Improving Privacy-Preserving CP-ABE with Hidden Access Policy

Leyou Zhang[1], Yilei Cui[1(✉)], and Yi Mu[2]

[1] School of Mathematics and Statistics, Xidian University, Xi'an 710071, Shaanxi, China
xidianzhangly@126.com, CYL_Study@163.com
[2] School of Computer Science and Software Engineering, University of Wollongong, Wollongong, NSW 2522, Australia
ymu@uow.edu.au

Abstract. User's privacy-preserving has become an urgent problem with the rapid development of cloud technologies. Anonymous ciphertext-policy Attribute Based Encryption (CP-ABE) not only protects the security of data, but also ensures that the privacy of the data user is not compromised. However, most of the known schemes have some shortcomings where those schemes either cannot achieve compact security or are inefficient in Encryption and Decryption. Additionally, recent works show the reality of the anonymity in some proposed schemes is doubtful. To address the problems above, we use the double exponent technique to construct an anonymous CP-ABE scheme which is more compact than the results at present. The proposed scheme with hidden access policy works in prime order groups. Meanwhile, we prove the security of our scheme under the decisional n-BDHE and decisional linear assumption.

Keywords: Privacy preserving · Cloud storage · Anonymity
Hidden access policy

1 Introduction

As an extension and development of cloud computing, cloud storage has solved the problems in big data storage and sharing, which allows users to store their data in cloud server and access data whenever and wherever through any networked device linking to the cloud. However, security and privacy problems are more and more serious at present. No users would like to share their documents containing sensitive information to a public cloud with no guarantee for security or privacy. It means that more flexible cryptosystem is demanded, where security and privacy protection must be both considered. Attribute-based encryption is one of the encryption techniques which can meet this requirement.

In 2005, Sahai and Waters introduced Attribute Based Encryption (ABE) [1], firstly. In attribute-based encryption, the ciphertext and decryption key are generated by the collection of attributes and data owner can establish a specific access control policy to limit who can decrypt the encrypted data. There are two categories of ABE schemes [2], one is ciphertext-policy ABE (CP-ABE) where user's attributes are used for key

X. Sun et al. (Eds.): ICCCS 2018, LNCS 11065, pp. 596–605, 2018.
https://doi.org/10.1007/978-3-030-00012-7_54

generation and the ciphertext is associated with a specific access policy, the other is the key-policy ABE (KP-ABE), in which the user can only decrypt encrypted data when his attributes satisfy the access policy embedded in the secret key. Because of the favorable feature of enabling data owner to set specific access policies to control who can decrypt the encrypted data, CP-ABE provides a novel way to solve the problem above. In 2007, Bethencourt et al. [3] proposed the first CP-ABE scheme with tree-access polices. To improve the efficiency, Emura [4] proposed a CP-ABE scheme with constant size ciphertexts with AND-gates on multi-valued attributes access structure. Then Waters [5] proposed an efficient and expressive CP-ABE scheme, by employing linear secret share scheme (LSSS). There have been many CP-ABE schemes [3–5] at present. However, in most of CP-ABE proposals, the access policy must be sent along with the ciphertext which means that anyone who can obtain the ciphertext will get the access policy. While, in some applications access policy may contain sensitive information of the users. For example, a data owner intends to upload a medical record to the cloud and wish that the record can only be accessed by a diabetologist in Central Hospital or a patient with the social security number NY12345678. If the data owner encrypts the record by a traditional CP-ABE scheme, with the access policy "(Patient: NY12345678 AND Hospital: Central Hospital) OR (Doctor: Diabetologist AND Hospital: Central Hospital)". Everyone who can get the access policy can infer that a patient with social security number NY12345678 is suffering diabetes. Obviously, the data owner would not like this as in Fig. 1. Thus, the CP-ABE schemes should not only guarantee the security of encrypted data but also must can satisfy the access structure protection.

