Traceable CP-ABE with Short Ciphertexts: How to Catch People Selling Decryption Devices on eBay Efficiently

Jianting Ning[1], Zhenfu Cao[2(✉)], Xiaolei Dong[2(✉)], Junqing Gong[1], and Jie Chen[2(✉)]

[1] Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
jtning@sjtu.edu.cn, gongjunqing@126.com

[2] Shanghai Key Lab for Trustworthy Computing, East China Normal University, Shanghai 200062, China
{zfcao,dongxiaolei}@sei.ecnu.edu.cn, S080001@e.ntu.edu.sg

Abstract. Ciphertext-policy attribute-based encryption (CP-ABE) is a highly promising solution for cloud computing, which has been widely applied to provide fine-grained access control in cloud storage services recently. However, for CP-ABE based cloud storage systems, if a decryption device appears on eBay described and advertised to be able to decrypt any ciphertexts with policies satisfied by an attribute set or even with a specific access policy only, no one can trace the malicious user(s) who built such a decryption device using their private key(s). This has been known as a major obstacle to deploying CP-ABE systems in real-world commercial applications. Due to the one-to-many encryption mechanism of CP-ABE, the same decryption privilege is shared by multiple users who have the same attributes. It is difficult to identity the malicious user(s) who built such a decryption device. To track people selling decryption devices on eBay efficiently, in this paper, we develop a new methodology for constructing traitor tracing functionality, and present the first black-box traceable CP-ABE (BT-CP-ABE) with short ciphertexts which are independent of the number of users $\mathcal{N}$. The black-box traceability is *public*, *fully collusion-resistant*, and adaptively traceable against both *key-like decryption black-box* and *policy-specific decryption black-box*.

Our construction combines the conventional CP-ABE with Anonymous Hierarchical Identity-Based Encryption (A-HIBE) in a novel way, which is the first to construct the (underlying) traitor tracing system from A-HIBE. The resulting ciphertexts are independent of $\mathcal{N}$ while the private keys are linear in $\mathcal{N}$, which partially answers an open problem posed by Boneh and Waters [CCS 2006]. We believe this work is a constructive step towards efficient traitor tracing system with short ciphertexts and private keys. In particular, we believe that following the route of this work, any progress in A-HIBE (i.e., with shorter ciphertexts and private keys) may result in some progress in BT-CP-ABE and finally give a satisfactory solution to this open problem.

I. Askoxylakis et al. (Eds.): ESORICS 2016, Part II, LNCS 9879, pp. 551–569, 2016.
DOI: 10.1007/978-3-319-45741-3_28

Keywords: Attribute-Based Encryption · Black-box traceability · Anonymous Hierarchical Identity-Based Encryption · Short ciphertexts

1 Introduction

Traditional public key encryption enables a user to share her/his sensitive data with others in a private manner. The access capability of the shared data is all or nothing. That is, if given the private key, one can get the entire access capability to the shared data; otherwise, nothing will be revealed. The traditional way is useful for applications where the user knows specifically who will get access to the shared data. However, in many cases, a user may want to share her/his data with multiple potential and authorized receivers. Ciphertext-Policy Attribute-Based Encryption (CP-ABE, [7]) is introduced to fulfill the above requirement, which enables fine-grained access control over encrypted data. In particular, CP-ABE provides a scalable way of encrypting data such that the data owner defines the attribute sets that the data consumer needs to possess in order to decrypt the ciphertext. As a sophisticated one-to-many encryption mechanism, CP-ABE has been widely applied to provide fine-grained access control for commercial applications, especially for cloud computing.

However, there exists an important and practicality issue that hinders the wide utilization of CP-ABE to date. In particular, a ciphertext can be decrypted by multiple users whose attributes satisfy the access structure of this ciphertxt. In other words, the decryption privilege is shared by multiple users who have the same attributes and not associated with individuals. As a result, malicious users may deliberately leak their decryption keys or some decryption privilege in the form of a decryption black-box/device to others for profits.

Consider a CP-ABE based commercial application (such as cloud storage service), if a decryption device which is described and advertised as a decryption black-box function is being sold on eBay for financial gain at a lower price, due to the nature of CP-ABE, no one can track the malicious user(s) who built such a decryption device using their secret key(s). In practice, such decryption black-box could be quite useful and deemed to be very attractive to potential buyers with their lower prices, and the resulting financial gain could be a big incentive for malicious users to build and sell such a decryption black-box online with little risk of getting caught.

The problem, as described above, is the one of the main obstacles to deploying CP-ABE systems in real-world commercial applications [4]. To address this problem, we need to add the *traceability* property to the conventional CP-ABE. According to the evidence of trace procedure, there are roughly two flavors of traceability. The first one is *white-box traceability*, given a well-formed decryption key, a tracing algorithm can identify the malicious user who leaks the key. The second one is *black-box traceability*, given a decryption black-box/device, a tracing algorithm can identify the malicious user(s) who built the device using their secret key(s). Intuitively, black-box traceability is stronger than white-box traceability. This paper investigates the black-box traceability.

Furthermore, there are two types of decryption black-boxes/devices [15,17] in general. A *key-like decryption black-box* behaves as a decryption key associated with an attribute set. A *policy-specific decryption black-box* is associated with an access policy and can decrypt ciphertexts with this access policy. These two types of decryption black-boxes reflect different practical scenarios. Policy-specific decryption black-box has weaker decryption capacity than key-like decryption black-box, and tracing it is deemed to be more difficult. In fact, Liu *et al.* [17] proved that, for CP-ABE, traceability against policy-specific decryption black-box implies traceability against key-like decryption black-box, and it is sufficient to investigate traceability against policy-specific decryption black-box. In the rest of the paper, we focus on the traceability against policy-specific decryption black-box.

The problem of building a black-box traceable CP-ABE has recently been studied in [15]. However, as we will review that an efficient (i.e., with short ciphertexts) and expressive CP-ABE supporting adaptive traceability against both key-like and policy-specific decryption black-boxes is yet to be built: the ciphertexts in [15] grow sub-linearly in the number of users $\mathcal{N}$ in the system. Technically, they adopted a traitor tracing method similar to [2,3,6] and indices for users are arranged in an $\sqrt{\mathcal{N}} \times \sqrt{\mathcal{N}}$ matrix. The resulting ciphertexts are sub-linear in $\mathcal{N}$, which is the most efficient level to date. In addition, they only achieved selective traceability against policy-specific decryption black-box.

1.1 Our Results

In this paper, we propose a new CP-ABE with high expressiveness (i.e., supporting any monotonic access structures) and full security (i.e., provably secure against adaptive adversaries in the standard model) as [15] as well as following features:

High efficiency: The ciphertexts are independent of the number of users $\mathcal{N}$ in the system rather than sub-linear in $\mathcal{N}$ (i.e. $\sqrt{\mathcal{N}}$) in [15] (which is the most efficient one so far), the public parameters are shorter than that of [15], while the private keys are linear in $\mathcal{N}$. We note that, in practice, since the ciphertexts are generated and transferred more frequently than secret keys, the ciphertext size has greater impact on overall system performance and the user experience. We emphasize that reducing ciphertext size is more significant. It is desirable to obtain a black-box traceable CP-ABE with short ciphertexts which are independent of $\mathcal{N}$.

Public, fully collusion-resistance, adaptive traceability: It achieves fully collusion-resistant adaptive traceability against policy-specific decryption black-box, that is, it can track at least one of the malicious users even if there are an arbitrary number of malicious users colluding by pulling all of their decryption keys together when building a policy-specific decryption black-box. The tracing algorithm needs no secrets and can be run by anyone.

