6-2011

Fully Secure Cipertext-Policy Hiding CP-ABE

Junzuo LAI
Singapore Management University, jzlai@smu.edu.sg

Robert H. DENG
Singapore Management University, robertdeng@smu.edu.sg

Yingjiu LI
Singapore Management University, yjli@smu.edu.sg

DOI: https://doi.org/10.1007/978-3-642-21031-0_3

Information Security Practice and Experience: 7th International Conference, ISPEC 2011, Guangzhou, China, May 30 - June 1: Proceedings. pp. 24-39.
http://dx.doi.org/10.1007/978-3-642-21031-0_3

Fully Secure Cipertext-Policy Hiding CP-ABE

Junzuo Lai, Robert H. Deng, and Yingjiu Li

School of Information Systems,
Singapore Management University, Singapore 178902
{junzuolai,robertdeng,yjli}@smu.edu.sg

Abstract. In ciphertext-policy attributed-based encryption (CP-ABE), each ciphertext is labeled by the encryptor with an access structure (also called ciphertext policy) and each private key is associated with a set of attributes. A user should be able to decrypt a ciphertext if and only if his private key attributes satisfy the access structure.

The traditional security property of CP-ABE is plaintext privacy, which ciphertexts reveal no information about the underlying plaintext. At ACNS'08, Nishide, Yoneyama and Ohta introduced the notion of ciphertext-policy hiding CP-ABE. In addition to protecting the privacy of plaintexts, ciphertext-policy hiding CP-ABE also protects the description of the access structures associated with ciphertexts. They observed that ciphertext-policy hiding CP-ABE can be constructed from attribute-hiding inner-product predicate encryption (PE), and presented two constructions of ciphertext-policy hiding CP-ABE supporting restricted access structures, which can be expressed as AND gates on multi-valued attributes with wildcards. However, their schemes were only proven *selectively* secure.

In this paper, we first describe the construction of ciphertext-policy hiding CP-ABE from attribute-hiding inner-product PE *formally*. Then, we propose a concrete construction of ciphertext-policy hiding CP-ABE supporting the same access structure as that of Nishide, Yoneyama and Ohta, but our scheme is proven *fully* secure.

Keywords: Ciphertext Policy Attribute-Based Encryption, Predicate Encryption, Dual System Encryption.

1 Introduction

In many distributed file systems, it requires complex access-control mechanisms, where access decisions depend upon attributes of the protected data and access control policies assigned to users, or users can establish specific access control policies on who can decrypt the protected data. Sahai and Waters [27] addressed this issue by introducing the concept of attribute-based encryption (ABE). There are two kinds of ABE schemes, key-policy and ciphertext-policy ABE schemes.

In a key-policy ABE scheme (KP-ABE) [15], every ciphertext is associated with a set of attributes, and every user's secret key is associated with an access structure on attributes. Decryption is enabled if and only if the ciphertext attribute set satisfies the access structure associated with the user's secret key. In

a ciphertext-policy ABE (CP-ABE) scheme [4], the situation is reversed. That is, attributes are associated with user's secret keys and access structures (also called ciphertext policies) with ciphertexts.

Prior work on CP-ABE [4,11,31] has focused on the security property that ciphertexts reveal no information about the underlying plaintext, called *plaintext privacy*. Nishide et al. [23] introduced the notion of ciphertext-policy hiding CP-ABE, i.e., CP-ABE that has both *plaintext privacy* and *ciphertext-policy privacy*. The latter refers to privacy protection of access structures associated with ciphertexts. Nishide et al. [23] also presented two constructions of ciphertext-policy hiding CP-ABE supporting restricted access structures, which can be expressed as AND gates on multi-valued attributes with wildcards. However, their schemes were only proven in a *weak* model, which can be considered to be analogous to the selective-ID model [9,5] used in identity-based encryption (IBE) schemes. Ciphertext-policy hiding CP-ABE has a wide range of applications. For example, in some military circumstances, the access control policy itself could be sensitive information.

1.1 Our Contributions

As mentioned in [23], CP-ABE can be constructed from inner-product predicate encryption (PE) [17]. In this paper, we formally describe the construction of ciphertext-policy hiding CP-ABE from attribute-hiding inner-product PE in detail. This CP-ABE supports a wide range of access structures on attributes, including arbitrary conjunctive normal form (CNF) and disjunctive normal form (DNF).

We also present a concrete construction of ciphertext-policy hiding CP-ABE supporting the same access structure as that of [23]. The scheme works in the composite-order setting [7], but we can use the method proposed by Freeman [12] to transform our scheme into one in the prime-order setting. Compared with [23], our scheme applies the dual system encryption methodology [30] to obtain *full* security. The security proof of the scheme does not rely on random oracles [3], and the scheme is more efficient than the instantiated construction from attribute-hiding inner-product PE.

1.2 Related Work

The notion of ABE was first introduced by Sahai and Waters as an application of their fuzzy identity-based encryption (IBE) scheme [27], where both ciphertexts and secret keys are associated with sets of attributes. Decryption is enabled if and only if the ciphertext and secret key attribute sets overlap by at least a fixed threshold value d.

Goyal et al. [15] formulated two complimentary forms of ABE: KP-ABE and CP-ABE. They also presented the first KP-ABE supporting monotonic access structures. To enable more flexible access control policy, Ostrovsky et al. [26] presented the first KP-ABE system that supports the expression of non-monotone

formulas in key policies. Goyal et al. [14] gave a general way to transform KP-ABE into CP-ABE. Chase [10] considered the problem of ABE with multiple authorities.

The notion of predicate encryption (PE) [17] is related to key-policy ABE. In a PE scheme, secret keys correspond to predicates and ciphertexts are associated with a set of attributes; the secret key SK_f corresponding to a predicate f can be used to decrypt a ciphertext associated with an attribute set I if and only if $f(I) = 1$. Katz, Sahai, and Waters [17] also introduced the idea of *attribute-hiding*, a security notion for PE that is stronger than the basic security requirement of *payload-hiding*. Roughly speaking, *attribute-hiding* requires that a ciphertext conceal the associated attributes as well as the plaintext, while *payload-hiding* only requires that a ciphertext conceal the plaintext. The special case of inner product predicates is obtained by having each attribute correspond to a vector $\boldsymbol{x}$ and each predicate $f_{\boldsymbol{v}}$ correspond to a vector $\boldsymbol{v}$, where $f_{\boldsymbol{v}}(\boldsymbol{x}) = 1$ iff $\boldsymbol{x} \cdot \boldsymbol{v} = 0$. ($\boldsymbol{x} \cdot \boldsymbol{v}$ denotes the standard inner-product.) Note that they represent a wide class of predicates including equality tests, disjunctions or conjunctions of equality tests, and more generally, arbitrary CNF or DNF formulas.

