A Ciphertext-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length

Keita Emura[1], Atsuko Miyaji[1], Akito Nomura[2],
Kazumasa Omote[1], and Masakazu Soshi[3]

[1] School of Information Science, Japan Advanced Institute of Science and Technology, 1-1, Asahidai, Nomi, Ishikawa, 923-1292, Japan
[2] Graduate School of Natural Science and Technology, Kanazawa University, Kakuma-machi, Kanazawa, Ishikawa, 920-1192, Japan
[3] Graduate School of Information Sciences, Hiroshima City University, 3-4-1 Ozuka-Higashi, Asa-Minami-Ku, Hiroshima, 731-3194, Japan
{k-emura, miyaji,omote}@jaist.ac.jp
anomura@t.kanazawa-u.ac.jp
soshi@hiroshima-cu.ac.jp

Abstract. An Attribute-Based Encryption (ABE) is an encryption scheme, where users with some attributes can decrypt ciphertexts associated with these attributes. However, the length of the ciphertext depends on the number of attributes in previous ABE schemes. In this paper, we propose a new Ciphertext-Policy Attribute-Based Encryption (CP-ABE) with constant ciphertext length. Moreover, the number of pairing computations is also constant.
keywords Attribute-based encryption, Ciphertext-Policy, Constant Ciphertext Length.

1 Introduction

A user identity (such as the name, e-mail address and so on) can be used for accessing control of some resources. For example, in Identity-Based Encryption (IBE) schemes such as [4, 6], an encryptor can restrict a decryptor to indicate the identity of the decryptor. An Attribute-Based Encryption (ABE) is an encryption scheme, where users with some attributes can decrypt the ciphertext associated with these attributes. The first ABE scheme has been proposed in [13], which is inspired by IBE. Although IBE schemes have a restriction such that an encryptor only indicates a single decryptor, in ABE schemes, an encryptor can indicate many decryptors by assigning common attributes of these decryptors such as gender, age, affiliation and so on. There are two kinds of ABE, Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE). KP-ABE [9, 13] are schemes such that each private key is associated with an access structure. CP-ABE [2, 7, 8, 12, 14] are schemes such that each ciphertext is associated with an access structure. This means that an encryptor can decide who should or should not be allowed to decrypt. However, in all previous ABE schemes [2, 7–9, 12–14], the length of the ciphertext depends on the number of attributes.

Also, the number of pairing computations depends on the number of attributes. A Predicate Encryption Scheme (PES), where secret keys correspond to predicates, and where ciphertexts are associated with attributes, has been proposed in [5,10]. It is shown that PES can be regarded as a kind of CP-ABE (see Appendix A and B in [12] for details). However, both the [5] and [10] schemes also have the same problems, in that the length of the ciphertext and the number of pairing computations are not constant.

Contribution. In this paper, for the first time we propose a CP-ABE with constant length of ciphertext and constant length of the number of pairing computations. The access structure used in our CP-ABE is constructed by AND-gates on multi-valued attributes. This is a subset of the access structures used in [7,12]. Although previous CP-ABE schemes [2, 7, 8, 12, 14] can complement our access structures, the length of the ciphertext depends on the number of attributes. This means that, until our work, to the best of our knowledge, there has been no scheme that enables a constant ciphertext length with AND-gates on multi-valued attributes.

Organization : The paper is organized as follows: Some definitions are presented in Section 2. The previous scheme is introduced in Section 3. Our scheme is described in Section 4. The security proof is presented in Section 5. Efficiency comparisons are made in Section 6.

2 Preliminary

In this section, some definitions are presented. Note that $x \in_R S$ means x is randomly chosen for a set S.

2.1 Bilinear Groups and Complexity Assumption

Definition 1. (**Bilinear Groups**) *Bilinear groups and a bilinear map are defined as follows:*

1. $\mathbb{G}_1$ *and* $\mathbb{G}_T$ *are cyclic groups of prime order* p.
2. g_1 *is a generator of* $\mathbb{G}_1$.
3. e *is an efficiently computable bilinear map* $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_T$ *with the following properties.*
   - *Bilinearity : for all* $u, u', v, v' \in \mathbb{G}_1$, $e(uu', v) = e(u, v)e(u', v)$ *and* $e(u, vv') = e(u, v)e(u, v')$.
   - *Non-degeneracy :* $e(g_1, g_1) \neq 1_{\mathbb{G}_T}$ ($1_{\mathbb{G}_T}$ *is the* $\mathbb{G}_T$*'s unit*).