Table 1. Comparison with other related work[a]

	Traceability	CS	PubKS	PriKS	Fully Secure
[12]	×	$2l+3$	$\|\mathcal{U}\|+4$	$\|S\|+3$	√
[16]	White-box	$2l+3$	$\|\mathcal{U}\|+4$	$\|S\|+4$	√
[18]	White-box	$3l+3$	7	$2\|S\|+4$	×
[15]	Black-box 1	$2l+17\sqrt{\mathcal{N}}$	$\|\mathcal{U}\|+3+4\sqrt{\mathcal{N}}$	$\|S\|+4$	√
Ours	Black-box 2	$2l+5$	$\|\mathcal{U}\|+8+\mathcal{N}$	$\|S\|+6+\mathcal{O}(\mathcal{N})$	√

[a] CS, PubKS, PriKS represent the ciphertext size, the public key size, the private key size respectively. Let l be the size of an access policy, $|\mathcal{U}|$ the size of the attribute universe, $|S|$ the size of the attribute set of a private key, $|I|$ the number of attributes in a private key that satisfies a ciphertext's access policy, $\mathcal{N}$ the number of users in the system. Black-box 1 means that it is public, fully collusion-resistant, adaptively traceable against key-like black-box, but only selectively traceable against policy-specific black-box. Black-box 2 means that it is public, fully collusion-resistant, adaptively traceable against both key-like and policy-specific black-boxes.

To the best of our knowledge, this is the first CP-ABE that simultaneously supports all these features. Table 1 gives the comparison between our work and some other related work.

1.2 Our Techniques

Following the routes of [2,3,6,15], to construct a black-box traceable CP-ABE with adaptive traceability against policy-specific decryption black-box (BT-CP-ABE for short), instead of building one from scratch, we first define a simpler primitive named Enhanced CP-ABE, then we extend it to BT-CP-ABE. An Enhanced CP-ABE can be extended to BT-CP-ABE provided that it is message-hiding and index-hiding secure.

However, taking a traitor tracing method similar to [2,3,6,15] (i.e., encode each user as an entry in a matrix and partition the ciphertexts) to construct an Enhanced CP-ABE, the resulting ciphertexts are sub-linear in the number of users $\mathcal{N}$ in the system, which is the most efficient level to date. To go beyond the sub-linear barrier, in this paper, we put forward a novel method to construct a message-hiding and index-hiding secure Enhanced CP-ABE where the ciphertexts are independent of $\mathcal{N}$. The inspiration for our construction comes from the notion of Anonymous Hierarchical Identity-Based Encryption (A-HIBE), which is an extension of Identity-Based Encryption (IBE) allowing high level users to delegate their key generation ability to the low level users. More concretely, we begin with a conventional CP-ABE [12] and an A-HIBE [24] with constant size ciphertexts (which is based on [10,25]), and obtain a message-hiding and index-hiding secure Enhanced CP-ABE with hierarchical key delegation and anonymous (short) ciphertexts via a novel combination. We construct the tracing part of our system from A-HIBE by utilizing its key delegation and anonymity

properties. Note that simply combine the tracing part (i.e. the A-HIBE part) and the CP-ABE part only provide weak traceability. Consider two users n_i (with attribute set S_{n_i} and index n_i) and n_i' (with attribute set $S_{n_i'}$ and index n_i') collude to make a decryption black-box $\mathcal{D}$ with only S_{n_i} satisfies an access policy $\mathbb{A}$ (i.e. $S_{n_i'}$ does not satisfy $\mathbb{A}$). $\mathcal{D}$ uses user n_i's key (the part corresponding to S_{n_i}) to decrypt the ciphertext associated with $\mathbb{A}$ from the underlying CP-ABE system and user n_i''s key (the part corresponding to index n_i') to decrypt the ciphertext from the underlying tracing system. As a result, user n_i' is identified to be malicious, but $S_{n_i'}$ does not satisfy $\mathbb{A}$. To achieve strong traceability, we use a randomly chosen "binder term" to bind the CP-ABE part and the A-HIBE part in a user's private key together, and set the private key such that it is used in both CP-ABE part and the A-HIBE part (i.e. the tracing part) in the ciphertext simultaneously.

Specifically, let $\mathcal{N}$ be the number of users in the system, and each user is assigned and identified by a unique index n_i for $n_i \in \{1, 2, ..., \mathcal{N}\}$. The index of a user n_i is encoded into her/his private key by generating her/his private key $sk_{n_i,S}$ according to her/his attribute set S and a sub-identity $ID_{n_i} = (ID_1, ID_2, ..., ID_{\mathcal{N}+1-n_i})$. Due to the key delegation property of the underlying A-HIBE, a user n_i can generate the decryption key $sk_{n_{i'},S}$ provided that $n_i > n_{i'}$. The $\mathbf{Encrypt}_E(pp, \mathbb{A}, n_j, m)$ algorithm is defined similar to conventional CP-ABE except for taking one more parameter $n_j \in \{1, ..., \mathcal{N}+1\}$, and the encrypted message m can be recovered using a decryption key $sk_{n_i,S}$ provided that S satisfies the access policy $\mathbb{A}$ and $n_i \geq n_j$.

The message-hiding security of Enhanced CP-ABE is a typical semantic security and is based on the underlying CP-ABE security and A-HIBE security against adaptive adversaries, except that each key is identified by a unique index. The index-hiding security of Enhanced CP-ABE roughly follows from the anonymity of the underlying A-HIBE.

1.3 Related Work

Sahai and Waters first introduced the notion of Fuzzy Identity-Based Encryption in [23]. Goyal *et al.* [7] later formalized two notions of ABE: CP-ABE and KP-ABE. Subsequently, lots of constructions of CP-ABE and KP-ABE systems were proposed [1,5,13,26]. And a series of work has been done for ABE as the following directions: new proof techniques to obtain adaptive security [1,10,13], secure outsourcing computation [8,14,21] and decentralizing trust by setting multiple authorities [11,22].

Katz *et al.* [9] introduced the notion of traceability in the context of predicate encryption. They added traceability to any inner-product predicate encryption with additional overhead linear in the number of users $\mathcal{N}$. Liu *et al.* [15] later proposed a black-box traceability CP-ABE system at the expense of sub-linear (i.e. $\sqrt{\mathcal{N}}$) overhead. Recently, Ning *et al.* [18–20] proposed practical CP-ABE systems with white-box traceability. However, there exists no efficient black-box traceable CP-ABE with short ciphertexts which are independent of $\mathcal{N}$.

1.4 Future Work

Our work raises the following open problems: (1) Can we reduce the sizes of the public parameters, private keys, ciphertexts to a constant simultaneously? (2) Can we further improve the system flexibility, say allowing unlimited number of users in the system, without sacrificing short ciphertexts, public parameters and private keys?

We note that progress on either problem would likely require improving on the A-HIBE and CP-ABE: for the first problem, reducing the public parameters, private keys and ciphertexts to a constant is a long-standing open problem; for the second problem, an unbounded A-HIBE and compact CP-ABE with short ciphertexts, public parameters and private keys are desirable which is also a long-standing open problem.

1.5 Organization

Section 2 introduces the background. Section 3 gives the definition of BT-CP-ABE and its security model. Section 4 gives the definition of Enhanced CP-ABE, its security model and the transformation from Enhanced CP-ABE to BT-CP-ABE. Section 5 presents the construction of our Enhanced CP-ABE as well as the security proof. Finally, Sect. 6 presents a briefly conclusion.

2 Background

We define $[l] = \{1, 2, ..., l\}$ and $[l_1, l_2] = \{l_1, l_1 + 1, ..., l_2\}$, where l, l_1, l_2 are positive integers. Let $\mathcal{N}$ be the number of users in the system, each user is assigned and identified by a unique index $n_i \in [\mathcal{N}]$.

Access Structure. Let U denote the attribute universe. A collection $\mathbb{A} \subseteq 2^U$ of non-empty sets of attributes is an access structure on U. The sets in $\mathbb{A}$ are called the authorized sets, and the sets not in $\mathbb{A}$ are called the unauthorized sets. A collection $\mathbb{A} \subseteq 2^U$ is called monotone if $\forall B, C \in \mathbb{A} : if\ B \in \mathbb{A}$ and $B \subseteq C$, then $C \in \mathbb{A}$.

Linear Secret-Sharing Schemes (LSSS). Let U denote the attribute universe. A secret-sharing scheme $\prod$ with domain of secrets $\mathbb{Z}_p$ realizing access structure on U in called linear (over $\mathbb{Z}_p$) if (1) The shares of a secret $s \in \mathbb{Z}_p$ for each attribute form a vector over $\mathbb{Z}_p$; (2) For each access structure $\mathbb{A}$ on U, there exists a matrix M with l rows and n columns called the share-generating matrix. For $i = 1, ..., l$, we define a function ρ labels row i of M with attribute $\rho(i)$ from the attribute universe U. When we consider the column vector $\overrightarrow{v} = (s, r_2, ..., r_n)^{\perp}$, where $r_2, ..., r_n \in \mathbb{Z}_p$ are randomly chosen. Then $M\overrightarrow{v}$ is the vector of l shares of the secret s according to $\prod$. The share $(M\overrightarrow{v})_j$ "belongs" to attribute $\rho(j)$, where $j \in [l]$.