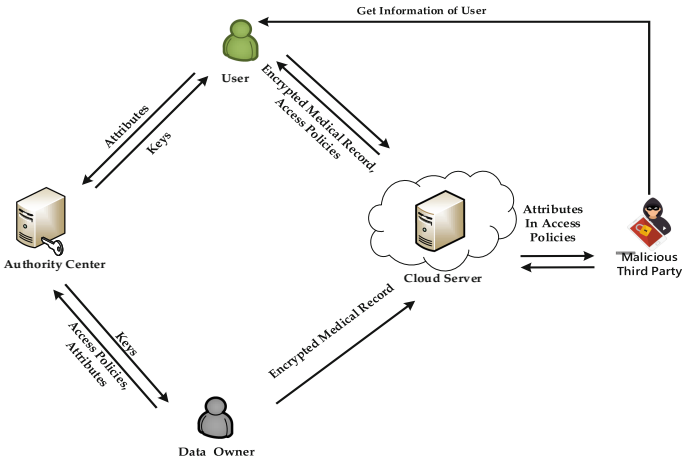

Fig. 1. Privacy leakage in traditional CP-ABE

For addressing the problem above, in 2008, Nishide et al. [6] proposed the idea of hiding the access policies of CP-ABE schemes and proposed two CP-ABE schemes partly hidden access policies with AND-gates on multi-valued attributes with wildcard

access policy. However, both schemes have high computational complexity. Following Nishide, Li et al. [7] proposed an anonymous CP-ABE scheme with the ability of forbidden illegal key sharing among users, but the computational complexity in this scheme is still very high. Later, Lai et al. [8, 9] proposed two fully secure CP-ABE schemes with hidden access policy in standard model. The first one only supports AND-gates on multi-valued attributes with wildcards, while the other one supports any monotone access policy. In addition, the size of ciphertexts and secret keys is linearly growing with the number of attributes. In order to tackle the problem, in 2013, Rao et al. [10] proposed a fully secure scheme with constant size ciphertexts and secret keys. However, their scheme only supports restrict access structures. Additionally, these schemes [8–10] are all over composite-order groups. In 2013, Zhang et al. [11] proposed a novel anonymous CP-ABE scheme over prime order groups under standard assumptions with match phase to allow data users to test whether their attributes satisfy the access policy before decryption, which can decrease the computational overhead of users. However, it has been found that the match phase will reveal the attributes belonging to the access policy. In 2016, Li et al. [12] proposed a more efficient scheme with decryption test to decrease the computational complexity before successful decryption. But the decryption phase destroyed its anonymity. Recently, CP-ABE scheme with hidden access structure can also be constructed from attribute hiding Inner-product Predicate Encryption (IPE) [13, 14], nevertheless this transformation will cause a super-polynomial growth in size of arbitrary access policy, which is extremely inefficient. Phuong et al. [15] introduced a way to construct hidden access policy CP-ABE from IPE under standard assumptions, but the communication cost is too high as that the size of secret keys and ciphertexts are linear to the number of attributes.

1.1 Our Technique and Contribution

Motivated by the above challenges, a construction of hidden access policy CP-ABE over prime-order groups in standard model is proposed. Our technique is based on anonymous IBE schemes in [16–19]. In [18], a splitting technique is used to protect the privacy of ciphertexts and result the following ciphertexts:

$$C = (A^s M, (g_0 g_1^{ID})^s, v_1^{s-s_1}, v_2^{s_1}, v_3^{s-s_3}, v_4^{s_2}) \tag{1}$$

Based on this construction, the authors in [16] introduced “double exponent” technique and issued the following ciphertexts:

$$C = (A^{s_1} M, (h_0 h_1^{ID})^{s_1} y_2^{s_2}, w^{s_1} y_3^{s_2}, g^{s_2}) \tag{2}$$

Both schemes achieve high efficiency and protect the test of the ciphertexts. Inspired by these good features, they are used to construct anonymous CP-ABE, where we aim at both solving the shortcomings in existing works and reserving the high efficiency of original schemes in [16, 18]. Our contributions are given as follows.