Definition 2. (**DBDH assumption**)

The Decision Bilinear Diffie-Hellman (DBDH) problem in $\mathbb{G}_1$ *is a problem, for input of a tuple* $(g_1, g_1^a, g_1^b, g_1^c, Z) \in \mathbb{G}_1^4 \times \mathbb{G}_T$ *to decide* $Z = e(g_1, g_1)^{abc}$ *or not. An algorithm* $\mathcal{A}$ *has advantage* ϵ *in solving DBDH problem in* $\mathbb{G}_1$ *if* $Adv_{DBDH}(\mathcal{A}) := |\Pr[\mathcal{A}(g_1, g_1^a, g_1^b, g_1^c, e(g_1, g_1)^{abc}) = 0] - \Pr[\mathcal{A}(g_1, g_1^a, g_1^b, g_1^c, e(g_1, g_1)^z) = 0]| \geq \epsilon(\kappa)$, *where* $e(g_1, g_1)^z \in \mathbb{G}_T \setminus \{e(g_1, g_1)^{abc}\}$. *We say that the DBDH assumption holds in* $\mathbb{G}_1$ *if no PPT algorithm has an advantage of at least* ϵ *in solving the DBDH problem in* $\mathbb{G}_1$.

2.2 Definition of Access Structures

Several access structures such as the threshold structure [13], the tree-based access structure [2, 8], AND-gates on positive and negative attributes with wildcards [7], AND-gates on multi-valued attributes with wildcards [12], and the linear access structure [14] are used in previous ABE schemes. In our scheme, the sum of master keys are used to achieve the constant ciphertext length. Therefore, we use AND-gates on multi-valued attributes (which can be represented by using the sum of master keys) as follows:

Definition 3. *Let $\mathcal{U} = \{att_1, \ldots, att_n\}$ be a set of attributes. For $att_i \in \mathcal{U}$, $S_i = \{v_{i,1}, v_{i,2}, \ldots, v_{i,n_i}\}$ is a set of possible values, where n_i is the number of possible values for att_i. Let $L = [L_1, L_2, \ldots, L_n]$, $L_i \in S_i$ be an attribute list for a user, and $W = [W_1, W_2, \ldots, W_n]$, $W_i \in S_i$ be an access structure. The notation $L \models W$ expresses that an attribute list L satisfies an access structure W, namely, $L_i = W_i$ $(i = 1, 2, \ldots, n)$.*

The number of access structures is $\prod_{i=1}^{n} n_i$. For each att_i, an encryptor has to *explicitly* indicate a status $v_{i,*}$ from $S_i = \{v_{i,1}, v_{i,2}, \ldots, v_{i,n_i}\}$.

Differences between the previous AND-gate structures [7, 12] and ours

If $n_i = 2$ $(i = 1, 2, \ldots, n)$, then our structure is the same as the access structures [7] excluding wildcards. In [12], an access structure W is defined as $W = [W_1, W_2, \ldots, W_n]$ for $W_i \subseteq S_i$, and $L \models W$ is defined as $L_i \in W_i$ $(i = 1, 2, \ldots, n)$. This means that our access structure is a subset of these in [7, 12]. However, even if previous CP-ABE schemes [7, 12] use our access structure, then the length of the ciphertext depends on the number of attributes.

2.3 Ciphertext-Policy Attribute-Based Encryption Scheme (CP-ABE)

CP-ABE is described using four algorithms, Setup, KeyGen, Encrypt and Decrypt [7].

Definition 4. *CP-ABE*

Setup: *This algorithm takes as input the security parameter κ, and returns a public key PK and a master secret key MK.*

KeyGen: *This algorithm takes as input PK, MK and a set of attributes L, and returns a secret key SK_L associated with L.*

Encrypt: *This algorithm takes as input PK, a message M and an access structure W. It returns a ciphertext C with the property that a user with SK_L can decrypt C if and only if $L \models W$.*

Decrypt: *This algorithm takes as input PK, C which was encrypted by W, and SK_L. It returns M if SK_L is associated with $L \models W$.*

2.4 Selective Game for CP-ABE

We use the definition of "Selective Game" for CP-ABE [7]. This CP-ABE game captures the indistinguishability of messages and the collusion-resistance of secret keys, namely, attackers cannot generate a new secret key by combining their secret keys. To capture the collusion-resistance, multiple secret key queries can be issued by the adversary $\mathcal{A}$ after the challenge phase. This means that $\mathcal{A}$ can issue the KeyGen queries L_1 and L_2 such as $(L_1 \not\models W^*) \wedge (L_2 \not\models W^*)$ and $(L_1 \cup L_2) \models W^*$. This collusion-resistance is an important property of CP-ABE scheme, which has not been considered in the Hierarchical IBE (HIBE) scheme such as [3].

