Hindawi
Security and Communication Networks
Volume 2017, Article ID 3596205, 11 pages
https://doi.org/10.1155/2017/3596205

Research Article

Verifiable Outsourced Decryption of Attribute-Based Encryption with Constant Ciphertext Length

Jiguo Li,[1] Fengjie Sha,[1] Yichen Zhang,[1] Xinyi Huang,[2] and Jian Shen[3]

[1]*College of Computer and Information, Hohai University, Nanjing 211000, China*
[2]*School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350117, China*
[3]*School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China*

Correspondence should be addressed to Jiguo Li; ljg1688@163.com

Received 28 June 2016; Accepted 1 September 2016; Published 10 January 2017

Academic Editor: Ángel Martín Del Rey

Outsourced decryption ABE system largely reduces the computation cost for users who intend to access the encrypted files stored in cloud. However, the correctness of the transformation ciphertext cannot be guaranteed because the user does not have the original ciphertext. Lai et al. provided an ABE scheme with verifiable outsourced decryption which helps the user to check whether the transformation done by the cloud is correct. In order to improve the computation performance and reduce communication overhead, we propose a new verifiable outsourcing scheme with constant ciphertext length. To be specific, our scheme achieves the following goals. (1) Our scheme is verifiable which ensures that the user efficiently checks whether the transformation is done correctly by the CSP. (2) The size of ciphertext and the number of expensive pairing operations are constant, which do not grow with the complexity of the access structure. (3) The access structure in our scheme is AND gates on multivalued attributes and we prove our scheme is verifiable and it is secure against selectively chosen-plaintext attack in the standard model. (4) We give some performance analysis which indicates that our scheme is adaptable for various limited bandwidth and computation-constrained devices, such as mobile phone.

1. Introduction

Attribute-based encryption (ABE) derives from identity-based encryption (IBE) introduced in [1]. A user's identity in IBE system is indicated by a binary bit string and the corresponding representation in ABE system is extended to an attribute set. The identity represented by an attribute set is not unique so ABE can realize the one-to-many encryption. Traditional IBE schemes can only provide coarse-grained access control. In order to solve this problem, Goyal et al. [2] presented a new scheme in which the fine-grained access control is associated with the user's private keys and ciphertexts are associated with a descriptive attribute set. ABE can be divided into two categories, namely, key-policy attribute-based encryption (KP-ABE) [2–4] and ciphertext-policy attribute-based encryption (CP-ABE) [5–11]. One of the main defects of current ABE schemes is expensive decryption operation for mobile device with low computing power and limited battery. To improve efficiency, Green et al. [12] presented an efficient ABE scheme by outsourcing expensive decryption operation to the cloud service provider (CSP). In their scheme, a user uses proxy reencryption method [13, 14] to generate a transformation key and sends the transformation key and ABE ciphertext to the CSP. Given the transformation key, the CSP transforms an ABE ciphertext into a simple ciphertext, from which the user recovers plaintext by using less computation overhead. In this process, the CSP does not get any information about original plaintext. Chase [15] extended single authority ABE to propose a multiauthority ABE scheme. However, he only proves that the scheme is secure against the selective ID model. Liu et al. [16] provided a fully secure multiauthority CP-ABE. In order to protect privacy of the user, Han et al. [17] presented a decentralized key-policy attribute-based encryption with preserving privacy. Qian et al. [18] provided a decentralized CP-ABE with fully hidden access structure. Furthermore, they [19] proposed a privacy-preserving

personal health record using multiauthority ABE with revocation. Several traceable CP-ABE schemes [20–22] were constructed to trace the identity of a misbehaving user who leaks its decryption key to others and thus reduces the trust assumptions on both users and attribute authorities. Recently, Li et al. [23] presented flexible and fine-grained attribute-based data storage in cloud computing. To protect data privacy, the sensitive data should be encrypted by the data owner prior to outsourcing. As the amount of encrypted files stored in cloud is becoming very huge, searchable encryption scheme over encrypted cloud data is a very challenging issue. To deal with above problem, Li et al. [24, 25] proposed a new cryptographic primitive called attribute-based encryption scheme with keyword search function [26–28]. In the proposed scheme, cloud service provider (CSP) performs partial decryption task delegated by data user without knowing anything about the plaintext. Moreover, the CSP can perform encrypted keyword search without knowing anything about the keywords embedded in trapdoor. In order to protect the privacy for the encryptor and decryptor, Li et al. [29] propose a CP-ABE scheme with hidden access policy and testing.

Our Motivations and Contributions. With the cloud service being more and more popular in modern society, ABE technology has become a promising orientation. It allows users to use flexible access control to access files stored in the cloud server with encrypted form. Though its advantages make it a powerful tool for cloud, one of its main performance challenges is that the complexity of decryption computation is linearly correlated with the access structure. By using the proxy reencryption technology, outsourced decryption ABE system can largely reduce the computation cost for users who intend to access the encrypted files stored in cloud. Given a ciphertext and a transformation key, CSP transforms a ciphertext into a simple ciphertext. The user only needs to spend less computational overhead to recover the plaintext from simple ciphertext. However, the correctness of the transformation ciphertext which the CSP gives to the user cannot be guaranteed because the latter does not have the original ciphertext. It is a security threat that malicious cloud service provider (CSP) may replace the original ciphertext and give the user a transformed ciphertext from another ciphertext which CSP wants the user to decrypt. The user is not aware of the CSP's malicious behavior. Mutual verifiable provable data auditing [30] in public cloud storage is a potential method to solve remote data possession checking. The security property about ABE with outsourcing decryption ensures that the malicious cloud server cannot obtain anything with respect to the encrypted message; nonetheless, the scheme does not ensure the validity of the transformation done by the CSP. In order to solve this problem, Lai et al. [31] put forward an ABE scheme with verifiable outsourcing decryption which guarantees verifiability of the transformation. Recently, Li et al. [32] presented an outsourcing ABE scheme which can check validity of the outsourced computation results. There is no doubt that verifiability brings about great progress to outsourced decryption of ABE. However, the ciphertext length and the amount of expensive pairing computations grow with the number of the attributes, which greatly limits its application in power constrained and bandwidth limited devices. Schemes in [33, 34] put forward a good solution to this problem in which the ciphertext length is constant. In this article, we present a novel verifiable outsourced CP-ABE scheme with constant ciphertext length to save the communication cost. The security of our scheme reduces to that of scheme in [33]. Similar to the proof in [31], the verifiability of our scheme reduces to the discrete logarithm assumption.

Organization. We organized the rest of the paper as follows. In Section 2, we review some preliminary knowledge and introduce the CP-ABE model of outsourced decryption. We also give the security definitions used in our paper in this section. In Section 3, we provide a new verifiable outsourced CP-ABE scheme with constant ciphertext length. We prove security and verifiability of our scheme in Section 4. In Section 5, we give some performance comparison with the existing schemes. Finally, we conclude the paper in Section 6.

2. Preliminaries

We introduce some basic knowledge about bilinear groups, security assumption, access structure, and CP-ABE which our scheme relies on.

2.1. Bilinear Pairing

Definition 1 (bilinear map). G_1 and G_T are multiplicative cyclic groups with prime order p. Suppose g is a generator in G_1. $e : G_1 \times G_1 \to G_T$ is bilinear map if it satisfies the following properties:

(1) Bilinearity: for all $u, v \in G_1$, $e(u^a, v^b) = e(u, v)^{ab}$, where $a, b \in \mathbb{Z}_p$ are selected randomly.

(2) Nondegeneracy: there exists $u, v \in G_1$ such that $e(u, v) \neq 1$.

(3) Computability: for all $u, v \in G_1$, there is an efficient algorithm to compute $e(u, v)$.

2.2. Security Assumption

Definition 2 (discrete logarithm (DL) assumption [31]). Let (p, G, G_T, e) be a prime-order bilinear group system. Given (p, G, G_T, e, g, g^x), where $g \in G$ is randomly selected, the DL problem for (p, G, G_T, e) is to calculate x. The DL assumption in (p, G, G_T, e) is that no probabilistic polynomial-time (PPT) algorithm $\mathcal{A}$ solves the DL problem at non-negligible advantage. The advantage for $\mathcal{A}$ is defined as $\Pr[\mathcal{A}(p, G, G_T, e, g, g^x) = x]$.

2.3. Access Structure.

Access structure is being referred to in [33]; we utilize AND gates with respect to multivalued attributes as follows.