Composite Order Bilinear Groups. We let $\mathcal{G}$ denote a group generator, which takes a security parameter λ and outputs a description of a bilinear group G. Define the output of $\mathcal{G}$ as $(p_1, p_2, p_3, p_4, G, G_T, e)$, where p_1, p_2, p_3, p_4 are

distinct primes, G, G_T are cyclic groups of order $N = p_1p_2p_3p_4$, and $e : G^2 \to G_T$ is a map such that: (1) Bilinearity: $\forall u, v \in G$ and $a, b \in \mathbb{Z}_p$, we have $e(u^a, v^b) = e(u, v)^{ab}$; (2) Non-degeneracy: $\exists g \in G$ such that $e(g, g)$ has order N in G_T.

Complexity Assumptions. The message-hiding security of our Enhanced CP-ABE in $Game^E_{MH_1}$ will rely on four assumptions (the Assumption 1, the General Subgroup Decision Assumption, the 3-Party Diffie-Hellman Assumption in a Subgroup, and the Source Group q-Parallel BDHE Assumption in a subgroup) which are used in [12] to achieve full security of their CP-ABE system, excepting that we extend them to four subgroups (i.e. $N = p_1p_2p_3p_4$) and give one more subgroup generator g_4 to the distinguisher D. The message-hiding security of our Enhanced CP-ABE in $Game^E_{MH_{\mathcal{N}+1}}$ will rely on three assumptions (the General Subgroup Decision Assumption, the Assumptions 5 and 6) which are used in [24] to achieve full security of their HIBE system. Assumption 7 will be used to prove the index-hiding security of our Enhanced CP-ABE in $Game^E_{IH}$, which is used in [24] to achieve the anonymity of their HIBE system.

Assumption 1. [12] *Given a group generator $\mathcal{G}$, define the following distribution:* $\mathbb{G} = (N = p_1p_2p_3p_4, G, G_T, e) \xleftarrow{R} \mathcal{G}, \alpha, s \xleftarrow{R} \mathbb{Z}_N$, $g_1 \xleftarrow{R} G_{p_1}, g_2, X_2, Y_2 \xleftarrow{R} G_{p_2}, g_3 \xleftarrow{R} G_{p_3}, g_4 \xleftarrow{R} G_{p_4}$, $D = (\mathbb{G}, g_1, g_2, g_3, g_4, g_1^{\alpha}X_2, g_1^{s}Y_2)$, $T_0 = e(g_1, g_1)^{\alpha s}, T_1 \xleftarrow{R} G_T$.

An algorithm $\mathcal{A}$'s advantage in breaking this assumption is: $Adv^1_{\mathcal{G},\mathcal{A}}(\lambda) = |\Pr[\mathcal{A}(D, T_0) = 1] - \Pr[\mathcal{A}(D, T_1) = 1]|$. We say that $\mathcal{G}$ satisfies Assumption 1 if $Adv^1_{\mathcal{G},\mathcal{A}}(\lambda)$ is a negligible function of λ for any PPT algorithm $\mathcal{A}$.

Assumption 2. *(The General Subgroup Decision Assumption):* [12] *Given a group generator $\mathcal{G}$ and a collection of non-empty subsets of $\{1, 2, 3, 4\}$ $Z_0, Z_1, ..., Z_k$ where each Z_i for $i \geq 2$ satisfies either $Z_0 \cap Z_i = \phi = Z_1 \cap Z_i$ or $Z_0 \cap Z_i \neq \phi \neq Z_1 \cap Z_i$. Define the following distribution:* $\mathbb{G} = (N = p_1p_2p_3p_4, G, G_T, e) \xleftarrow{R} \mathcal{G}$, $g_{Z_2} \xleftarrow{R} G_{Z_2}, ..., g_{Z_k} \xleftarrow{R} G_{Z_k}$, $D = (\mathbb{G}, g_{Z_2}, ..., g_{Z_k})$, $T_0 \xleftarrow{R} G_{Z_0}, T_1 \xleftarrow{R} G_{Z_1}$.

Fixing the collection of sets $Z_0, Z_1, ..., Z_k$, the advantage of an algorithm $\mathcal{A}$ in breaking this assumption is: $Adv^{SD}_{\mathcal{G},\mathcal{A}}(\lambda) = |\Pr[\mathcal{A}(D, T_0) = 1] - \Pr[\mathcal{A}(D, T_1) = 1]|$. We say that $\mathcal{G}$ satisfies the General Subgroup Decision Assumption if $Adv^{SD}_{\mathcal{G},\mathcal{A}}(\lambda)$ is a negligible function of λ for any PPT algorithm $\mathcal{A}$ and any suitable collection of subsets $Z_0, Z_1, ..., Z_k$.

Assumption 3. *(The 3-Party Diffie-Hellman Assumption in a Subgroup):* [12] *Given a group generator $\mathcal{G}$, define the following distribution:* $\mathbb{G} = (N = p_1p_2p_3p_4, G, G_T, e) \xleftarrow{R} \mathcal{G}, x, y, z \xleftarrow{R} \mathbb{Z}_N$, $g_1 \xleftarrow{R} G_{p_1}, g_2 \xleftarrow{R} G_{p_2}, g_3 \xleftarrow{R} G_{p_3}, g_4 \xleftarrow{R} G_{p_4}$, $D = (\mathbb{G}, g_1, g_2, g_3, g_4, g_2^x, g_2^y, g_2^z)$, $T_0 = g_2^{xyz}, T_1 \xleftarrow{R} G_{p_2}$.

An algorithm $\mathcal{A}$'s advantage in breaking this assumption is: $Adv^{3DH}_{\mathcal{G},\mathcal{A}}(\lambda) = |\Pr[\mathcal{A}(D, T_0) = 1] - \Pr[\mathcal{A}(D, T_1) = 1]|$. We say that $\mathcal{G}$ satisfies the 3-Party Diffie-Hellman Assumption in a Subgroup if $Adv^{3DH}_{\mathcal{G},\mathcal{A}}(\lambda)$ is a negligible function of λ for any PPT algorithm $\mathcal{A}$.

Assumption 4. *(The Source Group q-Parallel BDHE Assumption in a Subgroup):* [12] *Given a group generator* $\mathcal{G}$ *and a positive integer* q*, define the following distribution:* $\mathbb{G} = (N = p_1p_2p_3p_4, G, G_T, e) \xleftarrow{R} \mathcal{G}, c, d, f, b_1, ..., b_q \xleftarrow{R} \mathbb{Z}_N$, $g_1 \xleftarrow{R} G_{p_1}, g_2 \xleftarrow{R} G_{p_2}, g_3 \xleftarrow{R} G_{p_3}, g_4 \xleftarrow{R} G_{p_4}$, $D = (\mathbb{G}, g_1, g_2, g_3, g_4, g_2^f, g_2^{df}, g_2^c, g_2^{c^2}, ..., g_2^{c^q}, g_2^{c^{q+2}}, ..., g_2^{c^{2q}}, g_2^{c^i/b_j}\ \forall i \in [2q]\backslash\{q+1\}, j \in [q], g_2^{dfb_j}\ \forall j \in [q], g_2^{dfc^ib_{j'}/b_j}\ \forall i \in [q], j, j' \in [q]\ s.t.\ j \neq j')$, $T_0 = g_2^{dc^{q+1}}, T_1 \xleftarrow{R} G_{p_2}$.

An algorithm $\mathcal{A}$'s advantage in breaking this assumption is: $Adv^q_{\mathcal{G},\mathcal{A}}(\lambda) = |\Pr[\mathcal{A}(D, T_0) = 1] - \Pr[\mathcal{A}(D, T_1) = 1]|$. We say that $\mathcal{G}$ satisfies the Source Group q-Parallel BDHE Assumption in a Subgroup if $Adv^q_{\mathcal{G},\mathcal{A}}(\lambda)$ is a negligible function of λ for any PPT algorithm $\mathcal{A}$.

