2016

Ciphertext-policy attribute-based encryption with key-delegation abuse resistance

Yinhao Jiang
University of Wollongong, yj971@uowmail.edu.au

Willy Susilo
University of Wollongong, wsusilo@uow.edu.au

Yi Mu
University of Wollongong, ymu@uow.edu.au

Fuchun Guo
University of Wollongong, fuchun@uow.edu.au

Publication Details

Jiang, Y., Susilo, W., Mu, Y. & Guo, F. (2016). Ciphertext-policy attribute-based encryption with key-delegation abuse resistance. Lecture Notes in Computer Science, 9722 477-494. Melbourne, Australia Information Security and Privacy: 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part I

Ciphertext-policy attribute-based encryption with key-delegation abuse resistance

Abstract

Attribute-based encryption (ABE) is a promising cryptographic primitive that allows one-to-many encryption. In such a system, users' private keys are linked to their access rights. We note that if a user can generate a new private key for a portion of his/her access right, this could potentially lead to some undesirable situations, which violate the access control policy. Interestingly, to date, there is no work that looks into this matter in detail nor addresses it. We point out that this is a "property" that exists in ABE systems, which we refer to "key-delegation abuse". ABE systems that suffer from key-delegation abuse will hinder the adoption of these systems in practice. In this work, for the first time in the literature, we address the "key-delegation abuse" problem in Ciphertext-policy Attribute-based Encryption (CP-ABE) systems. We introduce a new mechanism to enhance CP-ABE schemes that provide protections against this key-delegation abuse issue. We formalize the security requirements for such a property, and subsequently construct a CP-ABE scheme that satisfies the new security requirements. We also present an application of our scheme to a traceable CP-ABE, where the "traitors", i.e. the users who have leaked their keys, can be traced. address the "key-delegation abuse" problem in Ciphertext-policy Attribute-based Encryption (CP-ABE) systems. We introduce a new mechanism to enhance CPABE schemes that provide protections against this key-delegation abuse issue. We formalize the security requirements for such a property, and subsequently construct a CP-ABE scheme that satisfies the new security requirements.We also present an application of our scheme to a traceable CP-ABE, where the "traitors", i.e. the users who have leaked their keys, can be traced.

Keywords

abuse, attribute, policy, resistance, ciphertext, key, delegation, encryption

Publication Details

Jiang, Y., Susilo, W., Mu, Y. & Guo, F. (2016). Ciphertext-policy attribute-based encryption with key-delegation abuse resistance. Lecture Notes in Computer Science, 9722 477-494. Melbourne, Australia Information Security and Privacy: 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part I

Ciphertext-Policy Attribute-Based Encryption with Key-Delegation Abuse Resistance

Yinhao Jiang, Willy Susilo, Yi Mu, and Fuchun Guo

Centre for Computer and Information Security Research, School of Computing and Information
Technology, University of Wollongong, Australia
{yj971,wsusilo,ymu,fuchun}@uow.edu.au

Abstract. Attribute-based encryption (ABE) is a promising cryptographic primitive that allows one-to-many encryption. In such a system, users' private keys are linked to their access rights. We note that if a user can generate a new private key for a portion of his/her access right, this could potentially lead to some undesirable situations, which violate the access control policy. Interestingly, to date, there is no work that looks into this matter in detail nor addresses it. We point out that this is a "property" that exists in ABE systems, which we refer to "key-delegation abuse". ABE systems that suffer from key-delegation abuse will hinder the adoption of these systems in practice. In this work, *for the first time in the literature*, we address the "key-delegation abuse" problem in Ciphertext-policy Attribute-based Encryption (CP-ABE) systems. We introduce a new mechanism to enhance CP-ABE schemes that provide protections against this key-delegation abuse issue. We formalize the security requirements for such a property, and subsequently construct a CP-ABE scheme that satisfies the new security requirements. We also present an application of our scheme to a traceable CP-ABE, where the "traitors", i.e. the users who have leaked their keys, can be traced.

Keywords: Attribute-based encryption, Key-delegation abuse, Ciphertext-policy

1 Introduction

In modern cryptography, one of the most promising cryptographic primitive is the notion of Attribute-based Encryption (ABE), which allows one-to-many encryption. In this notion, there are two variants, namely Ciphertext-policy Attribute-based Encryption (CP-ABE) and Key-policy Attribute-based Encryption (KP-ABE), which essentially denotes the location of the embedded access policy, whether it is in the ciphertext or in the key. In this work, we mainly discuss CP-ABE. In CP-ABE, a ciphertext on a message is encrypted with an access policy while a private key for a user associated with a set of attributes corresponding to the private key satisfying the access policy.

The basic security in CP-ABE requires that a user cannot generate a *new* private key for an attribute set ω' from a private key set for ω, if $\omega \subset \omega'$. It is an interesting question whether the reverse is also true. That is, whether the key generation for the reversed subset relationship also holds this property. Interestingly, this important issue receives a very limited attention in the literature. Specifically, the question is: given a private key for attribute set ω, can the user generate a new private key for any subset

$\omega' \subset \omega$? We note that if the answer is positive, this can lead to some undesirable situation. To illustrate this situation, consider the following scenario. A media broadcaster (who is the trusted authority in the cryptographic setting) controls the contents to its subscribers by encrypting the contents with a CP-ABE system. Without losing generality, the contents will be encrypted with an attribute set as follows: $\{Sport$, $Biography$, $Drama$, $Comedy$, $Action$, $Thriller$, $Fantasy$, $Sci\text{-}Fi$, $Documentary$, $War\}$. Note that there are ten attributes in the possible set in this example. Each possible channel is sold for \$10/month, and hence, it will cost \$100/month to subscribe to all channels. To make the package deal more attractive, the media broadcaster introduces a premium user package. For a premium user package, the user needs to subscribe to *all* channels, and hence the ten attributes, and the premium user will be granted two additional channels, namely $\{HD, Hollywood - movies\}$, and the premium price is \$100/month for the whole package. Consider the case where a malicious user, Malva, purchases the premium package. If the CP-ABE scheme that is adopted allows Malva to create a new private key for any attribute, which is a subset to the original attribute set that he has, then Malva can make money from this case. He will then construct a private key for the attribute $Sport$ for example, and sells this for \$9/month, and for the ten possible attributes, he will accrue \$90/month. Additionally, he can sell any combinations of the attribute sets (such as $\{Sport, Fantasy\}$) and again sell it at a cheaper price than \$20/month. Note that in total, he will make more than \$100/month by simply re-selling a combination of these channels. We should point out that in this case, it is clear that Malva will be able to manage his own groups of customers with private keys of different sets of attributes and in fact, Malva has functioned as an illegal "trusted authority", who will compete with the original media broadcaster. Throughout this paper, we shall call this "property" in ABE as the *key-delegation abuse*, if the adversary can generate a private key for any subset without revealing his/her entire access rights. It is clear that this property is undesirable in some scenarios, as outlined above.

