attacker $\mathcal{A}$ will win this game.*

Definition 7. *A black box T-CP-ABE scheme is secure if no $\mathtt{PPT}$ attacker $\mathcal{A}$ has non-negligible advantage in κ in the **IND-ID-CCA** security game, **Dishonest User Security Game** and **Dishonest Authority Security Game**.*

4. Scheme Construction

A ciphertext has a structure as follows: ($\mathtt{ID}$,$\mathbb{A}_1, \cdots, \mathbb{A}_Z$), where $\mathtt{ID}$ is the identity of the user and $\mathbb{A}_1, \cdots, \mathbb{A}_Z$ are Z (where Z is a positive integer) parallel repetitions, each comprising monotone access structure $\mathbb{A}_z (1 \leq z \leq Z)$. A private key has a structure as follows: ($\mathtt{ID}$,$S_1, \cdots, S_Z$), where each $S_z (1 \leq z \leq Z)$ comprises k out of N attributes. A ciphertext can be decrypted by a user $\mathtt{U}$ iff (the

$\texttt{ID}$ of the private key matches that of the ciphertext) $\texttt{AND}$ (S_1 satisfies monotone access structure $\mathbb{A}_1$) $\texttt{AND}\cdots$ $\texttt{AND}$ (S_Z satisfies monotone access structure $\mathbb{A}_Z$). Let L be the length of bits of the identity string $\texttt{ID} \in \mathbb{Z}_p$, N the global security parameter, Z super-logarithmic in N, C_{max} the maximum number of columns of the matrix M and $\texttt{ID}_j$ the j-th bit of the identity $\texttt{ID} \in \mathbb{Z}_p$. Let $[L]$, $[N]$, $[C_{max}]$ and $[Z]$ be the sets $\{1, \cdots, L\}$, $\{1, \cdots, N\}$, $\{1, \cdots, C_{max}\}$ and $\{1, \cdots, Z\}$, respectively.

Setup: For each $j \in [L]$, pick two random elements $\omega_{j,0}$ and $\omega_{j,1}$ from $\mathbb{Z}_p$ with the restriction that these $2L$ values are all different. For each $c \in [C_{max}]$, $j \in [N]$ and $z \in [Z]$, pick a random $t_{c,j,z}$ uniformly from $\mathbb{Z}_p$. Pick two random elements $\mu, \theta \in \mathbb{Z}_p$ uniformly. The public parameters are:

$$PP = (\{W_{j,z} = g^{\omega_{j,z}} : j \in [L], z \in \{0,1\}\}$$
$$\{T_{c,j,z} = g^{t_{c,j,z}} : c \in [C_{max}], j \in [N], z \in [Z]\}, U = e(g,g)^{\mu}, g, g^{\theta}).$$

The master secret key $MSK = (\{\omega_{j,z} : j \in [L], z \in \{0,1\}\}, \{t_{c,j,z} : c \in [C_{max}], j \in [N], z \in [Z]\}, \mu)$.

PriKeyGen: This protocol enables a user $\texttt{U}$ to obliviously pick which attributes she needs, employing a k-out-of-N oblivious transfer protocol upon each repetition. The corresponding same index in each repetition has distinct attributes. Distinct attributes correspond to distinct elements in $\mathbb{Z}_p$. The repetitions are conducted in parallel and are viewed as individual components of the private key.

The private key generation protocol between the **Authority** and a user $\texttt{U}$ is performed as follows:

Step 1. The user will abort if $W_{j,z}$ and $T_{c,j,z}$ are not all different.

Step 2. The **Authority** picks $Z+1$ elements $\mu_0, \cdots, \mu_Z \in \mathbb{Z}_p$ uniformly at random with the restriction that $\mu_0 + \cdots + \mu_Z = \mu$, where μ_0 is associated with the identity and $\mu_1, \cdots, \mu_Z$ are associated with the sets of attributes.