Assumption 5. [24] *Given a group generator* $\mathcal{G}$*, define the following distribution:* $\mathbb{G} = (N = p_1p_2p_3p_4, G, G_T, e) \xleftarrow{R} \mathcal{G}, X_1 \xleftarrow{R} G_{p_1}, Y_2 \xleftarrow{R} G_{p_2}, X_3, Y_3, Y_3' \xleftarrow{R} G_{p_3}, X_4 \xleftarrow{R} G_{p_4}$, $D \leftarrow (\mathbb{G}, X_1, Y_2Y_3, X_3, X_4)$, $T_0 \xleftarrow{R} Y_2Y_3', T_1 \xleftarrow{R} G_{p_2p_3}$.

An algorithm $\mathcal{A}$'s advantage in breaking this assumption is: $Adv^5_{\mathcal{G},\mathcal{A}}(\lambda) = |\Pr[\mathcal{A}(D, T_0) = 1] - \Pr[\mathcal{A}(D, T_1) = 1]|$. We say that $\mathcal{G}$ satisfies Assumption 5 if $Adv^5_{\mathcal{G},\mathcal{A}}(\lambda)$ is a negligible function of λ for any PPT algorithm $\mathcal{A}$.

Assumption 6. [24] *Given a group generator* $\mathcal{G}$*, define the following distribution:* $\mathbb{G} = (N = p_1p_2p_3p_4, G, G_T, e) \xleftarrow{R} \mathcal{G}, g, X_1, Y_1 \xleftarrow{R} G_{p_1}, X_2, Y_2, Z_2 \xleftarrow{R} G_{p_2}, X_3, Z_3 \xleftarrow{R} G_{p_3}, X_4 \xleftarrow{R} G_{p_4}$, $D = (\mathbb{G}, g, X_1X_2, X_3, Y_1Y_2, Z_2Z_3, X_4)$, $T_0 = e(X_1, Y_1), T_1 \xleftarrow{R} G_T$.

An algorithm $\mathcal{A}$'s advantage in breaking this assumption is: $Adv^6_{\mathcal{G},\mathcal{A}}(\lambda) = |\Pr[\mathcal{A}(D, T_0) = 1] - \Pr[\mathcal{A}(D, T_1) = 1]|$. We say that $\mathcal{G}$ satisfies Assumption 6 if $Adv^6_{\mathcal{G},\mathcal{A}}(\lambda)$ is a negligible function of λ for any PPT algorithm $\mathcal{A}$.

Assumption 7. [24] *Given a group generator* $\mathcal{G}$*, define the following distribution:* $\mathbb{G} = (N = p_1p_2p_3p_4, G, G_T, e) \xleftarrow{R} \mathcal{G}, X_1, Y_1, W_1 \xleftarrow{R} G_{p_1}, Y_2, Z_2, W_2, W_2' \xleftarrow{R} G_{p_2}, Z_3 \xleftarrow{R} G_{p_3}, X_4, Z_4, W_4, W_4' \xleftarrow{R} G_{p_4}$, $D \leftarrow (\mathbb{G}, X_1X_4, Y_1Y_2, Z_2, Z_3, Z_4, W_1W_2W_4)$, $T_0 = W_1W_2'W_4', T_1 \xleftarrow{R} G_{p_1p_2p_4}$.

An algorithm $\mathcal{A}$'s advantage in breaking this assumption is: $Adv^7_{\mathcal{G},\mathcal{A}}(\lambda) = |\Pr[\mathcal{A}(D, T_0) = 1] - \Pr[\mathcal{A}(D, T_1) = 1]|$. We say that $\mathcal{G}$ satisfies Assumption 7 if $Adv^7_{\mathcal{G},\mathcal{A}}(\lambda)$ is a negligible function of λ for any PPT algorithm $\mathcal{A}$.

3 Black-box Traceable CP-ABE

3.1 Definition

A black-box traceable CP-ABE (BT-CP-ABE) system is a CP-ABE system where a decryption black-box can be traced to the corresponding malicious users

who built it. We extend the conventional (non-traceable) CP-ABE by assigning and identifying users with unique indices, and adding a **Trace** algorithm to it. In particular, following the notation of the CP-ABE system introduced in [12], a BT-CP-ABE system consists of five algorithms as follows:

- **Setup**$(\lambda, \mathcal{U}, \mathcal{N}) \rightarrow (pp, msk)$. The algorithm takes a security parameter λ, the attribute universe description $\mathcal{U}$ and the number of users $\mathcal{N}$ in the system. It outputs the public parameters pp and a master secret key msk.
- **KeyGen**$(pp, msk, S) \rightarrow sk_{n_i,S}$. The algorithm takes the public parameters pp, the master secret key msk and a set of attributes S. It outputs a private key $sk_{n_i,S}$, which is assigned and identified by a unique index $n_i \in \{1, ..., \mathcal{N}\}$. And we assume that S is implicitly included in $sk_{n_i,S}$.
- **Encrypt**$(pp, \mathbb{A}, m) \rightarrow ct$. The algorithm takes the public parameters pp, an access structure $\mathbb{A}$ over the universe of attributes and a message m. It outputs a ciphertext ct. We assume that $\mathbb{A}$ is implicitly included in ct.
- **Decrypt**$(pp, sk_{n_i,S}, ct) \rightarrow m$ or $\perp$. The algorithm takes the public parameters pp, a secret key $sk_{n_i,S}$, and a ciphertext ct. If S satisfies ct's access policy, the algorithm outputs the message m. Otherwise, it outputs $\perp$.
- **Trace**$^{\mathcal{D}}(pp, \mathbb{A}_{\mathcal{D}}, \epsilon) \rightarrow \mathbb{N}_T$: The tracing algorithm takes the public parameters pp, an access policy $\mathbb{A}_{\mathcal{D}}$ and a probability value (lower-bound) ϵ[1]. It is an oracle algorithm interacts with a policy-specific decryption black-box $\mathcal{D}$. It runs in time polynomial in 1^{λ} and $1/\epsilon$, and outputs an index set $\mathbb{N}_T \subseteq \{1, ..., \mathcal{N}\}$ of malicious user(s). Note that in our setting, we treat $\mathcal{D}$ as a probabilistic circuit that takes as input a ciphertext ct and returns a message m or $\perp$. And such a decryption black-box does not need to be perfect, we only require it to decrypt successfully with non-negligible probability.

3.2 Message-Hiding Security

The message-hiding security is a typical semantic security similar to that of conventional CP-ABE system [12], excepting every key query is companied with a unique index. Similar to [15], to capture the security that an adversary can choose keys to corrupt adaptively, we allow an adversary to specify the index (which is originally assigned by the **KeyGen** algorithm) to a decryption key when he makes a key query. Note that to guarantee that each user/key can be identified by an index uniquely, an adversary can adaptively ask for a decryption key corresponding to (n_i, S_{n_i}) for $i \in \{1, ..., q\}$, where $n_i \in \{1, ..., \mathcal{N}\}, q \leq \mathcal{N}$. Also note that for any two pairs (n_i, S_{n_i}) and (n_j, S_{n_j}) where $n_i \neq n_j$ for $\forall i \neq j, i, j \in \{1, ..., q\}$, we do not require $S_{n_i} \neq S_{n_j}$.

The message-hiding security is described by a security game $Game_{MH}$ between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$. The phases of the game are as follows:

[1] Note that ϵ is the lower-bound of a policy-specific decryption black-box's decryption ability, and it has to be polynomially related to the security parameter.

- **Setup:** $\mathcal{C}$ runs **Setup**$(\lambda, \mathcal{U}, \mathcal{N})$ and sends pp to $\mathcal{A}$.
- **Query Phase 1:** For $i = 1$ to q_1, $\mathcal{A}$ adaptively submits (n_i, S_{n_i}), and $\mathcal{C}$ responds with $sk_{n_i, S_{n_i}}$.
- **Challenge:** $\mathcal{A}$ submits two equal length messages m_0, m_1 and an access policy $\mathbb{A}^*$. $\mathbb{A}^*$ cannot be satisfied by any of the queried $S_{n_1}, ..., S_{n_{q_1}}$. $\mathcal{C}$ flips a random coin $\beta \in \{0, 1\}$ and gives an encryption of m_β under $\mathbb{A}^*$ to $\mathcal{A}$.
- **Query Phase 2:** For $i = q_1 + 1$ to q, $\mathcal{A}$ adaptively submits (n_i, S_{n_i}) with the restriction that none of these queried attribute sets satisfy $\mathbb{A}^*$, and $\mathcal{C}$ responds with $sk_{n_i, S_{n_i}}$.
- **Guess:** $\mathcal{A}$ outputs a guess $\beta' \in \{0, 1\}$ for β.