Interestingly, the property of *key-delegation abuse* exists in majority of CP-ABE schemes since private keys are usually designed with flexibility in order to meet the requirement of complex and variable access policies in the ciphertexts. As a result, different components of a private key are used for different access policies, which makes it possible for a user to split his/her private key to different parts and construct new private keys from these parts or parts from other users. To the best of our knowledge, the *key-delegation abuse* problem in ABE systems is still not yet well explored in the literature, and hence, it becomes an inherent problem in ABE. For the *key-delegation abuse* problem, existing solutions combine users' private information with their private keys so that malicious users are wary of constructing new private keys based on theirs and introduce an extra trace device/algorithm to pinpoint malicious users from constructed new private keys. However, these approaches have two limitations: 1) they gave a deterrent solution, while users are still capable to issue new private keys; and 2) they need the constructed new key to trace who the malicious user is.

Our goal in this work. The aim of this work is to address the *key-delegation abuse* problem. In particular, we aim to make the notion of ABE to be more adoptable in practice, once the problem with key-delegation abuse is removed.

Our contribution In this paper, *for the first time* we propose a ciphertext-policy attribute-based encryption scheme in which users cannot illegally generate new private keys of a subset of the users' original sets of attributes. The access structure used in our CP-ABE is constructed by an AND-gate. This is a subset of the access structures used in [3,15]. In our scheme, a ciphertext with the access structure W, which consists of a single AND gate whose input are attributes described by an access policy attribute set W, can only be decrypted by a private key of a set of attributes ω when $W \subseteq \omega$. Our technique can be summarized as follows. We utilize the property of bilinear groups. Then, we construct private key components for all attributes but based on two different sets of group elements as if it is contained in the set of attributes of the private key or not. Subsequently, we apply the secret sharing scheme on all attributes, and enforce the bilinear map of key components and ciphertext components for all attributes so that the key cannot be split nor combined with other private keys. We prove the security properties of the scheme in standard selective model. We also introduce a new security game based on [5] for the *key-delegation abuse* problem and prove the new feature of our scheme in generic group model. Additionally, we present an application of our scheme to achieve a traceable CP-ABE scheme, where traitors can be traced efficiently.
Organization The paper is organized as follows: In Sec. 2, we discuss related work. Sec. 3 provides some background definitions and main properties of ABE system. In Sec. 4 our CP-ABE construction is presented, and the security proof is presented in Sec. 5. In Sec. 6, we discuss an application of our scheme to achieve a traceable CP-ABE scheme. Finally, in Sec. 7, we conclude with some discussions and future work.

2 Related work

The concept of Identity-based Encryption (IBE) was put forth by Shamir [19] in order to ease public-key encryption and certificate management. Specifically, there is no necessity to verify the validity of users' certificates, as users' public key is in fact their identities, such as e-mail addresses or phone numbers. An encryptor can create a ciphertext under the receiver's identity without any prior information. Subsequently, Sahai and Waters [18] proposed the notion of Attribute-based Encryption (ABE) by replacing the identity in IBE with an attribute set. ABE has been found very useful in providing fine-grained access control systems [6]. Subsequently, many flexible and efficient ABE schemes have been proposed in the literature. As classified by Goyal et al. [6], there are two variants of ABE, namely KP-ABE and CP-ABE. In a KP-ABE, ciphertext is associated with attribute sets, and each user private key is associated with an access structure that specifies which type of ciphertexts the key is able to decrypt. In contrast, in a CP-ABE system, each user's key is associated with an attribute sets and ciphertext will specify an access policy over attributes. Therefore, the difference between CP-ABE and KP-ABE relies on who determines the access control policy in the encryption system. In a CP-ABE, when a message is being encrypted, it will be associated with an access structure over a predefined attribute sets. The user will only be able to decrypt a given ciphertext if his/her attributes satisfy the access structure specified in the ciphertext. The first KP-ABE construction [6] realized the monotonic access structures for key policies. To enable more flexible access polices, Ostrovsky et al. [17] developed a

KP-ABE scheme to support the expression of non-monotone formulas in key policies. However, KP-ABE is less flexible than CP-ABE because in KP-ABE once a user's private key is issued the access policy is also determined, which makes the encryption more difficult as the encryptor needs to compare recipients' access policies to all other users' to choose a proper set of attributes for the ciphertext. Later, Bethencourt et al. [9] proposed the first CP-ABE construction. However, the construction [9] was only proved secure under the generic group model. To overcome this weakness, Cheung and Newport [3] presented another construction that is proved to be secure under the standard model. Then, Goyal et al. [4] presented another construction for more advanced access structures based on number theoretic assumption. Katz, Sahai, and Waters [10] proposed a novel predicate encryption scheme supporting inner product predicates. Their scheme is very general and can achieve both KP-ABE and hidden CP-ABE schemes. However, the constructions of [2,10] are very inefficient compared to [16].

In [7], Hinek et al. mentioned the problem of *key cloning*, and another third party should be involved in each users decryption in their scheme, which makes it impractical. Then, the problem of building a secure CP-ABE supporting traceability has recently been studied in [8,12,14,13]. The ciphertext access policies in [8,12] only support a single AND gate with wild-card. The traceable CP-ABE proposed in [14] is as fully secure, highly expressive and efficient as a conventional CP-ABE such as the one in [11], but it only supports tracing 'well-formed' illegally constructed private keys. Later, [13] proposed a new CP-ABE scheme proved fully secure which can trace not 'well-formed' illegally constructed private keys. However, traceability cannot prevent "key-delegation abuse" issue – malicious users can still illegally generate keys in private.

2.1 Violating Access Control Policy with "Key-Abuse" Property

The *key-delegation abuse* property is that a user who owns a private key for attribute set ω can generate a new private for a subset $\omega' \subset \omega$. This property exists in majority of CP-ABE schemes. In the following, we shall demonstrate that this key-delegation abuse property can lead to some undesirable situation where the access control policy is violated.

Without losing generality, we shall consider the Cheung and Newport scheme proposed in [3]. Cheung and Newport proposed a CP-ABE scheme [3] (which is referred to as the CN scheme throughout this paper), in which access structure is restricted to an AND gate, but attributes i are allowed to be either positive i, negative $\neg i$ or "don't care". In their system, let the attribute universe be $\mathcal{N} = \{1,2,3,4,5\}$, then the public key is $PK = (G = \langle g \rangle, e : G \times G \to G_T, Y = e(g,g)^y \in G_T, \{T_k = g^{t_k}\}_{k=1,\dots,15})$, and the master secret key is $MK = (y, t_1, \dots, t_{15} \in \mathbb{Z}_p)$. A private key for attribute set $\omega = \{1,2,3\}$ is

$$sk_\omega = \Big(\hat{D} = g^{y-r}, \{D_i = g^{\frac{r_i}{t_i}}\}_{i=1,2,3}, \{D_i = g^{\frac{r_i}{t_{5+i}}}\}_{i=4,5}, \{F_i = g^{\frac{r_i}{t_{10+i}}}\}_{i=1,\dots,5}\Big)$$

where $r = \sum_{i=1}^{5} r_i$. To encrypt a message M with AND gate $W = (1 \wedge 2)$ we have

$$C = \Big(W, \tilde{C} = MY^s, \hat{C} = g^s, \{C_i = T_i^s\}_{i=1,2}, \{C_i = T_{10+i}^s\}_{i=3,4,5}\Big).$$