Definition 5. *Selective Game for CP-ABE*

Init: *The adversary $\mathcal{A}$ sends the challenge access structure W^* to the challenger.*
Setup: *The challenger runs* Setup *and* KeyGen*, and gives PK to $\mathcal{A}$.*
Phase 1: *$\mathcal{A}$ sends an attribute list L to the challenger for a* KeyGen *query, where $L \not\models W^*$. The challenger answers with a secret key for these attributes. Note that these queries can be repeated adaptively.*
Challenge: *$\mathcal{A}$ sends two equal-length messages M_0 and M_1 to the challenger. The challenger chooses $\mu \in_R \{0,1\}$, and runs $C^* = \mathsf{Encrypt}(PK, M_\mu, W^*)$. The challenger gives the challenge ciphertext C^* to $\mathcal{A}$.*
Phase 2: *Same as Phase 1. $\mathcal{A}$ sends L to the challenger for a* KeyGen *query. The challenger answers with a secret key for these attributes. Note that $L \not\models W^*$, and these queries can be repeated adaptively.*
Guess: *$\mathcal{A}$ outputs a guess $\mu' \in \{0,1\}$.*

The advantage of $\mathcal{A}$ is defined as $Adv(\mathcal{A}) := |\Pr(\mu' = \mu) - \frac{1}{2}|$.

3 The Previous CP-ABE

In this section, we summarize the previous CP-ABE [7]. Let $\bar{\mathcal{U}} = \{\neg att_1, \ldots, \neg att_n\}$ a set of negative attributes for a set of attributes $\mathcal{U}$. We refer to attributes $att_i \in \mathcal{U}$ and their negations $\neg att_i$ as literals. Let $W = \bigwedge_{att_i \in I} a\bar{t}t_i$ be an access structure, where $I \subseteq \mathcal{U}$ and $a\bar{t}t_i$ is either att_i or $\neg att_i$. The public key elements T_i, T_{n+i}, T_{2n+i} correspond to the three properties of att_i, namely, *positive*, *negative* and *don't care*.

Protocol 1. *CP-ABE [CN07] [7]*

Setup(1^κ): *A trusted authority TA chooses a prime number p, a bilinear group $\mathbb{G}_1$ with order p, a generator $g_1 \in \mathbb{G}_1$, $y \in_R \mathbb{Z}_p$ and $t_i \in_R \mathbb{Z}_p$ $(i = 1, 2, \ldots, 3n)$, and computes $Y = e(g_1, g_1)^y$ and $T_i = g_1^{t_i}$ $(i = 1, 2, \ldots, 3n)$. TA outputs $PK = (e, g_1, Y, T_1, \ldots, T_{3n})$ and $MK = (y, t_1, \ldots, t_{3n})$.*

KeyGen(PK, MK, S): *Every* $att_i \notin S$ *is implicitly considered to be a negative attribute.* TA *chooses* $r_i \in_R \mathbb{Z}_p$ $(i = 1, 2, \ldots, n)$*, sets* $r = \sum_{i=1}^{n} r_i$*, and computes* $\hat{D} = g_1^{y-r}$*.* TA *computes* D_i *and* F_i *as follows:*

$$D_i = \begin{cases} g_1^{\frac{r_i}{t_i}} & (att_i \in S) \\ g_1^{\frac{r_i}{t_{n+i}}} & (att_i \notin S) \end{cases}, \quad F_i = g_1^{\frac{r_i}{t_{2n+i}}} \; (att_i \in \mathcal{U})$$

TA *outputs* $SK = (\hat{D}, \{D_i, F_i\}_{i \in [1,n]})$.

Encrypt(PK, M, W): *Let* $W = \bigwedge_{att_i \in I} a\bar{t}t_i$*. An encryptor chooses* $s \in_R \mathbb{Z}_p$*, and computes* $\tilde{C} = M \cdot Y^s$ *and* $\hat{C} = g_1^s$*. The encryptor computes* C_i *as follows:*

$$C_i = \begin{cases} T_i^s & (a\bar{t}t_i = att_i) \\ T_{n+i}^s & (a\bar{t}t_i = \neg att_i) \\ T_{2n+i}^s & (att_i \in \mathcal{U} \setminus I) \end{cases}$$

The encryptor outputs $C = (W, \tilde{C}, \hat{C}, \{C_i\}_{i \in [1,n]})$.

