Journal of Universal Computer Science, vol. 25, no. 3 (2019), 182-202
submitted: 28/3/18, accepted: 30/12/18, appeared: 28/3/19 © *J.UCS*

Provably Secure Ciphertext-Policy Attribute-Based Encryption from Identity-Based Encryption

Yi-Fan Tseng
(Department of Computer Science
National Chengchi University, Taipei, Taiwan
yftseng1989@gmail.com)

Chun-I Fan*
(Department of Computer Science and Engineering
National Sun Yat-sen University, Kaohsiung, Taiwan
Telecom Technology Center, Taiwan
cifan@mail.cse.nsysu.edu.tw
*Corresponding author)

Chih-Wen Lin
(Department of Computer Science and Engineering
National Sun Yat-sen University, Kaohsiung, Taiwan
ywenywen220@gmail.com)

Abstract: Ciphertext-policy attribute-based encryption (CP-ABE) is an access control mechanism where a data provider encrypts a secret message and then sends the ciphertext to the receivers according to the access policy which she/he decides. If the attributes of the receivers match the access policy, then they can decrypt the ciphertext. This paper shows a relation between CP-ABE and identity-based encryption (IBE), and presents a bi-directional conversion between an access structure and identities. By the proposed conversion, the CP-ABE scheme constructed from an IBE scheme will inherit the features, such as constant-size ciphertexts and anonymity, from the IBE scheme, and vice versa. It turns out that the proposed conversion also gives the first CP-ABE achieving access structures with wildcard and constant-size ciphertexts/private keys. Finally, we prove the CCA security for confidentiality and anonymity.
Key Words: Attribute-Based Encryption, Identity-Based Encryption, Constant-Size Ciphertexts/Keys, Hidden Access Policies
Category: D.4.6, E.3

1 Introduction

In an attribute-based encryption (ABE) scheme, if the attributes of users satisfy the access policy (also called access structure) which is decided by other users, then they can decrypt the ciphertext. The first ABE scheme was proposed by Sahai and Waters [Sahai and Waters, 2005], which is an extended concept from identity-based encryption (IBE). In such a scheme, an encryptor can send the ciphertext to many users by indicating the attributes about the expected receivers, and those users who possess the attributes matching the attributes assigned by the encryptor can successfully decrypt the ciphertext.

ABE has a variety of applications [Li et al., 2019, Yu et al., 2017a, Yu et al., 2017b, Yu et al., 2018, Xue et al., 2019]. There are two types of ABE, key-policy attribute-based encryption (KP-ABE) [Attrapadung et al., 2011, Goyal et al., 2006, Ostrovsky et al., 2007] and ciphertext-policy attribute-based encryption (CP-ABE) [Bethencournt et al., 2007, Cheung and Newport, 2007, Goyal et al., 2008, Liang et al., 2009, Waters, 2011]. The difference between these two types depends on where the access policy is, on the ciphertext or the private key of a user. In a key-policy ABE scheme, the access policies are associated with users' private keys and a set of attributes are associated with the ciphertexts. If the attributes associated with the ciphertext satisfy the access policy of the private key, the users with such private keys can decrypt the ciphertext. However, in KP-ABE, the data providers must trust the key generation center (KGC) who should issue the correct private keys of users with appropriate policies. In other words, the data providers have no control to determine who can access the data except the choice of attributes for ciphertexts. On the other hand, in a ciphertext-policy ABE scheme, the access policies are associated with the ciphertexts and a set of attributes are associated with users' private keys. It means that users can decrypt the ciphertext if and only if the attributes associated with users' private key satisfy the access policy of the ciphertext. That is, the data providers can enforce access policies themselves to determine who should or should not be allowed to decrypt, and the KGC has no control over the access policies. Compared with KP-ABE, CP-ABE may be more flexible and practical for many applications, such as cloud computing. This work focuses on CP-ABE.

Nowadays, many works on CP-ABE have been proposed [Balu and Kuppusamy, 2010a, Balu and Kuppusamy, 2010b, Chen et al., 2013, Chen et al., 2011, Emura et al., 2010, Ge et al., 2012, Guo et al., 2014, Herranz et al., 2010, Lai et al., 2011, Müller and Katzenbeisser, 2011, Nishide et al., 2008, Padhya and Jinwala, 2014, Phuong et al., 2014, Phuong et al., 2016, Rao and Dutta, 2013, Tran et al., 2012, Wang and He, 2016, Xu and Lang, 2015, Xu et al., 2013, Yadav, 2015, Yu et al., 2008, Zeng and Xu, 2014, Zhang et al., 2014, Zhang et al., 2016, Zhou and Huang, 2010, Zhou et al., 2015]. There are two directions in the development of CP-ABE. One is to improve the performance, such as the length of ciphertexts/private keys and the computation cost of encryption/decryption. It brings out large communication cost in data sharing if the length of ciphertext/private key increases linearly depending on the number of the attributes. It is a good property if a CP-ABE scheme supports constant-size ciphertexts or private keys. There have been lots of works [Chen et al., 2013, Chen et al., 2011, Emura et al., 2010, Ge et al., 2012, Guo et al., 2014, Herranz et al., 2010, Phuong et al., 2014, Tran et al., 2012, Zhang et al., 2014, Zhang et al., 2016, Zhou and Huang, 2010] dealing with the problems mentioned above. The other direction is to improve receivers' anonymity. That is, hide the access policies on the ciphertexts, since the access policies may disclose the receivers' private information during transmission. ABE with hidden access policy will achieve receiver anonymity. In order to avoid the attacks from adversaries, many works have been proposed [Balu and Kuppusamy, 2010a, Balu and Kuppusamy, 2010b, Lai et al., 2011, Müller and Katzenbeisser, 2011, Nishide et al., 2008, Padhya and Jinwala, 2014, Phuong et al., 2016, Wang and He, 2016, Xu and Lang, 2015, Xu et al., 2013, Yadav, 2015, Yu et al., 2008, Zeng and Xu, 2014] in addressing the issue of hidden access policy. In addition, there are only four CP-ABEs in which the access structures achieve hidden access policy and constant-size ciphertexts or private keys simultaneously [Doshi and Jinwal, 2011, Li et al., 2012, Rao and Dutta, 2013, Zhou et al., 2015].

1.1 Contributions

We discover an interesting relation between CP-ABE and IBE. The discovery inspires us to present a new generic construction of CP-ABE and IBE. We can construct a CP-ABE scheme from an IBE scheme by the proposed method, and vice versa. The main ideal of our method is to convert an AND-gate only access structure into an identity, and vice versa. Moreover, we also design two algorithms for converting an access structure in DNF into a set of identities, and vice versa. By adopting these two algorithms above, we can construct a CP-ABE scheme from an identity-based broadcast encryption (IBBE) scheme, and vice versa. The proposed conversion method would preserve features, such as constant-size ciphertexts, anonymity, wildcards, etc. Furthermore, our conversion method gives the first CP-ABE achieving hidden access structures with wildcard and constant-size ciphertexts/private keys. It may also imply some impossibility. For example, we can prove that one can never achieve hidden access structures and constant-size ciphertexts simultaneously in a CP-ABE supporting access structures in DNF. Furthermore, we provide the proof of the uniqueness of our conversion method and prove the CCA security for confidentiality and anonymity, which demonstrates the security of the proposed conversion.