$\mathcal{A}$'s advantage is defined as $Adv = \Pr[\beta' = \beta] - \frac{1}{2}$ in $Game_{MH}$.

Definition 1. *A $\mathcal{N}$-user BT-CP-ABE system is adaptively message-hiding secure if there exists no probabilistic polynomial-time (PPT) adversary has a non-negligible advantage in the above security game.*

Selective message-hiding security is defined by adding an initialization phase where the adversary must declare the access policy $\mathbb{A}^*$ before seeing the public parameters pp.

3.3 Black-box Traceability

The black-box traceability definition is described by a security game $Game_{BT}$ between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$. The phases of the game are as follows:

- **Setup:** $\mathcal{C}$ runs **Setup**$(\lambda, \mathcal{U}, \mathcal{N})$ and sends pp to $\mathcal{A}$.
- **Key Query:** For $i = 1$ to q, $\mathcal{A}$ adaptively submits (n_i, S_{n_i}), and $\mathcal{C}$ responds with $sk_{n_i, S_{n_i}}$.
- **(Policy-Specific) Decryption Black-box Generation:** $\mathcal{A}$ outputs a decryption black-box $\mathcal{D}$ associated with an access policy $\mathbb{A}_\mathcal{D}$ and a probability value ϵ.
- **Trace:** $\mathcal{C}$ runs $\mathbf{Trace}^\mathcal{D}(pp, \mathbb{A}_\mathcal{D}, \epsilon)$ to get an index set $\mathbb{N}_T \subseteq \{1, ..., \mathcal{N}\}$ of malicious user(s).

Let $\mathbb{N}_\mathcal{D} = \{n_i | 1 \leq i \leq q\}$ be the index set of corrupted keys. We say $\mathcal{A}$ wins the above game if the following conditions hold:

(1) $\mathcal{D}$ generated by $\mathcal{A}$ is a useful policy-specific decryption black-box. That is, it holds that $\Pr[\mathcal{D}(\mathbf{Encrypt}(pp, \mathbb{A}_\mathcal{D}, m)) = m] \geq \epsilon$, where the probability is taken over the random coins of $\mathcal{D}$ and the random choices of message m.
(2) S_{n_i} *does not satisfy* $\mathbb{A}_\mathcal{D}$ *for* $\forall n_i \in \mathbb{N}_T$, or $\mathbb{N}_T \nsubseteq \mathbb{N}_\mathcal{D}$, or $\mathbb{N}_T = \emptyset$.

Definition 2. *A $\mathcal{N}$-user BT-CP-ABE system is adaptively traceable against policy-specific decryption black-box if there exists no PPT adversary has a non-negligible advantage in the above game.*

Selective black-box traceability is defined by adding an initialization phase where the adversary must declare the access policy $\mathbb{A}_{\mathcal{D}}$ before seeing the public parameters pp.

Note that as of [2,3,6,9,15], in this paper, we are modeling a stateless (resettable) decryption black-box.

4 Enhanced CP-ABE

Following the routes of [2,3,6,15], instead of constructing BT-CP-ABE directly, We define a simpler primitive named Enhanced CP-ABE (EnCP-ABE for short) and its security notion first, then we show that BT-CP-ABE can be transformed from EnCP-ABE.

4.1 Definition

An EnCP-ABE system consists of the following five algorithms.

- $\mathbf{Setup}_E(\lambda, \mathcal{U}, \mathcal{N}) \rightarrow (pp, msk)$. The algorithm takes a security parameter λ, the attribute universe description $\mathcal{U}$ and the numbers of users $\mathcal{N}$ in the system. It outputs the public parameters pp and a master secret key msk.
- $\mathbf{KeyGen}_E(pp, msk, S) \rightarrow sk_{n_i,S}$. The algorithm takes the public parameters pp, the master secret key msk and a set of attributes S. It outputs a private key $sk_{n_i,S}$, which is assigned and identified by a unique index $n_i \in [\mathcal{N}]$.
- $\mathbf{KeyDel}_E(pp, sk_{n_i,S}) \rightarrow sk_{n'_i,S}{}_{s.t.\ n_i \in [2,\mathcal{N}], n'_i \in [\mathcal{N}], n'_i < n_i}$ [2]. The algorithm takes the public parameters pp and a secret key $sk_{n_i,S}$. It outputs a secret key $sk_{n'_i,S}$ corresponding to the attribute set S and index n'_i subject to $n'_i < n_i$.
- $\mathbf{Encrypt}_E(pp, \mathbb{A}, n_j, m) \rightarrow ct$. The algorithm takes the public parameters pp, an access structure $\mathbb{A}$ over the universe of attributes, an index $n_j \in [\mathcal{N}+1]$ and a message m. It outputs a ciphertext ct.
- $\mathbf{Decrypt}_E(pp, sk_{n_i,S}, ct) \rightarrow m$ or $\perp$. The algorithm takes the public parameters pp, a secret key $sk_{n_i,S}$, and a ciphertext ct encrypted with index n_j. If S satisfies ct's access policy and $n_i \geq n_j$, the algorithm outputs the message m. Otherwise, it output $\perp$.

Note that if we always set n_j of the $\mathbf{Encrypt}_E(pp, \mathbb{A}, n_j, m)$ algorithm equal to 1, the functions of EnCP-ABE are identical to that of BT-CP-ABE.

4.2 Message-Hiding Security

The message-hiding security is described by a security game between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$. The phases of the game are as follows:

[2] This key delegation algorithm is a weak one than that of [24]. We remove the key re-randomization operation since it will only be invoked by the **Decrypt** algorithm.

- **Setup:** $\mathcal{C}$ runs $\mathbf{Setup}_E(\lambda, \mathcal{U}, \mathcal{N})$ and sends pp to $\mathcal{A}$.
- **Query Phase 1:** For $i = 1$ to q_1, $\mathcal{A}$ adaptively submits (n_i, S_{n_i}), and $\mathcal{C}$ responds with $sk_{n_i, S_{n_i}}$.
- **Challenge:** $\mathcal{A}$ submits two equal length messages m_0, m_1 and an access policy $\mathbb{A}^*$. $\mathcal{C}$ flips a random coin $\beta \in \{0, 1\}$ and gives $ct \leftarrow \mathbf{Encrypt}_E(pp, \mathbb{A}^*, n_j, m_\beta)$ to $\mathcal{A}$.
- **Query Phase 2:** For $i = q_1 + 1$ to q, $\mathcal{A}$ adaptively submits (n_i, S_{n_i}), and $\mathcal{C}$ responds with $sk_{n_i, S_{n_i}}$.
- **Guess:** $\mathcal{A}$ outputs a guess $\beta' \in \{0, 1\}$ for β.

We define game $Game^E_{MH_1}$ as follows. We let $\mathcal{C}$ give $ct \leftarrow \mathbf{Encrypt}_E(pp, \mathbb{A}^*, 1, m_\beta)$ to $\mathcal{A}$ during the **Challenge** phase. And $\mathcal{A}$ wins the game if $\beta' = \beta$ with the restriction that none of the queried attribute sets $S_{n_1}, ..., S_{n_q}$ satisfy $\mathbb{A}^*$. $\mathcal{A}$'s advantage is defined to be $Adv_1 = \Pr[\beta' = \beta] - \frac{1}{2}$ in this game.

And we define game $Game^E_{MH_{\mathcal{N}+1}}$ as follows. We let $\mathcal{C}$ give $ct \leftarrow \mathbf{Encrypt}_E(pp, \mathbb{A}^*, \mathcal{N} + 1, m_\beta)$ to $\mathcal{A}$ during the **Challenge** phase. And $\mathcal{A}$ wins the game if $\beta' = \beta$. $\mathcal{A}$'s advantage is defined to be $Adv_{\mathcal{N}+1} = \Pr[\beta' = \beta] - \frac{1}{2}$ in this game.