Katz et al. [17] proposed the first inner-product PE. Shi and Waters [29] presented a delegation mechanism for a class of PE, which the admissible predicates of the system are more limited than inner-product predicates. Okamota and Takashima [24] presented a (hierarchical) delegation mechanism for a inner-product PE scheme. Shen et al. [28] introduced a new security notion of PE called predicate privacy and proposed a symmetric-key inner-product PE, which achieves both plaintext privacy and predicate privacy. These schemes were proven only selectively secure. Lweko et al. [18] proposed the first fully secure inner-product PE. Okamota and Takashima [25] presented a fully secure PE for a wide class of admissible predicates, that are specified by non-monotone access structures combined with inner-product predicates.

Bethencourt et al. [4] proposed the first CP-ABE construction, which is only proven secure under the generic group model. Cheung and Newport [11] presented a new CP-ABE construction that is proven to be secure under the standard model. The construction supports the types of access structures that are represented by AND of different attributes. The fully secure CP-ABE systems for expressive access structures were proposed in [31,18].

Nishide et al. [23] introduced the notion of ciphertext-policy hiding CP-ABE and proposed two concrete constructions. The admissible access structures in their schemes can be expressed as AND gates on multi-valued attributes with wildcards. Subsequently, some other ciphertext-policy hiding CP-ABE constructions were proposed in [21,2]. However, all these schemes were only proven *selectively* secure.

The dual system encryption methodology was introduced by Waters in [30]. It has been leveraged to obtain constructions of fully secure (H)IBE from simple assumptions [30], fully secure (H)IBE with short ciphertexts [20], fully secure (H)IBE and ABE with leakage resilience [19], fully secure ABE and inner-product PE [18,25].

1.3 Organization

The rest of the paper is organized as follows. In Section 2, we review some standard notations and cryptographic definitions. In Section 3, we show how to construct ciphertext-policy hiding CP-ABE supporting expressive access structures from attribute-hiding inner-product PE. In Section 4, we describe a more efficient ciphertext-policy hiding CP-ABE scheme but only supporting restricted access structures. Finally, we state our conclusion in Section 5.

2 Preliminaries

If S is a set, then $s \xleftarrow{\$} S$ denotes the operation of picking an element s uniformly at random from S. Let $\mathbb{N}$ denote the set of natural numbers. If $\lambda \in \mathbb{N}$ then 1^λ denotes the string of λ ones. Let $z \leftarrow \mathsf{A}(x, y, \ldots)$ denote the operation of running an algorithm A with inputs $(x, y, \ldots)$ and output z. A function $f(\lambda)$ is *negligible* if for every $c > 0$ there exists a λ_c such that $f(\lambda) < 1/\lambda^c$ for all $\lambda > \lambda_c$.

2.1 Composite Order Bilinear Groups

Composite order bilinear groups were first introduced in [7]. We use bilinear groups whose order is the product of three distinct primes.

Let $\mathcal{G}$ be an algorithm that takes as input a security parameter 1^λ and outputs a tuple $(p, q, r, \mathbb{G}, \mathbb{G}_T, \hat{e})$, where p, q, r are distinct primes, $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups of order $N = pqr$, and $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a map such that

1. (Bilinear) $\forall g, h \in \mathbb{G}, a, b \in \mathbb{Z}_N, \hat{e}(g^a, h^b) = \hat{e}(g, h)^{ab}$;
2. (Non-degenerate) $\exists g \in \mathbb{G}$ such that $\hat{e}(g, g)$ has order N in $\mathbb{G}_T$.

We further require that multiplication in $\mathbb{G}$ and $\mathbb{G}_T$, as well as the bilinear map $\hat{e}$, are computable in time polynomial in λ. We use $\mathbb{G}_p, \mathbb{G}_q, \mathbb{G}_r$ to denote the subgroups of $\mathbb{G}$ having order p, q, and r, respectively. Observe that $\mathbb{G} = \mathbb{G}_p \times \mathbb{G}_q \times \mathbb{G}_r$. Note also that if $h_p \in \mathbb{G}_p$ and $h_q \in \mathbb{G}_q$ then $\hat{e}(h_p, h_q) = 1$. A similar rule holds whenever $\hat{e}$ is applied to elements in distinct subgroups.

We now state the complexity assumptions we use. The first assumption is just the subgroup decision problem in the case where the group order is a product of three primes. We justify these assumptions in Appendix A by proving that they hold in the generic group model assuming finding a non-trivial factor of the group order N is hard. Note that our assumptions are non-interactive (in contrast to, e.g., the LRSW assumption [8]) and of fixed size (in contrast to, e.g., the q-SDH assumption [6]).

Assumption 1. *Let $\mathcal{G}$ be as above. We define the following distribution:*

$$(p, q, r, \mathbb{G}, \mathbb{G}_T, \hat{e}) \leftarrow \mathcal{G}(1^\lambda),\ N = pqr,\ g_p \xleftarrow{\$} \mathbb{G}_p,\ g_r \xleftarrow{\$} \mathbb{G}_r,$$

$$D = (\mathbb{G}, \mathbb{G}_T, N, \hat{e}, g_p, g_r),$$

$$T_1 \xleftarrow{\$} \mathbb{G}_p \times \mathbb{G}_q,\ T_2 \xleftarrow{\$} \mathbb{G}_p.$$

The advantage of an algorithm $\mathcal{A}$ in breaking Assumption 1 is defined as

$$Adv^1_{\mathcal{A}} = |\Pr[\mathcal{A}(D, T_1) = 1] - \Pr[\mathcal{A}(D, T_2) = 1]|.$$

Definition 1. *we say $\mathcal{G}$ satisfies Assumption 1 if for any polynomial time algorithm $\mathcal{A}$, $Adv^1_{\mathcal{A}}$ is negligible.*

Assumption 2. *Let $\mathcal{G}$ be as above. We define the following distribution:*

$$(p, q, r, \mathbb{G}, \mathbb{G}_T, \hat{e}) \leftarrow \mathcal{G}(1^\lambda),\ N = pqr,$$

$$g_p, X_1 \xleftarrow{\$} \mathbb{G}_p,\ X_2 \xleftarrow{\$} \mathbb{G}_q,\ g_r \xleftarrow{\$} \mathbb{G}_r,$$
$$D = (\mathbb{G}, \mathbb{G}_T, N, \hat{e}, g_p, X_1X_2, g_r),$$
$$T_1 \xleftarrow{\$} \mathbb{G}_p \times \mathbb{G}_q,\ T_2 \xleftarrow{\$} \mathbb{G}_p.$$