2 Preliminary

In this section, we first give the definition for two access structures and use them in our proposed method. Then we provide the definitions and security models associated with CP-ABE, IBE, and IBBE.

2.1 Access Structures

There are two types of access structures in the proposed method as follows.

Definition 1. (Generic Access Structure [Beimel, 1996]) Let $\mathcal{P} = \{P_1, P_2, ..., P_n\}$ be a set of parties. A collection $\mathbb{A} \subseteq 2^{\{P_1,P_2,...,P_n\}}$ is monotone if $\forall B, C$: if $B \in \mathbb{A}$ and $B \subseteq C$ then $C \in \mathbb{A}$. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) $\mathbb{A}$ of non-empty subsets of $\{P_1, P_2, ..., P_n\}$, i.e., $\mathbb{A} \subseteq 2^{\{P_1,P_2,...,P_n\}} \backslash \{\emptyset\}$. The sets in $\mathbb{A}$ are called the authorized sets, and the sets not in $\mathbb{A}$ are called the unauthorized sets. We can also represent the generic access structure as a disjunction of conjunctive clauses, i.e. disjunctive normal form (DNF).

In our context, the role of the parties is taken by the attributes. Thus, the access structure $\mathbb{A}$ will contain the authorized sets of attributes.

Definition AND-gate-only Access Structure *The universe of attributes is denoted by $\mathcal{U}$ and the size of the universe is $|\mathcal{U}|$. We can use an AND-gate-only access structure $\mathbb{A}$ such as (att_1 AND ... AND att_n), where $1 \leq n \leq |\mathcal{U}|$. It also can be written as a set of attributes, e.g. $\mathbb{A} = \{att_1, att_2, ..., att_n\}$. Let $S = \{X_1, ...X_n\}$, where $1 \leq n \leq |\mathcal{U}|$, be an attribute set of a user. We say that S satisfies the access structure $\mathbb{A}$ if and only if $att_i = X_i$, for all $1 \leq i \leq n$, denoted as $S \preceq \mathbb{A}$. By the definition of "monotone access" shown in Definition 1, we note that the AND-gate-only access structure is non-monotone.*

In our conversion method, we will use another access structure as well, called "and-gate with wildcard." It means that there are "don't care" attributes in an access structure, denoted by the symbol "$*$".

2.2 Definition

2.2.1 Ciphertext-Policy Attribute-Based Encryption

A CP-ABE scheme includes the following four algorithms:
- **Setup**(1^l)**:** The private key generator (PKG) takes a security parameter l as an input. Then it outputs a master secret key MK and a public key PK.
- **KeyGen**(PK, MK, U)**:** The PKG takes the master secret key MK, the attribute set of user U, and the public key PK as inputs. It outputs the private key SK_U.
- **Encrypt**$(M, PK, \mathbb{A})$**:** The encryptor takes a message $M \in \{0, 1\}^*$, the public key PK, and the access structure $\mathbb{A}$ as inputs. It outputs a ciphertext $CT_{\mathbb{A}}$.
- **Decrypt**$(CT_{\mathbb{A}}, SK_U)$**:** The decryptor takes the ciphertext $CT_{\mathbb{A}}$ and the private key SK_U as inputs. It outputs a message M.

These algorithms must satisfy the correctness condition, that is, for $SK_U \leftarrow$ **KeyGen**(PK, MK, U) and $CT_{\mathbb{A}} \leftarrow$**Encrypt**$(M, PK, \mathbb{A})$, we can decrypt the ciphertext from **Decrypt**$(CT_{\mathbb{A}}, SK_U) = M$ if $U \preceq \mathbb{A}$.

2.2.2 Identity-Based Broadcast Encryption

We slightly modify the algorithms *Encrypt* and *Decrypt* from an traditional IBBE scheme. The modified IBBE scheme includes the following four algorithms:

- **Setup**(1^l)**:** The PKG takes a security parameter l as an input. Then it outputs a master secret key MK and a public key PK.
- **KeyGen**(PK, MK, ID)**:** The PKG takes the public key PK, the master secret key MK, and the identity $ID \in \{0,1\}^l$ as inputs. It outputs the private key SK_{ID}.
- **Encrypt**(M, PK, S)**:** The encryptor takes a message $M \in \{0,1\}^*$, the public key PK, and a set of identities $S = \{ID_1, ...ID_n\}$ of receivers as inputs. It outputs a ciphertext CT_S.
- **Decrypt**(CT_S, SK_{ID})**:** The decryptor takes the ciphertext CT_S and the private key SK_{ID} as inputs. It outputs the message M.

These algorithms must satisfy the correctness condition, that is, for $SK_{ID} \leftarrow$ **KeyGen**(PK, MK, ID) and $CT_S \leftarrow$**Encrypt**(M, PK, S), then we can decrypt the ciphertext from **Decrypt**$(CT_S, SK_{ID}) = M$ if $ID \in S$.
Note that, in this definition, if we stress that the receiver set only contain one identity, then we will obtain the definition of Identity-Based Encryption (IBE).

2.3 Security Model

In this section, we provide the CCA security models for a CP-ABE scheme and a CP-ABE scheme with hidden policy (anonymous CP-ABE). Also, we provide the CCA security models for an IBBE scheme and an anonymous IBBE scheme. The models are shown below.

2.3.1 CCA Security Game for CP-ABE/Anonymous CP-ABE

A CP-ABE/anonymous CP-ABE is said to be secure against CCA if no probabilistic polynomial-time adversary has non-negligible advantage in the following game.
Setup. A challenger takes a security parameter l as an input, and returns PK to an adversary and keeps MK secret.
Phase 1. The adversary submits queries $q_1, ..., q_n$ to query for the private keys or the decryptions for the ciphertexts generated by the adversary, where q_i is either

- **Private Key Query**: The adversary sends a set of attributes U_i to the challenger. Then the challenger returns the private key SK_{U_i} to the adversary; or

- **Decryption Query**: The adversary sends a ciphertext CT_i and an attribute set U_i as inputs. The challenger returns the plaintext M_i to the adversary.

Challenge. The adversary submits two challenge messages and policies as (M_0^*, $\mathbb{A}_0^*$) and ($M_1^*, \mathbb{A}_1^*$) to the challenger where if any of the attributes during private key queries in *Phase 1* satisfy the challenge policy, then it should satisfy both the policies, or none of the queried attributes satisfy the challenge policies. Then the challenger randomly chooses $b^{'} \in \{0, 1\}$, and encrypts $M_{b'}^*$ under $\mathbb{A}_{b'}^*$ to get the ciphertext CT^*. The ciphertext CT^* is given to the adversary. Note that if we stress that $\mathbb{A}_0^* = \mathbb{A}_1^*$, then the security game is for confidentiality; if we stress that $M_0^* = M_1^*$, then the game is for anonymity.
Phase 2. The adversary repeats the steps in *Phase 1* except for querying the sets of attributes which satisfy the two access structures and the ciphertext corresponding to the challenge.
Guess. The adversary outputs a guess $b'' \in \{0, 1\}$ of $b^{'}$ and wins the game if $b'' = b^{'}$.