To decrypt ciphertext C, only part of the private key $\left(\hat{D}, D_1, D_2, F_3, F_4, F_5\right)$ is used during decryption since

$$M = \frac{\tilde{C}}{e(\hat{C},\hat{D})\cdot\prod_{i=1,2} e(C_i,D_i)\prod_{i=3,4,5} e(C_i,F_i)} = \frac{\tilde{C}}{e(g^s,g^{y-r})\prod\limits_{i=1}^{5} e(g,g)^{r_i\cdot s}} = \frac{\tilde{C}}{e(g,g)^{y\cdot s}} = \frac{\tilde{C}}{Y^s}.$$

Thus, the user who owns sk_ω can generate a new key

$$sk' = \left(\hat{D}' = \hat{D}, \{D'_i = D_i\}_{i=1,2}, \{F'_i = F_i\}_{i=1,\ldots,5}\right)$$

to decrypt ciphertexts with AND gate $(1), (1 \wedge 2), (2)$ or $\emptyset$ since sk' satisfies the decryption algorithm.

From the example, it can be seen that to decrypt ciphertexts with different access policies, different parts of a private key are used during the decryption, which makes it plausible to illegally generate new keys. This property of key-delegation abuse does not break the security of encryption schemes and sometimes is adopted for applications like key delegation. However, unauthorized key generation can lead to violation of access control policy.

3 Background

We first give formal definitions for the security of Ciphertext-policy Attribute Based Encryption (CP-ABE). Then we give background information on pairings and complexity assumptions.

3.1 Access Structure[3]

Generally speaking, an access structure on attributes is a rule $\mathbb{A}$ that returns either 0 or 1 given an attribute set ω. We say that ω satisfies $\mathbb{A}$ iff $\mathbb{A}$ answers 1 on ω. Access structures may be Boolean expressions, threshold trees, etc.

In this paper, we focus on access structures that consist of a single AND gate whose inputs are attributes. This is denoted $\mathbb{A} = \bigwedge_{i\in W} i$, where W is a subset of the universal attribute set and every i is an attribute. Given an attribute set ω, $\mathbb{A}$ answers 1 iff for all $i \in W$, $i \in \omega$. Thus, ω satisfies $\mathbb{A}$ iff $W \subseteq \omega$.

3.2 CP-ABE Definition

A ciphertext-policy attribute-based encryption system consists of four algorithms: Setup, Encrypt, KeyGen, and Decrypt.

Setup**.** The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters PK and a master secret key MK.

Encrypt$(PK, M, \mathbb{A})$**.** The encryption algorithm takes in the public parameters PK, the message M, and an access structure $\mathbb{A}$ over the universe of attributes. It will output a ciphertext CT such that only users whose private keys associated with attribute sets which satisfy the access structure $\mathbb{A}$ can decrypt M. We assume that the ciphertext implicitly contains $\mathbb{A}$.

$\mathsf{KeyGen}(MK, \omega)$**.** The key generation algorithm takes as input the master secret MK and a set of attributes ω. It outputs a private key sk associated with ω.

$\mathsf{Decrypt}(PK, CT, sk)$**.** The decryption algorithm takes as input the public parameters PK, a ciphertext CT, which contains an access structure $\mathbb{A}$, and a private key sk, which is a private key for a set of attributes ω. If the attribute set ω satisfies the access structure $\mathbb{A}$ then the algorithm will decrypt the ciphertext and return a message M.

Selective CPA Security Model. We now give the security definition for CP-ABE system. This is described by a security game between a challenger and an adversary. The game proceeds as follows:

Init The adversary outputs a challenge access structure $\mathbb{A}^*$ to the challenger.

Setup The challenger runs the Setup algorithm and gives the public parameters PK to the adversary.

Phase 1 The adversary queries the challenger for private keys corresponding to sets of attributes $\omega_1, \ldots, \omega_{q_1}$ without any satisfying the access policy $\mathbb{A}^*$.

Challenge The adversary declares two equal length messages M_0 and M_1. The challenger flips a random coin $\beta \in \{0, 1\}$, and encrypts M_β with $\mathbb{A}^*$, producing CT^*. It gives CT^* to the adversary.

Phase 2 The adversary queries the challenger for private keys corresponding to sets of attributes $\omega_{q_1+1}, \ldots, \omega_q$ with the same restriction in **Phase 1**.

Guess The adversary outputs a guess β' for β.

The advantage of an adversary in winning this game is defined to be $\Pr[\beta' = \beta] - \frac{1}{2}$.

Definition 1. *A ciphertext-policy attribute-based encryption system is selective chosen-plaintext attack secure if all polynomial time adversaries have at most a negligible advantage in this security game.*

Security Model against Key-Abuse Attack We now give the security definition against Key-Abuse Attack in CP-ABE system. This is described by a security game between a challenger and an adversary. The game is formalized based on [5] and proceeds as follows:

Setup The challenger runs the Setup algorithm and gives the public parameters PK to the adversary. The attribute universe $\mathcal{U}$ and message space $\mathcal{M}$ are also defined during this step.

Queries The adversary queries the challenger for private keys corresponding to different sets of attributes $\omega_1, \ldots, \omega_q \subseteq \mathcal{U}$. In response, for each query ω_j for $1 \leq j \leq q$ the challenger runs $\mathsf{KeyGen}(MK, \omega_j)$ to compute the private key sk_j, and send it back to the adversary $\mathcal{A}$. $\mathcal{A}$ can query the challenger adaptively.

Output The adversary chooses a new attribute set $\omega^* \neq \omega_j$ for $1 \leq j \leq q$, generates a new private key sk^* for attribute set ω^*, a new general decryption algorithm $\mathsf{Dec}^*(PK, CT, sk)$, and send them to the challenger.

The adversary ***wins*** if

1. $\mathsf{Dec}^*(sk^*, \mathsf{Enc}(PK, M, \mathbb{A}) = M$ for all $\mathbb{A} = \bigwedge_{i\in W} i$, $W \subseteq \omega^*$ and any message $M \in \mathcal{M}$.
2. For all possible decryption algorithm $\mathsf{Dec}'(sk^*, \mathsf{Enc}(PK, M, \mathbb{A}))$ outputs $\perp$ for all $W \not\subseteq \omega^*$ and any message $M \in \mathcal{M}$.

The advantage of $\mathcal{A}$ is defined to be the probability that $\mathcal{A}$ wins the security game.

Definition 2. *A ciphertext-policy attribute-based encryption system is secure against Key-Abuse Attack if all polynomial time adversaries have at most a negligible advantage in this security game.*

3.3 Pairings and Complexity Assumption

Bilinear Groups We briefly review the bilinear maps and bilinear map groups[1].

Let G, G_T be cyclic groups of prime order p, and let g be a generator of G. We say G has an admissible bilinear map, $e : G \times G \to G_T$, into G_T if the following three conditions hold:

1. *Bilinearity* $e(g^a, g^b) = e(g, g)^{ab}$ for all a, b.
2. *Non-degeneracy* $e(g, g) \neq 1$.
3. *Computability* $e(g^a, g^b)$ for all $g^a, g^b \in G$ can be computed efficiently.