Decrypt(PK, C, SK): *A decryptor computes the pairing* $e(C_i, D_i)$ $(att_i \in I)$ *and* $e(C_i, F_i)$ $(att_i \notin I)$ *as follows:*

$$e(C_i, D_i) = \left\{ \begin{array}{ll} e(g_1^{t_i \cdot s}, g_1^{\frac{r_i}{t_i}}) & (a\bar{t}t_i = att_i) \\ e(g^{t_{n+i} \cdot s}, g_1^{\frac{r_i}{t_{n+i}}}) & (a\bar{t}t_i = \neg att_i) \end{array} \right\} = e(g_1, g_1)^{r_i \cdot s} \; (att_i \in I)$$

$$e(C_i, F_i) = e(g_1^{t_{2n+i} \cdot s}, g_1^{\frac{r_i}{t_{2n+i}}}) = e(g, g)^{r_i \cdot s} \; (att_i \notin I)$$

Then $\tilde{C} / (e(\hat{C}, \hat{D}) \prod_{i=1}^{n} e(g_1, g_1)^{r_i \cdot s}) = M \cdot e(g_1, g_1)^{sy} / e(g_1, g_1)^{s(y-r)} e(g_1, g_1)^{sr} = M$ *holds.*

To compute $e(g_1, g_1)^{sr}$, the decryptor has to compute either $e(C_i, D_i)$ or $e(C_i, F_i)$ for each i. This means that all C_i are included in a ciphertext, and thus the length of a ciphertext depends on the number of attributes. This scheme does not provide for adding new attributes after Setup. If some attributes are added after Setup, then some users who have already obtained the secret key can decrypt a ciphertext which one must not be able to decrypt. For example, let $\mathcal{U} = \{att_1, att_2\}$, and assume that a user U has secret keys of att_1 and att_2, and that a ciphertext C is associated with $W = att_1 \wedge att_2$. Then, U can decrypt a ciphertext associated with $att_1 \wedge att_2 \wedge att_3$ without a secret key of att_3. Concretely, U ignores a part of the ciphertext for att_3. CP-ABE schemes which enable the addition of new attributes after Setup have been proposed in BSW07 [2] and NYO08 [12] (which is the second construction of the NYO08 paper). If a user wants to decrypt a ciphertext with an access structure including newly added attributes, then the user must obtain a new secret key (including newly added attributes) from the trusted authority again. However, the security proof of both schemes contains no reduction, namely, it is proven under the generic group heuristic.

4 Our construction

In this section, we propose a constant ciphertext length CP-ABE with a function of adding new attributes after Setup. Let $\mathbb{G}_1$ and $\mathbb{G}_T$ be cyclic groups of prime order p and $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$ be a bilinear map. Let $\mathcal{U} = \{att_1, \ldots, att_n\}$ be a set of attributes; $S_i = \{v_{i,1}, v_{i,2}, \ldots, v_{i,n_i}\}$ be a set of possible values with $n_i = |S_i|$; $L = [L_1, L_2, \ldots, L_n]$ $(L_i \in S_i)$ be an attribute list for a user; and $W = [W_1, W_2, \ldots, W_n]$ $(W_i \in S_i)$ be an access structure.

4.1 Proposed scheme

Protocol 2. ***Our CP-ABE Scheme with Constant Ciphertext Length***

Setup(1^κ)**:** *A trusted authority TA chooses a prime number p, a bilinear group $(\mathbb{G}_1, \mathbb{G}_T)$ with order p, a generator $g_1 \in \mathbb{G}_1$, $h \in \mathbb{G}_1$, $y \in_R \mathbb{Z}_p$ and $t_{i,j} \in_R \mathbb{Z}_p$ $(i \in [1,n], j \in [1,n_i])$. TA computes $Y = e(g_1,h)^y$ and $T_{i,j} = g_1^{t_{i,j}}$ $(i \in [1,n], j \in [1,n_i])$. TA outputs $PK = (e, g_1, h, Y, \{T_{i,j}\}_{i\in[1,n],j\in[1,n_i]})$ and $MK = (y, \{t_{i,j}\}_{i\in[1,n],j\in[1,n_i]})$. Note that $\forall L, L'$ $(L \neq L')$, $\sum_{v_{i,j}\in L} t_{i,j} \neq \sum_{v_{i,j}\in L'} t_{i,j}$ is assumed*

KeyGen(PK, MK, L)**:** *TA chooses $r \in_R \mathbb{Z}_p$, outputs $SK_L = (h^y (g_1^{\sum_{v_{i,j}\in L} t_{i,j}})^r, g_1^r)$, and gives SK_L to a user with L.*

Encrypt(PK, M, W)**:** *An encryptor chooses $s \in_R \mathbb{Z}_p$, and computes $C_1 = M \cdot Y^s$, $C_2 = g_1^s$ and $C_3 = (\prod_{v_{i,j}\in W} T_{i,j})^s$. The encryptor outputs $C = (W, C_1, C_2, C_3)$.*

