Constant-Ciphertext-Size Dual Policy Attribute Based Encryption

Atsuko Miyaji[1] ⋆ and Phuong V.X. TRAN[1,2] ⋆⋆

[1] Japan Advanced Institute of Science and Technology
miyaji@jaist.ac.jp, tvxphuong@jaist.ac.jp
[2] Vietnamese-University of Science
tvxphuong@fit.hcmus.edu.vn

Abstract. Dual-Policy Attribute Based Encryption (DP-ABE), proposed in 2009, is a combination of two variants, Ciphertext Policy-ABE (CP-ABE) and Key Policy-ABE (KP-ABE), where an encryptor can associate the data simultaneously with both a set of objective attributes and of subjective access policies. Or, a user is given a private key assigned simultaneously for both a set of objective attributes and a subjective access policy. A major problem of the above DP-ABE scheme is the ciphertext size linear to the number of attributes while the LSSS access structure can be assumed.
We propose two novel DP-ABEs, which achieve constant-size ciphertext, regardless of the number of attributes in a logical AND data access policy with wildcards. We present two constructions: the first scheme under the q-Bilinear Diffie Hellman Exponent (q-BDHE) and the second scheme under the Decisional Bilinear-Diffie-Hellman assumptions (DBDH).
Keywords: Attribute-based Encryption, Dual Policy, Constant Ciphertext Length Size

1 Introduction

Attribute-based encryption (ABE) [2, 5, 3, 1] achieves an attractive feature and is used to various applications [4]. In Attribute-based encryption (ABE), a user's credentials are represented by a set of strings called "attributes", and the predicate is represented by a formula over these attributes. It allows the encryptor embedding the access policies or the user credentials in the ciphertext or the private keys. Three types of ABE called Ciphertext-Policy ABE (CP-ABE) [2, 5], Key-Policy ABE(KP-ABE) [3] and Dual-Policy ABE (ABE) [1] are proposed.
In CP-ABE [2], a secret key is associated to a user's credentials, such as {"Student", "Faculty : CS", "Major: Cryptography"} and a ciphertext is associated to access policies by composing multiple attributes through logical operators such as "AND", "OR", such as "Student" ∧ ("Birthday:1988" ∨"Faculty:CS"). If a decryptor wants to decrypt the message successfully,

⋆ This study is partly supported by Grant-in-Aid for Exploratory Research, 19650002.
⋆⋆ This study is partly supported by Nafosted-National Foundation for Science and Technology Development of Vietnamese Government.

the attributes embedded in the secret key must satisfy the access policies embedded in the ciphertext. In KP-ABE scheme, data are associated with attributes for each of which a public key component is defined. An encryptor associates a set of attributes to the message by encrypting it with the corresponding public key components. Each user is assigned an access structure which is usually defined as an access tree over data attributes, i.e., interior nodes of the access tree are threshold gates and leaf nodes are associated with attributes. A user secret key is defined to reflect the access structure so that the user is able to decrypt a ciphertext if and only if the data attributes satisfy his access structure.

A combination of two variants CP-ABE and KP-ABE, called Dual-Policy ABE (DP-ABE), was proposed in 2009 [1], in which an encryptor can associate the data simultaneously with both a set of objective attributes that ascribe the data itself such as {".doc",".mp3","wma"} and a subjective access policy that states what kind of receivers "Age > 18" ∧ ("Student" ∨"Faculty:CS") will be able to decrypt. Otherwise, a user is given a private key assigned simultaneously for both a set of subjective attributes that annotates user's credentials {"Name : Alice","Student", "Age:24"} and a subjective access policy that states what kind of data (".doc" ∧ ".mp3") can be decrypted. The decryption can be done if the objective attribute set satisfies the objective policy and the subjective attribute set satisfies the subjective policy.

Apart from the promising features provided by the previous DP-ABE, a major problem of the DP-ABE is that the size of the ciphertext increases linearly with respect to the number of included attributes.

In this paper, we propose two novel DP-Abe's, named DP-ABE 1 and DP-ABE 2, which incur a constant size of ciphertext, regardless of the number of attributes in a logical AND data access policy with wildcards. Our two schemes achieve higher performance in the construction with the short length size of the ciphertext in the encryption and the reduced number of pairing in decryption. In addition, we prove that our schemes are secure under the selective-set security notion. To the best of our knowledge, this is the first DP-ABE with constant ciphertext.

Table 1. Comparison

Scheme	Encryption	Decryption	Ciphertext Length	Assumption	Access Structure
DP-ABE [1]	$4ex$	$4p$	$\lvert\mathbb{G}_T\rvert + (n+2)\lvert\mathbb{G}\rvert$	q-BDHE	Linear Structure
DP-ABE 1	$4ex$	$4p$	$\lvert\mathbb{G}_T\rvert + 3\lvert\mathbb{G}\rvert$	q-BDHE	AND Gates
DP-ABE 2	$4ex$	$4p$	$\lvert\mathbb{G}_T\rvert + 3\lvert\mathbb{G}\rvert$	DBDH	AND Gates

Table 1 compares our scheme to the previous scheme [1] from the following viewpoint: the computational complexity of encryption and decryption, access structure, ciphertext length and the security assumption. The computational complexity is measured by the number of pairing computation p and exponentiation computation ex. The computational cost over Z_p is ignored as usual. Compare with [1], our scheme yields a constant length size of ciphertext of DP-ABE 1 and DP-ABE 2 regardless of the

number of subject attributes embedded in the secret key and of the objective attributes embedded in the ciphertext. DP-ABE 1 is secure under the q-Bilinear Diffie-Hellman Exponent problem (q-BDHE) assumption. DP-ABE 2 is secure under the decisional Bilinear Diffie Hellman (DBDH) assumption and, thus it achieves stronger security than DP-ABE1. Both two schemes use the AND gates structure.
Organisation of paper: In Section 2, we provide preliminary materials such as the notion of access structure, bilinear pairing, security assumptions, functional definition and security notion of DP-ABE. In Section 3, we present our DP-ABE 1 and prove it is secure under the q-BDHE assumption. In Section 4, we construct our DP-ABE 2 and prove it is secure under the DBDH assumption. Finally, Section 5 concludes our result.