Step 3. The **Authority** picks L elements $\nu_1, \cdots, \nu_L \in \mathbb{Z}_p$ uniformly at random with the restriction that $\nu_1 + \cdots + \nu_L = \mu_0$.

Step 4. The **Authority** picks $r_{c,z}, \mu_z \in \mathbb{Z}_p : c \in [C_{max}], z \in [Z]$ uniformly at random with the restriction that $\mu_1 + \cdots + \mu_Z = \mu - \mu_0$.

Step 5. The **Authority** calculates the private key components $K_j = g^{\nu_j/\omega_{j,ID_j}}$ for any $j \in [L]$ and passes them on to the user $\texttt{U}$. It picks elements $r_{c,z} \in \mathbb{Z}_p : c \in [C_{max}], z \in [Z]$ uniformly at random, calculates the private key components $(\{K_{b,z} = g^{\mu_z} g^{\theta r_{1,z}}, D_{c,z} = g^{r_{c,z}} : c \in [C_{max}], z \in [Z]\}, \{\forall j \in S_z, K_{j,z} = \prod_{c \in [C_{max}]} T_{c,j,z}^{r_{c,z}} : c \in [C_{max}], j \in [N], z \in [Z]\})$, sends $\{K_{b,z}, D_{c,z}\}$ to the user $\texttt{U}$ and stores $K_{j,z}$.

Step 6. The **Authority** picks permutations $\mathcal{P} = (P_1, \cdots, P_Z) \in S_N^Z$ at random.

Step 7. The **Authority** and the user $\texttt{U}$ conduct Z executions of a k-out-of-N oblivious transfer protocol in which the **Authority** is a sender and the user $\texttt{U}$ is a receiver. In the z-th execution, the private input of the **Authority** is the private key components $\{K_{P_z(j),z}\}_{j=1}^{N}$, and the private input of the user $\texttt{U}$ is a set S_z of k attributes picked at random. The private output of the user is the private key component $\{P_z(j), K_{P_z(j),z}\}_{j \in S_z}$

Step 8. The **Authority** passes the permutation list $\mathcal{P}$ to the user $\texttt{U}$. The user $\texttt{U}$ checks whether she obtains the correct private key components as a percent $\mathcal{P}$. If not, it will abort.

Step 9. The user $\texttt{U}$ sets $K'_{ID,S} = (\{K_j\}_{j \in [L]}, \{K_{b,z} = g^{\mu_z} g^{\theta r_{1,z}}, D_{c,z} = g^{r_{c,z}} : c \in [C_{max}], z \in [Z]\}, \{(S_z), \{K_{j,z}\}_{j \in S_z}\}_{z \in [Z]})$ and checks whether a private key validity check on $K'_{ID,S}$ passes. If not, the user $\texttt{U}$ will abort.

Key Validity Check: For a given private key $K'_{ID,S} = (\{K_j\}_{j\in[L]}, \{K_{b,z} = g^{\mu_z} g^{\theta r_{1,z}}, D_{c,z} = g^{r_{c,z}} : c \in [C_{max}], z \in [Z]\}, \{(S_z), \{K_{j,z}\}_{j\in S_z}\}_{z\in[Z]})$ for the $\mathtt{ID}$ and attribute set S, to check whether this private key is well formed, a deterministic algorithm **Key Validity Check** is defined as follows:

Step 1.

$$e(K_{b,z}, g) \cdot e(g^\theta, D_{1,z})^{-1} = e(g^{\mu_z} g^{\theta r_{1,z}}, g) \cdot e(g^\theta, g^{r_{1,z}})^{-1} = e(g^{\mu_z}, g) = e(g,g)^{\mu_z}$$

Step 2. Check whether $e(g,g)^\mu = \prod_{j\in[L]} e(W_{j,z}, K_j) \prod_{z\in[Z]} e(g,g)^{\mu_z}$ and $\forall j \in S_z$, $e(K_{j,z}, g) = e(T_{c,j,z}, \prod_{c\in[C_{max}]} D_{c,z})$ holds. If not, it fails. If so, the private key validity check passed, and the user $\mathtt{U}$ sets $K_{ID,S} = K'_{ID,S}$.