The advantage of the adversary in this game is defined as $|\Pr[b^{'} = b''] - \frac{1}{2}|$.

2.3.2 CCA Security Game for IBBE/Anonymous IBBE

An IBBE/anonymous IBBE scheme is said to be secure against CCA if no probabilistic polynomial-time adversary has non-negligible advantage in the following game.
Setup. A challenger takes a security parameter l as an input, and returns PK to an adversary and keeps MK to secret.
Phase 1. The adversary submits queries $q_1, ..., q_n$ to query for the private keys or the decryptions for the ciphertexts generated by the adversary, where q_i is either

- **Private Key Query**: The adversary sends an identity ID_i to the challenger. The challenger returns the private key SK_{ID_i} to the adversary; or

- **Decryption Query**: The adversary sends a ciphertext CT_i and an identity ID_i as inputs. The challenger returns the plaintext M_i to the adversary.

Challenge. The adversary submits two challenge messages and sets of identities as (M_0^*, S_0^*) and (M_1^*, S_1^*) to the challenger where $ID_i \notin S_0^* \triangle S_1^*$ for $i = q_1, \ldots, q_n$ ($S_0^* \triangle S_1^*$ is the symmetric difference for S_0^*, S_1^*). Then the challenger randomly chooses $b^{'} \in \{0, 1\}$, and encrypts $M_{b'}^*$ under $S_{b'}^*$ to get the ciphertext CT^*. The ciphertext CT^* is given to the adversary. Note that if we stress that $S_0^* = S_1^*$, then the security game is for confidentiality; if we stress that $M_0^* = M_1^*$, then the game is for anonymity.
Phase 2. The adversary repeats the steps in *Phase 1* except for querying the identities and the ciphertext corresponding to the challenge.

Guess. The adversary outputs a guess $b'' \in \{0,1\}$ of $b^{'}$ and wins the game if $b'' = b^{'}$.

The advantage of the adversary in this game is defined as $|\Pr[b^{'} = b''] - \frac{1}{2}|$.

3 Our Construction

3.1 The Relationship Between IBE and AND-Gate-Only ABE

In this section, we discuss the relationship between IBE and ABE. Under certain conditions, IBE and ABE will be equivalent through some transformation. Such relationship can bring some interesting results. For instance, if we consider an AND-gate-only ABE, then our transformation gives the first ABE supporting hidden access policy, constant-size ciphertexts and private keys.

3.1.1 Conversion Between Access Structures and Identities

Consider an ABE supporting AND gates only. Note that, in an AND-gate-only ABE scheme, an access structure can be viewed as a non-empty set of attributes for simplicity. Therefore, in the rest of this section, we represent an access structure $\mathbb{A}$ as an attribute set. For such a scheme, we now propose a method to uniquely relate an access structure $\mathbb{A}$ to an identity $ID_{\mathbb{A}}$, whose length equals to $|\mathcal{U}|$, i.e. the size of the universe $\mathcal{U}$. Roughly speaking, given an access structure $\mathbb{A}$, for $i = 1$ to $|\mathcal{U}|$, if an attribute X_i is in $\mathbb{A}$, then set the i-th bit of $ID_{\mathbb{A}}$ as 1; otherwise set it to be 0. For instance, if $\mathcal{U} = \{A, B, C, D\}$ and $\mathbb{A} = A$ AND B AND $D = \{A, B, D\}$, then we can use the above method to construct an identity $ID_A = 1101$. The transformation mentioned above can be inverted, i.e., an identity can also be uniquely converted to an access structure.

Algorithm 1 Algorithm - Γ

Input: an access structure $\mathbb{A} = \{X_1, ..., X_n\}$, where $1 \leq n \leq |\mathcal{U}|$, a universe $\mathcal{U}$
Output: an identity ID_A

Let $ID_A[i]$ be the i-th bit of ID_A;
for $i = 1$ to $|\mathcal{U}|$ **do**
  if $X_i \in \mathbb{A}$ **then**
    $ID_A[i] = 1$;
  else
    $ID_A[i] = 0$;
  end if
end for
Return ID_A;

Algorithm 2 Algorithm - $\mathit{\Gamma}^{-1}$

Input: an identity ID_A, a universe $\mathcal{U}$

Output: an access structure $\mathbb{A} = \{X_1, ..., X_n\}$, where $1 \leq n \leq |\mathcal{U}|$

```
Let ID_A[i] be the i-th bit of ID_A, and A be a null set;
for i = 1 to |U| do
    if ID_A[i] = 1 then
        A ← A ∪ {X_i};
    end if
end for
Return A;
```

3.1.2 ABE from IBE

In this section, we discuss about the generic construction of an ABE scheme, which supports AND gates only, from an IBE scheme. In such an ABE scheme, the access structure may look like "*School*: XYZ **AND** (*Position*: Student **AND** *Grade*: College)." And as mentioned above, we view an access structure as a set of attributes, i.e. School: XYZ, Position: Student, Grade: College. Assume that IBE is an identity-based encryption scheme with the four algorithms: **Setup**, **KeyGen**, **Encrypt**, and **Decrypt**. We construct an ABE scheme as follows.

- **Setup**(1^l): Taking a security parameter l as an input, this algorithm runs $(IBE.MK, IBE.PK) \leftarrow IBE.\textbf{Setup}(1^l)$, then sets the master secret key MK and the public key PK of the system as $(MK, PK) = (IBE.MK, IBE.PK)$.
  It outputs MK and PK.

- **KeyGen**(PK, MK, U): Taking the master secret key MK, a set of attributes U, and the public key PK as inputs, this algorithm converts the set of attributes U to an identity $ID_U \in \{0,1\}^{|\mathcal{U}|}$ by running the algorithm - $\mathit{\Gamma}$, and gets the private key as $IBE.SK_{ID_U} \leftarrow IBE.\textbf{KeyGen}(PK, MK, \mathit{\Gamma}(U))$. It outputs the private key $SK_U = IBE.SK_{ID_U}$.

- **Encrypt**$(M, PK, \mathbb{A})$: Taking a message M, the public key PK, and an access structure $\mathbb{A}$ as inputs, this algorithm converts the access structure $\mathbb{A}$ to an identity $ID_{\mathbb{A}} \in \{0,1\}^{|\mathcal{U}|}$ by running the algorithm - $\mathit{\Gamma}$, and gets the ciphertext as $IBE.CT \leftarrow IBE.\textbf{Encrypt}(M, PK, \mathit{\Gamma}(\mathbb{A}))$. It outputs the ciphertext $CT = IBE.CT$.

- **Decrypt**(CT, SK_U): Taking the ciphertext CT and the private key SK_U as inputs, this algorithm gets the plaintext by computing $IBE.M \leftarrow IBE.\textbf{Decrypt}(CT, SK_U)$. It outputs the message $M = IBE.M$.

3.1.3 IBE from ABE

In this section, we discuss the generic construction of an IBE scheme from an ABE scheme supporting AND gates only.

Assume that ABE is an attribute-based encryption scheme with the four algorithms: **Setup**, **KeyGen**, **Encrypt**, and **Decrypt**. We construct an IBE scheme from an ABE scheme as follows.