2 Preliminaries

2.1 The Bilinear Map and Its Related Assumptions

Let $\mathbb{G}$ and $\mathbb{G}_{\mathbb{T}}$ be two multiplicative cyclic groups of prime order p, and e be a bilinear map, where $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_{\mathbb{T}}$. A bilinear map has the following properties:

1. Bileariry : for all u,$v \in \mathbb{G}$ and a,$b \in \mathbb{Z}_p$, we have $e(u^a, v^b) = e(u^b, v^a) = e(u, v)^{ab}$.
2. Non-degeneracy : $e(g, g) \neq 1$.

In this paper, we use a symmetric bilinear map such that $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$.

Definition 1 (Definition of q-BDHE) *Let $\mathbb{G}, \mathbb{G}_T$ be a bilinear group with prime order p and $\boldsymbol{y}$ be a given vector:*

$$\boldsymbol{y} = (g, h, g^{\alpha}, g^{\alpha^2} \ldots, g^{(\alpha^q)}, g^{(\alpha^{q+2})}, \ldots, g^{(\alpha^{2q})}, Z) \in \mathbb{G}^{2q+1} \times \mathbb{G}_T.$$

Then, the q-Bilinear Diffie-Hellman Exponent (q-BDHE) problem is a problem to determine whether $Z = e(g, h)^{\alpha^{q+1}}$.
Let $Y_{g,\alpha,q} = (g^{\alpha}, g^{\alpha^2}, \ldots, g^{(\alpha^q)}, g^{(\alpha^{q+2})}, \ldots, g^{(\alpha^{2q})})$. An algorithm $\mathcal{A}$ that solves q-BDHE problems has advantage ϵ in solving decisional q-BDHE in $\mathbb{G}$ if

$$| Pr[\mathcal{A}(g, h, Y_{g\alpha,q}, e(g, h)^{\alpha^{q+1}}) = 0] - Pr[\mathcal{A}(g, h, Y_{g,\alpha,q}, Z) = 0] | \geq \epsilon,$$

where the probability is over the random choice of generation $g, h \in \mathbb{G}$, randomly chosen $\alpha \in \mathbb{Z}_p$ and $Z \in \mathbb{G}_T$.
We say that the decision q-BDHE assumption holds in $\mathbb{G}$ if no polynomial-time algorithm has a non-negligible advantage in solving the q-BDHE problem.

Definition 2 *The Decisional Bilinear Diffie-Hellman (DBDH) problem in $\mathbb{G}_1$ is defined as: For input of a tuple $(g, g^a, g^b, g^c, T) \in \mathbb{G}_1^4 \times \mathbb{G}_T$, to decide whether $T = e(g, g)^{abc}$. An algorithm $\mathcal{A}$ that solves DBDH problems has advantage ϵ in solving the DBDH problem in $\mathbb{G}_1$ if*

$$Adv_{DBDH(\mathcal{A})} =| Pr[\mathcal{A}(g, g^a, g^b, g^c, e(g, g)^{abc}) = 0] - Pr[\mathcal{A}(g, g^a, g^b, g^c, T) = 0] | \geq \epsilon,$$

where the probability is over the random choice of $g \in \mathbb{G}, a, b, c \in \mathbb{Z}_p$.
We say that the DBDH assumptions hold in $\mathbb{G}_1$ if no polynomial-time algorithm has a non-negligible advantage in solving the DBDH problem in G_1.

2.2 Functional Definition of DP-ABE

A DP-ABE consists of four algorithms: **Setup, Encrypt, KeyGen**, and **Decrypt**.

Setup This is a randomised algorithm that takes no input other than the implicit security parameter. It outputs the public key *pk* and the master key *msk*.

Encrypt(pk, $\mathcal{M}, (\mathbb{S}, \omega)$) This is a randomised algorithm that takes as input the public key *pk*, a message $\mathcal{M}$, a subjective access structure $\mathbb{S}$, a set of objective attributes ω. It outputs the ciphertext *ct*.

KeyGen($pk, msk, (\psi, \mathbb{O})$) This is a randomised algorithm that takes as input the public key *pk*, the master key *msk*, a set of subjective attributes ψ, an objective access structure $\mathbb{O}$. It outputs a private decryption key *sk*.

Decrypt($pk, (\psi, \mathbb{O}), sk, (\mathbb{S}, \omega), ct$) This algorithm takes as input the public key *pk*, a decryption key *sk* and its associated pair of set of subjective attributes ψ and objective access structure $\mathbb{O}$, a ciphertext *ct* and its associated pair of subjective access structure $\mathbb{S}$ and set of objective attributes ω. It outputs the message $\mathcal{M}$ if the set ω of objective attributes satisfies the objective access structure $\mathbb{O}$ and the set ψ of subjective attributes satisfies the subjective access structure $\mathbb{S}$.

Here we explain the access structure. Let $U = \{A_1, A_2, ..., A_k\}$ be the Universe of attributes in the system. Each A_i has three values $\{A_i^+, A_i^-, A_i^*\}$, where A_i^+ represents a positive attribute, A_i^- represents a negative attributes and A_i^* represents a wildcard. When a user joins the system, the user is tagged with an attribute list defined as follows:

- A user's attribute list is denoted as $L = \{A_1^{+/-}, A_2^{+/-}, ..., A_k^{+/-}\}$, where $A_i^{+/-} \in \{A_i^+, A_i^-\}$ and k is the number of attributes in the universe. $L = L^+ \bigcup L^-$, $L^+ = \{A_i^+ \mid \forall i \in \{1...k\}\}$ and $L^- = \{A_i^- \mid \forall i \in \{1...k\}\}$. We have $L^+ \bigcap L^- = \emptyset$. Intuitively, A_i^+ means a user has A_i; A_i^- means a user does not have A_i, or A_i is not a proper attribute of this user.
- Let $W = \{A_1, A_2, ..., A_k\}$ be an *AND* gate access policy, where $A_i \in \{A_i^+, A_i^-, A_i^*\}$. The notation $L \models W$ denotes that the attribute list L of a user satisfies W, that is

$$L \models W \iff W \subset L \bigcup \{A_1^*, A_2^* \ldots A_k^*\}.$$

For example, suppose $U = \{A_1 = \text{CS}, A_2 = \text{EE}, A_3 = \text{Faculty}, A_4 = \text{Student}\}$. Alice is a student in the CS department; Bob is a faculty in the EE department; Carol is a faculty holding a joint position in the EE and CS department. Their attribute lists are illustrated in Table 2.