Definition 3. Assume that $U = \{\text{att}_1, \ldots, \text{att}_n\}$ is an attribute universe. $V_i = \{v_{i,1}, v_{i,2}, \ldots, v_{i,n_i}\}$ are some feasible values, where n_i is the amount of feasible values of $\text{att}_i \in U$. Let

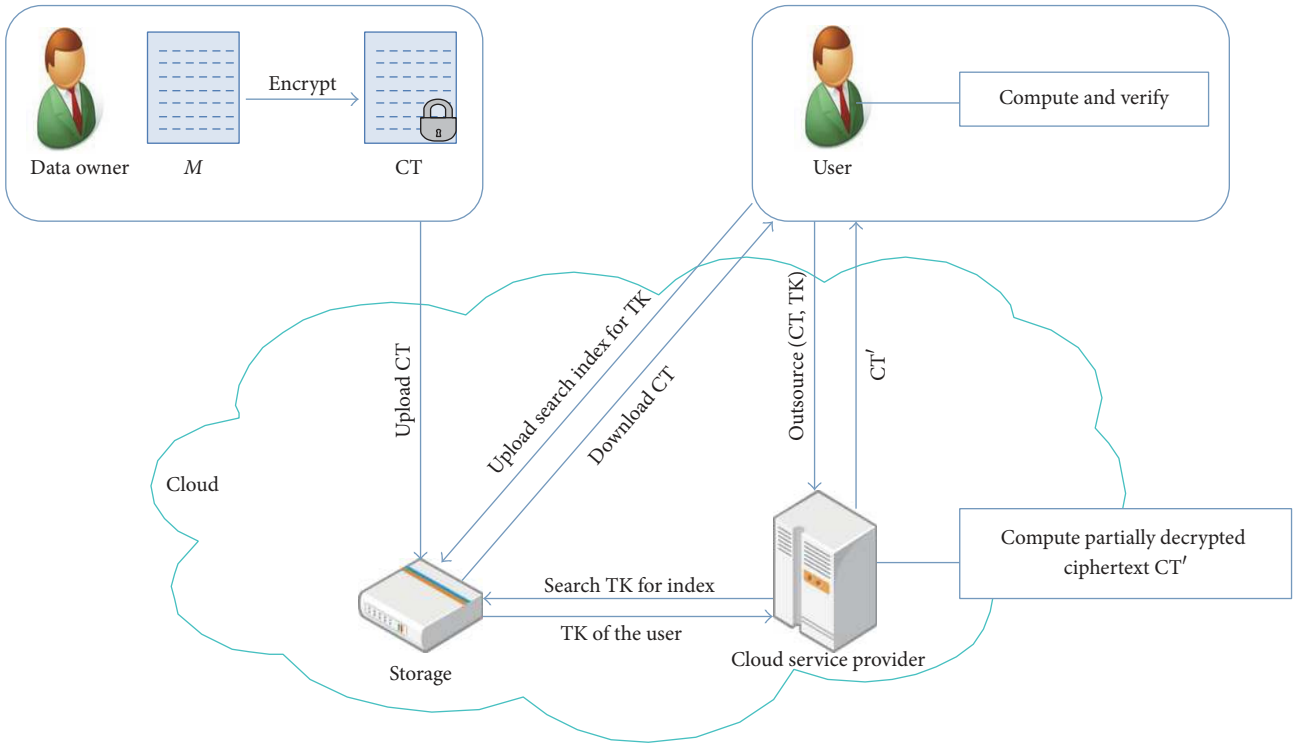

Figure 1: System architecture of our scheme.

$S = [S_1, S_2, \ldots, S_n]$, let $S_i \in V_i$ be an attribute set for a user, and $\mathbb{A} = [\mathbb{A}_1, \mathbb{A}_2, \ldots, \mathbb{A}_n]$; let $\mathbb{A}_i \in V_i$ be an access structure. The notation $S \vDash \mathbb{A}$ denotes that an attribute set S satisfies an access structure $\mathbb{A}$; that is to say, $S_i = \mathbb{A}_i$ $(i = 1, 2, \ldots, n)$.

2.4. Outline of CP-ABE with Outsourced Decryption. Briefly speaking, a user interacts with the CSP as illustrated in Figure 1. Data owner encrypts message M into ciphertext CT and uploads it to the storage in cloud. A user who is permitted to access the data downloads the ciphertext. Then the user sends the ciphertext and transformation key to the CSP for outsourcing decryption. CSP computes partially decrypted ciphertext CT′ and sends it to the user. The user computes the message from the partially decrypted ciphertext and verifies whether the message is the original one.

We review the notion of CP-ABE in [31] with outsourced decryption. It is described by the seven algorithms as follows.

$Setup(\lambda, U)$. This algorithm takes the security parameter λ and attribute universe U as input. It outputs public parameter PK and master secret key MK.

$KeyGen(PK, MK, S)$. This algorithm takes PK, MK, and attribute set S as input. It outputs private key SK_S related to S.

$Encrypt(PK, M, \mathbb{A})$. This algorithm takes PK, message M, and access structure $\mathbb{A}$ as input and outputs ciphertext CT.

$Decrypt(PK, SK_S, CT)$. This algorithm takes PK, SK_S, and CT as input. It outputs M if SK_S associated with S satisfies $\mathbb{A}$.

$GenTK_{out}(PK, SK_S)$. This algorithm takes PK and SK_S as input. It outputs transformation key TK_S associated with S and a corresponding retrieving key RK_S.

$Transform_{out}(PK, CT, TK_S)$. This algorithm takes PK, CT, and TK_S as input. It outputs a partially decrypted ciphertext CT′.

$Decrypt_{out}(PK, CT, CT', RK_S)$. This algorithm takes PK, CT, CT′, and RK_S for S as input. It outputs message M or $\perp$.

2.5. Security Model for CP-ABE with Outsourcing Decryption. Lai et al. [31] described security properties and verifiability for CP-ABE which supports outsourcing decryption. The traditional concept of security for chosen-ciphertext attack (CCA) is not suitable for the above CP-ABE scheme because it does not permit modifying any bit for the ciphertext. Therefore, they use a relaxation named replayed CCA (RCCA) security [35], which permits alternation for the ciphertext, so that they can change the potential message in a significant way.

2.5.1. Security. The RCCA security of outsourced decryption CP-ABE is described as a game in both an adversary and a challenger. According to the game in [31], it is described as follows.

Setup. The challenger $\mathscr{C}$ performs setup algorithm to get the public parameter PK and master secret key MK. It sends PK to the adversary $\mathscr{A}$ and keeps MK secret.

Query Phase 1. The challenger maintains a table Tb and a set D which are initialized empty. The adversary $\mathcal{A}$ adaptively issues queries.

(1) Private Key Query for Attribute Set S. The challenger runs $\mathrm{SK}_S \leftarrow \mathrm{KeyGen}(\mathrm{PK}, \mathrm{MK}, S)$ and sets $D = D \cup \{S\}$. It then sends the private key SK_S to the adversary.

(2) Transformation Key Query on Attribute Set S. $\mathcal{C}$ scans the tuple $(S, \mathrm{SK}_S, \mathrm{TK}_S, \mathrm{RK}_S)$ in table Tb. If such a tuple exists, it returns TK_S as the transformation key. Otherwise, it runs $\mathrm{SK}_S \leftarrow \mathrm{KeyGen}(\mathrm{PK}, \mathrm{MK}, S)$ and $(\mathrm{TK}_S, \mathrm{RK}_S) \leftarrow \mathrm{GenTK}_{\mathrm{out}}(\mathrm{PK}, \mathrm{SK}_S)$ and stores the tuple in table Tb. It then returns the transformation key TK_S to the adversary.

Without loss of generality, we suppose that an adversary does not launch transformation key query for attribute set S, if a private key query about the same attribute set S has been issued. Since anyone can generate a transformation key of the user utilizing the user's private key and $\mathrm{GenTK}_{\mathrm{out}}$ algorithm by himself, the assumption is rational.

(3) Decryption Query for Attribute Set S and Ciphertext CT. $\mathcal{C}$ runs $\mathrm{SK}_S \leftarrow \mathrm{KeyGen}(\mathrm{PK}, \mathrm{MK}, S)$ and $M \leftarrow \mathrm{Decrypt}(\mathrm{PK}, \mathrm{SK}_S, \mathrm{CT})$. It sends M to the adversary.

(4) Decryption$_{out}$ Query for Attribute Set S and Ciphertext (CT, CT'). $\mathcal{C}$ searches the tuple $(S, \mathrm{SK}_S, \mathrm{TK}_S, \mathrm{RK}_S)$ in table Tb. If such a tuple exists, it runs algorithm $M \leftarrow \mathrm{Decrypt}_{\mathrm{out}}(\mathrm{PK}, \mathrm{CT}, \mathrm{CT}', \mathrm{RK}_S)$ and returns M to $\mathcal{C}$; otherwise, it returns $\perp$.