Encrypt: The encryption algorithm takes in PP, a message $m \in \mathtt{G}_T$ and an $\mathtt{LSSS}$ access structure $\mathbb{A}_z = (M_z, \varphi_z) : z \in [Z]$, where φ_z associates rows of M_z to attributes and φ_z is an injective function. Let M_z denote an $h \times C_{max}$ matrix. This algorithm picks a random vector $\overrightarrow{v}_z = (s, y_{2,z}, \cdots, y_{C_{max},z})$ employed to share the encryption exponent $s \in \mathbb{Z}_p$. The ciphertext $\mathtt{CT}'_{\mathtt{ID},\mathbb{A}}$ is constructed as follows:

$$\begin{aligned}&\mathtt{CT}'_{\mathtt{ID},\mathbb{A}} = (\{\mathbb{A}_z\}_{z\in[Z]}, E = m \cdot e(g,g)^{\mu s}, E_{b,z} = g^s, \{(E_j = W^s_{j,ID_j}\}) : j \in [L]\},\\ &\{E_{i,c,z} = g^{\theta M_{i,c,z} v_{c,z}} T^{-s}_{c,j,z} : i \in \{1,\cdots,h\}, c \in [C_{max}], j \in S_z, z \in [Z]\})\end{aligned}$$

Ciphertext Validity Check: To check whether this ciphertext $\mathtt{CT}'_{\mathtt{ID},\mathbb{A}}$ is well formed, a deterministic **Ciphertext Validity Check** algorithm is defined as follows: If the attribute sets S_z of the private keys satisfy the access structures $\mathbb{A}_z$ of the ciphertexts, then there exist coefficients $\{\eta_{i,z} | \eta_{i,z} \in \mathbb{Z}_p : i = 1, \cdots, h, z \in [Z]\}$, such that $\sum_{\varphi(i)\in S_z} \eta_{i,z} \cdot \overrightarrow{M}_{i,z} = (1, 0, \cdots, 0)$, where $\overrightarrow{M}_{i,z}$ is the i-th row vector of the access matrix M_z. Check if $e(E_j, W_{1,ID_1}) = e(W_{j,ID_j}, E_1)$, $j \in [L]$ and $\prod_{\varphi(i)\in S_z} e(E_{i,c,z}, g)^{\eta_{i,z}} = e(g^\theta, E_{b,z}) \cdot \prod_{\varphi(i)\in S_z} e(T^{-1}_{c,j,z}, E_{b,z})^{\eta_{i,z}}$,$j \in S_z, z \in [Z]$ holds. If not, it fails and returns $\perp$. If so, the ciphertext validity check passed, and the user $\mathtt{U}$ sets $\mathtt{CT}_{\mathtt{ID},\mathbb{A}} = \mathtt{CT}'_{\mathtt{ID},\mathbb{A}}$.

Decrypt: The **Decrypt** algorithm takes in the public parameters $\mathtt{PP}$, the well-formed $\mathtt{CT}_{\mathtt{ID},\mathbb{A}}$ and $\mathtt{K}_{ID,S}$. If the identity of the private key matches that of the ciphertext and the attribute sets S_z of the private keys satisfy the access structures $\mathbb{A}_z$ of the ciphertexts, then there exist coefficients $\eta_{i,z} \in \mathbb{Z}_p$, such that $\sum_{\varphi(i)\in S_z} \eta_{i,z} \cdot \overrightarrow{M}_{i,z} = (1, 0, \cdots, 0)$; the ciphertext is decrypted to recover the message m as follows:

$$\begin{aligned}&E/\prod_{j\in[L]} e(E_j, K_j) \prod_{z\in[Z]} \{e(E_{b,z}, K_{b,z}) / \prod_{c\in[C_{max}]} e(D_{c,z}, \prod_{\varphi(i)\in S_z} E_{i,c,z})^{\eta_{i,z}} \prod_{\varphi(i)\in S_z} e(K_{j,z}, E_{b,z})^{\eta_{i,z}}\}\\ &= m \cdot e(g,g)^{\mu s} / \prod_{j\in[L]} e(W^s_{j,ID_j}, g^{\nu_j/\omega_{j,ID_j}}) \cdot \prod_{z\in[Z]}\\ &\{e(E_{b,z}, K_{b,z}) / \prod_{c\in[C_{max}]} e(g^{r_{c,z}}, \prod_{\varphi(i)\in S_z} g^{\theta M_{i,c,z} v_{c,z}} T^{-s}_{c,j,z})^{\eta_{i,z}} \prod_{\varphi(i)\in S_z} e(\prod_{c\in[C_{max}]} T^{r_{c,z}}_{c,j,z}, g^s)^{\eta_{i,z}}\}\\ &= m \cdot e(g,g)^{\mu s} / e(g,g)^{\mu_0 s} \prod_{z\in[Z]} \{e(E_{b,z}, K_{b,z}) / \prod_{c\in[C_{max}]} e(g^{r_{c,z}}, \prod_{\varphi(i)\in S_z} g^{\theta M_{i,c,z} v_{c,z}})^{\eta_{i,z}}\}\\ &= m \cdot e(g,g)^{\mu s} / e(g,g)^{\mu_0 s} \prod_{z\in[Z]} \{e(E_{b,z}, K_{b,z}) / e(g^{r_{1,z}}, \prod_{\varphi(i)\in S_z} g^{\theta M_{i,1,z} v_{1,z}})^{\eta_{i,z}}\}\\ &= m \cdot e(g,g)^{\mu s} / e(g,g)^{\mu_0 s} \prod_{z\in[Z]} \{e(g^s, g^{\mu_z} g^{\theta r_{1,z}}) / e(g^{r_{1,z}}, g^{\theta s})\}\\ &= m \cdot e(g,g)^{\mu s} / e(g,g)^{\mu_0 s} e(g,g)^{(\mu_1 + \cdots + \mu_Z)s}\\ &= m \cdot e(g,g)^{\mu s} / e(g,g)^{\mu s}\\ &= m\end{aligned}$$

Trace: The tracing algorithm runs a **Key Validity Check** to check whether the private key is well formed. It repeats the experiments $poly(\kappa)$ times as follows:

Pick a set of attributes S_z with the restriction with S_z not satisfying the access structure $\mathbb{A}_z$.

Pick a message m at random and encrypt m using the access structure $\mathbb{A}_z$.

The decoder box returns some message $m^\star = \mathcal{D}(CT_{ID,\mathbb{A}})$.

For any iteration, if $m^\star = m$, incriminate the **Authority**, else incriminate the user $\mathtt{U}$.

5. Security Proofs

The security of the aforementioned scheme is proven as follows:

Theorem 1. *The advantage of an attacker in the* ***IND-ID-CCA*** *security game is negligible for the* $\mathtt{T{-}CP{-}ABE}$ *scheme under the* $\mathtt{DBDH}$ *assumption.*

This theorem is trivially reduced to the **IND-ID-CCA** security of [9] and [12]. If an attacker breaks the **IND-ID-CCA** security of our scheme, it is trivial to construct an attacker breaking the **IND-ID-CCA** security of Naccache's scheme [12] and Waters's scheme [9]. For any message m, it is a secret shared with $m_1 \oplus m_2$ in which a random m_1 is picked uniformly and encrypted with the $\mathtt{CP{-}ABE}$ scheme [9] and m_2 with Naccache's $\mathtt{IBE}$ scheme [12] to achieve the $\mathtt{T{-}CP{-}ABE}$ scheme under the $\mathtt{DBDH}$ assumption.