2.3 Security Model of DP-ABE

Let us give the selective-set security notion for DP-ABE [1].

Init The adversary declares the target subjective access structure S^* and the target objective attribute set ω^*.

Setup The challenger runs the Setup algorithm and provides the public parameters *pk* to the adversary.

Table 2. List of attributes

Attributes	A_1	A_2	A_3	A_4
Description	CS	EE	Faculty	Student
Alice	A_1^+	A_2^-	A_3^-	A_4^+
Bob	A_1^-	A_2^+	A_3^+	A_4^-
Carol	A_1^+	A_2^+	A_3^+	A_4^-

Phase 1 The adversary makes repeated private-key queries for pairs of subjective attribute set and objective access structure $(\psi, \mathbb{O})$ such that $\omega* \notin \mathbb{O}$ or $\psi \notin \mathbb{S}^*$. That is, the negated condition of that of a legitimate key which can be used to decrypt a challenge ciphertext.

Challenge The adversary submits two equal length messages $\mathcal{M}_0$ and $\mathcal{M}_1$. The challenger, then, flips a random bit β, and encrypts $\mathcal{M}_\beta$ on the target pair (S^*, ω^*) subjective access structure and the target objective attribute set ω^*. Then, the resulting ciphertext ct^* is given to the adversary.

Phase 2 Phase 1 is repeated.

Guess The adversary outputs a guess β' of β.

The advantage of an adversary A in the above game is defined as Pr[β' =β]-1/2. Note that the model can easily be extended to handle chosen-ciphertext attacks by allowing for decryption queries in Phases 1 and 2.

Definition 3 *A DP-ABE scheme is secure in the selective-set security notion if all polynomial time adversaries have at most a negligible advantage in the above game.*

3 DP-ABE based on q-BDHE (DP-ABE 1)

Let $\mathcal{U}_s$ and $\mathcal{U}_o$ be the universe of subjective and objective attributes, respectively. We will show DP-ABE 1 below:

Setup There are k attributes $U_s = \{A_1, A_2, \ldots, A_k\}$ in the system, and $K = 3k$ attributes in total since each A_i has 3 values: $\{A_i^+, A_i^-, A_i^*\}$. A one-to-one map φ is used from $\{A_1^+, A_2^+, \ldots, A_k^+\}$ to $\{1, \ldots, k\}$, $\{A_1^-, A_2^-, \ldots, A_k^-\}$ to $\{k+1, \ldots, 2k\}$ and $\{A_1^*, A_2^*, \ldots, A_k^*\}$ to $\{2k+1, \ldots, 3k\}$ for the sake of simplicity.

The algorithm first picks a random generator $g \in \mathbb{G}$ and random exponent $\alpha, a, \gamma \in \mathbb{Z}_p$. It then defines two functions for randomly chosen $h, t \in \mathbb{G}$,

$$F_s : \mathbb{Z}_p \to \mathbb{G}\ (F_s(x) = h^{\alpha^x})$$
$$F_0 : \mathbb{Z}_p \to \mathbb{G}\ (F_o(x) = t^{\alpha^x}).$$

It assigns the public key as $pk = \{g, e(g,g)^\gamma, g^a, h^\alpha, \ldots, h^{\alpha^{3k}}, t^\alpha, \ldots, t^{\alpha^{3k}}\}$ and master key as $msk = \{\gamma, a\}$.

KeyGen The inputs the algorithm is a pair of objective policy $\mathbb{O}$ and subjective attributes $\psi \subset U_o$. The algorithm chooses $r, r_1, r_2, \ldots, r_{3k} \in \mathbb{Z}_p$ and computes $b = \gamma + a \cdot r$. The secret key sk is set to

$$sk = (\mathbb{O}, K, \{\hat{K}_i, K'_i | i \in B^+\}, \{\hat{K}_i, K'_i | i \in B^-\}, \{\hat{K}_i, K'_i | i \in B^*\}, \{K_x\}_{x \in \psi}, \{| i \in B^+\}),$$

which is computed as follows:

$$\begin{aligned}
&K = g^r, \\
&K_i = F_s(i)^r && (i \in \psi) \\
&\hat{K}_i = g^b \cdot F_o(i)^{-r_i}, \quad K'_i = g^{r_i} && (\forall i \in \psi \subset B^+) \\
&\hat{K}_i = g^b \cdot F_o(i)^{-r_{i+k}}, \ K'_i = g^{r_{i+k}} && (\forall i \in \psi \subset B^-) \\
&\hat{K}_i = g^b \cdot F_o(i)^{-r_{i+2k}}, K'_i = g^{r_{i+2k}} && (\forall i \in \psi \subset B^*).
\end{aligned}$$

Encryption The inputs of the algorithm is a message $\mathcal{M}$, the public key pk, a pair of subjective policy $\mathbb{S}$ and objective attributes $\omega \subset U_s$. A ciphertext $CT = (\mathbb{S}, C, C_i, \hat{C}, \{C'_x\}_{x \in \omega})$ is computed for a randomly chosen s in $\mathbb{Z}_p$ as follows:

$$\begin{aligned}
&C = \mathcal{M} \cdot e(g, g)^{\gamma s}, \ C_i = (\prod_{i \in \omega} g^a F_s(i))^{-s} \\
&\hat{C} = g^s, \qquad C'_x = F_o(x)^s \qquad (x \in \omega)
\end{aligned}$$