Challenge. $\mathcal{A}$ sends M_0 and M_1 with equal length and an access policy $\mathbb{A}^*$ to $\mathcal{C}$ subject to the restriction that, for all $S \in D$, $\mathbb{A}^*$ cannot be satisfied by S. The challenger chooses $b \in \{0, 1\}$ and computes $\mathrm{CT}^* = \mathrm{Encrypt}(\mathrm{PK}, M_b, \mathbb{A}^*)$. Then the challenger sends the challenge ciphertext CT^* to $\mathcal{A}$.

Query Phase 2. $\mathcal{A}$ proceeds to adaptively launch transformation key, decryption, $\mathrm{Decryption}_{\mathrm{out}}$, and private key queries as in phase 1 with the following restrictions:

(1) $\mathcal{A}$ cannot make private key query which results in attribute set S that satisfies the target access policy $\mathbb{A}^*$.

(2) $\mathcal{A}$ cannot issue any trivial decryption queries. Namely, $\mathrm{Decryption}_{\mathrm{out}}$ and decryption queries are replied to as phase 1; if the response is either M_0 or M_1, then $\mathcal{C}$ returns $\perp$.

Guess. The adversary $\mathcal{A}$ gives a guess $b' \in \{0, 1\}$ for b and succeeds in the game if $b' = b$.

$|\Pr(b' = b) - 1/2|$ is defined as the advantage for the adversary $\mathcal{A}$ in the game.

Definition 4. An outsourcing decryption CP-ABE scheme is RCCA secure if all probabilistic polynomial-time (PPT) adversaries have at most a negligible advantage of winning in this game.

CPA Security. An outsourcing decryption CP-ABE scheme is secure under chosen-plaintext attack (CPA) if $\mathcal{A}$ cannot launch decryption queries in the above game.

Selective Security. An outsourcing decryption CP-ABE scheme is selective security if we add an initialization phase prior to setup algorithm in above game, where the adversary gives the challenger access structure $\mathbb{A}^*$.

2.5.2. Verifiability. The verifiability for CP-ABE with outsourced decryption is depicted via a game in both an adversary and a challenger. The game proceeds as follows.

Setup. $\mathcal{C}$ performs algorithm setup to generate the public parameters PK and master secret key MSK. It returns PK to $\mathcal{A}$ and keeps MSK secret.

Query Phase 1. $\mathcal{C}$ initializes an empty table T. $\mathcal{A}$ adaptively issues the following queries.

(1) Private Key Query for Attribute Set S. $\mathcal{C}$ runs $\mathrm{SK}_S \leftarrow \mathrm{KeyGen}(\mathrm{PK}, \mathrm{MK}, S)$ and returns the private key SK_S to the adversary.

(2) Transformation Key Query for Attribute Set S. The challenger runs $\mathrm{SK}_S \leftarrow \mathrm{KeyGen}(\mathrm{PK}, \mathrm{MK}, S)$ and $(\mathrm{TK}_S, \mathrm{RK}_S) \leftarrow \mathrm{GenTK}_{\mathrm{out}}(\mathrm{PK}, \mathrm{SK}_S)$ and stores the entry $(S, \mathrm{SK}_S, \mathrm{TK}_S, \mathrm{RK}_S)$ in table T. It then returns the transformation key TK_S to the adversary.

Without loss of generality, we suppose that the adversary does not launch transformation key query for attribute set S, if a private key query about the same attribute set S has been issued. Anyone can generate a transformation key of the user utilizing the user's private key and $\mathrm{GenTK}_{\mathrm{out}}$ algorithm by himself.

(3) Decryption Query for Attribute Set S and a Ciphertext CT. $\mathcal{C}$ runs $\mathrm{SK}_S \leftarrow \mathrm{KeyGen}(\mathrm{PK}, \mathrm{MK}, S)$ and $M \leftarrow \mathrm{Decrypt}(\mathrm{PK}, \mathrm{SK}_S, \mathrm{CT})$. It sends M to $\mathcal{C}$.

(4) Decryption$_{out}$ Query for Attribute Set S and Ciphertexts (CT, CT'). $\mathcal{C}$ searches the tuple $(S, \mathrm{SK}_S, \mathrm{TK}_S, \mathrm{RK}_S)$ in table T. If such a tuple exists, it runs $M \leftarrow \mathrm{Decrypt}_{\mathrm{out}}(\mathrm{PK}, \mathrm{CT}, \mathrm{CT}', \mathrm{RK}_S)$ and returns M to $\mathcal{C}$; otherwise, it returns $\perp$.

Challenge. $\mathcal{A}$ sends challenge message M^* and challenge access policy $\mathbb{A}^*$ to the challenger $\mathcal{C}$. $\mathcal{C}$ computes $\mathrm{CT}^* = \mathrm{Encrypt}(\mathrm{PK}, M^*, \mathbb{A}^*)$ and returns CT^* to $\mathcal{A}$ as its challenge ciphertext.

Query Phase 2. $\mathcal{A}$ proceeds to adaptively launch transformation key, decryption, $\mathrm{Decryption}_{\mathrm{out}}$, and private key queries as in phase 1.

Output. $\mathcal{A}$ returns attribute set S^* and transformed ciphertext $\mathrm{CT}^{*\prime}$. We suppose that tuple $(S^*, \mathrm{SK}_{S^*}, \mathrm{TK}_{S^*}, \mathrm{RK}_{S^*})$ is included in table T. Otherwise, the challenger generates the tuple as the reply for transformation key query. $\mathcal{A}$ succeeds in the game if $\mathrm{Decrypt}_{\mathrm{out}}(\mathrm{PK}, \mathrm{CT}^*, \mathrm{CT}^{*\prime}, \mathrm{RK}_{S^*}) \notin \{M^*, \perp\}$.

Definition 5. An outsourcing decryption CP-ABE scheme is verifiable if PPT adversary has at most a negligible advantage in the above game.

3. Construction of Our New Scheme

Our new scheme consists of seven algorithms.

$Setup(1^k)$. A trusted authority (TA) picks two bilinear groups (G_1, G_T) of prime-order p, $g_1 \in G_1$, $h, u, v, d \in G_1$, $y \in_R \mathbb{Z}_p$, and $t_{i,j} \in_R \mathbb{Z}_p$ $(i \in [1,n], j \in [1,n_i])$. $H : G_T \to \mathbb{Z}_p^*$ is a hash function. TA computes $Y = e(g_1,h)^y$; $T_{i,j} = g_1^{t_{i,j}}$ $(i \in [1,n], j \in [1,n_i])$. It generates $PK = (e, g_1, h, u, v, d, Y, \{T_{i,j}\}_{i\in[1,n], j\in[1,n_i]}, H)$ as public parameters and $MK = (y, \{t_{i,j}\}_{i\in[1,n], j\in[1,n_i]})$ as master secret key. Note that, $\forall S, S'$ $(S \neq S')$, $\sum_{v_{i,j}\in S} t_{i,j} \neq \sum_{v_{i,j}\in S'} t_{i,j}$ is assumed.

$KeyGen(PK, MSK, S)$. TA selects $r \in_R \mathbb{Z}_p$, computes $K_1 = h^y(g_1^{\sum_{v_{i,j}\in S} t_{i,j}})^r$ and $K_2 = g_1^r$, and sends $SK_S = (K_1, K_2)$ to a user associated with attribute set S.

$Encrypt(PK, M, \mathbb{A})$. An encryptor randomly selects $s, s' \in_R \mathbb{Z}_p$; $\widetilde{M} \in G_T$. He calculates $\widehat{C} = u^{H(M)}v^{H(\widetilde{M})}d$, $C_1 = M \cdot Y^s$, $C_2 = g_1^s$, $C_3 = (\prod_{v_{i,j}\in\mathbb{A}} T_{i,j})^s$, $C_1' = \widetilde{M} \cdot Y^{s'}$, and $C_2' = g_1^{s'}$, $C_3' = (\prod_{v_{i,j}\in\mathbb{A}} T_{i,j})^{s'}$. The sender generates $CT = (\mathbb{A}, \widehat{C}, C_1, C_2, C_3, C_1', C_2', C_3')$.