Definition 3. *A $\mathcal{N}$-user Enhanced CP-ABE system is adaptively message-hiding secure if there exists no PPT adversary has a non-negligible advantage in the security game $Game^E_{MH_1}$ and $Game^E_{MH_{\mathcal{N}+1}}$.*

4.3 Index-Hiding Security

Similar to [15,17], the index-hiding security against policy-specific decryption black-box is to guarantee that there has no adversary can distinguish between $\mathbf{Encrypt}_E(pp, \mathbb{A}^*, n_j, m)$ and $\mathbf{Encrypt}_E(pp, \mathbb{A}^*, n_j + 1, m)$ for any access policy $\mathbb{A}^*$ without a secret key $sk_{n_j, S_{n_j}}$, where S_{n_j} satisfies $\mathbb{A}^*$. It is described by a security game $Game^E_{IH}$ between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$. The game takes as input a parameter $n_j \in [\mathcal{N}]$ which is given to both $\mathcal{A}$ and $\mathcal{C}$. The phases of the game are as follows:

- **Setup:** $\mathcal{C}$ runs $\mathbf{Setup}_E(\lambda, \mathcal{U}, \mathcal{N})$ and sends pp to $\mathcal{A}$.
- **Key Query:** For $i = 1$ to q, $\mathcal{A}$ adaptively submits (n_i, S_{n_i}), and $\mathcal{C}$ responds with $sk_{n_i, S_{n_i}}$.
- **Challenge:** $\mathcal{A}$ submits a message m and an access policy $\mathbb{A}^*$. $\mathcal{C}$ flips a random bit $\beta \in \{0, 1\}$ and gives $ct \leftarrow \mathbf{Encrypt}_E(pp, \mathbb{A}^*, n_j + \beta, m)$ to $\mathcal{A}$.
- **Guess:** $\mathcal{A}$ outputs a guess $\beta' \in \{0, 1\}$ for β.

We define $\mathcal{A}$ wins the game if $\beta' = \beta$ with the restriction that none of the queried pairs $\{(n_1, S_{n_1}), ..., (n_q, S_{n_q})\}$ satisfy $(S_{n_i}\ satisfies\ \mathbb{A}^*) \wedge (n_i = n_j)$ for any $i \in [q]$. $\mathcal{A}$'s advantage is defined as $Adv_{n_j} = \Pr[\beta' = \beta] - \frac{1}{2}$ in this game.

Definition 4. *A $\mathcal{N}$-user Enhanced CP-ABE system is adaptively index-hiding secure against policy-specific decryption black-box if there exists no PPT adversary has a non-negligible advantage Adv_{n_j} for any $n_j \in [\mathcal{N}]$ in $Game^E_{IH}$.*

4.4 Transform from EnCP-ABE to BT-CP-ABE

Following the routes of [2,3,6,15], we show that a BT-CP-ABE can be transformed from an EnCP-ABE with message-hiding and index-hiding security. We denote an EnCP-ABE as Γ_e, then a BT-CP-ABE can be transformed from Γ_e by the following three steps:

(1) Let EnCP-ABE be message-hiding secure and index-hiding secure.
(2) Set the parameter n_j of $\mathbf{Encrypt}_E(pp, \mathbb{A}, n_j, m)$ equal to 1, i.e., $\mathbf{Encrypt}_E(pp, \mathbb{A}, n_j, m) = \mathbf{Encrypt}_E(pp, \mathbb{A}, 1, m)$.
(3) Add a **Trace** algorithm to Γ_e defined as follows.

– $\mathbf{Trace}^{\mathcal{D}}(pp, \mathbb{A}_{\mathcal{D}}, \epsilon) \rightarrow \mathbb{N}_T \subseteq [\mathcal{N}]$: The tracing algorithm takes the public parameters pp, an access policy $\mathbb{A}_{\mathcal{D}}$ and a probability value ϵ. Given a decryption black-box $\mathcal{D}$ associated with the access policy $\mathbb{A}_{\mathcal{D}}$, it works as follows:
  1. For $n = 1$ to $\mathcal{N} + 1$, do as follows:
     (1) Repeat the following steps $8\lambda(\mathcal{N}/\epsilon)^2$ times: First, randomly sample message m from the message space. Then, let $ct \leftarrow \mathbf{Encrypt}_E(pp, \mathbb{A}_{\mathcal{D}}, n, m)$. Next, Call oracle $\mathcal{D}$ on input ct and compare the output of $\mathcal{D}$ with m;
     (2) Let f_n be the fraction of times that $\mathcal{D}$ decrypted the ciphertexts correctly.
  2. Let $\mathbb{N}_T$ be the set of all $n \in [\mathcal{N}]$ for which $f_n - f_{n+1} \geq \epsilon/(4\mathcal{N})$.
  3. Output the set $\mathbb{N}_T$ as the malicious users.

We denote Γ_{bt} as the modified Γ_e after the above transformation.

Theorem 1. *If Γ_e is adaptively (resp. selectively) message-hiding secure and adaptively (resp. selectively) index-hiding secure against policy-specific decryption black-box, then Γ_{bt} is a BT-CP-ABE with adaptive (resp. selective) traceability against policy-specific decryption black-box.*

Proof. The proof is nearly identical to that of Theorem 1 in [15], replacing "$S_{n_i} \supseteq S_{\mathcal{D}}$" with "$S_{n_i}$ $satisfies$ $\mathbb{A}_{\mathcal{D}}$".

5 An Efficient Enhanced CP-ABE

5.1 Construction

– $\mathbf{Setup}_E(\lambda, \mathcal{U}, \mathcal{N}) \rightarrow (pp, msk)$. The algorithm chooses a bilinear group G of order $N = p_1p_2p_3p_4$ (four distinct primes). It randomly chooses α, a, k, $\{b_i\}_{i\in\mathcal{U}}$, f, h, $\{u_i\}_{i\in[0,\mathcal{N}]} \in \mathbb{Z}_N$, $g \in G_{p_1}, Y_3 \in G_{p_3}$ and Y_4, $R_{g,4}$, $R_{a,4}$, $R_{k,4}$, $\{R_{b_i,4}\}_{i\in\mathcal{U}}$, $R_{f,4}$, $R_{h,4}$, $\{R_{u_i,4}\}_{i\in[0,\mathcal{N}]} \in G_{p_4}$. It then sets $G = gR_{g,4}$, $A = g^aR_{a,4}$, $K = g^kR_{k,4}$, $F = g^fR_{f,4}$, $H = g^hR_{h,4}$, $\{U_i = g^{u_i}R_{u_i,4}\}_{i\in[0,\mathcal{N}]}$, $\{B_i = g^{b_i}R_{b_i,4}\}_{i\in\mathcal{U}}$ and $E = e(g,g)^{\alpha}$. The public parameter pp is

$$(N, G, A, K, E, \{B_i\}_{i\in\mathcal{U}}, F, H, \{U_i\}_{i\in[0,\mathcal{N}]}, Y_4)$$

and the master secret key msk is

$$(g, g^{\alpha}, g^a, g^k, \{g^{b_i}\}_{i\in\mathcal{U}}, g^f, g^h, \{g^{u_i}\}_{i\in[0,\mathcal{N}]}, Y_3).$$

– $\mathbf{KeyGen}_E(pp, msk, S) \rightarrow sk_{n_i}$. For a user with index $n_i \in [\mathcal{N}]$, the algorithm represents n_i in its unary-style form (i.e., $1^{\mathcal{N}+2-n_i}$)[3]. It randomly chooses $t, c, \delta, t_0, t_1 \in \mathbb{Z}_N, R, R', R'', R_3, R'_3, R''_3, \{R_i\}_{i\in[\mathcal{N}+2-n_i,\mathcal{N}] \ s.t. \ n_i\geq 2}, \{R'_i\}_{i\in S} \in G_{p_3}$. The secret key sk_{n_i} is

$$\begin{pmatrix} K_1 = g^{\alpha} g^{at} g^{kc} g^{\delta} R, K_2 = g^c R', K_3 = g^t R'', \\ \{K'_i = (g^{b_i})^t R'_i\}_{i\in S}, \\ K_4 = g^{t_1} R_3, K_5 = g^{\delta} g^{ft_0} (g^h \Pi_{i=0}^{\mathcal{N}+1-n_i} g^{u_i})^{t_1} R'_3, \\ K_6 = g^{t_0} R''_3, \{T_i = (g^{u_i})^{t_1} R_i\}_{i\in[\mathcal{N}+2-n_i,\mathcal{N}] \ s.t. \ n_i\geq 2} \end{pmatrix}.$$