Decrypt The inputs of the algorithm is a ciphertext CT embedded the subjective policy $\mathbb{S}$ and a set of objective attributes $\omega \subset U_s$, and a secret key sk embedded the objective policy $\mathbb{O}$ and a set of subjective attributes $\psi \subset U_o$. The constraint to decrypt is the message that the set of subjective attributes ψ must satisfy the subjective policy $\mathbb{S}$ and the set of objective attribute ω must satisfy the objective policy $\mathbb{O}$. Decryption is done by:

$$\begin{aligned}
A &= e(C_i, K) \cdot e(\hat{C}, \prod_{i \in \omega} K_i) \\
&= e((\prod_{i \in \omega} g^a F_s(i))^{-s}, g^r) \cdot e(g^s, (\prod_{i \in \omega} F_s(i))^r) \\
&= e(g, g)^{-asr} \cdot e(\prod_{i \in \omega} F_s(i), g)^{-sr} \cdot e(\prod_{i \in \omega} F_s(i), g)^{sr} \\
&= e(g, g)^{-asr} \\
B &= e(\hat{C}, \prod_{i \in \psi} \hat{K}_i) \cdot e(\prod_{i \in \psi} C'_i, K'_i) \\
&= e(g^s, \prod_{i \in \psi} g^b F_o(i)^{-r_i}) \cdot e(\prod_{i \in \psi} F_o(i)^s, g^{r_i}) \\
&= e(g, g)^{bs} \cdot e(g, \prod_{i \in \psi} F_o(i))^{-sr_i} \cdot e(g, \prod_{i \in \psi} F_o(i))^{sr_i} \\
&= e(g, g)^{bs}.
\end{aligned}$$

Then $\mathcal{M}$ can be recovered by using $b = \gamma + ar$.

$$\begin{aligned} A \cdot B &= e(g,g)^{-ars}.e(g,g)^{bs} \\ &= e(g,g)^{-ars} \cdot e(e,g)^{\gamma s} \cdot e(g,g)^{ars} \\ &= e(g,g)^{\gamma s} \\ \frac{C}{A \cdot B} &= \frac{\mathcal{M} \cdot e(g,g)^{\gamma s}}{e(g,g)^{\gamma s}} = \mathcal{M} \end{aligned}$$

The security proof is shown below:

Theorem 1 *Suppose the decisional q-BDHE assumption holds. Then no polynomial-time adversary can break our DP-ABE 1 with a challenge ciphertext CT^* in the selective-set security notion.*

Proof: Let $\mathcal{A}$ be an adversary with an advantage $\epsilon = Adv_{\mathcal{A}}$ in attacking DP-ABE 1. We will show how to build a simulator, $\mathcal{B}$, that plays the decisional q-BDHE problem (recall that $g_i = g^{\alpha^i}$).
Init : The simulator $\mathcal{B}$ takes a q-BDHE challenge $(g, h, Y_{g,\alpha,q}, T)$. $\mathcal{A}$) gives $\mathcal{B}$ the algorithm a pair (S^*, ω^*) of challenge subjective access structure and objective attributes. Let $|\omega^*| = n$, and m be the number of elements in the AND gate access policy S^*, where $3m \leq q$.
Setup : $\mathcal{B}$ chooses $\gamma' \in \mathbb{Z}_p$ randomly and implicitly sets $\gamma = \gamma' + \alpha^{q+1}$ which satisfies $e(g,g)^{\gamma} = e(g,g)^{\gamma'} \cdot e(g^{\alpha^q}, g^{\alpha})$. Then $\mathcal{B}$ chooses $d \in \mathbb{Z}_p$ randomly and computes by setting a implicitly:

$$g^d (\prod_{j \in \mathbb{O}} g^{\alpha^{3k+1-j}})^{-1} = g^{d - \sum_{j \in \mathbb{O}} \alpha^{3k+1-j}} = g^a \text{ if } \omega^* \text{does not satisfy } \mathbb{O}.$$

$$g^d (\prod_{j \in \mathbb{S}^*} g^{\alpha^{3k+1-j}})^{-1} = g^{d - \sum_{j \in \mathbb{S}^*} \alpha^{3k+1-j}} = g^a \text{ if } \psi \text{ does not satisfy } \mathbb{S}^*.$$

$\mathcal{B}$ implicitly sets a function $F_s(x) = g^{p(x)}$ for a polynomial p in $\mathbb{Z}_p[x]$ with degree $m + 3k - 1$ as follows: set $3m + 3k + 1$ polynomials $p_0, \ldots, p_{3k+3m}$ in $\mathbb{Z}_p[x]$ with degree $m + 3k - 1$ to

$$p_i(x) = \begin{cases} x^i \ (i \in [1, 3m]) \\ 0 \ \ (i \in [3m+1, 3m+3k]) \end{cases}$$

and p_0 is set randomly from $\mathbb{Z}_p[x]$. Then $\mathcal{B}$ sets

$$p(x) = \sum_{i=0}^{3k+3m} p_i(x) \cdot \alpha^i, \ \ h_i = g_i^{p_i(x)} (i \in [0, 3k + m - 1]).$$

Then, F_s satisfies

$$F_s(x) = \prod_{i=0}^{3k+m-1} h_i = g^{p(x)},$$

which can be explicitly computed $\mathcal{B}$. Then set a function F_o as follows: For $f_i(x) = x - z_i$ with $z_i \in \{1, \cdots, 3k\}$ according to a set of attributes ω^*, set:

$$f(x) = \sum_{i=0}^{n-1} f_i(x),$$

which ensures that $f(x) = 0$ if and only if $x \in \omega^*$. Then let

$$F_o(x) = \prod_{i=0}^{n-1} g^{f_i(x)} = g^{f(x)},$$

and $t_i = g^{f_i(x)}$. The public key $pk = \{g, e(g,g)^\gamma, g^d, h_0, \ldots, h_{3m}, t_0, \ldots, t_{3m}\}$ is given to $\mathcal{A}$.

Phase 1: $\mathcal{A}$ submits a pair $(\mathbb{O}, \psi)$ of objective access structure and subjective attribute set for private keys, where ψ must not satisfy $\mathbb{S}^*$ or ω^* must not satisfy $\mathbb{O}$. We will prove 2 cases separately.