$Decrypt(PK, SK_S, CT)$. A decryptor calculates as follows:

$$\begin{aligned}
\frac{C_1 \cdot e(C_3, K_2)}{e(C_2, K_1)} &= \frac{M \cdot e(g_1,h)^{sy}\, e\left(\left(g_1^{\sum_{v_{i,j}\in\mathbb{A}} t_{i,j}}\right)^s, g_1^r\right)}{e\left(g_1^s, h^y\left(g_1^{\sum_{v_{i,j}\in S} t_{i,j}}\right)^r\right)} \\
&= \frac{M \cdot e(g_1,h)^{sy}\, e(g_1,g_1)^{sr\sum_{v_{i,j}\in\mathbb{A}} t_{i,j}}}{e(g_1,h)^{sy}\, e(g_1,g_1)^{sr\sum_{v_{i,j}\in S} t_{i,j}}} = M, \\
\frac{C_1' \cdot e(C_3', K_2)}{e(C_2', K_1)} &= \frac{\widetilde{M} \cdot e(g_1,h)^{s'y}\, e\left(\left(g_1^{\sum_{v_{i,j}\in\mathbb{A}} t_{i,j}}\right)^{s'}, g_1^r\right)}{e\left(g_1^{s'}, h^y\left(g_1^{\sum_{v_{i,j}\in S} t_{i,j}}\right)^r\right)} \\
&= \frac{\widetilde{M} \cdot e(g_1,h)^{s'y}\, e(g_1,g_1)^{s'r\sum_{v_{i,j}\in\mathbb{A}} t_{i,j}}}{e(g_1,h)^{s'y}\, e(g_1,g_1)^{s'r\sum_{v_{i,j}\in S} t_{i,j}}} = \widetilde{M}.
\end{aligned} \tag{1}$$

If $\widehat{C} = u^{H(M)}v^{H(\widetilde{M})}d$, it outputs the message M; otherwise, it outputs $\perp$.

$GenTK_{out}(PK, SK_S)$. A user generates his transformation key pair as follows. He chooses $z \in_R \mathbb{Z}_p$ and computes the transformation key as $TK_S = (K_1', K_2')$, where $K_1' = K_1^{1/z}$ and $K_2' = K_2^{1/z}$. The retrieving key is $RK_S = z$. Note that, with overwhelming probability, z has multiplicative inverse.

$Transform_{out}(PK, CT, TK_S)$. Given ciphertext CT and transformation key TK_S, the CSP computes as follows:

$$\begin{aligned}
\frac{e(C_2, K_1')}{e(C_3, K_2')} &= \frac{e\left(g_1^s, h^{y/z}\left(g_1^{\sum_{v_{i,j}\in S} t_{i,j}}\right)^{r/z}\right)}{e\left(\left(\prod_{v_{i,j}\in\mathbb{A}} T_{i,j}\right)^s, g_1^{r/z}\right)} \\
&= \frac{e(g_1,h)^{sy/z}\, e(g_1,g_1)^{sr/z\sum_{v_{i,j}\in S} t_{i,j}}}{e(g_1,g_1)^{sr/z\sum_{v_{i,j}\in\mathbb{A}} t_{i,j}}} \\
&= e(g_1,h)^{sy/z} = T', \\
\frac{e(C_2', K_1')}{e(C_3', K_2')} &= \frac{e\left(g_1^{s'}, h^{y/z}\left(g_1^{\sum_{v_{i,j}\in S} t_{i,j}}\right)^{r/z}\right)}{e\left(\left(\prod_{v_{i,j}\in\mathbb{A}} T_{i,j}\right)^{s'}, g_1^{r/z}\right)} \\
&= \frac{e(g_1,h)^{s'y/z}\, e(g_1,g_1)^{s'r/z\sum_{v_{i,j}\in S} t_{i,j}}}{e(g_1,g_1)^{s'r/z\sum_{v_{i,j}\in\mathbb{A}} t_{i,j}}} \\
&= e(g_1,h)^{s'y/z} = T'',
\end{aligned} \tag{2}$$

and it outputs the transformed ciphertext as $CT' = (\widehat{T} = \widehat{C}, T_1 = C_1, T_1' = C_1', T', T'')$.

$Decrypt_{out}(PK, CT, CT', RK_S)$. A user checks whether the transformed ciphertext $\widehat{T} \neq \widehat{C}$ or $T_1 \neq C_1$ or $T_1' \neq C_1'$; if the equations do not hold, he outputs $\perp$. Otherwise, he computes $M = C_1/T'^z$ and $\widetilde{M} = C_1'/T''^z$. If $\widehat{T} = u^{H(M)}v^{H(\widetilde{M})}d$, he outputs the message M; otherwise, he outputs $\perp$.

Note that $\sum_{v_{i,j}\in S} t_{i,j} \neq \sum_{v_{i,j}\in S'} t_{i,j}$ according to assumption. If there exist S and S' such that $\sum_{v_{i,j}\in S} t_{i,j} = \sum_{v_{i,j}\in S'} t_{i,j}$, the user with attribute set S' is able to decrypt ciphertext related to $\mathbb{A}$, where $S' \not\models \mathbb{A}$, $S \models \mathbb{A}$, and $S \neq S'$. We have that the assumption holds with overwhelming probability:

$$\begin{aligned}
\frac{p(p-1)\cdots(p-(N-1))}{p^N} &> \frac{(p-(N-1))^N}{p^N} \\
&= \left(1 - \frac{N-1}{p}\right)^N > 1 - \frac{N(N-1)}{p} > 1 - \frac{N^2}{p},
\end{aligned} \tag{3}$$

where $N = \prod_{i=1}^n n_i$. If we randomly choose $t_{i,j} \in \mathbb{Z}_p$ as secret key, then our assumption is reasonable.

4. Security Proof

Note that, in our scheme, a ciphertext consists of three parts: (C_1, C_2, C_3), (C_1', C_2', C_3'), and $\widehat{C}$. The first two elements are ciphertexts for message M and random message $\widetilde{M}$, respectively, utilizing the encryption algorithm [33]. In essence, the second and the third elements are redundant information.

The redundant information is mainly used to design a CP-ABE scheme with verifiable outsourcing decryption from [33], which has been proven to be selectively CPA-secure. We denote the first four algorithms as Basic CP-ABE. To guarantee the security for our scheme, we firstly prove that if the scheme in [33] is selectively CPA-secure, then Basic CP-ABE scheme is selectively CPA-secure.

Theorem 6. *Assume that the scheme in [33] is selectively CPA-secure. Then the Basic CP-ABE scheme is also selectively CPA-secure.*

Proof. We prove that our Basic CP-ABE scheme is selectively CPA-secure by the following two games.

Game$_0$. Game$_0$ is the originally selective CPA security game.

Game$_1$. In Game$_1$, the challenger randomly selects $\widehat{C} \in G_1$ and generates the remaining parts of the challenge ciphertext $\mathrm{CT} = (\mathbb{A}, \widehat{C}, C_1, C_2, C_3, C_1', C_2', C_3')$ as in Game$_0$. □

This theorem is proven via the following lemmas. Lemma 7 shows that Game$_0$ and Game$_1$ are indistinguishable. Lemma 8 shows that the advantage for an adversary in Game$_1$ is negligible. Thus, we come to a conclusion that the advantage for an adversary in Game$_0$ is negligible. Theorem 6 is correct from the two lemmas below.

Lemma 7. *Assume that the scheme in [33] is selectively CPA-secure; Game*$_0$ *and Game*$_1$ *are computationally indistinguishable.*

Proof. If the adversary $\mathscr{A}$ is able to distinguish Game$_0$ and Game$_1$ at nonnegligible advantage, then we find an algorithm $\mathscr{B}$ which attacks the scheme [33] under the selective CPA security model at nonnegligible advantage.

Let $\mathscr{C}$ be the challenger for the selective CPA security game in scheme [33]. $\mathscr{B}$ and the adversary $\mathscr{A}$ interact as follows.

Init. $\mathscr{A}$ gives $\mathbb{A}^*$ to $\mathscr{B}$ as its challenge access policy. $\mathscr{B}$ sends $\mathbb{A}^*$ to $\mathscr{C}$ as its challenge access policy. $\mathscr{C}$ sends the public parameters $\mathrm{PK}' = (e, g_1, h, Y, \{T_{i,j}\}_{i\in[1,n], j\in[1,n_i]})$ of the scheme [33] to $\mathscr{B}$.

Setup. $\mathscr{B}$ selects $x, y, z \in_R \mathbb{Z}_p$ and computes $u = g_1^x$, $v = g_1^y$, and $d = g_1^z$. $\mathscr{B}$ also selects hash function $H : G_T \to \mathbb{Z}_p^*$. $\mathscr{B}$ sends $\mathrm{PK} = (e, g_1, h, u, v, d, Y, \{T_{i,j}\}_{i\in[1,n], j\in[1,n_i]}, H)$ to the adversary $\mathscr{A}$.

Query Phase 1. $\mathscr{A}$ adaptively launches private key query on attribute set S_i; then $\mathscr{B}$ gets the private key SK_{S_i} via calling key generation oracle of $\mathscr{C}$ with respect to S_i. $\mathscr{B}$ returns the private key SK_{S_i} to $\mathscr{A}$.