Theorem 2. *Provided that the k-out-of-N oblivious transfer is secure based on the real/ideal world security definition, the advantage of an attacker in the* ***Dishonest Authority Security Game*** *is negligible for the* $\mathtt{T{-}CP{-}ABE}$ *scheme.*

Proof. This scheme comprises Z attribute sets in parallel and employs fully-simulatable oblivious transfer in the private key generation phase. If **Key Validity Check** and **Ciphertext Validity Check** pass, this scheme will incriminate the **Authority**, which can access a decryption oracle $\mathcal{D}$. Via **Key Validity Check** and **Ciphertext Validity Check**, all of the same ciphertexts can be decrypted by the users whose attributes satisfy the access structures associated with these ciphertexts to the same value, and the **Authority** can decrypt to this value.

Let $\mathcal{D}$ be a ε useful decoder box, where ε is non-negligible. Perform the experiment as follows:

Pick a set of attributes S_z, except that S_z does not satisfy the access structure $\mathbb{A}_z$.

Pick a message m at random; encrypt it employing the access structure $\mathbb{A}_z$, and this returns the resulting ciphertext $\mathtt{CT}_{\mathtt{ID},\mathbb{A}}$.

The decoder box returns $m^\star = \mathcal{D}(\mathtt{CT}_{\mathtt{ID},\mathbb{A}})$.

Return the **Authority** if $m^\star = m$. □

Theorem 3. *The advantage of an attacker in the* ***Dishonest User Security Game*** *is negligible for the* $\mathtt{T{-}CP{-}ABE}$ *scheme under the* $\mathtt{DBDH}$ *assumption.*

Proof. A user can adapt the security proof in [9] to show that the selective $\mathtt{ID}$ **Dishonest User Security Game** can be reduced to the decisional bilinear Diffie-Hellman (DBDH) assumption. □

Init: The attacker $\mathcal{A}$ declares a challenge identity $\mathtt{ID}^\star$. The ideal functionality $\mathcal{F}$ from the ideal world in the simulation based model of **Oblivious Transfer** picks $W_{j,z}$ and the challenge access structures $\{\mathbb{A}_z^\star\}_{z\in[Z]}$, which are employed to obtain the resulting challenge ciphertexts sent to the challenger $\mathcal{C}$ by $\mathcal{F}$.

Setup: The challenger $\mathcal{C}$ sends public parameters PP to $\mathcal{F}$, which transfers PP to $\mathcal{A}$.

Private Key Generation Query: If $\mathcal{A}$ makes a request for a private key on $ID \neq ID^*$, then sends the corresponding user attributes to $\mathcal{F}$ that passes it to $\mathcal{C}$, it outputs a well-formed private key that $\mathcal{F}$ sends back to $\mathcal{A}$. If $ID = ID^*$, since $\mathcal{F}$ obtains the private keys, it can pick permutations $P_1, \cdots, P_Z$, such that the private key received by $\mathcal{A}$ cannot decrypt a ciphertext containing the previously-picked access structure. $\mathcal{F}$ queries $\mathcal{C}$ for this private key and sends it back to $\mathcal{A}$.

Create Decoder Box: $\mathcal{A}$ submits a private key $K_{ID^\star,S}$ and a decoder box $\mathcal{D}$. If $\mathcal{A}$ wins the **Dishonest User Security Game**, then the **Authority** will be incriminated by the decoder box. $\mathcal{F}$ picks two messages m_0, m_1 at random sent to $\mathcal{C}$ that sends $\mathcal{F}$ a challenge ciphertext $\mathtt{CT}^\star_{\mathtt{ID},\mathbb{A}}$ under the previously-picked access structures. If $K_{ID^\star,S}$ can decrypt this message, so can $\mathcal{F}$, and $\mathcal{F}$ sends the right guess to $\mathcal{C}$; else $\mathtt{CT}_{\mathtt{ID}^\star,\mathbb{A}}$ is a random ciphertext that $ID^\star$ cannot decrypt. Hence, if $\mathcal{A}$ wins the **Dishonest User Security Game**, $\mathcal{D}$ has a non-negligible advantage in decrypting this ciphertext. Therefore, $\mathcal{F}$ has a non-negligible advantage in the attribute-based selective set game against $\mathcal{C}$, which is in contradiction with the security of the $\mathtt{CP-ABE}$ scheme under the DBDH assumption.