The advantage of an algorithm $\mathcal{A}$ in breaking Assumption 2 is defined as

$$Adv^2_{\mathcal{A}} = |\Pr[\mathcal{A}(D, T_1) = 1] - \Pr[\mathcal{A}(D, T_2) = 1]|.$$

Definition 2. *we say $\mathcal{G}$ satisfies Assumption 2 if for any polynomial time algorithm $\mathcal{A}$, $Adv^2_{\mathcal{A}}$ is negligible.*

Assumption 3. *Let $\mathcal{G}$ be as above. We define the following distribution:*

$$(p, q, r, \mathbb{G}, \mathbb{G}_T, \hat{e}) \leftarrow \mathcal{G}(1^\lambda),\ N = pqr,$$

$$\omega, s \in \mathbb{Z}_N,\ g_p, Z_1 \xleftarrow{\$} \mathbb{G}_p,\ X_2, Y_2, Z_2 \xleftarrow{\$} \mathbb{G}_q,\ g_r \xleftarrow{\$} \mathbb{G}_r,$$
$$D = (\mathbb{G}, \mathbb{G}_T, N, \hat{e}, g_p, g_p^\omega X_2, g_p^s Y_2, Z_1Z_2, g_r),$$
$$T_1 = \hat{e}(g_p, g_p)^{\omega s},\ T_2 \xleftarrow{\$} \mathbb{G}_T.$$

The advantage of an algorithm $\mathcal{A}$ in breaking Assumption 3 is defined as

$$Adv^3_{\mathcal{A}} = |\Pr[\mathcal{A}(D, T_1) = 1] - \Pr[\mathcal{A}(D, T_2) = 1]|.$$

Definition 3. *we say $\mathcal{G}$ satisfies Assumption 3 if for any polynomial time algorithm $\mathcal{A}$, $Adv^3_{\mathcal{A}}$ is negligible.*

Assumption 4. *Let $\mathcal{G}$ be as above. We define the following distribution:*

$$(p, q, r, \mathbb{G}, \mathbb{G}_T, \hat{e}) \leftarrow \mathcal{G}(1^\lambda),\ N = pqr,$$

$$a \in \mathbb{Z}_N,\ g_p \xleftarrow{\$} \mathbb{G}_p,\ g_q, Q_1, Q_2, Q \xleftarrow{\$} \mathbb{G}_q,\ g_r, R_0, R_1, R \xleftarrow{\$} \mathbb{G}_r,$$
$$D = (\mathbb{G}, \mathbb{G}_T, N, \hat{e}, g_pR_0, g_p^aR_1, g_pQ_1, g_p^{1/a}Q_2, g_q, g_r),$$
$$T_1 = g_p^aQR,\ T_2 \xleftarrow{\$} \mathbb{G}_T.$$

The advantage of an algorithm $\mathcal{A}$ in breaking Assumption 4 is defined as

$$Adv^4_{\mathcal{A}} = |\Pr[\mathcal{A}(D, T_1) = 1] - \Pr[\mathcal{A}(D, T_2) = 1]|.$$

Definition 4. *we say $\mathcal{G}$ satisfies Assumption 4 if for any polynomial time algorithm $\mathcal{A}$, $Adv^4_{\mathcal{A}}$ is negligible.*

2.2 Ciphertext-Policy Attribute-Based Encryption

A ciphertext-policy attribute-based encryption (CP-ABE) scheme consists of the following four algorithms:

$\mathsf{Setup}(1^\lambda)$. Takes as input a security parameter λ. It outputs a public key PK and a master secret key MSK.

$\mathsf{KeyGen}(\mathsf{PK}, \mathsf{MSK}, S)$. Takes as input the public key PK, the master secret key MSK and a set of attributes S. It outputs a secret key SK_S.

$\mathsf{Encrypt}(\mathsf{PK}, m, \mathbb{A})$. Takes as input the public key PK, a message m and an access structure $\mathbb{A}$. It outputs a ciphertext c.

$\mathsf{Decrypt}(\mathsf{PK}, \mathsf{SK}_S, c)$. Takes as input the public key PK, a secret key SK_S and a ciphertext c. It outputs a message m.

Let $(\mathsf{PK}, \mathsf{MSK}) \leftarrow \mathsf{Setup}(1^\lambda), \mathsf{SK}_S \leftarrow \mathsf{KeyGen}(\mathsf{PK}, \mathsf{MSK}, S), c \leftarrow \mathsf{Encrypt}(\mathsf{PK}, m, \mathbb{A})$. For correctness, we require the following to hold:

1. If the set S of attributes satisfies the access structure $\mathbb{A}$, then $m \leftarrow \mathsf{Decrypt}(\mathsf{PK}, \mathsf{SK}_S, c)$;
2. Otherwise, with overwhelming probability, $\mathsf{Decrypt}(\mathsf{PK}, \mathsf{SK}_S, c)$ outputs a random message.

2.3 Security Model for CP-ABE

The security model for ciphertext-policy hiding CP-ABE in previous constructions [23,21,2] is a weak model, since the adversary must commit to the challenge ciphertext policies before the setup phase. The weak model can be considered to be analogous to the selective-ID model [9,5] used in IBE schemes.

We now give the full security model for ciphertext-policy hiding CP-ABE, described as a security game between a challenger and an adversary $\mathcal{A}$. The game proceeds as follows:

Setup. The challenger runs $\mathsf{Setup}(1^\lambda)$ to obtain a public key PK and a master secret key MSK. It gives the public key PK to the adversary $\mathcal{A}$ and keeps MSK to itself.

Query phase 1. The adversary $\mathcal{A}$ adaptively queries the challenger for secret keys corresponding to sets of attributes $S_1, \ldots, S_q$. In response, the challenger runs $\mathsf{SK}_{S_i} \leftarrow \mathsf{KeyGen}(\mathsf{PK}, \mathsf{MSK}, S_i)$ and gives the secret key SK_{S_i} to $\mathcal{A}$, for $1 \leq i \leq q$.

Challenge. The adversary $\mathcal{A}$ submits two (equal length) messages m_0, m_1 and two access structures $\mathbb{A}_0, \mathbb{A}_1$, subject to the restriction that, $\mathbb{A}_0$ and $\mathbb{A}_1$ cannot be satisfied by any of the queried attribute sets. The challenger selects a random bit $\beta \in \{0, 1\}$, sets $c^* = \mathsf{Encrypt}(\mathsf{PK}, m_\beta, \mathbb{A}_\beta)$ and sends c^* to the adversary as its challenge ciphertext.

Query phase 2. The adversary continues to adaptively query the challenger for secret keys corresponding to sets of attributes with the added restriction that none of these satisfies $\mathbb{A}_0$ and $\mathbb{A}_1$.