1. The security of the proposed scheme is reduced to the decisional n-BDHE and decisional linear assumption in the standard model.
2. For the hidden control access policy, the user does not know whether his/her attributes satisfy the access policy, which makes him/her need to decrypt again and again to match the plaintexts. While, decryption in our scheme only needs four pairing computations, which can decrease the computation complexity efficiently. Moreover, the secret key size in our scheme achieves constant which is independent with the number of attributes.

2 Preliminaries

2.1 Complexity Assumptions

The Decisional n-Bilinear Diffie-Hellman Exponent (BDHE) Problem
Let g and h be two random generators of $\mathbb{G}$ and α be random element in $\mathbb{Z}_p^*$. The decisional n-BDHE assumption is defined as follows: given a tuple $(h, g, g^{\alpha}, \ldots, g^{\alpha^n}, g^{\alpha^{n+1}}, \ldots, g^{\alpha^{2n}}, Z)$, there is no probabilistic polynomial-time algorithm can distinguish whether $Z = e(g,h)^{\alpha^{n+1}}$ or Z is a random element in $\mathbb{G}_T$.

The Decisional Linear Assumptions
The D-Linear assumption was first proposed in [18]. The security of our scheme is reduced to Assumption 4. The confidence of these assumptions has been provided in [17, 19–21].

Assumption 1. Let $g \in_R \mathbb{G}$ be a random generator and $z_1, z_2, z_3, z_4 \in_R \mathbb{Z}_p^*$. When given a tuple $(g, g^{z_1}, g^{z_2}, g^{z_1 z_3}, g^{z_2 z_4}, Z)$, there is no probabilistic polynomial-time algorithm can distinguish whether $Z = g^{(z_3 + z_4)}$ or Z is a random element in $\mathbb{G}$.

Assumption 2. Let $g \in_R \mathbb{G}$ be a random generator and $z_1, z_2, z_3 \in_R \mathbb{Z}_p^*$. When given $(g, g^{z_1}, g^{z_2}, g^{z_2^2}, \ldots, g^{z_2^n + 1}, g^{z_2^n / z_1}, g^{z_2^{n+1} z_3}, g^{z_4}, Z)$, there is no probabilistic polynomial-time algorithm can distinguish whether $Z = g^{z_1 (z_3 + z_4)}$ or Z is a random element in $\mathbb{G}$.

Assumption 3. Let $g \in_R \mathbb{G}$ be a random generator and $z_1, z_2, z_3 \in_R \mathbb{Z}_p^*$. When given a tuple $(g, g^{z_1}, g^{z_2}, g^{z_2^2}, \ldots, g^{z_2^n}, g^{z_2^{n+2}}, g^{z_2^{2n}}, g^{z_3}, g^{z_4}, g^{z_2 z_4}, \ldots, g^{z_2^n z_4}, Z)$, there is no probabilistic polynomial-time algorithm can distinguish whether $Z = g^{z_1 (z_3 + z_4)}$ or Z is a random element in $\mathbb{G}$.

Assumption 4. Let $g \in_R \mathbb{G}$ be a random generator and $z_1, z_2, z_3 \in_R \mathbb{Z}_p^*$. When given a tuple $(g, g^{z_1}, g^{z_2}, g^{z_2^2}, \ldots, g^{z_2^n + 1}, g^{z_2^n / z_1}, g^{z_2 z_3}, \ldots, g^{z_2^{n+1} z_3}, g^{z_4}, Z)$, there is no probabilistic polynomial-time algorithm can distinguish whether $Z = g^{z_1 (z_3 + z_4)}$ or Z is a random element in $\mathbb{G}$.