Challenge. $\mathscr{A}$ sends two equal size messages M_0, M_1 to $\mathscr{B}$ as the challenge plaintext. $\mathscr{B}$ selects a random bit β and random messages $\widetilde{M}_0, \widetilde{M}_1 \in G_T$. $\mathscr{B}$ sends $\widetilde{M}_0, \widetilde{M}_1 \in G_T$ and $\mathbb{A}^*$ to $\mathscr{C}$. $\mathscr{C}$ randomly selects $\gamma \in \{0, 1\}$; the message $\widetilde{M}_\gamma$ is encrypted by PK' and $\mathbb{A}^*$ using the encryption algorithm in [32] and sends the resulting ciphertext $\mathrm{CT}^{*\prime}$ to $\mathscr{B}$. $\mathscr{B}$ denotes $\mathrm{CT}^{*\prime}$ as $\mathrm{CT}^{*\prime} = (\mathbb{A}^*, C_1', C_2', C_3')$. $\mathscr{B}$ selects $s \in_R \mathbb{Z}_p$ and computes $\widehat{C} = u^{H(M_\beta)} v^{H(\widetilde{M}_\beta)} d$, $C_1 = M_\beta \cdot Y^s$, $C_2 = g_1^s$, and $C_3 = (\prod_{v_{i,j}\in\mathbb{A}} T_{i,j})^s$ and sends $\mathrm{CT}^* = (\mathbb{A}^*, \widehat{C}, C_1, C_2, C_3, C_1', C_2', C_3')$ to $\mathscr{A}$ as its challenge ciphertext.

Query Phase 2. $\mathscr{A}$ adaptively launches private key query as in phase 1. $\mathscr{B}$ answers the queries as in phase 1.

Guess. $\mathscr{A}$ gives a guess $\beta' \in \{0, 1\}$ of $\mathscr{B}$. $\mathscr{B}$ outputs β' as a guess of γ.

Note that if $\beta = \gamma$, $\mathscr{B}$ appropriately simulates Game$_0$; else, $\mathscr{B}$ appropriately simulates Game$_1$. Therefore, if $\mathscr{A}$ is able to distinguish Game$_0$ and Game$_1$ at nonnegligible advantage, we are able to find an algorithm $\mathscr{B}$ that attacks the scheme [33] in selective CPA security model at nonnegligible advantage. □

Lemma 8. *Assume that the CP-ABE scheme in [33] is selectively CPA-secure; the advantage for the adversary* $\mathscr{A}$ *on Game*$_1$ *is negligible.*

Proof. If the adversary $\mathscr{A}$ has a nonnegligible advantage in Game$_1$, then we can find an algorithm $\mathscr{B}$ which attacks the scheme [33] at a nonnegligible advantage.

Let $\mathscr{C}$ be the challenger with respect to $\mathscr{B}$ of the scheme [33]. $\mathscr{B}$ interacts with $\mathscr{A}$ as demonstrated in the following steps.

Init. $\mathscr{A}$ submits challenge access policy $\mathbb{A}^*$ to $\mathscr{B}$. $\mathscr{B}$ gives $\mathbb{A}^*$ to $\mathscr{C}$ as its challenge access policy. $\mathscr{C}$ returns $\mathrm{PK}' = (e, g_1, h, Y, \{T_{i,j}\}_{i\in[1,n], j\in[1,n_i]})$ of scheme [25] to $\mathscr{B}$ as public parameters.

Setup. $\mathscr{B}$ chooses $x, y, z \in_R \mathbb{Z}_p$ and sets $u = g_1^x$, $v = g_1^y$, and $d = g_1^z$. $H : G_T \to \mathbb{Z}_p^*$ is a secure hash function. $\mathscr{B}$ sends $\mathrm{PK} = (e, g_1, h, u, v, d, Y, \{T_{i,j}\}_{i\in[1,n], j\in[1,n_i]}, H)$ to the adversary $\mathscr{A}$.

Query Phase 1. $\mathscr{A}$ adaptively launches private key query of attribute set S_i; $\mathscr{B}$ gets the private key SK_{S_i} via calling key generation oracle of $\mathscr{C}$ with respect to S_i. $\mathscr{B}$ sends the private key SK_{S_i} to $\mathscr{A}$.

Challenge. $\mathscr{A}$ submits messages M_0, M_1 with equal size. $\mathscr{B}$ sends M_0, M_1 and $\mathbb{A}^*$ to $\mathscr{C}$. $\mathscr{C}$ randomly chooses $\gamma \in \{0, 1\}$; the message M_γ is encrypted by PK' and $\mathbb{A}^*$ using the encryption algorithm in [33] and sends the resulting ciphertext $\mathrm{CT}^{*\prime}$ to $\mathscr{B}$. $\mathscr{B}$ parses $\mathrm{CT}^{*\prime}$ as $\mathrm{CT}^{*\prime} = (\mathbb{A}^*, C_1, C_2, C_3)$. $\mathscr{B}$ selects $s' \in_R \mathbb{Z}_p$, $\widetilde{M} \in_R G_T$, and $\widehat{C} \in_R G_1$ and computes $C_1' = \widetilde{M} \cdot Y^{s'}$, $C_2' = g_1^{s'}$, and $C_3' = (\prod_{v_{i,j}\in\mathbb{A}} T_{i,j})^{s'}$. $\mathscr{B}$ sends $\mathrm{CT}^* = (\mathbb{A}^*, \widehat{C}, C_1, C_2, C_3, C_1', C_2', C_3')$ to $\mathscr{A}$ as its challenge ciphertext.

Query Phase 2. $\mathscr{A}$ adaptively launches private key query as in phase 1. $\mathscr{B}$ answers the queries as in phase 1.

Guess. $\mathscr{A}$ gives a guess $\beta' \in \{0, 1\}$ on $\mathscr{B}$. $\mathscr{B}$ returns β' as its guess for γ. Obviously, $\mathscr{B}$ has appropriately simulated Game$_1$.

If $\mathcal{A}$ has a nonnegligible advantage in Game_1, then $\mathcal{B}$ attacks the scheme in [33] at a nonnegligible advantage.

Now we have proven that the Basic CP-ABE scheme is selectively CPA-secure. After that we prove that if Basic CP-ABE scheme is selectively CPA-secure, then our new scheme is selectively CPA-secure. □

Theorem 9. *Assume that Basic CP-ABE scheme is selectively CPA-secure. Then our new scheme is selectively CPA-secure.*

Proof. If $\mathcal{A}$ breaks our new CP-ABE scheme at nonnegligible advantage, then we find an algorithm $\mathcal{B}$ which breaks Basic CP-ABE scheme at nonnegligible advantage. We assume that $\mathcal{C}$ is the challenger with respect to $\mathcal{B}$ for Basic CP-ABE. $\mathcal{B}$ interacts with $\mathcal{A}$ as demonstrated in the following steps.

Init. $\mathcal{A}$ sends $\mathcal{B}$ its challenge access policy $\mathbb{A}^*$. $\mathcal{B}$ gives challenge access policy $\mathbb{A}^*$ to $\mathcal{C}$ and obtains the public parameters $\text{PK} = (e, g_1, h, u, v, d, Y, \{T_{i,j}\}_{i\in[1,n],j\in[1,n_i]}, H)$ for Basic CP-ABE.

Setup. $\mathcal{B}$ sends PK to $\mathcal{A}$.

Query Phase 1. $\mathcal{B}$ maintains a table Tb and a set D which are initialized as empty. $\mathcal{A}$ adaptively launches queries.

(1) Private Key Query on Attribute Set S. $\mathcal{B}$ obtains the private key SK_S by calling the key generation oracle of $\mathcal{C}$ with respect to S. Then, $\mathcal{B}$ lets $D = D \cup \{S\}$ and sends the private key SK_S to $\mathcal{A}$.

(2) Transformation Key Query on Attribute Set S. $\mathcal{B}$ scans the tuple $(S, \text{SK}_S, \text{TK}_S, \text{RK}_S)$ in table Tb. If such a tuple exists, it sends the transformation key TK_S to $\mathcal{A}$. Otherwise, $\mathcal{B}$ selects random exponents $z, r \in \mathbb{Z}_p$. $\mathcal{B}$ computes $K_1' = h^z(g_1^{\sum_{v_{i,j}\in S} t_{i,j}})^r$ and $K_2' = g_1^r$. $\mathcal{B}$ stores the tuple $(S, *, \text{TK}_S = (S, K_1', K_2'), z)$ in table Tb and returns TK_S to $\mathcal{A}$. Observe that $\mathcal{B}$ does not know the actual retrieving key $\text{RK}_S = y/z$. Here, we compute as follows:

$$\begin{aligned}\frac{e(C_2, K_1')}{e(C_3, K_2')} &= \frac{e\left(g_1^s, h^z\left(g_1^{\sum_{v_{i,j}\in S} t_{i,j}}\right)^r\right)}{e\left(\left(\prod_{v_{i,j}\in\mathbb{A}} T_{i,j}\right)^s, g_1^r\right)} \\ &= \frac{e(g_1,h)^{sz}\, e(g_1,g_1)^{sr\sum_{v_{i,j}\in S} t_{i,j}}}{e(g_1,g_1)^{sr\sum_{v_{i,j}\in\mathbb{A}} t_{i,j}}} \\ &= e(g_1,h)^{sz} = T', \\ \frac{C_1}{T'^{\text{RK}_S}} &= M \cdot \frac{e(g_1,h)^{ys}}{e(g_1,h)^{sz\cdot y/z}} = M.\end{aligned} \tag{4}$$

Challenge. $\mathcal{A}$ submits messages M_0, M_1 with same length and challenge access policy $\mathbb{A}^*$. $\mathcal{B}$ gives M_0, M_1 and $\mathbb{A}^*$ to $\mathcal{C}$ to obtain the challenge ciphertext CT^*. $\mathcal{B}$ returns CT^* to $\mathcal{A}$ as its challenge ciphertext.