Complexity Assumption We state our complexity assumption below.

Definition 3. *(Decisional Bilinear Diffie-Hellman (BDH) Assumption). Suppose a challenger chooses $a, b, c, z \in \mathbb{Z}_p$ at random. The Decisional BDH assumption is that no polynomial-time adversary is to be able to distinguish the tuple $(A = g^a, B = g^b, C = g^c, Z = e(g, g)^{abc})$ from the tuple $(A = g^a, B = g^b, C = g^c, Z = e(g, g)^z)$ with more than a negligible advantage.*

4 CP-ABE construction

In this section, we shall present our CP-ABE scheme. For simplicity, let the universe of attributes be $\mathcal{U} := \{1, ..., n\}$ for some natural number n.

In our construction the key generation algorithm will link the key components of one user with a specific set of group elements, and then apply the secret sharing technology to all attributes, so that the key cannot be split or combined to obtain other workable secret keys. Each private key will be generated including one key component per attribute: if the user owns this attribute the key component will be generated with the set of group elements of t_i; otherwise, generated with the set of group elements of t_{n+i}. The encryption algorithm will take as input an AND gate and distribute a random exponent $r \in \mathbb{Z}_p$ according to all attributes: if an attribute is included in the AND gate there will be only one ciphertext component for this attribute generated with the set of group elements h_i for decryption; otherwise, two ciphertext components for this attribute will be generated with h_i and h_{n+i}.

$\mathsf{Setup}(\lambda, \mathcal{U})$: Given a security parameter λ and an attribute universe $\mathcal{U}$ of size of n, the setup algorithm first chooses a bilinear group G of prime order p. It then chooses random numbers $t_1, \ldots, t_{2n}, \alpha \in \mathbb{Z}_p$, random group generators $g_0, h_0 \in G$, and computes

$$Y = e(g_0, h_0)^{\alpha}, h_1 = h_0^{t_1}, \ldots, h_n = h_0^{t_n}, h_{n+1} = h_0^{t_{n+1}}, \ldots, h_{2n} = h_0^{t_{2n}}.$$

The public parameters PK are $PK = (h_1, \ldots, h_{2n}, Y, e, G, G_T, \mathcal{U})$. The master secret key MK is $MK = (g_0, t_1, \ldots, t_{2n}, \alpha)$.

$\mathsf{Enc}(PK, M, \mathbb{A})$: To encrypt a message $M \in G_T$ with an access structure $\mathbb{A} = \bigwedge_{i \in W} i$ the following steps are taken. A random value $r \in \mathbb{Z}_p$ is chosen uniformly. The ciphertext is then created as:

$$CT = \left(\mathbb{A}, E' = MY^r, \{E_i = h_i^r\}_{i \in W}, \{E_i = h_{n+i}^r, E_i' = h_i^r\}_{i \in \mathcal{U} \setminus W}\right).$$

$\mathsf{KeyGen}(MK, \omega)$: To generate a private key for attribute set $\omega \subseteq \mathcal{U}$ the following steps are taken. $n-1$ random values $x_1, \ldots, x_{n-1}$ are randomly chosen in $\mathbb{Z}_p$ and compute $x_n = \alpha - x_1 - \cdots - x_{n-1} \in Z_p$. The private key for the attribute set ω:

$$sk = \left(\omega, \{D_i = g_0^{\frac{x_i}{t_i}}\}_{i \in \omega}, \{D_i = g_0^{\frac{x_i}{t_{n+i}}}\}_{i \in \mathcal{U} \setminus \omega}\right).$$

$\mathsf{Dec}(PK, CT, sk)$: Suppose that a ciphertext, CT, is encrypted with an access structure $\mathbb{A} = \bigwedge_{i \in W} i$ and we have a private key for attribute set ω, where $W \subseteq \omega$. Then, the ciphertext can be decrypted by following steps:

$$\begin{aligned}
\prod_{i \in W \cup \{\mathcal{U} \setminus \omega\}} e(D_i, E_i) \prod_{i \in \omega \setminus W} e(D_i, E_i') &= \prod_{i \in \omega} e(g_0^{\frac{x_i}{t_i}}, h_i^r) \prod_{i \in \mathcal{U} \setminus \omega} e(g_0^{\frac{x_i}{t_{n+i}}}, h_{n+i}^r) \\
&= \prod_{i \in \omega} e(g_0^{\frac{x_i}{t_i}}, h_0^{t_i r}) \prod_{i \in \mathcal{U} \setminus \omega} e(g_0^{\frac{x_i}{t_{n+i}}}, h_0^{t_{n+i} r}) \\
&= e(g_0, h_0)^{r \sum_{i \in \mathcal{U}} x_i} = e(g_0, h_0)^{\alpha r}. \\
\frac{E'}{\prod_{i \in W \cup \{\mathcal{U} \setminus \omega\}} e(D_i, E_i) \prod_{i \in \omega \setminus W} e(D_i, E_i')} &= \frac{MY^r}{e(g_0, h_0)^{\alpha r}} = M.
\end{aligned}$$

5 Security Proof

We shall prove the following theorem.

Theorem 1. *If the DBDH assumption holds, our CP-ABE scheme defined in Section 3 is secure in the sense of Definition 2.*

Proof. To prove the theorem, let us assume that there is an adversary $\mathcal{A}$ that can break our CP-ABE scheme with non-negligible probability. We show how to use this adversary to construct an algorithm $\mathcal{B}$ which breaks the DBDH assumption.

For the algorithm $\mathcal{B}$ breaking the DBDH assumption, we let the challenger set the groups G and G_T of prime p with an efficient bilinear map, e and generator g.

The challenger then flips a fair binary coin μ independent of $\mathcal{B}$'s view. If $\mu = 0$ the challenger sets $(A, B, C, Z) = (g^a, g^b, g^c, e(g,g)^{abc})$; otherwise $(A, B, C, Z) = (g^a, g^b, g^c, e(g,g)^z)$. At a high level, our simulation works as follows. We build a simulator that simulates the joint distribution consisting of adversary's view in its attack in the security game, and the hidden bit β which is not a part of the adversary's view.

We will show that if the input comes as $\mu = 0$, the simulation will be perfect, and so the adversary will launch its full ability breaking our CP-ABE. We will also show that if the input comes as $\mu = 1$, then the adversary's view is independent of β, and therefore the adversary's advantage is negligible. This immediately implies $\mathcal{B}$ distinguishing the distribution of its input tuple: run the simulator and adversary together, and if the simulator outputs β and the adversary outputs β', $\mathcal{B}$ outputs $\mu = 0$ if $\beta = \beta'$, and 1 otherwise.

We now give the details of the simulator.

The input to the simulator is $(p, G, G_T, e, g, A = g^a, B = g^b, C = g^c, Z)$.

Init During the *Init* phase, the simulator receives the challenge access structure $\mathbb{A}^* = \bigwedge_{i \in W^*} i$, where $W^* \subseteq \mathcal{U}$, from the adversary $\mathcal{A}$.