2.2 Definition and Security Model

2.2.1 Definition of Hidden Access Policy CP-ABE

A hidden access policy CP-ABE scheme consists of the following four algorithms:

- Setup $(\kappa, \mathcal{U}) \rightarrow (PK, MK)$: The setup algorithm takes security parameter κ and the universe of attribute $\mathcal{U}$ as input. Then it outputs the public parameters PK and the master key MK.
- KeyGen $(PK, MK, L) \rightarrow SK_L$: The keygen algorithm takes public parameters PK, the master key MK and a user's attribute set $L \subset \mathcal{U}$ as input. It outputs the secret keys SK_L associated with the attribute set L.
- Encrypt $(PK, M, W) \rightarrow CT$: The encrypt algorithm takes public parameters PK, a message M and an access policy W, then it generates the ciphertext CT as the encryption of M under W. Note that in a hidden access policy CP-ABE scheme, the access policy would not be included in the ciphertext.
- Decrypt $(SK_L, CT) \rightarrow M$ or $\perp$: The algorithm takes public parameters PK, secret keys SK_L and a ciphertext CT under a ciphertext policy W as input. If and only if the use's attribute set satisfies the access policy, it outputs the message M. Else it outputs $\perp$.

2.2.2 Security Model

Now we give the security model of the hidden access policy CP-ABE. It is presented as a security game between an adversary $\mathcal{A}$ and a simulator $\mathcal{B}$ as follows:

- **Init:** The adversary $\mathcal{A}$ submits two challenge ciphertext policies W_0^* and W_1^*.
- **Setup:** The simulator $\mathcal{B}$ runs the **Setup** algorithm and gives PK to the adversary $\mathcal{A}$.
- **Phase 1:** The adversary $\mathcal{A}$ submits the attribute list L, if $L \vDash W_0^* \wedge L \vDash W_1^*$ or $L \nvDash W_0^* \wedge L \nvDash W_1^*$, the simulator gives the secret key SK_L to $\mathcal{A}$. And $\mathcal{A}$ can repeat this for polynomial times.
- **Challenge:** The adversary $\mathcal{A}$ submits two equal length messages M_0 and M_1. If $L \vDash W_0^* \wedge L \vDash W_1^*$, then $M_0 = M_1$. Else $\mathcal{B}$ flips a random coin $b \in \{0, 1\}$, and sends **Encrypt** (PK, M_b, W_b^*) to $\mathcal{A}$.
- **Phase 2**: **Phase 1** is repeated.

Guess: The adversary outputs a guess $b' \in \{0, 1\}$ of b.

2.3 Access Policy

Assume that there are n categories of attributes as: $Att_1, Att_2, \ldots, Att_n$ and $Att_i = \{v_{i,1}, v_{i,2}, \ldots, v_{i,k_i}\} (\forall i \in [1, n])$ be the set of possible attributes belonging to Att_i. And each user has n attributes and different attribute belongs to different category. So that the universe of attributes can be donated as $\mathcal{U} = \bigcup_{i=1}^{n} Att_i$. For an access policy is donated as $W = \{W_1, W_2, \ldots, W_n\}$, in which $W_i \subset Att_i$ for $i \in [1, n]$. User's attribute set is donated as $L = \{L_1, L_2, \ldots, L_n\}$ in which $L_i \in Att_i$ for $i \in [1, n]$. If and only if $L_i \in W_i (\forall i \in [1, n])$ then it means that L satisfies W, denoted as $L \vDash W$, else it means that L does not satisfy W, denoted as $L \nvDash W$.

3 The Proposed Construction

3.1 Construction

- **Setup** $\rightarrow (PK, MK)$: Let $\mathbb{G}$ and $\mathbb{G}_T$ be two cyclic groups of prime order p and $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ be a bilinear map. It picks a random generator $g \in \mathbb{G}$ and random elements $u, \omega, h_0, h_1, h_2, \ldots, h_n$ from $\mathbb{G}$. Then it chooses $z_1, z_2, z_3, a_{i,j} \in \mathbb{Z}_p$ randomly, where $i \in [1, n]$, $j \in [1, k_i]$ and sets $y_1 = g^{z_1}$, $y_2 = g^{z_2}$, $y_3 = g^{z_3}$, $A = e(u, y_1)$. The public parameters PK and master keys MK are given as:

$$PK = (g, \omega, h_0, h_1, h_2, \ldots, h_n, y_1, y_2, y_3, A),\ MK = (u, z_1, z_2, z_3, \{a_{i,j}\}_{i\in[1,n], j\in[1,k_i]}). \quad (3)$$