Query Phase 2. $\mathcal{A}$ adaptively launches private key query as in phase 1, and $\mathcal{B}$ answers the queries as in phase 1.

Guess. $\mathcal{A}$ obtains μ'. $\mathcal{B}$ also obtains μ'.

If the guess μ' for $\mathcal{A}$ of our scheme is correct, the guess of $\mathcal{B}$ for Basic CP-ABE scheme is correct too. So we can conclude that if $\mathcal{A}$ can attack our scheme at nonnegligible advantage, then we will find an algorithm $\mathcal{B}$ which attacks Basic CP-ABE scheme under the selective CPA security model at nonnegligible advantage. □

Theorem 10. *Our CP-ABE scheme is verifiable if the discrete logarithm assumption defined in Section 2.2 holds.*

Proof. Suppose that there exists an adversary $\mathcal{A}$ that attacks verifiability of our new scheme at nonnegligible advantage. We find an algorithm $\mathcal{B}$ that can solve the DL problem at nonnegligible advantage.

Setup. $\mathcal{B}$ chooses $x, y, m, l \in_R \mathbb{Z}_p$, $h \in_R G_1$, and $t_{i,j} \in_R \mathbb{Z}_p$ $(i \in [1,n], j \in [1,n_i])$. $H : G_T \to \mathbb{Z}_p^*$ is a secure hash function. $\text{PK} = (e, g_1, h, u = g_1^x, v = g_1^m, d = g_1^l, Y = e(g_1,h)^y, \{T_{i,j}\}_{i\in[1,n],j\in[1,n_i]}, H)$ is the public parameter. The master secret key is $\text{MK} = (y, \{t_{i,j}\}_{i\in[1,n],j\in[1,n_i]})$. $\mathcal{B}$ returns PK to $\mathcal{A}$.

Query Phase 1. $\mathcal{A}$ adaptively launches transformation key, private key, decryption, and $\text{Decryption}_{\text{out}}$ queries. As $\mathcal{B}$ knows MK, it can answer the queries properly.

Challenge. $\mathcal{A}$ gives M^* and challenge access policy $\mathbb{A}^*$ to $\mathcal{B}$. $\mathcal{B}$ computes the ciphertext CT^* of M^* using the encryption algorithm in [33] and returns $\text{CT}^* = (\mathbb{A}^*, \widehat{C}, C_1, C_2, C_3, C_1', C_2', C_3')$ to $\mathcal{A}$, where $\widehat{C} = u^{H(M^*)}v^{H(\widetilde{M}^*)}d$ and $\widetilde{M}^* \in G_T$ is chosen by $\mathcal{B}$ randomly.

Query Phase 2. $\mathcal{A}$ adaptively launches private key queries as in phase 1. $\mathcal{B}$ answers queries as in phase 1.

Output. $\mathcal{A}$ returns attribute set S^* and transformed ciphertext $\text{CT}^{*\prime} = (\widehat{T} = \widehat{C}, T_1 = C_1, T_1' = C_1', T', T'')$.

$\mathcal{B}$ computes $T_1/T'^{z_{S^*}} = M$ and $T_1'/T''^{z_{S^*}} = \widetilde{M}$, where z_{S^*} is the retrieving key for attribute set S^*. If $\mathcal{A}$ wins the above game, then $\mathcal{B}$ can obtain

$$\begin{aligned} g_1^{xH(M^*)+mH(\widetilde{M}^*)+l} &= u^{H(M^*)}v^{H(\widetilde{M}^*)}d = \widehat{C} = \widehat{T} \\ &= u^{H(M)}v^{H(\widetilde{M})}d = g_1^{xH(M)+mH(\widetilde{M})+l}, \end{aligned} \tag{5}$$

where $M \neq M^*$ and $M^*, \widetilde{M}^*, M, \widetilde{M}, m, l$ are obtained by $\mathcal{B}$. Because H is a collision-resistant hash function, $H(M^*)$ is not equal to $H(M)$ with overwhelming probability. Thus, $\mathcal{B}$ gets $x = m(H(\widetilde{M}^*) - H(\widetilde{M}))/(H(M) - H(M^*))$, which breaks the DL assumption. It is paradoxical, so our CP-ABE scheme is verifiable □

Table 1: Size of each value.

	PK	MK	SK	CT	TK	RK	CT′
LCL 13 [11]	$(n+4)\lvert G_1\rvert$	$\lvert\mathbb{Z}_p\rvert$	None	$(N_1+2)\lvert G_1\rvert+\lvert G_T\rvert$	$2N_2\lvert G_1\rvert$	$2\lvert G_1\rvert$	$2\lvert G_1\rvert+2\lvert G_T\rvert$
LDG 13 [31]	$(5+n)\lvert G_1\rvert+\lvert G_T\rvert$	$\lvert\mathbb{Z}_p\rvert$	$(2+N_2)\lvert G_1\rvert$	$(4N_1+3)\lvert G_1\rvert+2\lvert G_T\rvert$	$(2+N_2)\lvert G_1\rvert$	$\lvert\mathbb{Z}_p\rvert$	$\lvert G_1\rvert+4\lvert G_T\rvert$
GHW 11 [12]	$2\lvert G_1\rvert+\lvert G_T\rvert$	$\lvert\mathbb{Z}_p\rvert$	None	$(2N_1+1)\lvert G_1\rvert+\lvert G_T\rvert$	$(2+N_2)\lvert G_1\rvert$	$\lvert\mathbb{Z}_p\rvert$	$2\lvert G_T\rvert$
Our scheme	$(N+5)\lvert G_1\rvert+\lvert G_T\rvert$	$(N+1)\lvert\mathbb{Z}_p\rvert$	$2\lvert G_1\rvert$	$5\lvert G_1\rvert+2\lvert G_T\rvert$	$2\lvert G_1\rvert$	$\lvert\mathbb{Z}_p\rvert$	$\lvert G_1\rvert+4\lvert G_T\rvert$

Table 2: Computational times.

	Encrypt	Decrypt	Transform	$\text{Decrypt}_{\text{out}}$
LCL 13 [11]	$C_e+2G_T+(3+2N_1)G_1$	None	$2(N_2-1)C_e+2N_2G_T$	$2C_e+3G_T$
LDG 13 [31]	$2H+(10+8N_1)G_1+4G_T$	$4(N_2-1)C_e+4N_2G_T$	$(4N_2-2)G_T+(4N_2-2)C_e$	$4G_T$
GHW 11 [12]	$(4N_1+1)G_1+3G_T+N_1H$	None	$(3N_2-1)G_1+(N_2+1)G_T+(N_2+2)C_e$	$2G_T$
Our scheme	$2H+(2N_1+6)G_1+4G_T$	$4C_e+4G_T$	$4C_e+2G_T$	$4G_T$

Table 3: Property of each scheme.

	Outsourcing	Verifiability	Constant ciphertext length
LCL 13 [11]	Yes	No	No
LDG 13 [31]	Yes	Yes	No
GHW 11 [12]	Yes	No	No
Our scheme	Yes	Yes	Yes

5. Performance Comparison

PK, MK, SK, CT, TK, RK, and CT′ represent the length of public key, master key, private key, ciphertext, transform key, retrieving key, and transformed ciphertext without the access policy, respectively. Additionally, Encrypt, Decrypt, Transform, and $\text{Decrypt}_{\text{out}}$ represent the computational costs of the algorithms' encryption, decryption, transformation, and outsourcing decryption, respectively. $|G_1|$, $|G_T|$, and $|\mathbb{Z}_p|$ denote the bit-length of the elements belonging to G_1, G_T, and $\mathbb{Z}_p$. kC_e, kH, and kG_1 denote the k-times computation in the pairing, hash function, and group G_1, respectively. $U = \{\text{att}_1, \ldots, \text{att}_n\}$ denote the attribute universe. N_1 and N_2 are the amounts of the attributes related to ciphertext and private key, respectively. $N = \sum_{i=1}^{n} n_i$ denotes the total number of possible attribute values.