Setup First simulator chooses random numbers $\upsilon, \nu, \lambda_1, \ldots, \lambda_n, \gamma_1, \ldots, \gamma_n \in \mathbb{Z}_p$. Next, the simulator computes

$$g_0 = g^{\upsilon}, h_0 = g^{\nu}, h_i|_{i \in \mathcal{U}} = g^{\nu\lambda_i} = h_0^{\lambda_i},$$
$$h_{n+i}|_{i \in \omega^*} = B^{\nu\gamma_i} = h_0^{b\gamma_i}, h_{n+i}|_{i \in \mathcal{U} \setminus \omega^*} = g^{\nu\gamma_i} = h_0^{\gamma_i},$$
$$Y = e(A, B)^{\upsilon\nu} = e(g_0, h_0)^{ab}.$$

Since $h_i = h_0^{t_i}$ and $h_{n+i} = h_0^{t_{n+i}}$ for each attribute $i \in \mathcal{U}$, the simulator sets $t_i := \lambda_i \in \mathbb{Z}_p$ for each attribute $i \in \mathcal{U}$, $t_{n+i} := b\gamma_i \in \mathbb{Z}_p$ for each attribute $i \in \omega^*$ and $t_{n+i} := \gamma_i \in \mathbb{Z}_N$ for each attribute $i \in \mathcal{U} \setminus \omega^*$. Since $Y = e(u_0, v_0)^{\alpha}$, the simulator also sets $\alpha := ab \in \mathbb{Z}_p$.

The simulated public parameters are $PK = (h_1, \ldots, h_{2n}, Y, e, G, G_T, \mathcal{U})$. The master secret key is $MK = (g_0, t_1, \ldots, t_{2n}, \alpha)$.

Phase 1 The adversary $\mathcal{A}$ makes private key queries. The simulator responds to a query on ω, where $W^* \not\subseteq \omega$, as follows. Observe that there must exist an attribute $k \in W^*$ such that $k \notin \omega$. The simulator first chooses such an attribute k. Next, the simulator chooses $x'_1, \ldots, x'_{n-1} \in \mathbb{Z}_N$ uniformly at random and computes $x'_n = -\sum_i x'_i$. Then the simulator sets $x_i := bx'_i$ for each attribute $i \neq k \in \mathcal{U}$ and $x_k := ab + bx'_k$ for the attribute k.

Finally, the simulator computes

$$\forall i \in \omega, D_i = B^{\frac{\upsilon x'_i}{\lambda_i}} = (g^{\upsilon})^{\frac{bx'_i}{\lambda_i}} = g_0^{\frac{x_i}{t_i}}$$
$$\forall i \notin \omega, i \in W^*, i \neq k, D_i = g^{\frac{\upsilon x'_i}{\gamma_i}} = (g^{\upsilon})^{\frac{bx'_i}{b\gamma_i}} = g_0^{\frac{x_i}{t_{n+i}}}$$
$$\forall i \notin \omega, i \in W^*, i = k, D_k = A^{\frac{\upsilon}{\gamma_k}} \cdot g^{\frac{\upsilon x_k}{\gamma_k}} = g^{\frac{(ab+bx'_k)\upsilon}{b\gamma_k}} = g_0^{\frac{x_k}{t_{n+k}}}$$
$$\forall i \notin \omega, i \notin W^*, D_i = B^{\frac{\upsilon x'_i}{\gamma_i}} = (g^{\upsilon})^{\frac{bx'_i}{\gamma_i}} = g_0^{\frac{x_i}{t_{n+i}}}$$

and passes $sk = (\omega, \{D_i\}_{i \in \mathcal{U}})$ onto $\mathcal{A}$.

Here we check the correctness of the simulated private key.

$$\sum_{i \in \mathcal{U}} x_i = \sum_{i \neq k, i \in \mathcal{U}} x_i + x_k = b \sum_{i \neq k, i \in \mathcal{U}} x'_i + ab + bx'_k = ab.$$

Challenge The adversary $\mathcal{A}$ outputs messages M_0, M_1. The simulator generates a bit $\beta \in \{0, 1\}$ and sends $\mathcal{A}$ the challenge ciphertext:

$$CT^* = \Big(\mathbb{A}^*, E' = M_\beta \cdot Z^{\upsilon\nu}, \{E_i = C^{\nu\lambda_i} = {h_i}^c\}_{i \in W^*},$$
$$\{E_i = C^{\nu\gamma_i} = h^c_{n+i}, E'_i = C^{\nu\lambda_i} = h^c_i\}_{i \in \mathcal{U} \setminus W^*} \Big).$$

Phase 2 $\mathcal{A}$ makes key generation queries, and the simulator responds as in Phase 1.

Guess Finally, the adversary outputs guesses β'. If $\beta = \beta'$, $\mathcal{B}$ outputs 0 indicating that $Z = e(g, g)^{abc}$; otherwise, it outputs 1.

Perfect Simulation: When $\mu = 1$ and $Z = e(g, g)^{abc}$, we have

$$E' = M_\beta e(g, g)^{abc\upsilon\nu} = M_\beta e(g_0, h_0)^{abc} = M \cdot Y^c.$$

Thus, CT^* is a valid ciphertext for $\mathbb{A}^*$, and the public key and challenge ciphertext issued by the simulator comes from a distribution identical to that in the actual construction; however, we still must show that the private keys issued by the simulator are appropriately distributed. To show that the keys issued by the simulator are appropriately distributed, it suffices to show that, from A's view, the value g^a, g^b is uniformly random and independent. But this follows from the fact that g^a, g^b is chosen uniformly random in G from the input.

Probability Analysis: We assume the adversary $\mathcal{A}$ breaks our CP-ABE scheme with non-negligible probability ϵ. If $Z = e(g, g)^{abc}$, then the simulation is perfect, and $\mathcal{A}$ will guess the bit β correctly with probability $1/2 + \epsilon$. Else, $Z = e(g, g)^z$ is uniformly random in G_T, and thus E' is uniformly random and independent element in G_T. In this case, with probability $1 - 1/p$ the value of β is independent from $\mathcal{A}$'s view. Thus, we have that

$$\Pr[\mathcal{B}(A, B, C, Z) = 0] - \Pr[\mathcal{B}(A, B, C, Z) = 0] \geq \epsilon - 1/p.$$

This concludes the proof of Theorem. □

Theorem 2. *Our CP-ABE scheme is secure against Key-Abuse Attack (in the sense of Definition 3) in the generic group model.*

Proof. We briefly discus the high level idea of the here. A full security proof is given in Appendix A.

High Level Idea

In the generic group model, the adversary can only manipulate group elements by using the canonical group operations, independent of the encoding for group elements. Thus if the adversary is given group elements $g^{\delta_1}, \ldots, g^{\delta_t} \in G$ as its only inputs, then each element of G output by the adversary must be of the form $g^{\pi(\delta_1,\ldots,\delta_t)}$, where π is a fixed multilinear polynomial.