Case 1: ω^* does not satisfy $\mathbb{O}$.

The simulator randomly chooses $r, r_i \in \mathbb{Z}_p (i = 1 \ldots k)$. It then lets $K = g^r$ and $K_x = F_s(x)^r$ for all $x \in \psi$. When attribute j in ω^*, either $j \in 1, \ldots, k$ and $j+k \in \mathbb{O}$, or $j \in k+1, \ldots, 2k$ and $j-k \in \mathbb{O}$ holds. It implicitly sets $b = a + \gamma \cdot r$. Then, for all $i \in \omega^{*+}$ and $i+k \in \mathbb{O}$, generate:

$$\hat{K}_i = g^\gamma g^{rd\alpha^i} \prod_{j \in \mathbb{O}} (g^{\alpha^{3k+1-j+i}})^{-1} g^{rdr_i} \prod_{j \in \mathbb{O}} (g^{\alpha^{3k+1-j}})^{-r_i} g^{f(i)-r_i} = g^b F_o(i)^{-r_i}$$

$$K_i = g^{r_i}.$$

For all $i \in \omega^{*-}$ and $i - k \in \mathbb{O}$, generate:

$$\hat{K}_i = g^\gamma g^{rd\alpha^i} \prod_{j \in \mathbb{O}} (g^{\alpha^{3k+1-j+i}})^{-1} g^{rdr_{i-k}} \prod_{j \in \mathbb{O}} (g^{\alpha^{3k+1-j}})^{-r_{i-k}} g^{f(i)-r_{i-k}} = g^b F_o(i)^{-r_{i-k}}$$

$$K'_i = g^{r_{i-k}}.$$

For all $i \in \omega^{**}$ and $i \notin \mathbb{O}$, generate:

$$\hat{K}_i = g^\gamma g^{rd\alpha^i} \prod_{j \in \mathbb{O}} (g^{\alpha^{3k+1-j+i}})^{-1} g^{rdr_{i-2k}} \prod_{j \in \mathbb{O}} (g^{\alpha^{3k+1-j}})^{-r_{i-2k}} g^{f(i)-r_{i-2k}} = g^b F_o(i)^{-r_{i-2k}}$$

$$K'_i = g^{r_{i-2k}}$$

Case 2: ψ does not satisfy $\mathbb{S}^*$.

$\mathcal{B}$ randomly chooses $r_i \in \mathbb{Z}_p$ for $i = 1 \ldots k$, and computes $K = g^r$ for $r = r_1 + \ldots + r_k$, and sets implicitly $b = a + \gamma \cdot r$. When attribute j in ψ, either $j \in 1, \ldots, k$ and $j + k \in \mathbb{S}^*$, or $j \in k+1, \ldots, 2k$ and $j - k \in \mathbb{S}^*$ holds. Then, for all $i \in \psi^+$ and $i + k \in \mathbb{S}^*$, generate:

$$\hat{K}_i = g^\gamma g^{rd\alpha^i} \prod_{j \in \mathbb{S}^*} (g^{\alpha^{3k+1-j+i}})^{-1} g^{rdr_i} \prod_{j \in \mathbb{S}^*} (g^{\alpha^{3k+1-j}})^{-r_i} g^{f(i)-r_i} = g^b F_o(i)^{-r_i}$$

$$K'_i = g^{r_i}$$

For all $i \in \psi^-$ and $i - k \in \mathbb{S}^*$, generate:

$$\hat{K}_i = g^\gamma g^{rd\alpha^i} \prod_{j \in \mathbb{S}^*} (g^{\alpha^{3k+1-j+i}})^{-1} g^{rdr_{i-k}} \prod_{j \in \mathbb{S}^*} (g^{\alpha^{3k+1-j}})^{-r_{i-k}} g^{f(i)-r_{i-k}} = g^b F_o(i)^{-r_{i-k}}$$

$$K'_i = g^{r_{i-k}}.$$

For all $i \in \psi^*$ and $i \notin \mathbb{S}^*$, generate:

$$\hat{K}_i = g^\gamma g^{rd\alpha^i} \prod_{j \in \mathbb{S}^*} (g^{\alpha^{3k+1-j+i}})^{-1} g^{rdr_{i-2k}} \prod_{j \in \mathbb{S}^*} (g^{\alpha^{3k+1-j}})^{-r_{i-2k}} g^{f(i)-r_{i-2k}} = g^b F_o(i)^{-r_{i-2k}}$$

$$K'_i = g^{r_{i-2k}}.$$

For all $x \in \psi$, compute:

$$K_x = g^{rp_o(x)} \prod_{j=1}^{k} (g^{r_i} \prod_{i=1}^{3k+3m} g^{p_i(x)}) = (g^r)^{p(x)} = F_s(x)^r.$$

Challenge: Finally, $\mathcal{A}$ gives two messages M_0 and M_1 to $\mathcal{B}$. The simulator flips a coin $\beta \in \{0, 1\}$ and outputs $C = M_\beta Z \cdot e(g^s, g^{\alpha'})$ and $\hat{C} = g^s$ by using randomly chosen $s \in \mathbb{Z}_p$. As for other components C_i and C_x, output:

$$C_i = (\prod_{i \in \mathbb{S}^*} (g^{sd})(\prod_{i \in \mathbb{S}^*} (g^{s\alpha^{3k+1-j}})(\prod_{i=1}^{3m} (g^{sp_i(x)}) = (\prod_{i \in \omega} g^a F_s(i))^{-s}$$

$$C_x = (\prod_{i=1}^{3m} g^{f_i(x)})^s = F_o(x)^s.$$

Phase 2: Repeat Phase 1.
Guess: $\mathcal{A}$ will eventually output a guess β' of β. $\mathcal{B}$ outputs 0 if $\beta' = \beta$, which means that $Z = e(g, h)^{a^{q+1}}$ is guessed; otherwise, it outputs 1, which means that Z is guessed to be a random group element in $\mathbb{G}_T$.
When Z is a correct tuple, the simulator $\mathcal{B}$ gives a perfect simulation, so we obtain:

$$\mid Pr[(\mathcal{B}(g, h, Y_{g,\alpha,q}, Z = e(g, h)^{\alpha^{q+1}}) = 0] - \frac{1}{2} \mid \leq Adv_{\mathcal{A}}$$

When Z is a random group element, the message M_β is completely hidden from the adversary, and we have $Pr[\mathcal{B}(g, h, Y_{g,\alpha,q}, Z = R) = 0] = \frac{1}{2}$. Therefore, $\mathcal{B}$ has the advantage ϵ at least in attacking the decisional q-BDHE problem since $\mid Pr[\mathcal{A}(g, g^a, g^b, g^c, e(g, g)^{abc}) = 0] - Pr[\mathcal{A}(g, g^a, g^b, g^c, T) = 0] \mid \geq \epsilon$ holds. □

4 DP-ABE based on DBDH (DP-ABE 2)

Let $\mathcal{U}_s$ and $\mathcal{U}_o$ be the universe of subjective and objective attributes.