- **KeyGen** $(PK, MK, L) \rightarrow SK_L$: Let $L = \{L_1, L_2, \ldots, L_n\} (L_i \in Att_i)$ be a set of attributes of a user who is going to obtain secret keys corresponding to L. Let $k_i = h_0^{t_i} \cdot h_i^{a_{i,j}}$, where $\sum_{i=1}^{n} t_i = 1$. Last it picks r_1, r_2 at random from $\mathbb{Z}_p$ and constructs the secret keys as:

$$\begin{aligned} SK_L =& (\{k_i^{r_1}\}_{i\in[1,n]}, g^{r_1 z_1 z_2 + r_2 z_1 z_3}, g^{r_1 z_1}, g^{r_2 z_1}, u\omega^{r_2}) \\ =& (\{sk_{1,i}\}_{i\in[1,n]}, sk_2, sk_3, sk_4, sk_5). \end{aligned} \quad (4)$$

- **Encrypt** $(PK, M, W) \rightarrow CT$: The algorithm takes as input the public parameters PK, a message $M \in \mathbb{G}_T$ and a ciphertext policy $W = \{W_1, W_2, \ldots, W_n\}$, $W_i \subset Att_i$, the data owner chooses $s_{1,i}, s_{2,i} \in \mathbb{Z}_p$ randomly for $1 \leq i \leq n$ and sets $s_1 = \sum_{i=1}^{n} s_{1,i}$, $s_2 = \sum_{i=1}^{n} s_{2,i}$. Then the data owner computes

$$C_1 = y_1^{s_1},\ C_2 = g^{s_2},\ C_4 = \omega^{s_1} y_3^{s_2},\ C_5 = A^{s_1}.$$

If $v_{i,j} \in W_i$, $C_{i,j} = h_0^{s_{1,i}} h_i^{a_{i,j} s_1} y_2^{s_{2,i}}$, else $C_{i,j}$ is a random element in $\mathbb{G}$. Then C_3 is computed as: $C_3 = \{C_{i,j}\}_{\{1\leq i\leq n, 1\leq j\leq k_i\}}$. Finally, it outputs the ciphertexts as

$$CT = \{C_1, C_2, C_3, C_4, C_5\} \quad (5)$$

- **Decrypt** $(SK_L, CT) \rightarrow M$ or $\perp$: In this algorithm, user's secret key SK_L and ciphertext CT are taken as input. If user's attribute set satisfies the access policy then he/she can decrypt as follows:

$$M = C_5 / \frac{\prod_{i=1}^{n} e(sk_{1,i}, C_1) \cdot e(sk_5, C_1) \cdot e(sk_2, C_2)}{\prod_{i=1, v_{i,j}\in W_i}^{n} e(C_{i,j}, sk_3) \cdot e(sk_4, C_4)} \quad (6)$$

3.2 Correctness and Anonymity

Correctness

Assuming the ciphertext is well-formed for W and L. The verification is run as follows.