Suppose the adversary gives a new private key sk^* with a decryption algorithm $Dec^*(\cdot)$ for an attribute set ω^*, with which ciphertexts encrypted with $\mathbb{A}^* = \bigwedge_{i\in\omega^*} i$ can be decrypted. Using a standard argument for the generic group model, we first show that if this is to happen with non-negligible probability, then the multi-linear polynomials as described above in the new private key must also satisfy corresponding constraints. Thus our approach is to assume that the multi-linear polynomials corresponding to the adversary's output satisfy the required constraints, and then obtain a contradiction. We proceed by arguing that in order to satisfy the constraints, the polynomials must have certain structure (i.e., they can only depend on certain given group elements).

First, for a ciphertext CT encrypted under $\mathbb{A}^* = \bigwedge_{i\in\omega^*} i$ the new private key can decrypt M from E' if it can be used to compute $Y^r = e(g_0, h_0)^{\alpha r}$. Thus, it contains a group element in G for each attribute in $\mathcal{U}$ to pair the corresponding E_i (or E'_i) in the ciphertext in bilinear map. We denote these group elements by D^*_i for attribute i in $\mathcal{U}$ and the necessary structure of the new private key can be presented as $(\omega^*, \{D^*_i\}_{i\in\mathcal{U}})$.

After narrowing down the necessary construction for sk^*, we note that D^*_i needs to be constructed based on key components $D^{(j)}_i$ from j-th queried private key $sk^{(j)}$ for attribute set ω_j since there is no other given group elements related to the unknown master secret key α for the adversary. Nevertheless, we also note that because of the difference of the queried attribute sets, for the same attribute i the key components $D^{(j)}_i$ might be generated based on different sets of group elements, which makes them irreconcilable to be combined together. Thus, the new private key sk^* can only depend on one queried private key sk_j where $\omega^* \subset \omega_j$. But this will result in that $sk*$ can be used to decrypt ciphertexts encrypted with ω_j that is an attribute set beyond the supposed ω^*, which contradicts the second condition in the security game's definition.

6 Application: Traceable CP-ABE

In this section, we shall discuss an application of our CP-ABE scheme to realize a traceable CP-ABE scheme, which is a CP-ABE scheme that is equipped with a traitor tracing mechanism. The main purpose of traitor tracing in ABE system is to guarantee that any user who illegally shared his/her private key can be traced. Many works have explored traceability in ABE schemes [8,12,14,13]. Most of them focused on tracing new keys generated in collusive way, but few can prevent one user generating new workable keys in private. Based on our "key-delegation abuse" resistant CP-ABE scheme, we can obtain a *Traceable CP-ABE* system that can trace privately generated illegal new keys with an extended attribute universe. Each user is given an attribute set that consists of attributes from the original attribute universe, which present his/her access right, as well as attributes from the extended attribute set, which indicate his/her identity. To be specific, we first let the original attribute universe be $\mathcal{U} := \{1, \ldots, n\}$ and a user identity space be $\mathcal{I}$ of size of 2^l, and we have the extended universe $\mathcal{U}' := \{1, \ldots, n + l\}$ in which attributes $\{1, \ldots, n\}$ are used for describing access right and attributes $\{n+1, \ldots, n+l\}$ are used to indicate identities. Next, when a private key for an attribute set ω (which only consists of attributes $\{1,\ldots,n\}$) and a user identity ID is queried, the user's identity ID is mapped to a distinct binary string $L_{ID} \in \{0,1\}^l$ by a collision-resistant hash function. According to the identity binary string L_{ID}, if the k-th digit is 1 the corresponding $(n+k)$-th attribute is added into a dummy attribute set ω_{ID}. The private key is then generated based on attribute set $\omega' = \omega \cup \omega_{ID}$. Since the decryption algorithm of our CP-ABE scheme requires corresponding key components for all attributes in the extended universe and our CP-ABE scheme is key-delegation abuse resistant, a user who wants to share his/her private key needs to give away the whole key, which will also give away the unique dummy attribute set. Thus, if a private key is shared, then the user will be traceable.

Using this technique, we can now describe our traceable CP-ABE construction using our key-delegation abuse resistant CP-ABE scheme $\mathit{\Pi}^{KAR}_{CP-ABE} = (\mathsf{Setup}^{KAR}$, KeyGen^{KAR}, Enc^{KAR}, $\mathsf{Dec}^{KAR})$ as follows.

$\mathsf{Setup}(\lambda,\mathcal{I},\mathcal{U})$: Given a security parameter λ, a user identity space $\mathcal{I}$ of size of 2^l and an attribute universe $\mathcal{U}$ of size of n, the setup algorithm first sets the new universe $\mathcal{U}' := \{1,\ldots,n+l\}$. Next, it runs $\mathsf{Setup}^{KAR}(\lambda,\mathcal{U}')$ to get the master secret key MK^{KAR} and the public parameters PK^{KAR} of $\mathit{\Pi}^{KAR}_{CP-ABE}$. Then it chooses a collision-resistant hash function $H : \{0,1\}^* \to \{0,1\}^l$. Finally, it sets the public parameters $PK = (PK^{KAR}, H)$, and the master secret key $MK = MK^{KAR}$.

$\mathsf{Enc}(PK, M, \mathbb{A})$: To encrypt a message $M \in G_T$ with an access structure $\mathbb{A} = \bigwedge_{i\in W} i$ the encryption algorithm publishes $CT = \mathsf{Enc}^{KAR}(PK^{KAR}, W, M)$.

$\mathsf{KeyGen}(PK, MK, \omega, ID)$: To generate a private key for attribute set $\omega \subseteq \mathcal{U}$ and a user identity $ID \in \mathcal{I}$ the following steps are taken. First, compute the identity binary string $L_{ID} = H(ID)$ and store the tuple of $\langle ID, L_{ID}\rangle$ into an internal list in the Trace algorithm. Then, a dummy attribute set ω_{ID} is generated by adding $(n+k)$-th attribute if k-th digit of L_{ID} equals to 1. Finally, it outputs $sk_{\omega,ID} = \mathsf{KeyGen}^{KAR}(PK^{KAR}, MK^{KAR}, \omega \cup \omega_{ID})$.

$\mathsf{Dec}(PK, CT, sk_{\omega,ID})$: Suppose that a ciphertext, E, is encrypted with a set of attribute W and a private key has an access right of the attribute set ω, where $W \subseteq \omega$. Then, the message is recovered as $M = \mathsf{Dec}^{KAR}(PK^{KAR}, E_W, sk_{\omega,ID})$.

$\mathsf{Trace}(PK, sk')$ Let $sk' = \big(\omega', \{D'_i\}_{i\in\omega'}, \{D'_i\}_{i\in\mathcal{U}'\setminus\omega'}\big)$ be a valid decryption key. It means that $\prod_{i\in\omega'} e(D'_i, h_i)\prod_{i\in\mathcal{U}'\setminus\omega'} e(D'_i, h_{n+i}) = Y$. Then, reconstruct the user identity binary string $L_{ID'} \in \{0,1\}^l$ by setting k-th digit to 1 if $(n+k) \in \omega'$; otherwise 0. Next, search the internal list for a tuple $\langle ID, L_{ID}\rangle$ where $L_{ID} = L_{ID'}$ and reveal the corresponding ID as the identity of the traitor.