Guess. The adversary $\mathcal{A}$ outputs its guess $\beta' \in \{0,1\}$ for β and wins the game if $\beta = \beta'$.

The advantage of the adversary in this game is defined as $|\mathsf{Pr}[\beta = \beta'] - \frac{1}{2}|$ where the probability is taken over the random bits used by the challenger and the adversary.

Definition 5. *A ciphertext-policy attribute-based encryption scheme is ciphertext-policy hiding (or fully secure) if all polynomial time adversaries have at most a negligible advantage in this security game.*

2.4 Inner-Product PE

A inner-product PE consists of the following four algorithms [17]:

$\mathsf{Setup}(1^\lambda)$ Takes as input a security parameter λ. It outputs a public key PK and a master secret key MSK.

$\mathsf{KeyGen}(\mathsf{PK}, \mathsf{MSK}, \boldsymbol{v})$ Takes as input the public key PK, the master secret key MSK and a vector $\boldsymbol{v}$. It outputs a secret key $\mathsf{SK}_{\boldsymbol{v}}$.

$\mathsf{Encrypt}(\mathsf{PK}, m, \boldsymbol{x})$ Takes as input the public key PK, a message m and a vector $\boldsymbol{x}$. It outputs a ciphertext c.

$\mathsf{Decrypt}(\mathsf{PK}, \mathsf{SK}_{\boldsymbol{v}}, c)$ Takes as input the public key PK, a secret key $\mathsf{SK}_{\boldsymbol{v}}$ and a ciphertext c. It outputs a message m. We require that, if $\boldsymbol{x} \cdot \boldsymbol{v} = 0$ then

$$m \leftarrow \mathsf{Decrypt}(\mathsf{PK}, \mathsf{SK}_{\boldsymbol{v}}, \mathsf{Encrypt}(\mathsf{PK}, m, \boldsymbol{x})).$$

The security model for inner-product PE is defined using the following game between an adversary $\mathcal{A}$ and a challenger.

Setup. The challenger runs $\mathsf{Setup}(1^\lambda)$ to obtain a public key PK and a master secret key MSK. It gives the public key PK to the adversary $\mathcal{A}$ and keeps MSK to itself.

Query phase 1. The adversary $\mathcal{A}$ adaptively makes secret key queries for predicate vectors, $\boldsymbol{v}$. In response, the challenger gives the corresponding secret key $\mathsf{SK}_{\boldsymbol{v}} \leftarrow \mathsf{KeyGen}(\mathsf{PK}, \mathsf{MSK}, \boldsymbol{v})$ to $\mathcal{A}$.

Challenge. The adversary $\mathcal{A}$ submits two (equal length) messages m_0, m_1 and two attribute vectors $\boldsymbol{x}_0, \boldsymbol{x}_1$, subject to the restriction that, $\boldsymbol{v} \cdot \boldsymbol{x}_0 \neq 0$ and $\boldsymbol{v} \cdot \boldsymbol{x}_1 \neq 0$ for all the secret key queried predicate vectors, $\boldsymbol{v}$. The challenger selects a random bit $\beta \in \{0,1\}$, sets $c^* = \mathsf{Encrypt}(\mathsf{PK}, m_\beta, \boldsymbol{x}_\beta)$ and sends c^* to the adversary as its challenge ciphertext.

Query phase 2. The adversary continues to adaptively issue secret key queries for additional predicate vectors, $\boldsymbol{v}$, subject to the restriction that $\boldsymbol{v} \cdot \boldsymbol{x}_0 \neq 0$ and $\boldsymbol{v} \cdot \boldsymbol{x}_1 \neq 0$. $\mathcal{A}$ is given the corresponding secret key $\mathsf{SK}_{\boldsymbol{v}} \leftarrow \mathsf{KeyGen}(\mathsf{PK}, \mathsf{MSK}, \boldsymbol{v})$ to $\mathcal{A}$.

Guess. The adversary $\mathcal{A}$ outputs its guess $\beta' \in \{0,1\}$ for β and wins the game if $\beta = \beta'$.

The advantage of the adversary in this game is defined as $|\mathsf{Pr}[\beta = \beta'] - \frac{1}{2}|$ where the probability is taken over the random bits used by the challenger and the adversary.

Definition 6. *A inner-product PE scheme is attribute-hiding (or fully secure) if all polynomial time adversaries have at most a negligible advantage in this security game.*

3 CP-ABE from Inner-Product PE

In this section, we describe the generic construction of ciphertext-policy hiding CP-ABE from attribute-hiding inner-product PE formally. This CP-ABE supports a wide range of access structures on attributes, including arbitrary CNF and DNF formulas. An example of such access structures is

$$\begin{aligned} &\mathit{Department} : \text{CIA} \\ &\quad \mathsf{AND}\ (\mathit{Position} : \text{Manager}\ \mathsf{OR}\ \mathit{Seniority} : \text{Senior}). \end{aligned}$$

Suppose that Π is a fully secure (namely *attribute hiding*) inner-product PE scheme with algorithms Setup, KeyGen, $\mathsf{Encrypt}$ and $\mathsf{Decrypt}$. We now construct a fully secure CP-ABE scheme by defining the corresponding CP-ABE algorithms as specified in Subsection 2.2.

$\mathsf{Setup}(1^\lambda)$. Given a security parameter λ, this algorithm first runs

$$(\Pi.\mathsf{PK}, \Pi.\mathsf{MSK}) \leftarrow \Pi.\mathsf{Setup}(1^\lambda)$$

and then sets the system's public key PK and master secret key SK as

$$(\mathsf{PK}, \mathsf{SK}) = (\Pi.\mathsf{PK}, \Pi.\mathsf{MSK}).$$

$\mathsf{Encrypt}(\mathsf{PK}, m, \mathbb{A})$. Given an access structure $\mathbb{A}$, which is a CNF or DNF formula, this algorithm first represents the access structure $\mathbb{A}$ by a multivariate polynomial p.

Note that, if we assume that there are t categories of attributes in the CP-ABE system, and that every user has t attributes with each attribute belonging to a different category, then arbitrary CNF or DNF formulas can be represented by polynomials in t variables of degree at most d in each variable.

Let $\boldsymbol{x}$ be the $(d+1)^t$-element coefficient vector of the polynomial p. Then the algorithm runs

$$\Pi.c \leftarrow \Pi.\mathsf{Encrypt}(\mathsf{PK}, m, \boldsymbol{x})$$

and outputs $c = \Pi.c$.