Setup There are k attributes $U_s = \{A_1, A_2, \ldots, A_k\}$ in the system, and $K = 3k$ attributes in total since each A_i has 3 values: $\{A_i^+, A_i^-, A_i^*\}$. A one-to-one map φ is used from $\{A_1^+, A_2^+, \ldots, A_k^+\}$ to $\{1, \ldots, k\}$, $\{A_1^-, A_2^-, \ldots, A_k^-\}$ to $\{k + 1, \ldots, 2k\}$ and $\{A_1^*, A_2^*, \ldots, A_k^*\}$ to $\{2k + 1, \ldots, 3k\}$ for the sake of simplicity.

The algorithm first picks a random generator $g \in \mathbb{G}$ and random exponent $a, \gamma \in \mathbb{Z}_p$. It then defines two functions for randomly chosen $h, t \in \mathbb{G}$,

$$F_s : \mathbb{Z}_p \to \mathbb{G} \ (F_s(x) = h^x)$$
$$F_0 : \mathbb{Z}_p \to \mathbb{G} \ (F_o(x) = t^x).$$

It assigns the public key as $pk = \{g, e(g, g)^\gamma, g^a, h, \ldots, h^{3k}, t, \ldots, t^{3k}\}$ and master key as $sk = \{\gamma, a\}$.

KeyGen The algorithm inputs to the pair of objective policy $\mathbb{O}$ and subjective attributes $\psi \subset U_o$. Then, the algorithm chooses randomly $r, r_1, r_2, \ldots, r_{3k} \in \mathbb{Z}_p$ and computes $b = \gamma + a \cdot r$. The secret key sk is set to

$$sk = (\mathbb{O}, K, \{\hat{K}_i, K'_i | i \in B^+\}, \{\hat{K}_i, K'_i | i \in B^-\}, \{\hat{K}_i, K'_i | i \in B^*\}, \{K_x\}_{x \in \psi}, \{|i \in B^+\}),$$

which is computed as follows:

$$\begin{array}{lll} K = g^r, & & \\ K_i = F_s(i)^r & & (i \in \psi) \\ \hat{K}_i = g^b \cdot F_s(i)^{-r_i}, & K'_i = g^{r_i} & (\forall i \in \psi \subset B^+) \\ \hat{K}_i = g^b \cdot F_s(i)^{-r_{i-k}}, & K'_i = g^{r_{i-k}} & (\forall i \in \psi \subset B^-) \\ \hat{K}_i = g^b \cdot F_s(i)^{-r_{i-2k}}, & K'_i = g^{r_{i-2k}} & (\forall i \in \psi \subset B^*). \end{array}$$

Encryption The inputs of the algorithm is a message $\mathcal{M}$, the public key pk, a pair of subjective policy $\mathbb{S}$ and objective attributes $\omega \subset U_s$. A ciphertext $CT = (\mathbb{S}, C, C_i, \hat{C}, \{C'_x\}_{x \in \omega})$ is computed for a randomly chosen s in $\mathbb{Z}_p$ as follows:

$$\begin{array}{lll} C = \mathcal{M} \cdot e(g,g)^{\gamma s}, & C_i = (\prod_{i \in \omega} g^a F_s(i))^{-s} & \\ \hat{C} = g^s, & C'_x = F_o(x)^s & (x \in \omega) \end{array}$$

Decrypt The inputs of the algorithm is a ciphertext CT embedded the subjective policy $\mathbb{S}$ and a set of objective attributes $\omega \subset U_s$, and a secret key sk embedded the objective policy $\mathbb{O}$ and a set of subjective attributes $\psi \subset U_o$. The constraint to decrypt is the message that the set of subjective attributes ψ must satisfy the subjective policy $\mathbb{S}$ and the set of objective attribute ω must satisfy the objective policy $\mathbb{O}$. Decryption is done by:

$$\begin{aligned} A &= e(C_i, K) \cdot e(\hat{C}, \prod_{i \in \omega} K_i) \\ &= e((\prod_{i \in \omega} g^a F_s(i))^{-s}, g^r) \cdot e(g^s, (\prod_{i \in \omega} F_s(i))^r) \\ &= e(g,g)^{-asr} \cdot e(\prod_{i \in \omega} F_s(i), g)^{-sr} \cdot e(\prod_{i \in \omega} F_s(i), g)^{sr} \\ &= e(g,g)^{-asr} \\ B &= e(\hat{C}, \prod_{i \in \psi} \hat{K}_i) \cdot e(\prod_{i \in \psi} C'_i, K'_i) \\ &= e(g^s, \prod_{i \in \psi} g^b F_o(i)^{-r_i}) \cdot e(\prod_{i \in \psi} F_o(i)^s, g^{r_i}) \\ &= e(g,g)^{bs} \cdot e(g, \prod_{i \in \psi} F_o(i))^{-sr_i} \cdot e(g, \prod_{i \in \psi} F_o(i))^{sr_i} \\ &= e(g,g)^{bs}. \end{aligned}$$

Then $\mathcal{M}$ can be recovered by using $b = \gamma + ar$.