Theorem 3. *If the DBDH assumption holds, our Traceable CP-ABE scheme defined in Section 3 is secure in the sense of Definition 2.*

Proof. The proof is similar to that for Theorem 1, and hence, we omit it.

Theorem 4. *Our Traceable CP-ABE scheme is secure against Key-Abuse Attack (in the sense of Definition 3) in the generic group model.*

Proof. The proof is similar to that for Theorem 2, and hence, we omit it.

7 Conclusion

In this paper, we investigated an important property in ABE schemes, which we call as the "key-delegation abuse". When an ABE scheme is not key-delegation abuse resistant, it means that the private keys that the users have will allow those users to generate new set of private keys without the need of the trusted authority's involvement. To be more specific, the new *derivative keys* can be generated for attribute set ω' from a private key set for ω, if $\omega' \subset \omega$. We outlined some severeness of this situation in practice, and we also pointed out that the existing schemes in the literature suffer from this problem. It is indeed interesting that this issue has not been well studied in the literature despite its importance for the adoption of ABE in the real situation. In this work, we proposed a security notion for the key-delegation abuse property and presented a new CP-ABE scheme that is key-delegation abuse resistant. We also proved the security of the scheme in both of standard selective CPA model and the proposed model. Additionally, we also presented an extension of our CP-ABE scheme to a traceable CP-ABE scheme, which will allow the "traitors" to be traced in the system. Our scheme is *the first* CP-ABE scheme that is key-delegation abuse resistant. For the future work, it will be interested to construct a key-delegation abuse resistant ABE scheme that is based on standard hardness assumption.

Acknowledgement

This work is partially supported by ARC Project (DP130101383).

References

1. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Advances in CryptologyCRYPTO 2001. pp. 213–229. Springer (2001)
2. Boneh, D., Waters, B.: Conjunctive, subset, and range queries on encrypted data. In: Vadhan, S. (ed.) Theory of Cryptography, Lecture Notes in Computer Science, vol. 4392, pp. 535–554. Springer Berlin Heidelberg (2007)
3. Cheung, L., Newport, C.: Provably secure ciphertext policy abe. In: Proceedings of the 14th ACM Conference on Computer and Communications Security. pp. 456–465. CCS '07, ACM, New York, NY, USA (2007)
4. Goyal, V., Jain, A., Pandey, O., Sahai, A.: Bounded ciphertext policy attribute based encryption. In: Halldorsson , M.M., INgolfsdottir,A., Walukiewicz, I .(eds) ICALP 2008, Part II. LNCS , Vol 5126, pp 579- 591, Springer , Heidelberg (2008)
5. Goyal, V., Sahai, A., Lu, S., Waters, B.: Black box accountable authority identity-based encryption (2008)
6. Goyal, V., Sahai, A., Pandey, O., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: In Proc. of ACMCCS06. pp. 89–98 (2006)
7. Hinek, M.J., Jiang, S., Safavi-Naini, R., Shahandashti, S.F.: Attribute-based encryption with key cloning protection. Cryptology ePrint Archive, Report 2008/478 (2008), `http://eprint.iacr.org/`
8. Jin Li, Kui Ren, K.K.: A2be: Accountable attribute-based encryption for abuse free access control. IACR Cryptology ePrint Archive (2009)

9. John Bethencourt, Amit Sahai, B.W.: Ciphertext-policy attribute-based encryption. Security and Privacy, 2007. SP '07. IEEE Symposium on pp. 321 – 334 (2007)
10. Jonathan Katz, Amit Sahai, B.W.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. Journal of Cryptology 26(2), 191–224 (2013)
11. Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In: Gilbert, H. (ed.) Advances in Cryptology EUROCRYPT 2010, Lecture Notes in Computer Science, vol. 6110, pp. 62–91. Springer Berlin Heidelberg (2010)
12. Li, J., Huang, Q., Chen, X., Chow, S.S.M., Wong, D.S., Xie, D.: Multi-authority ciphertext-policy attribute-based encryption with accountability. In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. pp. 386–390. ASIACCS '11, ACM, New York, NY, USA (2011)
13. Liu, Z., Cao, Z., Wong, D.S.: Blackbox traceable cp-abe: how to catch people leaking their keys by selling decryption devices on ebay. IACR Cryptology ePrint Archive pp. 475–486 (2013)
14. Liu, Z., Cao, Z., Wong, D.S.: White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures. Nformaon Forn and Ry Ranaon on 8(1), 76 – 88 (2013)
15. Nishide, T., Yoneyama, K., Ohta, K.: Attribute-based encryption with partially hidden encryptor-specified access structures. In: Bellovin, S., Gennaro, R., Keromytis, A., Yung, M. (eds.) Applied Cryptography and Network Security, Lecture Notes in Computer Science, vol. 5037, pp. 111–129. Springer Berlin Heidelberg (2008)
16. NISHIDE, T., YONEYAMA, K., OHTA, K.: Attribute-based encryption with partially hidden ciphertext policies. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 92(1), 22–32 (jan 2009)
17. Ostrovsky, R., Sahai, A., Waters, B.: Attribute-based encryption with non-monotonic access structures. Cryptology ePrint Archive, Report 2007/323 (2007), `http://eprint.iacr.org/`
18. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In EUROCRYPT pp. 457–473 (2004)
19. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakley, G., Chaum, D. (eds.) Advances in Cryptology, Lecture Notes in Computer Science, vol. 196, pp. 47–53. Springer Berlin Heidelberg (1985)

Appendix A Proof of Theorem 2

Proof. We consider two random encodings ψ_0, ψ_1 of the additive group $\mathbb{Z}_p$ respectively, that is injective maps $\psi_0, \psi_1 : \mathbb{Z}_p \to \{0,1\}^L$, where $L > 3\log(p)$. We write $G = \psi_0(x) : x \in \mathbb{Z}_p$,$G_T = \psi_1(x) : x \in \mathbb{Z}_p$. We are given oracles to compute the induced group action on G, G_T and an oracle to compute a non-degenerate bilinear map $e : G \times G \to G_T$. We refer to G as a generic bilinear group.

We now proceed with the proof, following the standard approach for generic groups with ψ_0, ψ_1, G, G_T defined as above. Let $g = \psi_0(1)$(we will write g^x to denote $\psi_0(x)$, and $e(g,g)^x$ to denote $\psi_1(x)$).

For any generic-group adversary, the security game against *key-delegation abuse* is considered carried out by a simulator as follows. For each group element seen or created by the adversary, this simulator keeps track of its discrete logarithm by means of a multivariate rational functions in the following indeterminate formal variables:

$$\sum = \{\upsilon, \nu\} \cup \{t_i\}_{i \in \mathcal{U}} \cup \{x_i^{(j)}\}_{i \in \mathcal{U}, j \in [q]}.$$

The simulation also associates each group element with some rational function. For each distinct rational function in its collection, it inputs the value of the rational function to corresponding encoding ψ_0 or ψ_1 and gives the result to the adversary as the encoding of that particular group element. The functions are associated with the group elements in the simulation as follows:

First, we suppose $g_0 = g^{\upsilon}, h_0 = g^{\nu}$.