$\mathsf{KeyGen}(\mathsf{PK}, \mathsf{MSK}, S)$. Given the public key PK, the master secret key MSK and a set of attributes S, this algorithm first represents the set of attributes S by a $(d+1)^t$-element vector $\boldsymbol{v}$. Then the algorithm runs

$$\Pi.\mathsf{SK}_{\boldsymbol{v}} \leftarrow \Pi.\mathsf{KeyGen}(\mathsf{PK}, \mathsf{MSK}, \boldsymbol{v})$$

and outputs a secret key $\mathsf{SK}_S = \Pi.\mathsf{SK}_{\boldsymbol{v}}$.

$\mathsf{Decrypt}(\mathsf{PK}, \mathsf{SK}_S, c)$. Given the public key PK, a secret key SK_S and a ciphertext c. The decryption algorithm runs

$$\Pi.m \leftarrow \Pi.\mathsf{Decrypt}(\mathsf{PK}, \mathsf{SK}_S, c)$$

and outputs $m = \Pi.m$.

It is easy to observe that, if the inner-product PE scheme Π is attribute-hiding, then the proposed CP-ABE scheme supporting arbitrary CNF or DNF formulas is ciphertext-policy hiding.

Now, we give an example to show how arbitrary CNF or DNF formulas and sets of attributes can be represented by a $(d+1)^t$-element vector. Suppose that, in the CP-ABE system, there are $t = 3$ categories of attributes: *Department*, *Position* and *Seniority*, and $d = 1$. Then, the access structure

$$\begin{aligned}\mathbb{A} = {} & \mathit{Department} : \text{CIA} \\ & \mathsf{AND}\ (\mathit{Position} : \text{Manager}\ \mathsf{OR}\ \mathit{Seniority} : \text{Senior})\end{aligned}$$

can be represented by the polynomial

$$\begin{aligned}& p(x_1, x_2, x_3) \\ &= r(x_1 - I_1) + (x_2 - I_2) \cdot (x_3 - I_3) \\ &= 0 \cdot x_1x_2x_3 + 0 \cdot x_1x_2 + 0 \cdot x_1x_3 + 1 \cdot x_2x_3 + r \cdot x_1 \\ &\quad + (-I_3) \cdot x_2 + (-I_2) \cdot x_3 + (I_2I_3 - rI_1),\end{aligned}$$

where r is chosen from $\mathbb{Z}_N$ at random, $I_1 = H(\mathit{Department} : \text{CIA})$, $I_2 = H(\mathit{Position} : \text{Manager})$, $I_3 = H(\mathit{Seniority} : \text{Senior})$ and H is a collision-resistant hash function from $\{0,1\}^*$ to $\mathbb{Z}_N$. Hence, the access structure associated with ciphertexts can be represented by a $(d+1)^t = 2^3 = 8$-element vector

$$\boldsymbol{x} = (0, \ldots, 0, 1, r, -I_3, -I_2, I_2I_3 - rI_1).$$

On the other hand, a user with a set of attributes $S = (\mathit{Department} : \text{CIA}, \mathit{Position} : \text{Director}, \mathit{Seniority} : \text{Senior})$ also can be represented by an 8-element vector

$$\boldsymbol{v} = (I_1'I_2'I_3', I_1'I_2', I_1'I_3', I_2'I_3', I_1', I_2', I_3', 1),$$

where $I_1' = H(\mathit{Department} : \text{CIA})$, $I_2' = H(\mathit{Position} : \text{Director})$ and $I_3' = H(\mathit{Seniority} : \text{Senior})$.

It is obvious that if the set of attributes of a user S satisfies the access structure $\mathbb{A}$, then $\boldsymbol{x} \cdot \boldsymbol{v} = 0$.

4 CP-ABE Supporting Restricted Access Structures

In this section, we propose a ciphertext-policy hiding CP-ABE scheme which supports access structures with AND operation on multi-valued attributes with wildcards. An example of such access structures is

$$\begin{aligned}& \mathit{Department} : \text{CIA}\ \mathsf{AND}\ \mathit{Position} : \text{Manager} \\ & \quad \mathsf{AND}\ (\mathit{Seniority} : \text{Junior}\ \mathsf{OR}\ \mathit{Seniority} : \text{Senior}).\end{aligned}$$

The ciphertext size of the scheme is $O(n \times \ell)$, where n is the number of categories of attributes in the system and ℓ is the number of possible values in each category. Note that, as showed in Section 3, we can construct fully secure CP-ABE supporting the same access structures from inner-product PE, but the ciphertext size of such a scheme is $(\ell + 1)^n$.

Without loss of generality, we assume that there are n categories of attributes and that every user has n attributes with each attribute belonging to a different category.

We will associate each attribute with a unique element in $\mathbb{Z}_N$. Let the $n \times \ell$ matrix $\mathbf{V} = (V_1, \ldots, V_i, \ldots, V_n)$ be the possible attributes in the universe, where the vector $V_i = (v_{i,1}, \ldots, v_{i,j}, \ldots, v_{i,\ell})$ and $v_{i,j} \in \mathbb{Z}_N$. We also assume that V_i be the set of all possible values of the i^{th} category attribute. In other words, if $S = (w_1, \ldots, w_i, \ldots, w_n)$ denotes the set of attributes of a user, then $w_i \in V_i$. So, to keep the presentation clear, let $S = (v_{1,j_1}, v_{2,j_2}, \ldots, v_{i,j_i}, \ldots, v_{n,j_n})$ denote the set of attributes of a user, where $j_i \in \{1, \ldots, \ell\}$.

Denote the restricted ciphertext policy as $\mathbb{A} = (W_1, \ldots, W_n)$, where $W_i \subseteq V_i$. The set of attributes $S = (v_{1,j_1}, v_{2,j_2}, \ldots, v_{i,j_i}, \ldots, v_{n,j_n})$ satisfies the ciphertext policy $\mathbb{A}$ if and only if $v_{i,j_i} \in W_i$ for $1 \leq i \leq n$.