- **Setup**(1^l): Taking a security parameter l as an input, this algorithm runs $(ABE.MK, ABE.PK) \leftarrow ABE.\mathbf{Setup}(1^l)$, then sets the master secret key MK and the public key PK of the system as $(MK, PK) = (ABE.MK, ABE.PK)$. It outputs MK and PK.
- **KeyGen**(MK, ID_U): Taking the master secret key MK and an identity $ID_U \in \{0,1\}^{|\mathcal{U}|}$ as inputs, this algorithm converts the identity ID_U to the set of attributes U by running the algorithm - Γ^{-1}, and gets the private key $ABE.SK_U \leftarrow ABE.\mathbf{KeyGen}(PK, MK, \Gamma^{-1}(ID_U))$. It outputs the private key $SK_{ID_U} = ABE.SK_U$.
- **Encrypt**(M, PK, ID): Taking a message M, the public key PK, and an identity $ID \in \{0,1\}^{|\mathcal{U}|}$ as inputs, this algorithm converts the identity ID to an access structure $\mathbb{A}$ by running the algorithm - Γ^{-1}, and gets the ciphertext $ABE.CT \leftarrow ABE.\mathbf{Encrypt}(M, PK, \Gamma^{-1}(ID))$. It outputs the ciphertext $CT = ABE.CT$.
- **Decrypt**(CT, SK_{ID_U}): Taking the ciphertext CT and the private key SK_{ID_U} as inputs, this algorithm gets the plaintext by computing $ABE.M \leftarrow ABE.\mathbf{Decrypt}(CT, SK_{ID_U})$. It outputs the message $M = ABE.M$.

3.1.4 Discussion

By transforming an AND-gate-only access structure into an identity, and vice versa, we realize the conversion between ABE and IBE. One can observe that, the features of the encryption scheme may be inheritable through the conversion. For instance, if we use an IBE with receiver anonymity to construct an ABE, then we will have an ABE with hidden access policy. Therefore, we can realize an AND-gate-only ABE with constant-size ciphertexts/private keys and hidden access policy from an anonymous IBE [Boyen and Waters, 2006, Gentry, 2006].

3.2 The Relationship Between IBBE and ABE with DNF

In this section, we give a conversion between an IBBE and an ABE with access structures in DNF. Note that the formal definition of an access structure we use here is equivalent to a DNF formula, as mentioned in Definition 1. Since every clause in a DNF formula contains only AND gates, we can use the algorithm Γ to transform each clause into an identity. Thus a DNF formula implies a set of identities, which can be viewed as the receiver set in an IBBE scheme. Also, the concept allows us to convert an identity set into an access structure. Following the concept above, we propose a generic construction of ABE from IBBE. Our conversion method gives many interesting results. By adopting the conversion, we can construct the first ABE achieving access structures with wildcard and constant-size ciphertexts/private keys. Our conversion method may also imply some impossibilities. For instance, through our method, we can prove that, if an ABE supports access structures in DNF, then it will never achieve hidden access structures and constant-size ciphertexts simultaneously.

3.2.1 Conversion Between Access Structures in DNF and a Set of Identities

Consider an ABE supporting boolean functions in DNF. For such a scheme, we now propose a method to uniquely relate an access structure $\mathbb{A}$ to a set of identities $S = \{ID_1, ...ID_n\}$ for some integer n.

Algorithm 3 Algorithm - Ψ

Input: an access structure $\mathbb{A} = \{A_1, A_2, \ldots, A_n\} \subseteq 2^{\mathcal{U}}$, where $\mathcal{U}$ is the universe
Output: a receiver set $S = \{ID_1, ...ID_n\}$
1: Let S be a null set;
2: **for** $i = 1$ to n **do**
3: $\quad ID_i \leftarrow \Gamma(A_i)$;
4: $\quad S \leftarrow S \cup \{ID_i\}$;
5: **end for**
6: Return S;

3.2.2 ABE from IBBE

In this section, we discuss the generic construction of an ABE scheme, which supports access structures in DNF, from an IBBE scheme. Assume that $IBBE$ is an identity-based broadcast encryption scheme with the four algorithms: **Setup**, **KeyGen**, **Encrypt**, and **Decrypt**. We construct an ABE scheme from an IBBE scheme as follows.

Algorithm 4 Algorithm - Ψ^{-1}

Input: a receiver set $\{ID_1, ...ID_n\}$
Output: an access structure $\mathbb{A} = \{A_1, A_2, \dots, A_n\} \subseteq 2^{\mathcal{U}}$

```
Let 𝔸 be a null set;
for i = 1 to n do
    A_i ← Γ^{-1}(ID_i);
    𝔸 ← 𝔸 ∪ {A_i};
end for
Return 𝔸;
```

- **Setup(1^l)**: Taking a security parameter l as an input, this algorithm runs $(IBBE.MK, IBBE.PK) \leftarrow IBBE.\mathbf{Setup}(1^l)$, then sets the master secret key MK and the public key PK of the system as $(MK, PK) = (IBBE.MK, IBBE.PK)$. It outputs MK and PK.
- **KeyGen(PK, MK, U)**: Taking the public key PK, the master secret key MK, and the set of attributes U as inputs, this algorithm converts the set of attributes U to an identity $ID_U \in \{0,1\}^{|\mathcal{U}|}$ by running the algorithm - Γ defined in Algorithm 1, and gets the private key as $IBBE.SK_{ID_U} \leftarrow IBBE.\mathbf{KeyGen}(PK, MK, \Gamma(U))$. It outputs the private key $SK_U = IBBE.SK_{ID_U}$.
- **Encrypt$(M, PK, \mathbb{A})$**: Taking a message M, the public key PK, and an access structure $\mathbb{A}$ as inputs, this algorithm converts the access structure $\mathbb{A}$ to a set of identities $S = \{ID_1, ...ID_n\}$ of receivers by running the algorithm - Ψ, and gets the ciphertext $IBBE.CT \leftarrow IBBE.\mathbf{Encrypt}(M, PK, \Psi(\mathbb{A}))$. It outputs the ciphertext $CT = IBBE.CT$.
- **Decrypt(CT, SK_U)**: Taking the ciphertext CT and the private key SK_U as inputs, this algorithm gets the plaintext by computing $IBBE.M \leftarrow IBBE.\mathbf{Decrypt}(CT, SK_U)$. It outputs the message $M = IBBE.M$.

3.2.3 IBBE from ABE

Using the algorithm Ψ^{-1}, we can also give a generic construction of IBBE from ABE. Assume that ABE is an attribute-based encryption scheme with the four algorithms: **Setup**, **KeyGen**, **Encrypt**, and **Decrypt**. We construct an IBBE scheme from an ABE scheme as follows.

- **Setup(1^l)**: Taking a security parameter l as an input, this algorithm runs $(ABE.MK, ABE.PK) \leftarrow ABE.\mathbf{Setup}(1^l)$, then sets the master secret key MK and the public key PK of the system as $(MK, PK) = (ABE.MK, ABE.PK)$. It outputs MK and PK.