Tables 1–3 show that our scheme is efficient. Table 1 illustrates that the size of private key, ciphertext, and transform key in our scheme is constant. However, the size of private key, ciphertext, and transform key in [11, 12, 31] depends upon the number of attributes. Therefore, our scheme greatly reduces the communication overhead and is very suitable for bandwidth limited devices. As the operation cost over $\mathbb{Z}_p$ is much smaller than group and pairing operation, we ignore the computation time over $\mathbb{Z}_p$. Compared with the scheme in [11, 12, 31], the computational overhead for the decryption and transformation operations in our scheme is much smaller. From Table 2, we observe that the computational overhead over group and pairing in [11, 12, 31] depends on the number of attributes, while it is constant in our scheme. The computational overhead for the outsourcing decryption is constant in above schemes. Table 3 illustrates that only our scheme satisfies all properties.

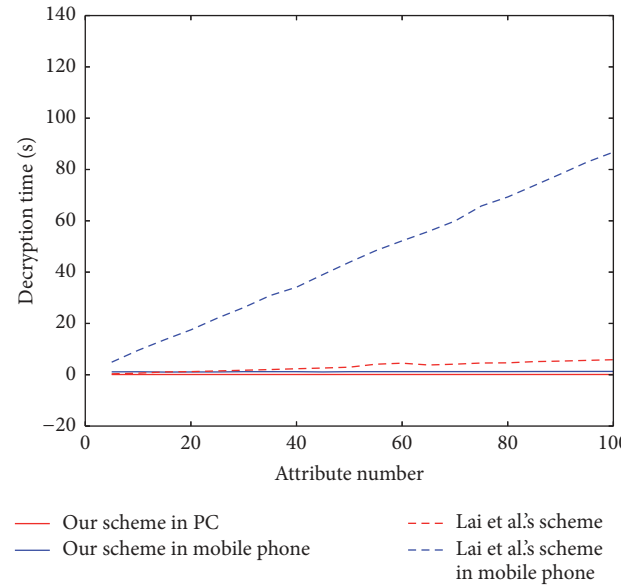

Figure 2: Decryption time.

In order to evaluate the efficiency for our scheme, we implement our scheme with java pairing-based cryptography (JPBC) library [36], a port for the pairing-based cryptography (PBC) library in C [37]. The elliptic curve parameter we choose is type-A, and the order of group is 160 bits. We run our code on a PC with 64-bit 2.6-GHz Intel Core i5-3320M CPU, with 6 GB RAM, and mobile phone with 4-core 1.8 GHz Processor 2 G memory Android OS 4.4.2, respectively. We also implement the scheme [31] for comparison. Figure 2 compares the times of decryption algorithm spent in our scheme and Lai et al.'s scheme [31]. The result shows that our scheme is much more efficient than Lai et al.'s scheme [31] because the time spent in our scheme does not grow with the amount of attributes involved in the access policy. Figure 3 shows the time of the transformation algorithm in PC and mobile phone for two schemes. Similar to the decryption algorithm, the time required by transformation grows linearly with the number of attributes for Lai et al.'s scheme [31],

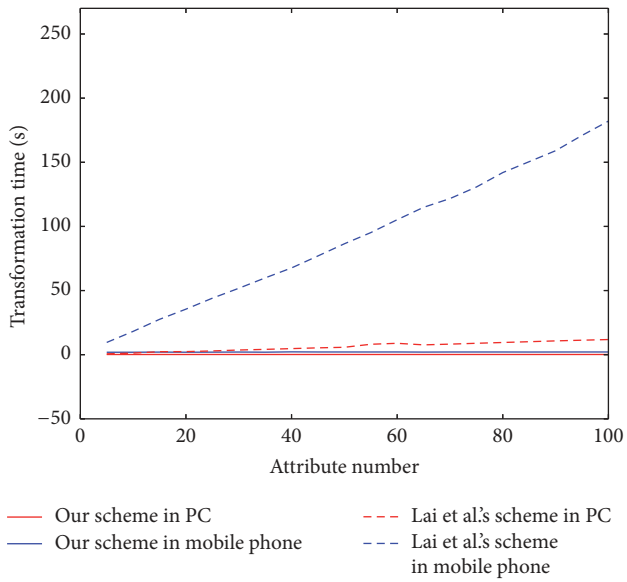

Figure 3: Transformation time.

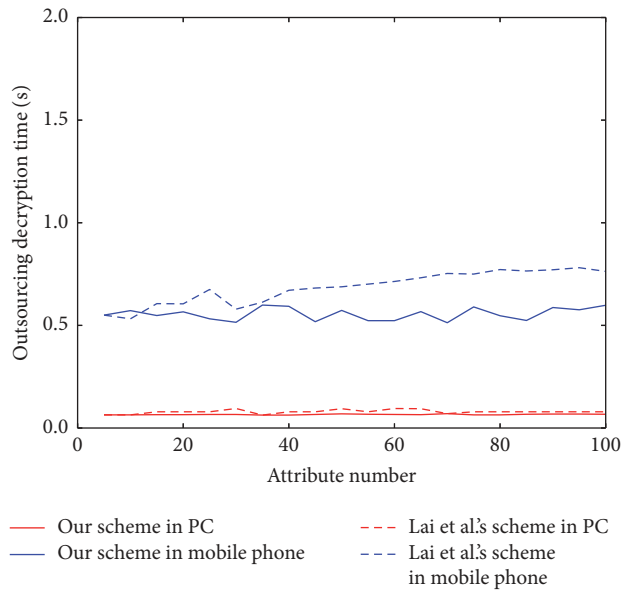

Figure 4: Outsourcing decryption time.

while it is almost constant for our scheme. Figure 4 shows that the times of the outsourcing decryption algorithm in PC and mobile phone for two schemes are nearly same. Figure 5 shows the ciphertext length in our scheme and Lai et al.'s scheme [31]. We can find that the ciphertext length in our scheme is constant, while it will grow with the amount of attributes involved in access policy linearly. So we can conclude that our scheme greatly reduces the communication overhead and is very suitable for bandwidth limited devices. Figure 6 illustrates that the length of partially decrypted ciphertext in two schemes is almost same.

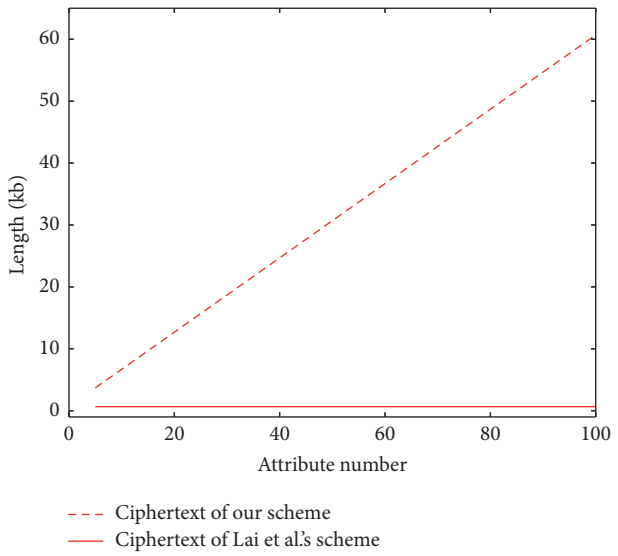

Figure 5: Ciphertext length.

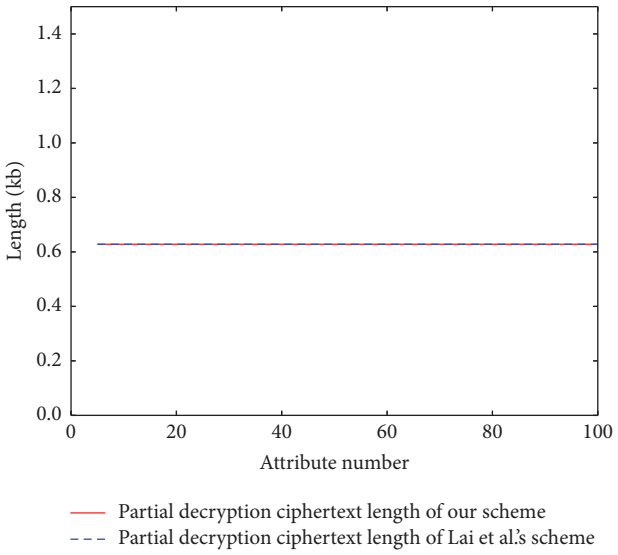

Figure 6: Partial decryption ciphertext length.