$$\begin{aligned} A \cdot B &= e(g,g)^{-ars}.e(g,g)^{bs} \\ &= e(g,g)^{-ars} \cdot e(e,g)^{\gamma s} \cdot e(g,g)^{ars} \\ &= e(g,g)^{\gamma s} \\ \frac{C}{A \cdot B} &= \frac{\mathcal{M} \cdot e(g,g)^{\gamma s}}{e(g,g)^{\gamma s}} = \mathcal{M} \end{aligned}$$

Then we can recover $\mathcal{M}$.

$$\frac{C}{A \cdot B} = \frac{\mathcal{M} \cdot e(g,g)^{\gamma s}}{e(g,g)^{\gamma s}} = \mathcal{M}$$

The security proof is shown below:

Theorem 2 *Suppose the decisional BDH assumption holds. Then no polynomial time can break our DP-ABE 2 in the selective-set security notion.*

Proof: Let $\mathcal{A}$ be an adversary with an advantage $\epsilon = Adv_{\mathcal{A}}$ in attacking DP-ABE 2. We show how to build a simulator, $\mathcal{B}$, that plays the decisional BDH problem.

Init: The simulator takes in a decisional BDH challenge $\{\boldsymbol{y}, T\}$, where $\boldsymbol{y} = (g, g^x, g^y, g^s)$ and $T = e(g,g)^{xys}$ or a random element in $\mathbb{G}_T$. The adversary gives the algorithm a pair of challenge subjective access structure $\mathbb{S}^*$ and objective attributes ω^*. Let $|\omega^*| = n$, and $m =$ the number of elements in the AND gate access policy S^*, where $3m \leq q$.

Setup: $\mathcal{B}$ chooses random $\gamma' \in \mathbb{Z}_p$ and implicitly sets $\gamma = \gamma' + xy$ by letting $e(g,g)^{\gamma} = e(g,g)^{\gamma'} \cdot e(g^x, g^y)$. Then $\mathcal{B}$ chooses $d \in \mathbb{Z}_p$ randomly and computes by setting$a$ implicitly:

$$g^d (\prod_{j \in \mathbb{O}} g^{\alpha^{3k+1-j}})^{-1} = g^{d - \sum_{j \in \mathbb{O}} \alpha^{3k+1-j}} = g^a \text{ if } \omega^* \text{does not satisfy } \mathbb{O}.$$

$$g^d (\prod_{j \in \mathbb{S}^*} g^{\alpha^{3k+1-j}})^{-1} = g^{d - \sum_{j \in \mathbb{S}^*} \alpha^{3k+1-j}} = g^a \text{ if } \psi \text{ does not satisfy } \mathbb{S}^*.$$

$\mathcal{B}$ implicitly sets a function $F_s(x) = g^{p(x)}$ for a polynomial p in $\mathbb{Z}_p[x]$ with degree $m + 3k - 1$ as follows: set $3m + 3k + 1$ polynomials $p_0, \ldots, p_{3k+3m}$ in $\mathbb{Z}_p[x]$ with degree $m + 3k - 1$ to

$$p_i(x) = \begin{cases} ix \ (i \in [1, 3m]) \\ 0 \ \ (i \in [3m+1, 3m+3k]) \end{cases}$$

and p_0 is set randomly from $\mathbb{Z}_p[x]$. Then $\mathcal{B}$ sets

$$p(x) = \sum_{i=0}^{3k+3m} p_i(x), \ \ h_i = g_i^{p_i(x)} (i \in [0, 3k+m-1]).$$

Then, F_s satisfies

$$F_s(x) = \prod_{i=0}^{3k+m-1} h_i = g^{p(x)},$$

which can be explicitly computed $\mathcal{B}$.
Then set a function F_o as follows: For $f_i(x) = x - z_i$ with $z_i \in \{1, \cdots, 3k\}$ according to a set of attributes ω^*, set:

$$f(x) = \sum_{i=0}^{n-1} f_i(x),$$

which ensures that $f(x) = 0$ if and only if $x \in \omega^*$. Then let

$$F_o(x) = \prod_{i=0}^{n-1} g^{f_i(x)} = g^{f(x)},$$

and $t_i = g^{f_i(x)}$. The public key $pk = \{g, e(g,g)^\gamma, g^d, h_0, \ldots, h_{3m}, t_0, \ldots, t_{3m}\}$ is given to $\mathcal{A}$.
Phase 1: The adversary $\mathcal{A}$ submits a pair of objective access structure $\mathbb{O}$ and subjective attribute set ψ for private keys. Then, either condition that ψ does not satisfy $\mathbb{S}^*$ or ω^* does not satisfy $\mathbb{O}$ holds. We will prove 2 cases separately.
Case 1: ω^* does not satisfy $\mathbb{O}$.
The simulator randomly chooses $r, r_i \in \mathbb{Z}_p$ for $i = 1 \ldots k$. It then lets $K = g^r$ and $K_x = F_s(x)^r$ for all $x \in \psi$ and implicitly lets $b = a + \gamma \cdot r$. There must exist a j in ω^* such that: $j \in 1, \ldots, k$ and $j + k \in \mathbb{O}$ or $j \in k+1, \ldots, 2k$ and $j - k \in \mathbb{O}$.
Then, for all $i \in \omega^{*+}$ and $i + k \in \mathbb{O}$, generate:

$$\begin{aligned}\hat{K}_i &= g^\gamma g^{rdi} \prod_{j \in \mathbb{O}} (g^{3k+1-j+i})^{-1} g^{rdr_i} \prod_{j \in \mathbb{O}} (g^{3k+1-j})^{-r_i} g^{f(i)-r_i} \\ &= g^b F_o(i)^{-r_i} \\ K'_i &= g^{r_i}\end{aligned}$$

For all $i \in \omega^{*-}$ and $i - k \in \mathbb{O}$, generate:

$$\begin{aligned}\hat{K}_i &= g^\gamma g^{rdi} \prod_{j \in \mathbb{O}} (g^{3k+1-j+i})^{-1} g^{rdr_{i-k}} \prod_{j \in \mathbb{O}} (g^{3k+1-j})^{-r_{i-k}} g^{f(i)-r_{i-k}} \\ &= g^b F_o(i)^{-r_{i-k}} \\ K'_i &= g^{r_{i-k}}\end{aligned}$$