$$\begin{aligned}
&\frac{\prod_{i=1}^{n} e(sk_{1,i}, C_1) \cdot e(sk_5, C_1) \cdot e(sk_2, C_2)}{\prod_{i=1, v_{i,j} \in W_i}^{n} e(C_{i,j}, sk_3) \cdot e(sk_4, C_4)} \\
&= \frac{e((h_0 \prod_{i=1}^{n} h_i^{a_{i,j}})^{r_1},) e(u\omega^{r_2}, y_1^{s_1}) \cdot e(g^{r_1 z_1 z_2 + r_2 z_1 z_3}, g^{s_2})}{e(g^{r_1 z_1}, (h_0 \prod_{i=1}^{n} h_i^{a_{i,j}})^{s_1} \cdot y_2^{s_2}) \cdot e(g^{r_2 z_1}, \omega^{s_1} y_3^{s_2})} \\
&= \frac{e(u, g^{s_1 z_1}) \cdot e((h_0 \prod_{i=1}^{n} h_i^{a_{i,j}})^{r_1}, g^{s_1 z_1}) \cdot e(\omega^{r_2}, g^{s_1 z_1})}{e(g^{r_1 z_1}, (h_0 \prod_{i=1}^{n} h_i^{a_{i,j}})^{s_1}) \cdot e(g^{r_1 z_1}, g^{z_2 s_2}) \cdot e(g^{r_2 z_1}, \omega^{s_1})} \cdot \frac{e(g^{r_1 z_1 z_2 + r_2 z_1 z_3}, g^{s_2})}{e(g^{r_2 z_1}, g^{z_3 s_2})} \\
&= e(u, g^{z_1 s_1}) \cdot \frac{e((h_0 \prod_{i=1}^{n} h_i^{a_{i,j}})^{r_1}, g^{s_1 z_1})}{e(g^{r_1 z_1}, (h_0 \prod_{i=1}^{n} h_i^{a_{i,j}})^{s_1})} \cdot \frac{e(\omega^{r_2}, g^{s_1 z_1})}{e(g^{r_2 z_1}, \omega^{s_1})} \cdot \frac{e(g^{r_1 z_1 z_2 + r_2 z_1 z_3}, g^{s_2})}{e(g^{r_1 z_1}, g^{z_2 s_2}) \cdot e(g^{r_2 z_1}, g^{z_3 s_2})} \\
&= e(u, g^{z_1 s_1}) = A^{s_1}.
\end{aligned} \tag{7}$$

Anonymity

By using the technique in [17] multiplying $h_0^{s_{1,i}} h_i^{a_{i,j} s_1}$ by $y_2^{s_{2,i}}$, and ω^{s_1} by $y_3^{s_2}$, if an adversary intends to test whether an attribute $v_{i,j}$ is embed into $C_{i,j}$, he has to use C_1, C_2 and C_4, which are comprised in $C_{i,j}$ and C_4, respectively. It can resist the DDH-test. The specific proof will be given in Sect. 4.

4 Security Proof

Theorem 1. Under the decisional n-BDHE and Decisional Linear assumption, our scheme achieves selective secure and user's privacy protection.

Proof. In this section we will give the security proof using hybrid argument over a sequence of games as follows:

Game$_0$: This game is the real security game as described in security model, in which the challenge ciphertext is normal as $CT_0^* = \{C_1^*, C_2^*, C_3^*, C_4^*, C_5^*\}$.
Game$_1$: In this game C_5 is replaced by a random element $R_5 \in \mathbb{G}_T$, the challenge ciphertext is: $CT_1^* = \{C_1^*, C_2^*, C_3^*, C_4^*, R_5\}$.
Game$_2$: In this game both C_4 and C_5 are replaced by a random element $R_4 \in \mathbb{G}$ and a random element $R_5 \in \mathbb{G}_T$, the challenge ciphertext is: $CT_2^* = \{C_1^*, C_2^*, C_3^*, R_4, R_5\}$.

Then we modify *Game*$_2$ by changing the way to generate the components $\{C_{i,j}\}_{\{1 \le i \le n, 1 \le j \le k_i\}}$ and define a sequence of games as follows. For $v_{i,j}$ such that $(v_{i,j} \in W_{0,i} \wedge v_{i,j} \in W_{1,i})$ or $(v_{i,j} \notin W_{0,i} \wedge v_{i,j} \notin W_{1,i})$ the ciphertext component $C_{i,j}$ is

obtained from the real game. But for $v_{i,j}$ such that $(v_{i,j} \in W_{0,i} \wedge v_{i,j} \notin W_{1,i})$ or $(v_{i,j} \notin W_{0,i} \wedge v_{i,j} \in W_{1,i})$, the ciphertext component $C_{i,j}$ which is generated normally in $Game_{2,\ell-1}$ is replaced by random value in $Game_{2,\ell}$. We will not define a new game by replacing ciphertext component $C_{i,j}$, until there is no $v_{i,j}$ satisfies $(v_{i,j} \in W_{0,i} \wedge v_{i,j} \notin W_{1,i})$ or $(v_{i,j} \notin W_{0,i} \wedge v_{i,j} \in W_{1,i})$.

