Ciphertext-Policy Attribute-Based Encryption Against Post-challenge Continuous Auxiliary Inputs Leakage

Yuyan Guo, Zhenhua Lu, Mingming Jiang, and Dongbing Zhang
(Corresponding author: Zhenhua Lu)

Department of Computer Science and Technology, Huaibei Normal University
Huaibei, Anhui 235000
Email: adrienlu@163.com

(Received Aug. 21, 2021; Revised and Accepted Jan. 13, 2022; First Online Apr. 9, 2022)

Abstract

Leakage-resilient attribute-based encryption (ABE) is widely used because it not only ensures data security but also enables fine-grained access. However, most leak-resistant ABE schemes consider only continuous and auxiliary input leakage models and are not concerned with post-challenge leakage. We propose a security model for post-challenge continuous auxiliary input (pCAI) leakage by combining the post-challenge leakage model with the continuous leakage model and the auxiliary input leakage model. Moreover, we propose a CP-ABE scheme that can protect against the continuous leakage of the secret user key and masters private key and the post-challenge leakage. The security of the proposed scheme is proved under the assumption of composite order bilinear group using dual-system encryption technology. At last, the scheme is proved to be effective through performance comparison with other schemes.

Keywords: Ciphertext-Policy Attribute-Based Encryption; Dual System Encryption; Linear Secret Sharing Scheme; Post-Challenge Continuous Auxiliary Inputs Leakage

1 Introduction

Nowadays, it has become the norm for users to store important data and information in cloud servers. However, due to the different types, quantities, and importance of information stored on cloud servers, personal data will become increasingly insecure [10]. On this basis, many encryption schemes have been proposed. In 2005, the concept of attribute-based encryption (ABE) was first proposed by Sahai and Waters [21], which is a new and improved encryption scheme for identity-based encryption (IBE). The difference between ABE and IBE is that the identity in an ABE scheme is regarded as a set of attributes. However, in their scheme, the threshold parameter is set by the authorized institution, besides the access structure cannot be determined by the sender. More importantly, in practical applications, the access structure needs to be more flexible to support different attribute operations. Therefore, Goyal *et al.* [8] proposed key-policy ABE (KP-ABE), in which the ciphertext is associated with a set of attributes, and the access policy is embedded in the key. In addition, Bethencourt *et al.* [3] proposed ciphertext policy ABE (CP-ABE), in which the key and attribute set and access policy are embedded in the ciphertext. After that, many ABE solutions were proposed, such as ABE with verifiable outsourcing decryption [14], ABE data sharing scheme [1], multi-authority ABE [2,17,20], traceable ABE [19], anonymous ABE [7,27], ABE under the hash proof system [30] and hierarchical ABE [11,15].

Traditional cryptosystems are secure primarily because the keys are not exposed, however, this is an ideal assumption. In recent years, the emergence of side-channel attacks has shattered this ideal assumption. In practice, various leaked information generated during the encryption operation can be used to obtain secret information, such as secret key information. Such attacks are known as side channel attacks. Many studies have shown that there are different attack methods for side-channel attacks and some schemes are also vulnerable to attacks [2,4,6]. Therefore, the introduction of leakage-resilient encryption technology guarantees the security of the scheme. Only computation leakage model [18], bounded retrieval model [6] and other leakage models have been proposed. In these models, the key has the ability resilient to leakage and can withstand certain leakage. However, these two leakage models do not consider the continuous leakage of the keys.

After that, the emergence of the continuous leakage model can allow the key to be continuously updated [12,15,16]. The model can get the updated secret key and the updated master private key through the

key update algorithm, which further improves the leakage-resilient capability. In 2009, The concept of auxiliary input (AI) leakage model was first given by Dodis *et al.* [5], then Yuen *et al.* [25] first proposed an IBE scheme that is resilient to AI leakage and proved its security. However, The security model in above schemes only considers the leakage that occurs before the challenge phase, but does not consider the leakage after the challenge phase. Therefore, Halevi *et al.* first proposed after-the-fact disclosure and formulates the concept of entropic leakage public-key cryptography in [9], which allows leakage after the challenge ciphertext is generated. Subsequently, the post-attack auxiliary input (pAI) leakage was defined by Yuen *et al.* [26], and an IBE scheme against pAI leakage is given in [26].