For all $i \in \omega^{**}$ and $i \notin \mathbb{O}$, generate:

$$\begin{aligned}\hat{K}_i &= g^\gamma g^{rdi} \prod_{j \in \mathbb{O}} (g^{3k+1-j+i})^{-1} g^{rdr_{i-2k}} \prod_{j \in \mathbb{O}} (g^{3k+1-j})^{-r_{i-2k}} g^{f(i)-r_{i-2k}} \\ &= g^b F_o(i)^{-r_{i-2k}} \\ K'_i &= g^{r_{i-2k}}\end{aligned}$$

Case 2: ψ does not satisfy $\mathbb{S}^*$.
The simulator k randomly chooses $r_i \in \mathbb{Z}_p$ for $i = 1 \ldots k$, sets $K = g^r$ for $r = r_1 + \ldots + r_k$, and implicitly sets $b = a + \gamma \cdot r$. There must exist a j in ψ such that $j \in 1, \ldots, k$ and $j + k \in \mathbb{S}^*$ or $j \in k+1, \ldots, 2k$ and $j - k \in \mathbb{S}^*$.
Then, for all $i \in \psi^+$ and $i + k \in \mathbb{S}^*$, generate:

$$\begin{aligned}\hat{K}_i &= g^{\gamma} g^{rd^i} \prod_{j\in\mathbb{S}^*}(g^{3k+1-j+i})^{-1} g^{rdr_i} \prod_{j\in\mathbb{S}^*}(g^{3k+1-j})^{-r_i} g^{f(i)-r_i}\\ &= g^b F_o(i)^{-r_i}\\ K'_i &= g^{r_i}\end{aligned}$$

For all $i \in \psi^-$ and $i - k \in \mathbb{S}^*$, generate:

$$\begin{aligned}\hat{K}_i &= g^{\gamma} g^{rdi} \prod_{j\in\mathbb{S}^*}(g^{3k+1-j+i})^{-1} g^{rdr_{i-k}} \prod_{j\in\mathbb{S}^*}(g^{3k+1-j})^{-r_{i-k}} g^{f(i)-r_{i-k}}\\ &= g^b F_o(i)^{-r_{i-k}}\\ K'_i &= g^{r_{i-k}}\end{aligned}$$

For all $i \in \psi^*$ and $i \notin \mathbb{S}^*$, generate:

$$\begin{aligned}\hat{K}_i &= g^{\gamma} g^{rd^i} \prod_{j\in\mathbb{S}^*}(g^{3k+1-j+i})^{-1} g^{rdr_{i-2k}} \prod_{j\in\mathbb{S}^*}(g^{3k+1-j})^{-r_{i-2k}} g^{f(i)-r_{i-2k}}\\ &= g^b F_o(i)^{-r_{i-2k}}\\ K'_i &= g^{r_{i-2k}}\end{aligned}$$

For all $x \in \psi$, compute:

$$K_x = g^{rp_o(x)} \prod_{j=1}^{k}(g^{r_i} \prod_{i=1}^{3k+3m} g^{p_i(x)}) = (g^r)^{p(x)} = F_s(x)^r.$$

Challenge: Finally, $\mathcal{A}$ gives two messages M_0 and M_1 to $\mathcal{B}$. The simulator flips a coin $\beta \in \{0, 1\}$ and outputs $C = M_\beta T \cdot e(g^s, g^{\alpha'})$ and $\hat{C} = g^s$ by using randomly chosen $s \in \mathbb{Z}_p$. As for other components C_i and C_x, output:

$$\begin{aligned}C_i &= (\prod_{i\in\mathbb{S}^*}(g^{sd})(\prod_{i\in\mathbb{S}^*}(g^{s^{3k+1-j}})(\prod_{i=1}^{3m}(g^{sp_i(x)}) = (\prod_{i\in\omega} g^a F_s(i))^{-s}\\ C_x &= (\prod_{i=1}^{3m} g^{f_i(x)})^s = F_o(x)^s.\end{aligned}$$

Phase 2: Repeat Phase 1.
Guess: The adversary will eventually output a guess β' of β. The simulator outputs 0 if $\beta' = \beta$, which means $T = e(g, g)^{xys}$ is guessed; otherwise, it outputs 1, which means that that T is guessed to be a random group element in $\mathbb{G}_T$.
When T is a tuple, the simulator $\mathcal{B}$ gives a perfect simulation so we obtain that:

$$Pr[\mathcal{B}(\boldsymbol{y}, T = e(g, g)^{xys}) = 0] = \frac{1}{2} + Adv_{\mathcal{A}}.$$

When T is a random group element, the message M_β is completely hidden from the adversary and we have $Pr[\mathcal{B}(\boldsymbol{y}, T = R) = 0] = \frac{1}{2}$. Therefore, $\mathcal{B}$ has advantage ϵ at least in attacking the decisional BDH problem. □

5 Conclusion

In this paper, two constant Dual Policy Attribute Based Encryption, DP-ABE 1 and DP-ABE 2 have been proposed. The ciphertext size of both our proposed schemes is constant to attributes and can support expressive access policies. The security of our proposals is based on a selective-ID attack. One open problem would be to construct DP-ABE secure against the adaptive adversary model.

References

1. Nuttapong Attrapadung and Hideki Imai. Dual-policy attribute based encryption. In Michel Abdalla, David Pointcheval, Pierre-Alain Fouque, and Damien Vergnaud, editors, *Applied Cryptography and Network Security*, volume 5536 of *Lecture Notes in Computer Science*, pages 168–185. Springer, 2009.
2. John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In *IEEE Symposium on Security and Privacy, S&P 2007*, pages 321–334. IEEE, 2007.
3. Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security*, CCS' 06, pages 89–98. ACM, 2006.
4. Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In Ronald Cramer, editor, *Advances in Cryptology-EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 457–473. Springer, 2005.
5. Brent Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *Public Key Cryptography-PKC 2011*, volume 6571 of *Lecture Notes in Computer Science*, pages 53–70. Springer, 2011.