Lemma 1. Under the decisional n-BDHE assumption, there is no adversary can distinguish the difference from $Game_0$ and $Game_1$ with non-negligible advantage in polynomial time.

Lemma 2. Under the Decisional Linear assumption, there is no adversary can distinguish the difference from $Game_1$ and $Game_2$ with non-negligible advantage in polynomial time.

Lemma 3. Under the Decisional Linear assumption, there is no adversary can distinguish the difference from $Game_{2,\ell-1}$ and $Game_{2,\ell}$ with non-negligible advantage in polynomial time.

Thus, the proposed scheme is IND-sCP-CPA secure under decisional n-BDHE assumption and Decisional Linear assumption.

5 Performance Comparison

In this section, the proposed construction will be compared with previous works. Tables 1 and 2 give the detailed comparisons between the proposed scheme in Sect. 3.1 and the others. For ease of expression the size of the public parameter, the secret key, and the ciphertext length excepting the access policy are denoted by PK, SK, and CT, respectively. Let N be the order of bilinear group, generally it is a big prime order number, but in some schemes, it is a composite number $N = pqr$, where p, q, r are prime order numbers. $|\mathbb{G}|, |\mathbb{G}_T|, |\mathbb{Z}_N|$ are the bit-length of the element belonging to each group, respectively. Let $\mathcal{U} = \{Att_1, Att_2, \cdots, Att_n\}$ be the universe of the attributes k_i is the number of attributes in Att_i and $K = \sum_{i=1}^{n} k_i$ is the number of all the attributes in $\mathcal{U}$.

Table 1. Security comparisons with previous works

Schemes	Order of bilinear groups	Fully hidden attribute	Assumption	Anonymity
[6]	$N = p$	✗	DBDH D-linear	✓
[8]	$N = pqr$	✗	Non-standard	✓
[11]	$N = p$	✗	DBDH D-linear	✗
[12]	$N = p$	✗	DDH	✗
Ours	$N = p$	✓	Decisional n-DBHE D-linear	✓

Table 2. Comparisons of the computation cost with others

Schemes	*PK*	*SK*	*CT*
[6]	$(2K+1)\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$(3n+1)\|\mathbb{G}\|$	$(2K+1)\|\mathbb{G}\|+\|\mathbb{G}_T\|$
[8]	$(K+1)\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$(n+1)\|\mathbb{G}\|$	$(K+1)\|\mathbb{G}\|$
[11]	$3\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$(5n+2)\|\mathbb{G}\|$	$(3K+4)\|\mathbb{G}\|+2\|\mathbb{G}_T\|$
[12]	$(K+1)\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$(2K+2)\|\mathbb{G}\|$	$(K+n)\|\mathbb{G}\|+\|\mathbb{G}_T\|$
Ours	$(n+6)\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$(n+3)\|\mathbb{G}\|$	$(K+3)\|\mathbb{G}\|+\|\mathbb{G}_T\|$

Our scheme is efficient in commutation overhead where the size of *SK* and the size of *PK* and *CT* is relatively small.

6 Conclusion

We proposed an efficient hidden access policy CP-ABE scheme over prime-order groups. The security of the proposed scheme is selectively secure and anonymous under the decisional n-BDHE and the Decision Linear assumptions.

Unfortunately, the proposed scheme only supports AND gate and achieves selectively security. It is also desirable to construct a strong secure and more flexible CP-ABE scheme with fully hidden access structures using pairings in the prime-order groups.