6. Related Work

To mitigate the trust on the PKG, Boneh *et al.* [13] proposed an approach that has the multiple PKGs distributed based on threshold cryptography. However, their scheme brings about extra infrastructure and communication. Without employing multiple PKGs, the known mitigation approaches are as follows: Goyal [14] presented a traceable identity based encryption scheme. To obtain black box security, Libert *et al.* [15] presented an IBE scheme, which is weak black box traceable, while ciphertexts and private keys are short, and Goyal *et al.* [16] proposed the black box traceable IBE scheme. Both schemes are selectively secure. To enhance the security, Libert *et al.* [15] proposed the fully-secure traceable IBE scheme. Since ABE schemes are the generalizations of IBE schemes, they inherit the key escrow problem from IBE schemes. Some traceable CP-ABE schemes [17] have been presented to handle this problem. Unfortunately, the access structures of these schemes only support the `AND` gate, which makes them less expressive. To enhance the expressiveness, Liu *et al.* [18] presented a novel T-CP-ABE scheme, which supports access polices as monotone access structures. Their scheme achieves traceability and high expressiveness at the same time. However, their scheme only achieves white box traceability. Furthermore, since their scheme builds on Lewko *et al.*'s scheme [8], which is based on the composite order group, which incurs some efficiency loss, and Lewko *et al.*'s scheme is based on non-standard assumption, Liu *et al*'s scheme [18] inherits the same drawbacks as Lewko *et al.*'s scheme.

7. Conclusions and Future Work

We present a traceable ciphertext policy attribute-based encryption scheme that addresses black box decoders. Security is proven in the **IND-ID-CCA** security game, **Dishonest User Security Game** and **Dishonest Authority Security Game**. Here, we only investigate the accountability of the attribute-based encryption scheme, which is only payload hiding, but not attribute hiding. In future work, we will design a traceable predicate encryption scheme to catch the malicious authority. Furthermore, there exists the key escrow problem in the attribute-based encryption scheme from lattice resisting quantum cryptoanalysis. To the best of our knowledge, the problem is still an open problem. In future work, we will solve this problem.

Acknowledgments

This work is supported by the NSF of China (No. 61402376) and the science and technology foundation of Sichuan Province of China (No. 2014GZ0109). The authors thank Shengke Zeng for many helpful suggestions and gratefully acknowledge the anonymous reviewers for their valuable comments.

Author Contributions

Xingbing Fu designed research and wrote the paper, Xunyun Nie and Fagen Li proposed suggestions and revised this paper. All authors have read and approved the final manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Boneh, D.; Sahai, A.; Waters, B. Functional encryption: Definitions and challenges. In *Theory of Cryptography*, Proceedings of the 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, 28–30 March 2011; Springer: Berlin/Heidelberg, Germany, 2011; Lecture Notes in Computer Science, Volume 6597, pp. 253–273.
2. Hoeteckee, W. Functional Encryption and Its Impact on Cryptography. In *Security and Cryptography for Networks*, Proceedings of the 9th International Conference, SCN 2014, Amalfi, Italy, 3–5 September 2014; Springer: Berlin/Heidelberg, Germany, 2014; Lecture Notes in Computer Science, Volume 8642, pp. 318–323.
3. Sahai, A.; Waters, B. Fuzzy identity-based encryption. In *Advances in Cryptology—EUROCRYPT 2005*, Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 22–26 May 2005; Springer: Berlin/Heidelberg, Germany, 2005; Lecture Notes in Computer Science, Volume 3494, pp. 457–473.
4. Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. Attribute-based Encryption for Fine-Grained access Control of Encrypted Data. In Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 30 October–3 November 2006; pp. 89–98.
5. Bethencourt, J.; Sahai, A.; Waters, B. Ciphertext-Policy Attribute-Based Encryption. In Proceedings of the IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 20–23 May 2007; pp. 321–334.
6. Cheung, L.; Newport, C. Provably Secure Ciphertext Policy ABE. In Proceedings of the 14th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 29 October–2 November 2007; pp. 456–465.