- Public parameters PK generated by Setup
  $PK = (h_1, \ldots, h_{2n}, Y)$.
  1. $\{\nu t_i\}_{i \in \mathcal{U}}$, representing $h_i = h_0^{t_i} = g^{\nu t_i}$.
  2. $\{\nu t_{n+i}\}_{i \in \mathcal{U}}$, representing $h_i = h_0^{t_{n+i}} = g^{\nu t_i}$.
- Private key components given by KeyGen. Let sk_j be the j-th queried private key for the attribute set ω_j.

$$sk_j = \left(\omega_j, \{D_i^{(j)} = g_0^{\frac{x_i^{(j)}}{t_i}}\}_{i \in \omega}, \{D_i^{(j)} = g_0^{\frac{x_i^{(j)}}{t_{n+i}}}\}_{i \in \mathcal{U} \setminus \omega} \right)$$

  1. $\{\frac{\upsilon}{t_i} x_i^{(j)}\}_{j \in [q], i \in \omega_j}$, representing $D_i^{(j)} = g_0^{\frac{x_i^{(j)}}{t_i}}$.
  2. $\{\frac{\upsilon}{t_{n+i}} x_i^{(j)}\}_{j \in [q], i \in \mathcal{U} \setminus \omega_j}$, representing $D_i^{(j)} = g_0^{\frac{x_i^{(j)}}{t_{n+i}}}$.

We note that in the actual game, the values of the formal variables are chosen uniformly at random in $\mathbb{Z}_p$. Two distinct functions may in that case evaluate to the same value. The simulation is faithful to the standard interaction in a generic group, except in the event that two of the distinct functions evaluate to the same value on a random assignment to the formal variables. For any two distinct functions of the form listed above, the probability of this happening is at most $O(q)/p$, since the degree of distinct multivariate polynomials is at most $O(q)$. Since this probability is negligible, we ignore this case.

Now the adversary outputs a purported new private key sk^* for a new attribute set ω^* with a suitable decryption algorithm $Dec^*(\cdot)$. We first observe that to decrypt a ciphertext CT encrypted with an access structure $\mathbb{A} = \bigwedge_{i \in W} i$, where W is equal to or a subset of ω^*. The new private key sk^* should contain a group element for each attribute to pair the corresponding group element E_i (or E_i') in the ciphertext in bilinear map for $Y^r = e(g_0, h_0)^{\alpha r}$. We denote these group elements by D_i^* and the necessary structure of the new private key can be presented as $(\omega^*, \{D_i^*\}_{i \in \mathcal{U}})$. On the other hand, as long as the new private key satisfies the winning conditions the adversary can construct the new key sk^* the way it wants to make it look different, which means the adversary can construct the new private key component D_i^* using a linear combination of the functions listed above.

Here, we note that if the adversary tries to construct D_i^* using any functions other than $D_i^{(j)}$, then using this part of D_i^* in bilinear map will result in meaningless group element in G_T for decryption, which also needs to be eliminated by computing it separately; since it needs to be eliminated afterwards, we do not include it in following discussion.

WLOG, we assume the new private key sk^* contains the following least structure for each attribute i:

$$\begin{aligned} D_i^* &= \pi_i(D_i^{(1)}, \dots, D_i^{(q)}) := (D_i^{(1)})^{\beta_{i,1}}(D_i^{(2)})^{\beta_{i,2}} \cdots (D_i^{(q)})^{\beta_{i,q}} \\ &= u_0^{\frac{1}{t_i}\sum_{i\in\omega_j}\beta_{i,j}x_i^{(j)}+\frac{1}{t_{n+i}}\sum_{i\notin\omega_j}\beta_{i,j}x_i^{(j)}} \end{aligned}$$

where $\pi_i(D_i^{(1)}, \dots, D_i^{(q)}) := (D_i^{(1)})^{\beta_{i,1}}(D_i^{(2)})^{\beta_{i,2}} \cdots (D_i^{(q)})^{\beta_{i,q}}$ represents a function in G using components $D_i^{(j)}$ from queried private keys.

Then we can represent D_i^* as $\frac{v}{t_i}\sum_{i\in\omega_j}\beta_{i,j}x_i^{(j)} + \frac{v}{t_{n+i}}\sum_{i\notin\omega_j}\beta_{i,j}x_i^{(j)}$.

To win in the game, D_i^* needs to meet following conditions:

1. $\sum_{i\in\mathcal{U}}\sum_{j\in[q]}\beta_{i,j}x_i^{(j)} = \alpha$.
2. $\forall i \in \omega^*, \sum_{i\notin\omega_j}\beta_{i,j}x_i^{(j)} = 0$.
3. $\forall i \notin \omega^*, \sum_{j\notin\omega_j}\beta_{i,j}x_i^{(j)} \neq 0$ and $\sum_{i\in\omega_j}\beta_{i,j}x_i^{(j)} = 0$.

The rest of our proof proceeds by assuming the new private key sk^* satisfies the conditions above, and obtaining a contradiction: that the new private key sk^* can be used to decrypt ciphertexts encrypted with a queried attribute set ω_j which contradicts the second condition in the security game's definition.

Considering condition 1, $\sum_{i\in\mathcal{U}}\sum_{j\in[q]}\beta_{i,j}x_i^{(j)} = \alpha$. Since $\sum_i x_i^{(j)} = \alpha$ for $j \in [q]$ and $x_i^{(j)}$ is uniformly random chosen in $\mathbb{Z}_p$, we have

$$\beta_{1,j} = \beta_{2,j} = \cdots = \beta_{n,j}.$$

We denote them by β_j.

Considering condition 2, for all $i \in \omega^*$, $\sum_{i\notin\omega_j}\beta_{i,j}x_i^{(j)} = \sum_{ji\notin\omega_j}\beta_j x_i^{(j)} = 0$. Since $x_i^{(j)}$ is uniformly random chosen in $\mathbb{Z}_p$, it can be concluded that

$$\text{if } \exists i \in \omega^* \text{ and } i \notin \omega_j, \beta_j = 0$$

which is equivalent to

$$\text{if } \beta_j \neq 0, \omega^* \subseteq \omega_j.$$

Considering condition 3, for all $i \notin \omega^*$, $\sum_{j\notin\omega_j}\beta_{i,j}x_i^{(j)} = \sum_{j\notin\omega_j}\beta_j x_i^{(j)} \neq 0$ and $\sum_{i\in\omega_j}\beta_{i,j}x_i^{(j)} = \sum_{i\in\omega_j}\beta_j x_i^{(j)} = 0$. Since $x_i^{(j)}$ is uniformly random chosen in $\mathbb{Z}_p$, it can be concluded that

$$\text{if } \exists i \notin \omega^* \text{ and } i \in \omega_j, \beta_j = 0$$

which is equivalent to

$$\text{if } \beta_j \neq 0, \omega_j \subseteq \omega^*.$$

So ω^* equals to a queried attribute set ω_j, which results in either the adversary cannot generate a new key as $\omega^* \neq \omega_j$ for $j \in [q]$ or the new key will be able to decrypt ciphertexts encrypted with ω_j as well since only one queried private key sk_j can be used. Therefore, our assumptions cannot be true. The adversary cannot successfully generate a new private key sk^* to win the game. □