Acknowledgement. This work was supported in part by the National Cryptography Development Fund under Grant (MMJJ20180209).

References

1. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005). https://doi.org/10.1007/11426639_27
2. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: ACM Conference on Computer and Communications Security, pp. 89–98 (2006)
3. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy, pp. 321–334. IEEE Computer Society (2007)
4. Emura, K., Miyaji, A., Nomura, A., Omote, K., Soshi, M.: A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. In: Bao, F., Li, H., Wang, G. (eds.) ISPEC 2009. LNCS, vol. 5451, pp. 13–23. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-00843-6_2
5. Waters, B.: Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 53–70. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19379-8_4

6. Nishide, T., Yoneyama, K., Ohta, K.: Attribute-based encryption with partially hidden encryptor-specified access structures. In: Bellovin, S.M., Gennaro, R., Keromytis, A., Yung, M. (eds.) ACNS 2008. LNCS, vol. 5037, pp. 111–129. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-68914-0_7
7. Li, J., Ren, K., Zhu, B., Wan, Z.: Privacy-aware attribute-based encryption with user accountability. In: Samarati, P., Yung, M., Martinelli, F., Ardagna, Claudio A. (eds.) ISC 2009. LNCS, vol. 5735, pp. 347–362. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-04474-8_28
8. Lai, J., Deng, R.H., Li, Y.: Fully secure cipertext-policy hiding CP-ABE. In: Bao, F., Weng, J. (eds.) ISPEC 2011. LNCS, vol. 6672, pp. 24–39. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-21031-0_3
9. Lai, J., Deng, R.H., Li, Y.: Expressive CP-ABE with partially hidden access structures. In: Youm, H.Y., Won, Y. (eds.) Proceedings ACM Conference on Computer and Communications Security, ASIACCS 2012, pp. 18–19 (2012)
10. Rao, Y.S., Dutta, R.: Recipient anonymous ciphertext-policy attribute based encryption. In: Bagchi, A., Ray, I. (eds.) ICISS 2013. LNCS, vol. 8303, pp. 329–344. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-45204-8_25
11. Zhang, Y., Chen, X., Li, J., Wong, D.S., Li, H.: Anonymous attribute-based encryption supporting efficient decryption test. In: ACM Symposium on Information, Computer and Communications Security 2013, pp. 511–516. ACM, New York (2013)
12. Li, J., Wang, H., Zhang, Y., Shen, J.: Ciphertext-policy attribute-based encryption with hidden access policy and testing. Ksii Trans. Internet Inf. Syst. **10**(7), 3339–3352 (2016)
13. Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smart, N. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 146–162. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-78967-3_9
14. Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 62–91. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_4
15. Phuong, T.V.X., Yang, G., Susilo, W.: Hidden ciphertext policy attribute-based encryption under standard assumptions. IEEE Trans. Inf. Forensics Secur. **11**(1), 35–45 (2015)
16. Park, J.H., Lee, D.H.: Anonymous HIBE: compact construction over prime-order groups. IEEE Trans. Inf. Theory **59**(4), 2531–2541 (2013)
17. Seo, J.H., Kobayashi, T., Ohkubo, M., Suzuki, K.: Anonymous hierarchical identity-based encryption with constant size ciphertexts. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 215–234. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-00468-1_13
18. Boneh, D., Boyen, X., Shacham, H.: Short group signatures using strong Diffie Hellman. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-28628-8_3
19. Boyen, X., Waters, B.: Anonymous hierarchical identity-based encryption (without random oracles). In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 290–307. Springer, Heidelberg (2006). https://doi.org/10.1007/11818175_17
20. Gentry, C.: Practical identity-based encryption without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445–464. Springer, Heidelberg (2006). https://doi.org/10.1007/11761679_27
21. Wu, Q., Wu, Q., Mu, Y., Zhang, J.: Privacy-preserving and secure sharing of PHR in the cloud. J. Med. Syst. **40**(12), 267 (2016)