The CP-ABE scheme consists of the following algorithms:

$\mathsf{Setup}(1^\lambda)$. The setup algorithm first runs $\mathcal{G}(1^\lambda)$ to obtain $(p, q, r, \mathbb{G}, \mathbb{G}_T, \hat{e})$ with $\mathbb{G} = \mathbb{G}_p \times \mathbb{G}_q \times \mathbb{G}_r$, where $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups of order $N = pqr$. Next it picks generators g_p, q_r of $\mathbb{G}_p, \mathbb{G}_r$, respectively, then chooses $a_{i,j} \in \mathbb{Z}_N$ and $R_{i,j} \in \mathbb{G}_r$ uniformly at random for $i = 1$ to n and $j = 1$ to ℓ. It also chooses $\omega \in \mathbb{Z}_N$ and $R_0 \in \mathbb{G}_r$ uniformly at random. The public key is

$$\mathsf{PK} = (A_0 = g_p \cdot R_0,\ \{A_{i,j} = g_p^{a_{i,j}} \cdot R_{i,j}\}_{1 \leq i \leq n, 1 \leq j \leq \ell},\ g_r,\ Y = \hat{e}(g_p, g_p)^\omega).$$

and the master secret key is

$$\mathsf{MSK} = (g_p,\ \{a_{i,j}\}_{1 \leq i \leq n, 1 \leq j \leq \ell},\ \omega).$$

$\mathsf{KeyGen}(\mathsf{PK}, \mathsf{MSK}, S)$. Let $S = (v_{1,j_1}, v_{2,j_2}, \ldots, v_{i,j_i}, \ldots, v_{n,j_n})$ with $j_i \in \{1, \ldots, \ell\}$, and recall

$$\mathsf{MSK} = (g_p,\ \{a_{i,j}\}_{1 \leq i \leq n, 1 \leq j \leq \ell},\ \omega).$$

This algorithm chooses $t_i \in \mathbb{Z}_N$ uniformly at random for $i = 1$ to n, and sets $t = \sum_{i=1}^{n} t_i$. It then computes $D_0 = g_p^{\omega - t}$. For $1 \leq i \leq n$, it also computes $D_i = g_p^{t_i / a_{i,j_i}}$. Finally, it outputs the secret key

$$\mathsf{SK}_S = (D_0,\ \{D_i\}_{1 \leq i \leq n}).$$

$\mathsf{Encrypt}(\mathsf{PK}, m, \mathbb{A})$. Let $\mathbb{A} = (W_1, \ldots, W_n)$ with $W_i \subseteq V_i$. This algorithm chooses random $s \in \mathbb{Z}_N$ and $R_0' \in \mathbb{G}_r$. It also chooses random $s_{i,j} \in \mathbb{Z}_N$

and $R'_{i,j} \in \mathbb{G}_r$ for $1 \le i \le n$ and $1 \le j \le \ell$. It then computes $\tilde{C} = m \cdot Y^s$ and $C_0 = A_0^s \cdot R'_0$, where $m \in \mathbb{G}_T$. For $1 \le i \le n$ and $1 \le j \le \ell$, it also computes

$$C_{i,j} = \begin{cases} A_{i,j}^s \cdot R'_{i,j}, & \text{if } v_{i,j} \in W_i; \\ A_{i,j}^{s_{i,j}} \cdot R'_{i,j}, & \text{otherwise.} \end{cases}$$

Finally, it outputs the ciphertext

$$c = (\tilde{C},\ C_0,\ \{C_{i,j}\}_{1 \le i \le n, 1 \le j \le \ell}).$$

Note that, a random element $R \in \mathbb{G}_r$ can be sampled by choosing random $\delta \in \mathbb{Z}_N$ and setting $R = g_r^\delta$.

$\mathsf{Decrypt}(\mathsf{PK}, \mathsf{SK}_S, c)$. Let $c = (\tilde{C},\ C_0,\ \{C_{i,j}\}_{1 \le i \le n, 1 \le j \le \ell})$, $\mathsf{SK}_S = (D_0,\ \{D_i\}_{1 \le i \le n})$ and $S = (v_{1,j_1}, v_{2,j_2}, \ldots, v_{i,j_i}, \ldots, v_{n,j_n})$ be as above. The decryption algorithm outputs

$$\frac{\tilde{C}}{\hat{e}(C_0, D_0) \cdot \prod_{i=1}^n \hat{e}(C_{i,j_i}, D_i)}.$$

Correctness. Let SK_S and c be as above. If the set of attributes $S = (v_{1,j_1}, v_{2,j_2}, \ldots, v_{i,j_i}, \ldots, v_{n,j_n})$ satisfies the access structure $\mathbb{A} = (W_1, \ldots, W_n)$, then

$$\begin{aligned} \frac{\tilde{C}}{\hat{e}(C_0, D_0) \cdot \prod_{i=1}^n \hat{e}(C_{i,j_i}, D_i)} &= \frac{m \cdot Y^s}{\hat{e}(A_0^s \cdot R'_0, g_p^{\omega - t}) \cdot \prod_{i=1}^n \hat{e}(A_{i,j_i}^s \cdot R'_{i,j_i}, g_p^{t_i / a_{i,j_i}})} \\ &= \frac{m \cdot \hat{e}(g_p, g_p)^{\omega s}}{\hat{e}(g_p^s, g_p^{\omega - t}) \cdot \prod_{i=1}^n \hat{e}((g_p^{a_{i,j_i}})^s, g_p^{t_i / a_{i,j_i}})} \\ &= \frac{m \cdot \hat{e}(g_p, g_p)^{\omega s}}{\hat{e}(g_p^s, g_p^{\omega - t}) \cdot \prod_{i=1}^n \hat{e}(g_p^s, g_p^{t_i})} \\ &= \frac{m \cdot \hat{e}(g_p, g_p)^{\omega s}}{\hat{e}(g_p^s, g_p^{\omega})} = m. \end{aligned}$$

Recently, Freeman [12] proposed a method for transforming schemes secure in the composite-order setting into ones secure (under different but analogous assumptions) in the prime-order setting. We can use the method to transform our scheme into one in the prime-order setting. Now, we turn to security.

Theorem 1. *Suppose that $\mathcal{G}$ satisfies Assumptions 1, 2, 3, and 4. Then the proposed CP-ABE is ciphertext-policy hiding.*

Proof. To obtain full security, we apply the dual system encryption concept recently introduced by Waters [30]. We first define two additional structures: *semi-functional* ciphertexts and *semi-functional* keys. These will not be used in the real system, but will be used in our proof. A normal key can decrypt normal or semi-functional ciphertexts, and a normal ciphertext can be decrypted by normal or semi-functional keys. However, when a semi-functional key is used to decrypt a semi-functional ciphertext, decryption will fail.