Decrypt(PK, C, SK_L)**:** *A decryptor computes what follows:*

$$\frac{C_1 \cdot e(C_3, g_1^r)}{e(C_2, h^y (g_1^{\sum_{v_{i,j}\in L} t_{i,j}})^r)} = \frac{M \cdot e(g,h)^{sy} e(g_1,g_1)^{sr \sum_{v_{i,j}\in W} t_{i,j}}}{e(g_1,h)^{sy} e(g_1,g_1)^{sr \sum_{v_{i,j}\in L} t_{i,j}}} = M$$

4.2 Construction of secret keys $t_{i,j}$

In our scheme, $\sum_{v_{i,j}\in L} t_{i,j} \neq \sum_{v_{i,j}\in L'} t_{i,j}$ is assumed. If there exist L and L' $(L \neq L')$ such that $\sum_{v_{i,j}\in L} t_{i,j} = \sum_{v_{i,j}\in L'} t_{i,j}$, a user with the attribute list L' can decrypt a ciphertext associated with W, where $L' \not\models W$ and $L \models W$. Remark that the assumption holds with overwhelming probability $\frac{p(p-1)\cdots(p-(N-1))}{p^N} > \frac{(p-(N-1))^N}{p^N} = (1 - \frac{N-1}{p})^N > 1 - \frac{N(N-1)}{p} > 1 - \frac{N^2}{p}$, where $N := \prod_{i=1}^n n_i$. Therefore, if each secret key $t_{i,j}$ is chosen at random from $\mathbb{Z}_p$, then our assumption is natural.

5 Security Analysis

Theorem 1. *Our scheme satisfies the indistinguishability of messages under the DBDH assumption.*

Proof. We suppose that the adversary $\mathcal{A}$ wins the selective game for CP-ABE with the advantage ϵ. Then we can construct an algorithm $\mathcal{B}$ that breaks the DBDH assumption with the advantage $\frac{\epsilon}{2}(1 - \frac{N^2}{p})$, where $N := \prod_{i=1}^{n} n_i$ is the number of expressed access structures. The DBDH challenger selects $a, b, c, z \in_R \mathbb{Z}_p$, $\nu \in_R \{0, 1\}$, and g_1, where $\langle g_1 \rangle = \mathbb{G}_1$. If $\nu = 0$, then $Z = e(g_1, g_1)^{abc}$. Otherwise, if $\nu = 1$, then $Z = e(g_1, g_1)^z$. The DBDH challenger gives the DBDH instance $(g_1, g_1^a, g_1^b, g_1^c, Z) \in \mathbb{G}_1^4 \times \mathbb{G}_T$ to $\mathcal{B}$. First, $\mathcal{B}$ is given the challenge access structure W^* from $\mathcal{A}$. Let $W^* = [W_1^*, \ldots, W_n^*]$. $\mathcal{B}$ selects $u \in_R \mathbb{Z}_p^*$, and sets $h = g_1^u$ and $Y = e(g_1^a, (g_1^b)^u) = e(g_1, h)^{ab}$. Moreover, $\mathcal{B}$ selects $t'_{i,j} \in_R \mathbb{Z}_p$ ($i \in [1, n], j \in [1, n_i]$), and sets $t_{i,j} = t'_{i,j}$ (in the case where $v_{i,j} = W_i^*$) and $t_{i,j} = bt'_{i,j}$ (in the case where $v_{i,j} \neq W_i^*$), and computes public keys $T_{i,j}$ ($i \in [1, n], j \in [1, n_i]$) as follows:

$$T_{i,j} = g_1^{t_{i,j}} = \begin{cases} g_1^{t'_{i,j}} & (v_{i,j} = W_i^*) \\ (g_1^b)^{t'_{i,j}} & (v_{i,j} \neq W_i^*) \end{cases}$$

$\mathcal{B}$ gives $PK = (e, g_1, h, Y, \{T_{i,j}\}_{i \in [1,n], j \in [1,n_i]})$ to $\mathcal{A}$. For KeyGen query L, there exists $v_{i,\ell}$ such that $v_{i,\ell} = L_i \wedge v_{i,\ell} \neq W_i^*$, since $L \not\models W^*$. Therefore, $\sum_{v_{i,j} \in L} t_{i,j}$ can be represented as $\sum_{v_{i,j} \in L} t_{i,j} = T_1 + bT_2$, where $T_1, T_2 \in \mathbb{Z}_p$. Note that both T_1 and T_2 are represented by the sum of $t'_{i,j}$. Therefore, $\mathcal{B}$ can compute T_1 and T_2. $\mathcal{B}$ chooses $\beta \in_R \mathbb{Z}_p$, sets $r := \frac{\beta - ua}{T_2}$, and computes $SK_L = ((g_1^b)^\beta g_1^{\frac{T_1}{T_2}\beta} (g_1^a)^{-\frac{T_1 u}{T_2}}, g_1^{\frac{\beta}{T_2}} (g_1^a)^{-\frac{u}{T_2}})$. We show that SK_L is a valid secret key as follows:

$$\begin{aligned} (g_1^b)^\beta g_1^{\frac{T_1}{T_2}\beta} (g_1^a)^{-\frac{T_1 u}{T_2}} &= g_1^{uab} \cdot g_1^{-uab} (g_1^b)^\beta g_1^{\frac{T_1}{T_2}\beta} (g_1^a)^{-\frac{T_1 u}{T_2}} \\ &= g_1^{uab} \cdot g_1^{\frac{T_1}{T_2}(\beta - ua)} \cdot g_1^{b(\beta - ua)} \\ &= g_1^{uab} (g_1^{T_1} \cdot g_1^{bT_2})^{\frac{\beta - ua}{T_2}} \\ &= g_1^{uab} (g_1^{T_1 + bT_2})^{\frac{\beta - ua}{T_2}} \\ &= h^y (g_1^{\sum_{v_{i,j} \in L} t_{i,j}})^r, \end{aligned}$$

and

$$g_1^{\frac{\beta}{T_2}} (g_1^a)^{-\frac{u}{T_2}} = g_1^{\frac{\beta - ua}{T_2}} = g_1^r$$

If $T_2 = 0 \bmod p$, then $\mathcal{B}$ aborts. If $T_2 = 0 \bmod p$ holds, then there exists L such that $\sum_{v_{i,j} \in L} t_{i,j} = \sum_{v_{i,j} \in W^*} t_{i,j}$ holds. Therefore, this probability is at

Table 1. Size of each value

	PK	MK	SK	Ciphertext
SW05 [13]	$n\|\mathbb{G}_1\| + \|\mathbb{G}_T\|$	$(n+1)\|\mathbb{Z}_p\|$	$r_2\|\mathbb{G}_1\|$	$r_1\|\mathbb{G}_1\| + \|\mathbb{G}_T\|$
GPSW06 [9]	$n\|\mathbb{G}_1\| + \|\mathbb{G}_T\|$	$(n+1)\|\mathbb{Z}_p\|$	$r_2\|\mathbb{G}_1\|$	$r_1\|\mathbb{G}_1\| + \|\mathbb{G}_T\|$
CN07 [7]	$(3n+1)\|\mathbb{G}_1\| + \|\mathbb{G}_T\|$	$(3n+1)\|\mathbb{Z}_p\|$	$(2n+1)\|\mathbb{G}_1\|$	$(n+1)\|\mathbb{G}_1\| + \|\mathbb{G}_T\|$
BSW07 [2]	$3\|\mathbb{G}_1\| + \|\mathbb{G}_T\|$	$\|\mathbb{Z}_p\| + \|\mathbb{G}\|$	$(2n+1)\|\mathbb{G}_1\|$	$(2r_2+1)\|\mathbb{G}_1\| + \|\mathbb{G}_T\|$
NYO08 [12]	$(2N'+1)\|\mathbb{G}_1\| + \|\mathbb{G}_T\|$	$(2N'+1)\|\mathbb{Z}_p\|$	$(3n+1)\|\mathbb{G}_1\|$	$(2N'+1)\|\mathbb{G}_1\| + \|\mathbb{G}_T\|$
W08 [14]	$2\|\mathbb{G}_1\| + \|\mathbb{G}_T\|$	$\|\mathbb{G}_1\|$	$(1+n+r_2)\|\mathbb{G}_1\|$	$(1+r_1 n)\|\mathbb{G}_1\| + \|\mathbb{G}_T\|$
Our scheme	$(2N'+3)\|\mathbb{G}_1\| + \|\mathbb{G}_T\|$	$(N'+1)\|\mathbb{Z}_p\|$	$2\|\mathbb{G}_1\|$	$2\|\mathbb{G}_1\| + \|\mathbb{G}_T\|$

Table 2. Computational time of each algorithm

	Enc.	Dec.
SW05 [13]	$r_1\mathbb{G}_1 + 2\mathbb{G}_T$	$r_1 C_e + (r_1+1)\mathbb{G}_T$
GPSW06 [9]	$r_1\mathbb{G}_1 + 2\mathbb{G}_T$	$r_1 C_e + (r_1+1)\mathbb{G}_T$
CN07 [7]	$(n+1)\mathbb{G}_1 + 2\mathbb{G}_T$	$(n+1)C_e + (n+1)\mathbb{G}_T$
BSW07 [2]	$(2r_1+1)\mathbb{G}_1 + 2\mathbb{G}_T$	$2r_1 C_e + (2r_1+2)\mathbb{G}_T$
NYO08 [12]	$(2N'+1)\mathbb{G}_1 + 2\mathbb{G}_T$	$(3n+1)C_e + (3n+1)\mathbb{G}_T$
W08 [14]	$(1+3r_1 n)\mathbb{G}_1 + 2\mathbb{G}_T$	$(1+n+r_1)C_e + (3r_1-1)\mathbb{G}_1 + 3\mathbb{G}_T$
Our scheme	$(n+1)\mathbb{G}_1 + 2\mathbb{G}_T$	$2C_e + 2\mathbb{G}_T$