- **KeyGen**(PK, MK, ID_i): Taking the public key PK, the master secret key MK, and the identity $ID_U \in \{0,1\}^{|\mathcal{U}|}$ as inputs, this algorithm converts the identity ID_U to the set of attributes U by running the algorithm - Γ^{-1} defined in Algorithm 2, and gets the private key $ABE.SK_U \leftarrow ABE.\mathbf{KeyGen}(PK, MK, \Gamma^{-1}(ID_U))$. It outputs the private key $SK_{ID_U} = ABE.SK_U$.
- **Encrypt**(M, PK, S): Taking a message M, the public key PK, and a set of identities $S = \{ID_1, ...ID_n\}$ of receivers as inputs, this algorithm converts the set of identities S to the the access structure $\mathbb{A}$ by running the algorithm - Ψ^{-1}, and gets the ciphertext $ABE.CT \leftarrow ABE.\mathbf{Encrypt}(M, PK, \Psi^{-1}(S))$. It outputs the ciphertext $CT = ABE.CT$.
- **Decrypt**(CT, SK_{ID_U}): Taking the ciphertext CT and the private key SK_{ID_U} as inputs, this algorithm gets the plaintext by computing
$ABE.M \leftarrow ABE.\mathbf{Decrypt}(CT, SK_{ID_U})$. It outputs the message $M = ABE.M$.

3.2.4 Discussion

In this section, we discuss the effect about the transformation between ABE and IBBE. According to the method for converting an access structure in DNF into a set of identities, and vice versa, as mentioned above, we can realize a generic construction of an ABE scheme from an IBBE scheme, and vice versa. Furthermore, this conversion method will bring some interesting results as follows.

- We can obtain an ABE with hidden access policies from an IBBE with receiver anonymity, and vice versa.
- We can use an IBBE with constant-size ciphertexts/private keys to construct an ABE with constant-size ciphertexts/private keys, and vice versa.
- We can realize an AND-gate-only ABE with wildcard.
The conversion method is shown below. Consider an AND-gate-only ABE scheme with wildcard from an IBBE. It means that there are “don't care” attributes in an access structure. Let the symbol “$*$” denote wildcard, e.g. an attribute a^* is a “don't care” attribute in access structure $\mathbb{A}$. For such a scheme, given the access structure $\mathbb{A}$, if there is a “don't care” attribute X_i^* in $\mathbb{A}$, then we will obtain a pair of identities $(ID_A,\ ID_B)$ by our converted method, where the value of the i-th bit in ID_A is 1 and the value of the i-th bit in ID_B is 0. For instance, if $\mathcal{U} = \{a, b, c, d\}$ and $\mathbb{A} = \{a, c^*, d\}$, then we can obtain two different identities, $ID_A = 1011$ and $ID_B = 1001$, by applying the above method. And the ciphertext is generated by the encryption algorithm of IBBE with the receiver set $S = \{ID_A, ID_B\}$. Moreover, if we take

advantage of an IBBE with constant-size ciphertexts/private keys [Delerablée, 2007, Zhang et al., 2012], we can obtain the first AND-gate-only ABE with wildcard supporting constant-size ciphertexts/private keys.

- In 2012, Kiayias and Samari [Kiayias and Samari, 2012] have proved that the size of a ciphertext in an anonymous broadcast encryption is at least of linear size in the number of receivers. Following their result, we can use our transformation technique to prove that there is no ABE supporting access structures in DNF that can achieve hidden access structures and constant-size ciphertexts simultaneously. This is because that if there exist such schemes, we can use the proposed method to obtain an anonymous IBBE with constant-size ciphertexts, which will go against the result of [Kiayias and Samari, 2012].

For the results above, we conclude that if there is an IBE scheme with some features, then the ABE scheme will inherit those features from the IBE by our conversion methods.

4 Security Proofs

4.1 The Security Proof for Confidentiality

This section presents the proof of the CCA security for confidentiality of the ABE scheme from an IBBE scheme, and the IBBE scheme from an ABE scheme.

4.1.1 The ABE Scheme from an IBBE Scheme

Theorem 2. *The ABE scheme from an IBBE scheme is CCA secure if the underlying IBBE scheme is CCA secure.*

Proof. The basic concept is to prove by contradiction. Assume that the ABE scheme is not secure. That is, there exists a polynomial-time adversary $\mathcal{A}$ that can break the ABE scheme with non-negligible advantage. Then we will construct a polynomial-time algorithm that has non-negligible advantage to win the security game of IBBE (denoted as Θ) shown in Section 2.3.2. The challenger simulates the game for $\mathcal{A}$ as follows.
Setup. The challenger interacts with Θ and is given the public key PK from Θ. Then the challenger sends the public key PK to the adversary $\mathcal{A}$.
Phase 1. The adversary $\mathcal{A}$ submits queries $q_1, ..., q_n$ to query for the private keys or the decryptions for the ciphertexts generated by the adversary, where q_i is either

- **Private Key Query**: Upon receiving a set of attributes U_i from the adversary $\mathcal{A}$, the challenger uses the algorithm $\Gamma(U_i)$ to transform the attribute set into an identity ID_i, submits the ID_i to Θ for private key query, and is given the private key SK_{ID_i} from Θ. Then the challenger returns SK_{ID_i} to adversary $\mathcal{A}$; or

- **Decryption Query**: Upon receiving a ciphertext CT_i and an attribute set U_i from the adversary $\mathcal{A}$, the challenger submits the ciphertext CT_i and $\Gamma(U_i)$ to Θ and is given the plaintext M from Θ. Then the challenger returns the plaintext M to the adversary $\mathcal{A}$.

Challenge. Upon receiving two distinct equal length messages (M_0, M_1) and a challenge access structure $\mathbb{A}^*$ in DNF from the adversary $\mathcal{A}$, where the access structure $\mathbb{A}^*$ cannot satisfy any of the queried attribute sets in *Phase 1*, the challenger uses the algorithm $\Psi(\mathbb{A}^*)$ to transform the access structure in DNF into a set of identities S^*. Then the challenger submits (M_0, M_1) and S^* to Θ and is given the ciphertext CT^*. Finally, the challenger returns CT^* to the adversary $\mathcal{A}$.
Phase 2. The adversary $\mathcal{A}$ repeats the steps in *Phase 1* except for querying the sets of attributes which satisfy the access structure and the ciphertext corresponding to the challenge.
Guess. The adversary $\mathcal{A}$ outputs a guess $b^{'} \in \{0, 1\}$.
Finally, the challenger outputs $b^{'}$ to Θ as the guess. Thus we have that the challenger wins the underlying IBBE security game with the same advantage as that of $\mathcal{A}$ winning the ABE security game. Therefore, we conclude that the ABE scheme is CCA secure if the IBBE scheme is CCA secure.