Semi-functional Ciphertext. Let g_q denote a generator of the subgroup $\mathbb{G}_q$. A semi-functional ciphertext is created as follows:

1. First, a normal ciphertext
$$c' = (\tilde{C}',\ C_0',\ \{C_{i,j}'\}_{1\le i\le n, 1\le j\le \ell}),$$
is generated by the encryption algorithm $\mathsf{Encrypt}$.
2. Random exponents $x_0, x_{i,j} \in \mathbb{Z}_N$ are chosen for $1 \le i \le n$ and $1 \le j \le \ell$.
3. Then, the semi-functional ciphertext c is set to be
$$c = (\tilde{C} = \tilde{C}',\ C_0 = C_0' \cdot g_q^{x_0},\ \{C_{i,j} = C_{i,j}' \cdot g_q^{x_{i,j}}\}_{1\le i\le n, 1\le j\le \ell}).$$

Semi-functional Key. Let g_q denote a generator of the subgroup $\mathbb{G}_q$. A semi-functional key is created as follows:

1. First, a normal key $\mathsf{SK}_S' = (D_0',\ \{D_i'\}_{1\le i\le n})$ is generated by the key generation algorithm KeyGen.
2. Random exponents $y_0, y_i \in \mathbb{Z}_N$ are chosen for $1 \le i \le n$.
3. Then, the semi-functional key SK_S is set to be
$$\mathsf{SK}_S = (D_0 = D_0' \cdot g_q^{y_0},\ \{D_i = D_i' \cdot g_q^{y_i}\}_{1\le i\le n}).$$

We will prove security by a hybrid argument using a sequence of games. The first game, Game 0, will be the real security game. In Game 1 (or Game 2-0), all the keys are normal and the ciphertext is semi-functional. In Game 2-k, the ciphertext given to the adversary is semi-functional and the first k keys are semi-functional. The rest of the keys are normal. In Game 3, all the keys are semi-functional, and the ciphertext is a semi-functional encryption of a random message, not one of the messages provided by the adversary.

Then our proof relies on four lemmas, whose formal descriptions and proofs will be given in the full version of the paper. Lemma 1 states that Game 0 and Game 1 (i.e., Game 2-0) are indistinguishable. For $1 \le k \le \nu$, where ν denotes the number of secret key queries the adversary makes, Lemma 2 states Game 2-(k-1) and Game 2-k are indistinguishable. Lemma 3 states Game 2-ν and Game 3 are indistinguishable; and finally Lemma 4 states that the advantage of the adversary in Game 3 is negligible. Therefore, we conclude that the advantage of the adversary in Game 0 (i.e., the real security game) is negligible. This completes the proof of Theorem 1.

5 Conclusions

In this paper, we described the construction of ciphertext-policy hiding CP-ABE from inner-product PE formally. We also proposed a more efficient ciphertext-policy hiding CP-ABE construction but only supporting restricted access structures. Compared with previous ciphertext-policy hiding CP-ABE constructions, our schemes were proven fully secure. Note that we used some non-standard complexity assumptions. A further direction is to find more efficient and expressive ciphertext-policy hiding CP-ABE constructions from simple assumptions in the full security model.

Acknowledgement

We are grateful to the anonymous reviewers for their helpful comments. This research is supported by A*STAR SERC Grant No. 102 101 0027 in Singapore.

References

1. Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M.M., Ingólfsdóttir, A., Walukiewicz, I. (eds.): ICALP 2008, Part II. LNCS, vol. 5126. Springer, Heidelberg (2008)
2. Balu, A., Kuppusamy, K.: Ciphertext policy attribute based encryption with anonymous access policy. CoRR abs/1011.0527 (2010)
3. Bellare, M., Rogaway, P.: Random oracles are practical: A paradigm for designing efficient protocols. In: ACM Conference on Computer and Communications Security, pp. 62–73 (1993)
4. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy, pp. 321–334. IEEE Computer Society, Los Alamitos (2007)
5. Boneh, D., Boyen, X.: Efficient selective-id secure identity-based encryption without random oracles. In: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004)
6. Boneh, D., Boyen, X.: Short signatures without random oracles and the sdh assumption in bilinear groups. J. Cryptology 21(2), 149–177 (2008)
7. Boneh, D., Goh, E.J., Nissim, K.: Evaluating 2-dnf formulas on ciphertexts. In: Kilian, J. (ed.) TCC 2005. LNCS, vol. 3378, pp. 325–341. Springer, Heidelberg (2005)
8. Camenisch, J., Lysyanskaya, A.: Signature schemes and anonymous credentials from bilinear maps. In: Franklin, M.K. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 56–72. Springer, Heidelberg (2004)
9. Canetti, R., Halevi, S., Katz, J.: A forward-secure public-key encryption scheme. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 255–271. Springer, Heidelberg (2003)
10. Chase, M.: Multi-authority attribute based encryption. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 515–534. Springer, Heidelberg (2007)
11. Cheung, L., Newport, C.C.: Provably secure ciphertext policy abe. In: Ning, et al [22], pp. 456–465
12. Freeman, D.M.: Converting pairing-based cryptosystems from composite-order groups to prime-order groups. In: Gilbert [13], pp. 44–61
13. Gilbert, H. (ed.): EUROCRYPT 2010. LNCS, vol. 6110. Springer, Heidelberg (2010)
14. Goyal, V., Jain, A., Pandey, O., Sahai, A.: Bounded ciphertext policy attribute based encryption. In: Aceto, et al [1], pp. 579–591
15. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Juels, A., Wright, R.N., di Vimercati, S.D.C. (eds.) ACM Conference on Computer and Communications Security, pp. 89–98. ACM, New York (2006)
16. Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. Cryptology ePrint Archive, Report 2007/404 (2007), `http://eprint.iacr.org/`

17. Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 146–162. Springer, Heidelberg (2008)
18. Lewko, A.B., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In: Gilbert [13], pp. 62–91
19. Lewko, A.B., Rouselakis, Y., Waters, B.: Achieving leakage resilience through dual system encryption. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 70–88. Springer, Heidelberg (2011)
20. Lewko, A.B., 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)
21. Li, J., Ren, K., Zhu, B., Wan, Z.: Privacy-aware attribute-based encryption with user accountability. In: Samarati, P., Yung, M., Martinelli, F., Ardagna, C.A. (eds.) ISC 2009. LNCS, vol. 5735, pp. 347–362. Springer, Heidelberg (2009)
22. Ning, P., di Vimercati, S.D.C., Syverson, P.F. (eds.): Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA, October 28-31. ACM, New York (2007)
23. Nishide, T., Yoneyama, K., Ohta, K.: Attribute-based encryption with partially hidden encryptor-specified access structures. In: Bellovin, S.M., Gennaro, R., Keromytis, A.D., Yung, M. (eds.) ACNS 2008. LNCS, vol. 5037, pp. 111–129. Springer, Heidelberg (2008)
24. Okamoto, T., Takashima, K.: Hierarchical predicate encryption for inner-products. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 214–231. Springer, Heidelberg (2009)
25. Okamoto, T., Takashima, K.: Fully secure functional encryption with general relations from the decisional linear assumption. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 191–208. Springer, Heidelberg (2010)
26. Ostrovsky, R., Sahai, A., Waters, B.: Attribute-based encryption with non-monotonic access structures. In: Ning, et al [22], pp. 195–203
27. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005)
28. Shen, E., Shi, E., Waters, B.: Predicate privacy in encryption systems. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 457–473. Springer, Heidelberg (2009)
29. Shi, E., Waters, B.: Delegating capabilities in predicate encryption systems. In: Aceto, et al [1], pp. 560–578
30. Waters, B.: Dual system encryption: Realizing fully secure ibe and hibe under simple assumptions. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619–636. Springer, Heidelberg (2009)
31. 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)