most $\frac{N^2}{p}$. See Section 4.2 for details. For the challenge ciphertext, $\mathcal{B}$ chooses $\mu \in_R \{0,1\}$, computes $C_1^* = M_\mu \cdot Z^u$, $C_2^* = g_1^c$ and $C_3^* = (g_1^c)^{\sum_{v_{i,j} \in W^*} t'_{i,j}}$, and sends (C_1^*, C_2^*, C_3^*) to $\mathcal{A}$. Finally, $\mathcal{A}$ outputs $\mu' \in \{0,1\}$. $\mathcal{B}$ outputs 1 if $\mu' = \mu$, or outputs 0 if $\mu' \neq \mu$. If $Z = e(g_1, g_1)^{abc}$, then (C_1^*, C_2^*, C_3^*) is a valid ciphertext associated with W^*. Therefore, $\mathcal{A}$ has the advantage ϵ. Hence, $\Pr[\mathcal{B} \to 1 | Z = e(g_1, g_1)^{abc}] = \Pr[\mu' = \mu | Z = e(g_1, g_1)^{abc}] = \frac{1}{2} + \epsilon$. Otherwise, if $Z = e(g_1, g_1)^z$, $\mathcal{A}$ has no advantage to distinguish a bit μ, since all parts of the challenge ciphertext when $\mu = 0$ and when $\mu = 1$ have the same distributions. Hence, $\Pr[\mathcal{B} \to 0 | Z = e(g_1, g_1)^z] = \Pr[\mu' \neq \mu | Z = e(g_1, g_1)^z] = \frac{1}{2}$. It follows that $\mathcal{B}$'s advantage in the DBDH game is $\frac{\epsilon}{2}(1 - \frac{N^2}{p})$. □

Although a symmetric bilinear map is required in this proof, our scheme can be proven with an asymmetric bilinear map such as the Weil or Tate pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ over MNT curves [11], where $\mathbb{G}_1$ and $\mathbb{G}_2$ are distinct groups. Then the indistinguishability of messages can be proven under the DBDH assumption over $\mathbb{G}_2$ [1].

6 Comparison

Let PK, MK, SK and Ciphertext be the size of the public key, of the master key, of the secret key, and the ciphertext length excluding the access structure, respectively. Moreover, Enc. and Dec. are the computational times of encryption and decryption, respectively. We use the terms DBDH, DMBDH [13] and

Table 3. Some properties of ABE schemes

	Policy	Recipient Anonymity	Assumption
SW05 [13]	Key	No	DMBDH
GPSW06 [9]	Key	No	DBDH
CN07 [7]	Ciphertext	No	DBDH
BSW07 [2]	Ciphertext	No	Generic Group Model
NYO08 [12]	Ciphertext	Yes	DBDH, D-Linear
W08 [14]	Ciphertext	No	DBDH
Our scheme	Ciphertext	No	DBDH

Table 4. Expressiveness of policy

SW05 [13]	Threshold Structure
GPSW06 [9]	Tree-based Structure
CN07 [7]	AND-gates on positive and negative attributes with wildcards
BSW07 [2]	Tree-Based Structure
W08 [14]	Linear Structure
NYO08 [12]	AND-gates on multi-valued attributes with wildcards
Our scheme	AND-gates on multi-valued attributes

Table 5. Performance Results for $n = 3$

	Enc. Time	Dec. Time
CN07 [7]	0.028sec	0.031sec
NYO08 [12]	0.032sec	0.078sec
Our scheme	0.015sec	0.015sec

D-Linear [12] to refer to the Decision Bilinear Diffie-Hellman assumption, the Decision Modified Bilinear Diffie-Hellman assumption and the Decision Linear assumption, respectively. The notation $|\mathbb{G}|$ is the bit-length of the element which belongs to $\mathbb{G}$. Let the notations $k\mathbb{G}$ and kC_e (where $k \in \mathbb{Z}_{>0}$) be the k-times calculation over the group $\mathbb{G}$ and pairing, respectively. Let $\mathcal{U} = \{att_1, att_2, \ldots, att_n\}$ be the set of attributes. Let γ_1 ($|\gamma_1| = r_1$) be a set of attributes associated with the ciphertext, and γ_2 ($|\gamma_2| = r_2$) a set of attributes associated with the secret key. Actually, γ_2 is different for each user. Let $N' := \sum_{i=1}^{n} n_i$ be the total number of possible statements of attributes. The computational time over $\mathbb{Z}_p$ is ignored as usual.