– $\mathbf{KeyDel}_E(sk_{n_i}, pp) \rightarrow sk_{n'_i \ s.t. \ n_i\in[2,\mathcal{N}], n'_i\in[\mathcal{N}], n'_i<n_i}$. Given a secret key sk_{n_i}, the algorithm creates a secret key $sk_{n'_i}$ subject to $n'_i < n_i$, where $n_i \in [2, \mathcal{N}], n'_i \in [\mathcal{N}]$. Without loss of generality, the algorithm generates $sk_{n'_i}$ for $n'_i = n_i - 1$ as follows.
  (1) It parses sk_{n_i} as $(\tilde{K}_1, \tilde{K}_2, \tilde{K}_3, \tilde{K}_4, \tilde{K}_5, \tilde{K}_6, \{\tilde{K}'_i\}_{i\in S}, \{\tilde{T}_i\}_{i\in[\mathcal{N}+2-n_i,\mathcal{N}] \ s.t. \ n_i\geq 2})$.
  (2) It takes the following (weak) delegation step to generate $sk_{n'_i}$ for $n'_i = n_i - 1$. It sets

$$\begin{pmatrix} K_1 = \tilde{K}_1, K_2 = \tilde{K}_2, \\ \{K'_i = \tilde{K}'_i\}_{i\in S}, \\ K_4 = \tilde{K}_4, K_5 = \tilde{K}_5 \tilde{T}_{\mathcal{N}+2-n_i}, \\ K_6 = \tilde{K}_6, \{T_i = \tilde{T}_i\}_{i\in[\mathcal{N}+3-n_i,\mathcal{N}] \ s.t. \ n_i\geq 3} \end{pmatrix}.$$

  It returns $sk_{n'_i} = (K_1, K_2, K_3, K_4, K_5, K_6, \{K'_i\}_{i\in S}, \{T_i\}_{i\in[\mathcal{N}+2-n'_i,\mathcal{N}] \ s.t. \ n'_i\geq 2})$.

  We note that, the algorithm will only be invoked by the decryption algorithm, we focus on the decryption ability. The distribution of the secret key does not matter in our case. A user with sk_{n_i} who can delegate all the secret keys $sk_{n'_i}$ subject to $n'_i < n_i$ is deemed to have all the decryption abilities corresponding to $sk_{n'_i}$ for all $n'_i < n_i$.
– $\mathbf{Encrypt}_E(pp, (M, \rho), n_j, m) \rightarrow ct$. M is an $l \times n$ matrix and ρ is a map from each row M_j of M to an attribute $\rho(i) \in \mathcal{U}$. The algorithm represents n_j in its unary-style form (i.e., $1^{\mathcal{N}+2-n_j}$). It then randomly chooses a random vector $\boldsymbol{y} = (s, y_2, ..., y_n)$, where s is the random secret to be shared. For each row M_j of M, it randomly chooses $r_j \in \mathbb{Z}_N$. Then it randomly chooses $R_{4,1}, R_{4,2}, R_{4,3}, R_{4,4}, \{R_{j,1,4}, R_{j,2,4}\}_{j\in[l]} \in G_{p_4}$. The ciphertext ct is

$$\begin{pmatrix} C_0 = m \cdot E^s, C_1 = G^s R_{4,1}, C_2 = K^s R_{4,2}, \\ \{C_{j,1} = A^{M_j \boldsymbol{y}} B_{\rho(j)}^{-r_j} R_{j,1,4}, C_{j,2} = G^{r_j} R_{j,2,4}\}_{j\in[l]}, \\ C_3 = (H \cdot \Pi_{i=0}^{\mathcal{N}+1-n_j} U_i)^s R_{4,3}, C_4 = F^s R_{4,4} \end{pmatrix}.$$

[3] For each index $n_i \in [\mathcal{N}]$, instead of picking a sub-identity $ID_{n_i} = (ID_0, ID_1, ID_2, ..., ID_{\mathcal{N}+1-n_i})$ from a random pseudo identity $ID = (ID_0, ID_1, ID_2, ..., ID_{\mathcal{N}}) \in \mathbb{Z}_N^{\mathcal{N}+1}$, we represents n_i in a unary-style form similar to the unary representation, i.e., $1^{\mathcal{N}+2-n_i}$. Concretely, we may view our unary-style representation as a special form of the pseudo identity in the paper, i.e., we actually set $ID_0 = ID_1 = \cdots = ID_{\mathcal{N}} = 1$.

– $\mathbf{Decrypt}_E(pp, sk_{n_i}, ct) \rightarrow m$ or $\perp$. Assume ct is encrypted with index n_j. If $n_i > n_j$, the algorithm calls $\mathbf{KeyDel}_E(sk_{n_i}, pp)$ algorithm and gets the secret key sk_{n_j}. If S does not satisfy (A, ρ), the algorithm outputs $\perp$. Otherwise, it computes the constants $\omega_j \in \mathbb{Z}_N$ such that $\sum_{\rho(j)\in S} \omega_j A_j = (1, 0, ..., 0)$. It then computes:

$$\frac{e(K_1, C_1)e(K_4, C_3)e(K_6, C_4)(e(K_2, C_2)e(K_5, C_1))^{-1}}{\prod_{\rho(j)\in S}(e(K_3, C_{j,1})e(K'_{\rho(j)}, C_{j,2}))^{\omega_j}} = e(g, g)^{\alpha s}.$$

Then m can be recovered as $C_0/e(g, g)^{\alpha s}$. Note that the decryption works if and only if S satisfies the access policy of ct and $n_i \geq n_j$.

5.2 Message-Hiding Security in $Game^E_{MH_1}$

Theorem 2. *If Assumption 1, the General Subgroup Decision Assumption, the 3-Party Diffie-Hellman Assumption in a Subgroup, the Source Group q-Parallel BDHE Assumption in a Subgroup hold, no PPT adversary can achieve a non-negligible advantage in winning* $Game^E_{MH_1}$.

Due to space, we refer the reader to Appendix A for the proof of this theorem.

5.3 Message-Hiding Security in $Game^E_{MH_{\mathcal{N}+1}}$

Theorem 3. *If the General Subgroup Decision Assumption, Assumptions 5 and 6 hold, no PPT adversary can achieve a non-negligible advantage in winning* $Game^E_{MH_{\mathcal{N}+1}}$.

Due to space, we refer the reader to Appendix B for the proof of this theorem.

5.4 Index-Hiding Security

Theorem 4. *If the General Subgroup Decision Assumption, the 3-Party Diffie-Hellman Assumption in a Subgroup, the Source Group q-Parallel BDHE Assumption in a Subgroup, Assumptions 5, 6 and 7 hold, no PPT adversary can achieve a non-negligible advantage in winning* $Game^E_{IH}$.

Due to space, we refer the reader to Appendix C for the proof of this theorem.

6 Conclusions

In this paper, we proposed an efficient traceable CP-ABE supporting public fully collusion-resistant black-box traceability and high expressiveness. The system is proved fully secure and adaptively traceable against both key-like and policy-specific decryption black-boxes in the standard model. Compared with the most efficient black-box traceable CP-ABE currently available with high expressiveness and full security, ciphertexts in the proposed system are independent of the

number of users $\mathcal{N}$ in the system, rather than sub-linear in $\mathcal{N}$, while the public parameters and private keys are linear in $\mathcal{N}$. These make our proposed system more suitable and more practical for commercial applications. We thought our new methodology of realizing traitor tracing functionality may serve as the first step towards more practical solution to BT-CP-ABE.

Acknowledgments. This work is supported in part by the National Natural Science Foundation of China (Grant No. 6163000206, 61373154, 61371083, 61472142 and 61411146001), in part by the Prioritized Development Projects through the Specialized Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20130073130004), in part by Shanghai High-tech field project (Grant No. 16511101400), and in part by Science and Technology Commission of Shanghai Municipality (Grant No. 14YF1404200).