7. Goyal, V.; Jain, A.; Pandey, O.; Sahai, A. Bounded Ciphertext Policy Attribute-Based Encryption. In *Automata, Languages and Programming*, Proceedings of the 35th International Colloquium, ICALP 2008, Part II, Reykjavik, Iceland, 7–11 July 2008; Springer: Berlin/Heidelberg, Germany, 2008; Lecture Notes in Computer Science, Volume 5126, pp. 579–591.
8. Lewko, A.; Okamoto, T.; Sahai, A.; Takashima, K.; Waters, B. Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption. In *Advances in Cryptology—EUROCRYPT 2010*, Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Riviera, French, 30 May–3 June 2010; Springer: Berlin/Heidelberg, Germany, 2010; Lecture Notes in Computer Science, Volume 6110, pp. 62–91.
9. Waters, B. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization. In *Public Key Cryptography—PKC 2011*, Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, 6–9 March 2011; Springer: Berlin/Heidelberg, Germany, 2011; Lecture Notes in Computer Science, Volume 6571, pp. 53–70.
10. Beimel, A. Secure Schemes for Secret Sharing and Key Distribution. Ph.D. Thesis, Israel Institute of Technology, Technion, Israel, 1996.
11. Camenisch, J.; Neven, G.; Shelat, A. Simulatable Adaptive Oblivious Transfer. In *Advances in Cryptology—EUROCRYPT 2007*, Proceedings of the 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Barcelona, Spain, 20–24 May 2007; Springer: Berlin/Heidelberg, Germany, 2007; Lecture Notes in Computer Science, Volume 4515, pp. 573–590.
12. Naccache, D. Secure and Practical Identity-Based Encryption. *IET Inf. Secur.* **2007**, *1*, 59–64.
13. Boneh, D.; Franklin, M. Identity-Based Encryption from the Weil Pairing. In *Advances in Cryptology—CRYPTO 2001*, Proceedings of the 21st Annual International Cryptology Conference, Santa Barbara, CA, USA, 19–23 August 2001; Springer: Berlin/Heidelberg, Germany, 2001; Lecture Notes in Computer Science, Volume 2139, pp. 213–229.
14. Goyal, V. Reducing Trust in the PKG in Identity Based Cryptosystems. In *Advances in Cryptology—CRYPTO 2007*, Proceedings of the 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, 19–23 August 2007; Springer: Berlin/Heidelberg, Germany, 2007; Lecture Notes in Computer Science, Volume 4622, pp. 430–447.
15. Libert, B.; Vergnaud, D. Towards Black-Box Accountable Authority IBE with Short Ciphertexts and Private Keys. In *Public Key Cryptography—PKC*, Proceedings of the 12th International Conference on Practice and Theory in Public Key Cryptography, Irvine, CA, USA, 18–20 March 2009; Springer: Berlin/Heidelberg, Germany, 2009; Lecture Notes in Computer Science, Volume 5443, pp. 235–255.
16. Goyal, V.; Lu, S.; Sahai, A.; Waters, B. Black-Box Accountable Authority Identity-Based Encryption. In Proceedings of the 15th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 27–31 October 2008; pp. 427–436.
17. Li, J.; Ren, K.; Kim, K. A2BE: Accountable Attribute-based Encryption for Abuse Free Access Control. IACR Cryptology ePrint Archive, **2009**, 118.

18. Liu, Z.; Cao, Z.; Wong, D. White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Any Monotone Access Structures. *IEEE Trans Inf. Forensics Secur.* **2013**, *8*, 76–88.