Our scheme is efficient in that the ciphertext length and the costs of decryption do not depend on the number of attributes. Especially, the number of pairing computations is constant. No previous schemes provide these properties. An access structure is constructed by AND-gates on multi-valued attributes defined in section 2.2, which is a subset of the access structures in [12]. Although previous CP-ABE schemes [2, 7, 8, 12, 14] can complement our access structures, the length of the ciphertext depends on the number of attributes. To the best of our knowledge, our scheme is the first constant ciphertext length CP-ABE with

AND-gates on multi-valued attributes. In future work, we plan to construct a CP-ABE with both a constant ciphertext length and more flexible structures, such as linear structures.

Our scheme does not provide recipient anonymity. Some parts of a ciphertext for attributes $(C_2, C_3) = (g_1^s, g_1^{s\sum_{v_{i,j} \in W} t_{i,j}})$ is a DDH (Decision Diffie-Hellman)-tuple. Therefore, some information about attributes is exposed. Concretely, for an access structure W', an attacker can run the DDH test $e(C_2, \prod_{v_{i,j} \in W'} T_{i,j}) \stackrel{?}{=} e(C_3, g_1)$. Then, the attacker can determine whether an encryptor used the policy W' or not. We expect that our scheme will enable the property of the hidden encryptor-specified policies when a DDH-hard bilinear group is applied. However, we could not give the proof of security. Added to this, our scheme is inefficient in that the size of public key grows linearly with the number of attributes. There are rooms for argument on these points.

The CN07 scheme [7], the NYO08 scheme [12] and ours are implemented with *the same access structure* $\{v_{1,1}, v_{2,1}, v_{3,1}\}$, by using the Pairing-Based Cryptography (PBC) Library ver. 0.4.18 [**?**]. The performance results are shown in Table 5. Our experiment was performed by using a PC with an Intel(R) Core(TM)2 Duo CPU P8400 2.26GHz Windows Vista Home Premium Edition Service Pack 1. The execution of our scheme takes a very small amount of time, which is quite feasible for practical implementation. When $n = 3$, our decryption algorithm is approximately twice as fast as that of the CN07 scheme, and approximately five times faster than that of the NYO08 scheme.

7 Conclusion

In this paper, we propose a constant ciphertext length CP-ABE with AND-gates on multi-valued attributes. Moreover, the number of pairing computations is also constant. To the best of our knowledge, this is the first such construction.

References

1. M. Abdalla, A.W. Dent, J. M. Lee, G. Neven, D.H. Phan, and N. Smart. Identity-based traitor tracing. In *Proc. PKC 2007*, pages 361–367. Springer-Verlag LNCS 4450, January 2007.
2. J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *IEEE Symposium on Security and Privacy*, pages 321–334, 2007.
3. D. Boneh, X. Boyen, and E. Goh. Hierarchical identity based encryption with constant size ciphertext. In *EUROCRYPT*, page 440, 2005.
4. D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. pages 213–229. Springer-Verlag, 2001.
5. D. Boneh and B. Waters. Conjunctive, subset, and range queries on encrypted data. In *TCC*, pages 535–554, 2007.
6. X. Boyen and B. Waters. Anonymous hierarchical identity-based encryption (without random oracles). In *In CRYPTO*, pages 290–307. Springer-Verlag, 2006.

7. L. Cheung and C. Newport. Provably secure ciphertext policy abe. In *CCS '07: Proceedings of the 14th ACM conference on Computer and communications security*, pages 456–465, New York, NY, USA, 2007. ACM.
8. V. Goyal, A. Jain, O. Pandey, and A. Sahai. Bounded ciphertext policy attribute based encryption. In *The 35th International Colloquium on Automata, Languages and Programming, ICALP*, pages 579–591, 2008.
9. V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *ACM Conference on Computer and Communications Security*, pages 89–98, 2006.
10. J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In *EUROCRYPT*, pages 146–162, 2008.
11. A. Miyaji, M. Nakabayashi, and S. Takano. New explicit conditions of elliptic curve traces for fr-reduction. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 84(5):1234–1243, 2001.
12. T. Nishide, K. Yoneyama, and K. Ohta. Attribute-based encryption with partially hidden encryptor-specified access structures. In *ACNS*, pages 111–129, 2008.
13. A. Sahai and B. Waters. Fuzzy identity-based encryption. In *EUROCRYPT*, pages 457–473, 2005.
14. B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *Cryptology ePrint report 2008/290, September 1*, 2008.