A Proof of Theorem 2

Proof Overview. Roughly speaking, the message-hiding security of our EnCP-ABE in the sense of $Game^{E}_{MH_1}$ is guaranteed by the IND-CPA security of the CP-ABE system in [12]. Hence the proof of this theorem mainly follows the proof of IND-CPA in [12]. For simplicity, here we prove this theorem by reducing the message-hiding of our EnCP-ABE in $Game^{E}_{MH_1}$ to the IND-CPA security of the CP-ABE system in [12]. Due to space, complete proof will be given in the full paper.

B Proof of Theorem 3

Proof Overview. Roughly speaking, the message hiding of our EnCP-ABE in the sense of $Game^{E}_{MH_{\mathcal{N}+1}}$ is guaranteed by the IND-CPA of the HIBE system in [24]. The proof of this theorem also follows that of [24]. For simplicity, here we prove this theorem by reducing the message-hiding of our EnCP-ABE in $Game^{E}_{MH_{\mathcal{N}+1}}$ to the IND-CPA security of the HIBE system in [24]. Due to space, complete proof will be given in the full paper.

C Proof of Theorem 4

We prove the theorem by considering two cases separately. Let $\bar{n}_j$ be the parameter which is given to both the adversary $\mathcal{A}$ and the challenger defined in $Game^{E}_{IH}$. $\mathcal{A}$ will eventually behave in one of two different ways in $Game^{E}_{IH}$:

Case 1: In Key Query phase, each query (n_i, S_{n_i}) submitted by $\mathcal{A}$ satisfies $n_i \neq \bar{n}_j$. It will not violate the restriction in the model even when $S_{n_i} \in \mathbb{A}^*$.

Case 2: In Key Query phase, $\mathcal{A}$ will submit an query (n_i, S_{n_i}) such that $(n_i = \bar{n}_j)$. The restriction in the security model implies that $S_{n_i} \notin \mathbb{A}^*$.

We prove our EnCP-ABE is index-hiding in both cases in the following Theorems 5 and 6 respectively. Since our classification above is complete, combining them together immediately concludes the proof of Theorem 4.

Proof of Case 1

Theorem 5. *If the General Subgroup Decision Assumption, Assumptions 5, 6 and 7 hold, no PPT adversary can achieve a non-negligible advantage in winning* $Game^{E}_{IH}$ *in Case 1.*

Proof Overview. Basically, the case-1 index-hiding of our Enhanced CP-ABE in the sense of $Game^{E}_{IH}$ is almost the same to that of [24]. Due to space, complete proof will be given in the full paper.

Proof of Case 2. From high-level point of view, the index-hiding in the second case relies on both the CP-ABE part and the A-HIBE part. For query with $n_i \neq \bar{n}_j$, we may deal with the key in a similar way as the proof of case 1. The main challenge is how to deal with the query with $n_i = \bar{n}_j$ in which case the above technique fails. Fortunately, our construction allows us to borrow the security from the CP-ABE part using the restriction that attribute set S_{n_i} must not satisfy the challenge policy $\mathbb{A}^*$. We prove the following theorem.

Theorem 6. *If the General Subgroup Decision Assumption, the 3-Party Diffie-Hellman Assumption in a Subgroup, the Source Group q-Parallel BDHE Assumption in a Subgroup, Assumptions 5 and 7 hold, no PPT adversary can achieve a non-negligible advantage in winning* $Game^{E}_{IH}$ *in Case 2.*

Proof Overview. We prove the theorem via a hybrid argument over a sequence of games similar to those used for proving index-hiding in case 1. Due to space, complete proof will be given in the full paper.

References

1. Attrapadung, N.: Dual system encryption via doubly selective security: framework, fully secure functional encryption for regular languages, and more. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 557–577. Springer, Heidelberg (2014)
2. Boneh, D., Sahai, A., Waters, B.: Fully collusion resistant traitor tracing with short ciphertexts and private keys. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 573–592. Springer, Heidelberg (2006)
3. Boneh, D., Waters, B.: A fully collusion resistant broadcast, trace, and revoke system. In: Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 211–220. ACM (2006)
4. Cao, Z.: New trends of information security - how to change people's life style? Sci. China Inf. Sci. **59**(5), 050106:1–050106:3 (2016)
5. Chen, J., Gay, R., Wee, H.: Improved dual system ABE in prime-order groups via predicate encodings. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9057, pp. 595–624. Springer, Heidelberg (2015)
6. Garg, S., Kumarasubramanian, A., Sahai, A., Waters, B.: Building efficient fully collusion-resilient traitor tracing and revocation schemes. In: Proceedings of the 17th ACM Conference on Computer and Communications Security, pp. 121–130. ACM (2010)

7. 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, pp. 89–98. ACM (2006)
8. Green, M., Hohenberger, S., Waters, B.: Outsourcing the decryption of ABE ciphertexts. In: USENIX Security Symposium, p. 3 (2011)
9. Katz, J., Schröder, D.: Tracing insider attacks in the context of predicate encryption schemes. In: ACITA (2011)
10. Lewko, A., Waters, B.: New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 455–479. Springer, Heidelberg (2010)
11. Lewko, A., Waters, B.: Decentralizing attribute-based encryption. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 568–588. Springer, Heidelberg (2011)
12. Lewko, A., Waters, B.: New proof methods for attribute-based encryption: achieving full security through selective techniques. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 180–198. Springer, Heidelberg (2012)
13. Lewko, A., Waters, B.: New proof methods for attribute-based encryption: achieving full security through selective techniques. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 180–198. Springer, Heidelberg (2012)
14. Li, J., Lin, X., Zhang, Y., Han, J.: KSF-OABE: outsourced attribute-based encryption with keyword search function for cloud storage. IEEE Trans. Serv. Comput. **PP**(99) (2016). doi:10.1109/TSC.2016.2542813
15. Liu, Z., Cao, Z., Wong, D.S.: Blackbox traceable CP-ABE: how to catch people leaking their keys by selling decryption devices on ebay. In: Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, pp. 475–486. ACM (2013)
16. Liu, Z., Cao, Z., Wong, D.S.: White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures. IEEE Trans. Inf. Foren. Secur. **8**(1), 76–88 (2013)
17. Liu, Z., Cao, Z., Wong, D.S.: Traceable CP-ABE: how to trace decryption devices found in the wild. IEEE Trans. Inf. Foren. Secur. **10**(1), 55–68 (2015)
18. Ning, J., Cao, Z., Dong, X., Wei, L., Lin, X.: Large universe ciphertext-policy attribute-based encryption with white-box traceability. In: Kutyłowski, M., Vaidya, J. (eds.) ESORICS 2014, Part II. LNCS, vol. 8713, pp. 55–72. Springer, Heidelberg (2014)
19. Ning, J., Dong, X., Cao, Z., Wei, L.: Accountable authority ciphertext-policy attribute-based encryption with white-box traceability and public auditing in the cloud. In: Computer Security–ESORICS 2015, pp. 270–289. Springer (2015)
20. Ning, J., Dong, X., Cao, Z., Wei, L., Lin, X.: White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes. IEEE Trans. Inf. Foren. Secur. **10**(6), 1274–1288 (2015)
21. Parno, B., Raykova, M., Vaikuntanathan, V.: How to Delegate and verify in public: verifiable computation from attribute-based encryption. In: Cramer, R. (ed.) TCC 2012. LNCS, vol. 7194, pp. 422–439. Springer, Heidelberg (2012)
22. Qian, H., Li, J., Zhang, Y.: Privacy-preserving decentralized ciphertext-policy attribute-based encryption with fully hidden access structure. In: Qing, S., Zhou, J., Liu, D. (eds.) ICICS 2013. LNCS, vol. 8233, pp. 363–372. Springer, Heidelberg (2013)
23. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005)

24. Seo, J.H., Cheon, J.H.: Fully secure anonymous hierarchical identity-based encryption with constant size ciphertexts. IACR Cryptology ePrint Archive, 2011:21 (2011)
25. Seo, J.H., Kobayashi, T., Ohkubo, M., Suzuki, K.: Anonymous hierarchical identity-based encryption with constant size ciphertexts. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 215–234. Springer, Heidelberg (2009)
26. Waters, B.: Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 53–70. Springer, Heidelberg (2011)