Appendix A

We now prove that our complexity assumptions hold in the generic group model, as long as it is hard to find a nontrivial factor of the group order, N. We prove this by applying the theorems of Katz et al. [16]. Let g_1, g_2, g_3 be random generators of $\mathbb{G}_p, \mathbb{G}_q, \mathbb{G}_r$, respectively. Then every element of $\mathbb{G}$ can be expressed as $g_1^{a_1} g_2^{a_2} g_3^{a_3}$,

and every element of $\mathbb{G}_T$ can be expressed as $\hat{e}(g_1, g_1)^{a_1}\hat{e}(g_2, g_2)^{a_2}\hat{e}(g_3, g_3)^{a_3}$ for some values of a_1, a_2, a_3. We denote an element of $\mathbb{G}, \mathbb{G}_T$ by $(a_1, a_2, a_3), [a_1, a_2, a_3]$, respectively. We adopt the notation of [16] to express our assumptions. We use capital letters to denote random variables, and reuse random variables to denote relationships between elements.

Assumption 1. We can express this assumption as:

$$A_1 = (1, 0, 0),\ A_2 = (0, 0, 1),\ T_1 = (X_1, X_2, 0),\ T_2 = (X_1, 0, 0).$$

Let $S = \{i | \hat{e}(T_1, A_i) \neq \hat{e}(T_2, A_i)\}$. We note that $S = \emptyset$ in this case. It is clear that T_1 and T_2 are both independent of $\{A_1, A_2\}$ because X_1 does not appear in A_1 or A_2. According to Theorem A.2 of [16], thus, Assumption 1 is generically secure, assuming it is hard to find a nontrivial factor of N.

Assumption 2. We can express this assumption as:

$$A_1 = (1, 0, 0),\ A_2 = (X_1, 1, 0),\ A_3 = (0, 0, 1),$$

$$T_1 = (Y_1, Y_2, 0),\ T_2 = (Y_1, 0, 0).$$

Let $S = \{i | \hat{e}(T_1, A_i) \neq \hat{e}(T_2, A_i)\}$. We note that $S = \{2\}$ in this case. It is clear that T_1 and T_2 are both independent of $\{A_i\}$ because Y_1 does not appear in $\{A_i\}$. We see that $\hat{e}(T_1, A_2)$ is independent of $\{\hat{e}(A_i, A_j)\} \cup \{\hat{e}(T_1, A_i)\}_{i\neq 2}$ because it is impossible to obtain X_1Y_1 in the first coordinate of a combination of elements of $\{\hat{e}(A_i, A_j)\} \cup \{\hat{e}(T_1, A_i)\}_{i\neq 2}$. This also allows to conclude that $\hat{e}(T_2, A_2)$ is independent of $\{\hat{e}(A_i, A_j)\} \cup \{\hat{e}(T_2, A_i)\}_{i\neq 2}$. According to Theorem A.2 of [16], thus, Assumption 2 is generically secure, assuming it is hard to find a nontrivial factor of N.

Assumption 3. We can express this assumption as:

$$A_1 = (1, 0, 0),\ A_2 = (X_1, 1, 0),\ A_3 = (Y_1, Y_2, 0),\ A_4 = (Z_1, Z_2, 0),\ A_5 = (0, 0, 1),$$

$$T_1 = [X_1Y_1, 0, 0],\ T_2 = [W_1, W_2, W_3].$$

T_1 is independent of $\{\hat{e}(A_i, A_j)\}$ because the only way to obtain X_1Y_1 in the first coordinate is to take $\hat{e}(A_2, A_3)$, but then we are left with a Y_2 in the second coordinate that cannot be canceled. T_2 is independent of $\{\hat{e}(A_i, A_j)\}$ because W_1, W_2, W_3 do not appear in $\{A_i\}$. According to Theorem A.1 of [16], thus, Assumption 3 is generically secure, assuming it is hard to find a nontrivial factor of N.

Assumption 4. We can express this assumption as:

$$A_1 = (1, 0, 1),\ A_2 = (X_1, 0, X_3),\ A_3 = (1, 1, 0),$$

$$A_4 = (1/X_1, X_2, 0),\ A_5 = (0, Y_2, 0),$$

$$A_6 = (0, 0, Y_3),\ T_1 = (X_1, Z_2, Z_3),\ T_2 = (Z_1, Z_2, Z_3).$$

Let $S = \{i|\hat{e}(T_1, A_i) \neq \hat{e}(T_2, A_i)\}$. We note that $S = \{1, 2, 3, 4\}$ in this case. It is clear that T_1 and T_2 are both independent of $\{A_i\}$ because Z_2 does not appear in $\{A_i\}$. We see that $\hat{e}(T_1, A_1)$ is independent of $\{\hat{e}(A_i, A_j)\} \cup \{\hat{e}(T_1, A_i)\}_{i\neq 1}$ and $\hat{e}(T_2, A_1)$ is independent of $\{\hat{e}(A_i, A_j)\} \cup \{\hat{e}(T_2, A_i)\}_{i\neq 1}$ because we cannot obtain Z_3 in the third coordinate. We note that $\hat{e}(T_1, A_2)$ is independent of $\{\hat{e}(A_i, A_j)\} \cup \{\hat{e}(T_1, A_i)\}_{i\neq 2}$ and $\hat{e}(T_2, A_2)$ is independent of $\{\hat{e}(A_i, A_j)\} \cup \{\hat{e}(T_2, A_i)\}_{i\neq 2}$ because we cannot obtain X_3Z_3 in the third coordinate. We also note that $\hat{e}(T_1, A_3)$ is independent of $\{\hat{e}(A_i, A_j)\} \cup \{\hat{e}(T_1, A_i)\}_{i\neq 3}$ and $\hat{e}(T_2, A_3)$ is independent of $\{\hat{e}(A_i, A_j)\} \cup \{\hat{e}(T_2, A_i)\}_{i\neq 3}$ because we cannot obtain Z_2 in the second coordinate. We similarly note that $\hat{e}(T_1, A_4)$ is independent of $\{\hat{e}(A_i, A_j)\} \cup \{\hat{e}(T_1, A_i)\}_{i\neq 4}$ and $\hat{e}(T_2, A_4)$ is independent of $\{\hat{e}(A_i, A_j)\} \cup \{\hat{e}(T_2, A_i)\}_{i\neq 4}$ because we cannot obtain X_2Z_2 in the second coordinate. According to Theorem A.2 of [16], thus, Assumption 4 is generically secure, assuming it is hard to find a nontrivial factor of N.