4.1.2 The IBBE Scheme from an ABE Scheme

Theorem 3. *The IBBE scheme from an ABE scheme is CCA secure if the underlying ABE scheme is CCA secure.*

Proof. Assume that the IBBE scheme from an ABE scheme is not secure. That is, there exists a polynomial-time adversary $\mathcal{A}$ that can break the IBBE scheme with non-negligible advantage. Then we will construct a polynomial-time algorithm that has non-negligible advantage to win the security game of ABE (denoted as Ω) shown in Section 2.3.1. The challenger simulates the game for $\mathcal{A}$ below.
Setup. The challenger interacts with underlying Ω and is given the public key PK from Ω. The challenger then sends the public key PK to the adversary $\mathcal{A}$.
Phase 1. The adversary $\mathcal{A}$ submits queries $q_1, ..., q_n$ to query for the private keys or decryptions for the ciphertexts generated by the adversary, where q_i is either

- **Private Key Query**: Upon receiving an identity ID_i from the adversary $\mathcal{A}$, the challenger uses the algorithm $\Gamma^{-1}(ID_i)$ to transform the identity ID_i into a set of attributes U_i, submits the U_i to Ω for private key query, and is given the private key SK_{U_i} from Ω. Then the challenger returns SK_{U_i} to adversary $\mathcal{A}$; or

- **Decryption Query**: Upon receiving a ciphertext CT_i and an identity ID_i from the adversary $\mathcal{A}$, the challenger submits CT_i and $\Gamma^{-1}(ID_i)$ to Ω and is given the plaintext M from Ω. Then the challenger returns the plaintext M to the adversary $\mathcal{A}$.

Challenge. Upon receiving two distinct equal length messages (M_0, M_1) and a challenge set of identities $(ID_1^*, ..., ID_n^*)$ from the adversary $\mathcal{A}$, where ID_i^* for $i = 1, ..., n$ cannot be any of the queried identities in *Phase 1*, the challenger uses the algorithm $\Psi^{-1}(ID_1^*, ..., ID_n^*)$ to transform the set of identities into the access structure $\mathbb{A}^*$ in DNF. Then the challenger submits (M_0, M_1) and $\mathbb{A}^*$ to Ω and is given the ciphertext CT^*. Finally, the challenger returns CT^* to the adversary $\mathcal{A}$.
Phase 2. The adversary $\mathcal{A}$ repeats the steps in *Phase 1* except for querying the identities and the ciphertext corresponding to the challenge.
Guess. The adversary $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$.

Finally, the challenger outputs b' to Ω as the guess. Thus, we have that the challenger wins the underlying ABE security game with the same advantage as that of $\mathcal{A}$ winning the IBBE security game. It turns out that the IBBE scheme is CCA secure if the ABE scheme is CCA secure.

The proofs of confidentiality of the constructions in Section 3.1.2 and Section 3.1.3 are similar to the above. Actually, these two constructions can be regarded as the special cases of the constructions in Section 3.2.2 and Section 3.2.3, resprectively.

4.2 The Security Proof for Anonymity

In this section, we show the proof of the CCA security for the anonymity of the ABE scheme with hidden access policies from an anonymous IBBE scheme, and the anonymous IBBE scheme from an ABE scheme with hidden access policies. The following proofs can be also applied to the special case - the transformation between an AND-gate-only ABE scheme with hidden access policies and an anonymous IBE scheme.

4.2.1 The ABE Scheme with Hidden Access Policy from an Anonymous IBBE Scheme

Theorem 4. *The ABE scheme with hidden access policies from an anonymous IBBE scheme is CCA secure if the underlying anonymous IBBE scheme is CCA secure.*

Proof. Assume that the ABE scheme with hidden access policies is not secure. That is, there exists a polynomial-time adversary $\mathcal{A}$ that can break the ABE scheme with hidden access policies with non-negligible advantage. Then we will construct a polynomial-time algorithm that has non-negligible advantage to win the security game of anonymous IBBE (denoted as $\Theta^{'}$) shown in Section 2.3.2. The challenger simulates the game for $\mathcal{A}$ as follows.
Setup. The challenger interacts with $\Theta^{'}$ and is given the public key PK from $\Theta^{'}$. The challenger then sends the public key PK to $\mathcal{A}$.
Phase 1. $\mathcal{A}$ submits queries $q_1, ..., q_n$ to query for the private keys or decryptions for the ciphertexts generated by the adversary, where q_i is either

- **Private Key Query**: Upon receiving a set of attributes U_i from $\mathcal{A}$, the challenger performs the algorithm $\Gamma(U_i)$ to transform the attribute set into an identity ID_i, submits the ID_i to $\Theta^{'}$ for private key query, and is given the private key SK_{ID_i} from $\Theta^{'}$. The challenger returns SK_{ID_i} to $\mathcal{A}$; or

- **Decryption Query**: Upon receiving a ciphertext CT_i and an attribute set U_i from $\mathcal{A}$, the challenger submits the ciphertext CT_i and $\Gamma(U_i)$ to $\Theta^{'}$ and is given the plaintext M from $\Theta^{'}$. The challenger returns the plaintext M to $\mathcal{A}$.

Challenge. Upon receiving two messages and policies as $(M_0^*, \mathbb{A}_0^*)$ and $(M_1^*, \mathbb{A}_1^*)$ from $\mathcal{A}$ with the restriction that if any of the attributes during private key queries in *Phase 1* satisfies the challenge policy then it satisfies both the policies $(\mathbb{A}_0^*, \mathbb{A}_1^*)$ and $M_0^* = M_1^*$, or none of the queried attributes satisfies the challenge policies $(\mathbb{A}_0^*, \mathbb{A}_1^*)$, the challenger executes the algorithm Ψ to transform the two access structures in DNF into two sets of identities (S_0^*, S_1^*), respectively. Then, the challenger submits (M_0^*, S_0^*) and (M_1^*, S_1^*) to $\Theta^{'}$ and is given the ciphertext CT^*. Finally, the challenger returns CT^* to $\mathcal{A}$.
Phase 2. The adversary $\mathcal{A}$ repeats the steps in *Phase 1* except for querying the sets of attributes which satisfy the access structure and the ciphertext corresponding to the challenge.
Guess. Finally, the adversary $\mathcal{A}$ outputs a guess $b^{'} \in \{0, 1\}$.
Remark. According to the restriction in *Challenge*, we have that, for each U_i queried in *Phase 1*, $U_i \notin (\mathbb{A}_0^* \triangle \mathbb{A}_1^*)$, if we view $\mathbb{A}_0^*, \mathbb{A}_1^*$ as two sets of "set of attributes" (Definition 1), by our proposed conversion method - Γ and Ψ, we can obtain that $ID_i \notin (S_0^* \triangle S_1^*)$ for every ID_i that the challenger queries with. Finally, the challenger outputs $b^{'}$ to $\Theta^{'}$ as the guess. Thus we have that the challenger wins the underlying anonymous IBBE security game with the same advantage as that of $\mathcal{A}$ winning the security game of ABE with hidden access policies. Therefore, the ABE scheme with hidden access policies is CCA secure if the anonymous IBBE scheme is CCA secure.