6. Conclusions

In this article, we propose a new verifiable outsourced CP-ABE scheme with constant ciphertext length and, moreover, we prove that our scheme is secure and verifiable in standard model. Security in our scheme is reduced to that of scheme in [33] and verifiability is reduced to DL assumption. The computational overhead for the decryption and transformation operations in our scheme is constant, which does not rely on the amount of attributes. In addition, we outsource the expensive operation to the cloud service provider and leave the slight operations to be done on user's device. Therefore, our scheme is very efficient. What is more, the ciphertext length in our scheme does not grow with the number of attributes, which reduces the communication cost greatly. The proposed scheme has the potential application in various

lower power devices with limited computational power, such as mobile phone.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This research is supported by the National Natural Science Foundation of China (61272542, 61472083, 61202450, 61402110, and 61672207), Jiangsu Provincial Natural Science Foundation of China (BK20161511), the Priority Academic Program Development of Jiangsu Higher Education Institutions, the Fundamental Research Funds for the Central Universities (2016B10114), Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology, and the Project of Scientific Research Innovation for College Graduate Student of Jiangsu Province (KYZZ15_0151).

References

[1] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proceedings of the 21st Annual International Cryptology Conference (CRYPTO '01), Santa Barbara, Calif, USA, August 2001*, vol. 2139 of *Lecture Notes in Computer Science*, pp. 213–229, Springer, Berlin, Germany, 2001.

[2] V. Goyal, O. Pandey, A. Sahai, and B. 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)*, pp. 89–98, ACM, November 2006.

[3] J. Li, C. Jia, J. Li, and X. Chen, "Outsourcing encryption of attribute-based encryption with MapReduce," in *Information and Communications Security*, T. W. Chim and T. H. Yuen, Eds., vol. 7618 of *Lecture Notes in Computer Science*, pp. 191–201, Springer, Berlin, Germany, 2012.

[4] A. Lewko and B. Waters, "Unbounded HIBE and attribute-based encryption," in *Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT '11), Tallinn, Estonia, May 2011*, vol. 6632 of *Lecture Notes in Computer Science*, pp. 547–567, Springer, Berlin, Germany, 2011.

[5] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the IEEE Symposium on Security and Privacy (SP '07)*, pp. 321–334, May 2007.

[6] B. D. Qin, R. H. Deng, S. L. Liu, and S. Q. Ma, "Attribute-based encryption with efficient verifiable outsourced decryption," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 7, pp. 1384–1393, 2015.

[7] H. Deng, Q. Wu, B. Qin et al., "Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts," *Information Sciences*, vol. 275, pp. 370–384, 2014.

[8] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*, pp. 195–203, ACM, Alexandria, Va, USA, November 2007.

[9] T. Okamoto and K. Takashima, "Fully secure functional encryption with general relations from the decisional linear assumption," in *Advances in Cryptology—CRYPTO 2010*, T. Rabin, Ed., vol. 6223 of *Lecture Notes in Computer Science*, pp. 191–208, Springer, Berlin, Germany, 2010.

[10] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*, pp. 456–465, November 2007.

[11] J. Li, X. Chen, J. Li, C. Jia, J. Ma, and W. Lou, "Fine-grained access control system based on outsourced attribute-based encryption," in *Computer Security—ESORICS 2013*, J. Crampton, S. Jajodia, and K. Mayes, Eds., vol. 8134 of *Lecture Notes in Computer Science*, pp. 592–609, Springer, Berlin, Germany, 2013.

[12] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," in *Proceedings of the 20th USENIX Conference on Security (SEC '11)*, p. 34, 2011.

[13] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Transactions on Information and System Security*, vol. 9, no. 1, pp. 1–30, 2006.

[14] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Advances in Cryptology—EUROCRYPT'98*, K. Nyberg, Ed., vol. 1403 of *Lecture Notes in Computer Science*, pp. 127–144, Springer, Berlin, Germany, 1998.

[15] M. Chase, "Multi-authority attribute based encryption," in *Proceedings of the 4th Theory of Cryptography Conference (TCC '07), Amsterdam, The Netherlands, February 2007*, Lecture Notes in Computer Science, pp. 515–534, Springer, Berlin, Germany, 2007.

[16] Z. Liu, Z. Cao, Q. Huang, D. S. Wong, and T. H. Yuen, "Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles," in *Computer Security—ESORICS 2011: 16th European Symposium on Research in Computer Security, Leuven, Belgium, September 12–14,2011. Proceedings*, vol. 6879 of *Lecture Notes in Computer Science*, pp. 278–297, Springer, Berlin, Germany, 2011.

[17] J. G. Han, W. Susilo, Y. Mu, and J. Yan, "Privacy-preserving decentralized key-policy attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 11, pp. 2150–2162, 2012.

[18] H. L. Qian, J. G. Li, and Y. C. Zhang, "Privacy-preserving decentralized ciphertext-policy attribute-based encryption with fully hidden access structure," in *Proceedings of the 15th International Conference on Information and Communications Security (ICICS '13)*, vol. 8233 of *Lecture Notes in Computer Science LNCS*, pp. 363–372, Springer, Berlin, Germany, 2013.

[19] H. L. Qian, J. G. Li, Y. C. Zhang, and J. G. Han, "Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation," *International Journal of Information Security*, vol. 14, no. 6, pp. 487–497, 2015.

[20] Z. Liu, Z. F. Cao, and D. S. Wong, "Blackbox traceable CP-ABE: how to catch people leaking their keys by selling decryption devices on eBay," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS '13)*, pp. 475–486, Berlin, Germany, November 2013.

[21] Z. Liu, Z. F. Cao, and D. S. Wong, "White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 76–88, 2013.

[22] J. T. Ning, Z. F. Cao, X. L. Dong, L. F. Wei, and X. D. Lin, "Large universe ciphertext-policy attribute-based encryption with white-box traceability," in *Computer Security—ESORICS 2014: 19th European Symposium on Research in Computer*

Security, Wroclaw, Poland, September 7–11, 2014. Proceedings, Part II, vol. 8713 of *Lecture Notes in Computer Science*, pp. 55–72, Springer, Berlin, Germany, 2014.

[23] J. G. Li, W. Yao, Y. C. Zhang, H. L. Qian, and J. G. Han, "Flexible and fine-grained attribute-based data storage in cloud computing," *IEEE Transactions on Services Computing*, 2016.

[24] J. G. Li, X. N. Lin, Y. C. Zhang, and J. G. Han, "KSF-OABE: outsourced attribute-based encryption with keyword search function for cloud storage," *IEEE Transactions on Services Computing*, 2016.

[25] J. G. Li, Y. R. Shi, and Y. C. Zhang, "Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage," *International Journal of Communication Systems*, 2015.

[26] Z. J. Fu, X. M. Sun, Q. Liu, L. Zhou, and J. G. Shu, "Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing," *IEICE Transactions on Communications*, vol. 98, no. 1, pp. 190–200, 2015.

[27] Z. H. Xia, X. H. Wang, X. M. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 2, pp. 340–352, 2015.

[28] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 9, pp. 2546–2559, 2016.

[29] J. G. Li, H. P. Wang, Y. C. Zhang, and J. Shen, "Ciphertext-policy attribute-based encryption with hidden access policy and testing," *KSII Transactions on Internet and Information Systems*, vol. 10, no. 8, pp. 3339–3352, 2016.

[30] Y.-J. Ren, J. Shen, J. Wang, J. Han, and S.-Y. Lee, "Mutual verifiable provable data auditing in public cloud storage," *Journal of Internet Technology*, vol. 16, no. 2, pp. 317–323, 2015.

[31] J.-Z. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 8, pp. 1343–1354, 2013.

[32] J. Li, X. Y. Huang, J. W. Li, X. F. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 8, pp. 2201–2210, 2014.

[33] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A Ciphertext-policy attribute-based encryption scheme with constant ciphertext length," in *Information Security Practice and Experience: 5th International Conference, ISPEC 2009 Xi'an, China, April 13–15, 2009 Proceedings*, vol. 5451 of *Lecture Notes in Computer Science*, pp. 13–23, Springer, Berlin, Germany, 2009.

[34] J. Herranz, F. Laguillaumie, and C. Rafols, "Constant size ciphertexts in threshold attribute-based encryption," in *Proceedings of the 13th International Conference on Practice and Theory in Public Key Cryptography (PKC '10), Paris, France, May 2010*, vol. 6056 of *Lecture Notes in Computer Science*, pp. 19–34, Springer, Berlin, Germany, 2010.

[35] R. Canetti, H. Krawczyk, and J. B. Nielsen, "Relaxing chosen-ciphertext security," in *Proceedings of the 23rd Annual International Cryptology Conference (CRYPTO '03), Santa Barbara, Calif, USA, August 2003*, vol. 2729 of *Lecture Notes in Computer Science*, pp. 565–582, Springer, Berlin, Germany, 2003.

[36] A. D. Caro, "Java pairing-based cryptography library," 2012, http://libeccio.dia.unisa.it/projects/jpbc/.

[37] B. Lynn, PBC (Pairing-Based Cryptography) Library, 2012, http://crypto.stanford.edu/pbc/.