4.2.2 The Anonymous IBBE Scheme from an ABE Scheme with Hidden Access Policy

Theorem 5. *The anonymous IBBE scheme from an ABE scheme with hidden access policies is CCA secure if the underlying ABE scheme with hidden access policies is CCA secure.*

Proof. Assume that the IBBE scheme from an ABE scheme is not secure. That is, there exists a polynomial-time adversary $\mathcal{A}$ that can break the IBBE scheme with non-negligible advantage. Then, we will construct a polynomial-time algorithm that has non-negligible advantage to win the security game of ABE with hidden access policies (denoted as $\Omega^{'}$) shown in Section 2.3.1. The challenger simulates the game for $\mathcal{A}$ as follows.
Setup. The challenger interacts with $\Omega^{'}$ and is given the public key PK from $\Omega^{'}$. Then the challenger sends the public key PK to $\mathcal{A}$.
Phase 1. The adversary $\mathcal{A}$ submits queries $q_1, ..., q_n$ to query for the private keys or decryptions for the ciphertexts generated by the adversary, where q_i is either

- **Private Key Query**: Upon receiving an identity ID_i from $\mathcal{A}$, the challenger runs the algorithm $\Gamma^{-1}(ID_i)$ to transform the identity ID_i into a set of attributes U_i, submits the U_i to $\Omega^{'}$ for private key query, and is given the private key SK_{U_i} from $\Omega^{'}$. Then, the challenger returns SK_{U_i} to $\mathcal{A}$; or

- **Decryption Query**: Upon receiving a ciphertext CT_i and an identity ID_i from $\mathcal{A}$, the challenger submits CT_i and $\Gamma^{-1}(ID_i)$ to $\Omega^{'}$ and is given the plaintext M from $\Omega^{'}$. Then the challenger returns the plaintext M to $\mathcal{A}$.

Challenge. Upon receiving two challenge messages and sets of identities as (M_0^*, S_0^*) and (M_1^*, S_1^*) from $\mathcal{A}$ with restriction that if any of identities during private key queries in *Phase 1* exists in the challenge set of identities then it must exist in both the sets of identities and $M_0^* = M_1^*$, or none of the queried identities exists in the challenge sets of identities, the challenger performs the algorithm Ψ^{-1} to transform the two sets of identities into two access structures $(\mathbb{A}_0^*, \mathbb{A}_1^*)$ in DNF, respectively. Then the challenger submits $(M_0^*, \mathbb{A}_0^*)$ and $(M_1^*, \mathbb{A}_1^*)$ to $\Omega^{'}$ and is given the ciphertext CT^*. Finally, the challenger returns CT^* to $\mathcal{A}$.
Phase 2. The adversary $\mathcal{A}$ repeats the steps in *Phase 1* except for querying the identities and the ciphertext corresponding to the challenge.
Guess. Finally, the adversary $\mathcal{A}$ outputs a guess $b^{'} \in \{0, 1\}$.
Remark. It is similar to the proof in Section 4.2.1 except that the conversion methods are replaced with Γ^{-1} and Ψ^{-1}.
Finally, the challenger outputs $b^{'}$ to $\Omega^{'}$ as the guess. Thus, the challenger wins the security game of ABE with hidden access policies with the same advantage as that of $\mathcal{A}$ winning the anonymous IBBE security game. Hence, the anonymous

IBBE scheme is CCA secure if the ABE scheme with hidden access policies is CCA secure.

The proofs of the anonymity for the constructions in Section 3.1.2 and Section 3.1.3 are similar to the above. Actually, these two constructions can be regarded as the special cases of the constructions in Section 3.2.2 and Section 3.2.3, respectively.

5 Conclusion

In this paper, we have proposed the algorithms for the transformation between access structures and identities. Generic constructions of CP-ABE and IBE are given in the paper as well. Our conversion methods bring some interesting results in constant-size ciphertexts, anonymity, wildcards, etc. The CP-ABE scheme will inherit from the properties of the underlying IBE/IBBE scheme, and vice versa. Furthermore, we provided the proofs for the uniqueness of the proposed conversion methods and the CCA security proofs for confidentiality and anonymity to demonstrate the security of the proposed conversion methods.

Acknowledgements

This work was partially supported by Taiwan Information Security Center at National Sun Yat-sen University (TWISC@NSYSU) and the Ministry of Science and Technology of Taiwan under grant MOST 107-2218-E-110-014. It also was financially supported by the Information Security Research Center at National Sun Yat-sen University in Taiwan and the Intelligent Electronic Commerce Research Center from The Featured Areas Research Center Program within the framework of the Higher Education Sprout Project by the Ministry of Education (MOE) in Taiwan.

References

[Attrapadung et al., 2011] Attrapadung, N., Libert, B., and de Panafieu, E.: Expressive key-policy attribute-based encryption with constant-size ciphertexts. In International Workshop on Public Key Cryptography. Springer, 2011, 90-108.

[Balu and Kuppusamy, 2010a] Balu, A. and Kuppusamy, K.: Ciphertext policy attribute based encryption with anonymous access policy. CoRR, abs/1011.0527. 2010.

[Balu and Kuppusamy, 2010b] Balu, A. and Kuppusamy, K.: Privacy preserving ciphertext policy attribute based encryption. In Recent Trends in Network Security and Applications. Springer, 402-409, 2010.

[Beimel, 1996] Beimel, A.: Secure schemes for secret sharing and key distribution. PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel. 1996.

[Bethencournt et al., 2007] Bethencournt, J., Sahai, A., and Waters, B.: Ciphertext-policy attribute-based encryption. In Proceedings of the 2007 IEEE Symposium on Security and Privacy, SP '07, 2007, 321-334.

[Boyen and Waters, 2006] Boyen, X. and Waters, B.: Anonymous hierarchical identity-based encryption (without random oracles). In Advances in Cryptology-CRYPTO 2006. Springer, 2006, 209-307.

[Chen et al., 2013] Chen, C., Chen, J., Lim, H. W., Zhang, Z., Feng, D., Ling, S., and Wang, H.: Fully secure attribute-based systems with short ciphertexts/ signatures and threshold access structures. In Cryptographers Track at the RSA Conference. Springer, 2013, 50-67.

[Chen et al., 2011] Chen, C., Zhang, Z., and Feng, D.: Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost. In Provable Security. Springer, 2011, 84-101.

[Cheung and Newport, 2007] Cheung, L. and Newport, C.: Provably secure ciphertext policy abe. In Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, 456-465.

[Delerablée, 2007] Delerablée, C.: Identity-based broadcast encryption with constant size ciphertexts and private keys. In Advances in Cryptology - ASIACRYPT 2007. Springer, 2007, 200-215.

[Doshi and Jinwal, 2011] Doshi, N. and Jinwal, D.: Hidden access structure ciphertext policy attribute based encryption with constant length ciphertext. In International Conference on Advanced Computing, Networking and Security. Springer, 2011, 525-523.

[Emura et al., 2010] Emura, K., Miyaji, A., Nomura, A., Omote, K., and Soshi, M.: A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. International Journal of Applied Cryptography, 2(1):46 - 59, 2010.

[Ge et al., 2012] Ge, A., Zhang, R., Chen, C., Ma, C., and Zhang, Z.: Threshold ciphertext policy attribute-based encryption with constant size ciphertexts. In Australasian Conference on Information Security and Privacy. Springer, 2012, 336-349.

[Gentry, 2006] Gentry, C.: Practical identity-based encryption without random oracles. In Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2006, 445-464.

[Goyal et al., 2008] Goyal, V., Jain, A., Pandey, O., and Sahai, A.: Bounded ciphertext policy attribute based encryption. In Automata, languages and programming. Springer, 2008, 579-591.

[Goyal et al., 2006] Goyal, V., O.Pandey, Sahai, A., and Waters, B.: Attributebased encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS '06, 2006, 89-98.

[Guo et al., 2014] Guo, F., Mu, Y., Susilo, W., Wong, D. S., and Varadharajan, V.: CP-ABE with constant-size keys for lightweight devices. IEEE transactions on information forensics and security, 9(5):763 - 771, 2014.

[Herranz et al., 2010] Herranz, J., Laguillaumie, F., and RÃăfols, C.: Constant size ciphertexts in threshold attribute-based encryption. In International Workshop on Public Key Cryptography. Springer, 2010, 19-34.

[Kiayias and Samari, 2012] Kiayias, A. and Samari, K.: Lower bounds for private broadcast encryption. In International Workshop on Information Hiding. Springer, 2013, 176-190.

[Lai et al., 2011] Lai, J., Deng, R. H., and Li, Y.: Fully secure cipertextpolicy hiding cp-abe. In Information Security Practice and Experience. Springer, 2011, 24-39.

[Li et al., 2012] Li, X., Gu, D., Ren, Y., Ding, N., and Yuan, K.: Efficient ciphertext-policy attribute based encryption with hidden policy. In International Conference on Internet and Distributed Computing Systems. Springer, 2012, 146-159.

[Li et al., 2019] Li, Y., Yu, Y., Susilo, W., Min, G., Ni, J., and Choo., R.: Fuzzy identity-based data integrity auditing for reliable cloud storage systems. IEEE Transactions on Dependable and Secure Computing, 16(1):72 - 83, 2019.

[Liang et al., 2009] Liang, X., Cao, Z., Lin, H., and Xing, D.: Provably secure and efficient bounded ciphertext policy attribute based encryption. In Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. ACM, 2009, 343-352.

[Müller and Katzenbeisser, 2011] Müller, S. and Katzenbeisser, S.: Hiding the policy in cryptographic access control. In Security and Trust Management. Springer 2011, 90-105.

[Nishide et al., 2008] Nishide, T., Yoneyama, K., and Ohta, K.: Attribute-based encryption with partially hidden encryptor-specified access structures. In Applied cryptography and network security. Springer, 2008, 111-129.

[Ostrovsky et al., 2007] Ostrovsky, R., Sahai, A., and Waters, B.: Attribute-based encryption with non-monotonic access structures. In Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, 195-203.

[Padhya and Jinwala, 2014] Padhya, M. and Jinwala, D.: A novel approach for searchable CP-ABE with hidden ciphertext-policy. In Information Systems Security. Springer, 2014, 167-184.

[Phuong et al., 2014] Phuong, T. V. X., Yang, G., and Susilo, W.: Poster: Efficient ciphertext policy attribute based encryption under decisional linear assumption. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2014, 1490-1492.

[Phuong et al., 2016] Phuong, T. V. X., Yang, G., and Susilo, W.: Hidden ciphertext policy attribute-based encryption under standard assumptions. IEEE Transactions on Information Forensics and Security, 11(1):35 - 45, 2016.

[Rao and Dutta, 2013] Rao, Y. S. and Dutta, R.: Recipient anonymous ciphertext-policy attribute based encryption. In Information Systems Security. Springer, 2013, 329-344.

[Sahai and Waters, 2005] Sahai, A. and Waters, B.: Fuzzy identity-based encryption. In Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques, EUROCRYPT'05. 2005, 457-473.

[Tran et al., 2012] Tran, P. V. X., Dinh, T. N., and Miyaji, A.: Efficient ciphertext-policy ABE with constant ciphertext length. In 2012 7th International Conference on Computing and Convergence Technology (ICCCT). IEEE, 2012, 543-549.

[Wang and He, 2016] Wang, Z. and He, M.: CP-ABE with hidden policy from waters efficient construction. International Journal of Distributed Sensor Networks, 2016:11.

[Waters, 2011] Waters, B.: Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In Public Key Cryptography, Lecture Notes in Computer Science, 2011, 53-70.

[Xu and Lang, 2015] Xu, R. and Lang, B.: A CP-ABE scheme with hidden policy and its application in cloud computing. International Journal of Cloud Computing, 4(4):279-298, 2015.

[Xu et al., 2013] Xu, R., Wang, Y., and Lang, B. (2013). A tree-based CP-ABE scheme with hidden policy supporting secure data sharing in cloud computing. In Advanced Cloud and Big Data (CBD), 2013 International Conference on. IEEE, 2013, 51-57.

[Xue et al., 2019] Xue, L., Yu, Y., Li, Y., Au, M. H., Du, X., and Yang., B.. Efficient attribute-based encryption with attribute revocation for assured data deletion. Information Sciences, 479:640-650, 2019.

[Yadav, 2015] Yadav, U. C. (2015). Ciphertext-policy attribute-based encryption with hiding access structure. In 2015 IEEE International Advance Computing Conference (IACC). IEEE, 2015, 6-10.

[Yu et al., 2008] Yu, S., Ren, K., and Lou, W.: Attribute-based content distribution with hidden policy. In Secure Network Protocols, 2008. NPSec 2008. 4th Workshop on. IEEE, 2008, 39-44.

[Yu et al., 2017a] Yu, Y., Au, M. H., Ateniese, G., Huang, X., Susilo, W., Dai, Y., and Min., G.: Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. IEEE Transactions on Information Forensics and Security, 12(4):767-778, 2017.

[Yu et al., 2017b] Yu, Y., Li, Y., Yang, B., Susilo, W., Yang, G., and Bai., J.: Attribute-based cloud data integrity auditing for secure outsourced storage. IEEE Transactions on Emerging Topics in Computing, doi:10.1109/TETC.2017.2759329, 2017.

[Yu et al., 2018] Yu, Y., Xue, L., Li, Y., Du, X., Guizani, M., and Yang, B.: Assured data deletion with fine-grained access control for fog-based industrial applications. IEEE Transactions on Industrial Informatics, 14(10):4538-4547, 2018.

[Zeng and Xu, 2014] Zeng, F. and Xu, C.: Attribute-based encryption with hidden threshold access structure. Computer Modelling and New Technologies, 18(12):19-22, 2014.

[Zhang et al., 2012] Zhang, L., Hu, Y., and Wu, Q. Adaptively secure identity-based broadcast encryption with constant size private keys and ciphertexts from the subgroups. Mathematical and computer Modelling, 55(1):12-18, 2012.

[Zhang et al., 2014] Zhang, Y., Zheng, D., Chen, X., Li, J., and Li, H.: Computationally efficient ciphertext-policy attribute-based encryption with constantsize ciphertexts. In International Conference on Provable Security. Springer, 2014, 259-273.

[Zhang et al., 2016] Zhang, Y., Zheng, D., Chen, X., Li, J., and Li, H.: Efficient attribute-based data sharing in mobile clouds. Pervasive and Mobile Computing, 28:135-149, 2016.

[Zhou and Huang, 2010] Zhou, Z. and Huang, D.: On efficient ciphertext-policy attribute based encryption and broadcast encryption. In Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010, 753-755.

[Zhou et al., 2015] Zhou, Z., Huang, D., and Wang, Z.: Efficient privacy preserving ciphertext-policy attribute based-encryption and broadcast encryption. IEEE Transactions on Computers, 64(1):126-138, 2015.