1.1 Related Work

The original ABE structure can only be used for the specified threshold access strategy. Since then, in order to apply the ABE scheme to variety scenarios, linear secret sharing schemes [2], monotonic span programs (MSPs) [13], minimum sets [29] and Boolean formulas began to appear in many ABE schemes as access structures. In [23], Waters constructed a CP-ABE scheme under the assumption of concrete rather than interactive passwords, using the LSSS matrix as the access structure. Lewko *et al.* [13] used Monotonic Span Program (MSP) as the access structure to construct ABE schemes and proved that it has adaptive security in complex bilinear groups. Then Zhang *et al.* [29] propose two ABE schemes with the access structure encoded as a minimum set, Zhang *et al.* [30] proposed the attribute-based hash proof system (AB-HPS) and gave the structure of AB-HPS in the lattice. However, this scheme is not efficient because the leakage rate is related to the ciphertext and key size.

After this, many leakage-resilient ABE schemes were proposed. Later, Li *et al.* [15] propose a hierarchical ABE scheme of ciphertext strategy with continuous leakage recovery capability, the security is proved under the assumption of composite order bilinear group using dual-system encryption technology. Wang *et al.* [22] proposed for the first time a CP-ABE scheme resilient to auxiliary inputs leakage, and proved the scheme is full security. Recently, an ABE scheme was constructed under the hypothesis of truncated decision q-augmented bilinear Diffie-Hellman exponent (q-ABDHE) [28], and the scheme was proved to be CCA2 security. Ma *et al.* [17] proposed a multi-authority ABE scheme against auxiliary input leakage, Li *et al.* [16] proposed a specific KP-ABE scheme against continuous auxiliary input leakage, and proved security under static assumptions. However, none of the above ABE schemes can achieve post-challenge continuous auxiliary input (pCAI) leakage, so it is of great significance to structure a pCAI-CP-ABE scheme.

1.2 Our Motivation and Contributions

According to the above trends, there are few studies on the ABE scheme for post-challenge continuous auxiliary input (pCAI). However, the pCAI leakage model is more practical because it allows the leakage of key information after the challenge phase.

Based on the work of [16] and [22], we proposed the framework of CP-ABE, which can resilient to pCAI leakage, we also give its security model and a CP-ABE scheme against pCAI leakage. Our scheme uses the LSSS matrix as the access structure, so it has a certain degree of flexibility.

Due to the existence of the auxiliary input function, Goldreich-Levin (GL) theorem for Large Fields [5] is used for divide master private key into several parts to resist leakage attacks. In the proof phase, we use the dual-system encryption technology, which divides the key and ciphertext into two types (such as normal and semi-functional) [24]. The semi-functional key is limited to decrypting normal ciphertext, while the normal key can decrypt normal ciphertext and semi-functional ciphertext. The master private key and user key will be randomized by using master private key update algorithm and secret key update algorithm to agsinst continuous leakage. In addition, a hard-to-invert strong extractor randomizes the user key to against post-challenge leakage. Therefore, this scheme prevents stronger key leakage compared with existing schemes.

1.3 Organization

In Section 2, some preliminaries were reviewed, including the three modified static assumptions proposed in Wang's proposal. In Section 3, we propose the security model and outline of CP-ABE against pCAI leakage. In Section 4, the structure of the scheme is proposed. In Section 5, the security of the program is proven through the use of dual-system encryption. In Section 6, the scheme is compared with other well-known schemes and performance comparison is given. In Section 7, a brief conclusion is given to summarize this work.

2 Preliminaries

2.1 Composite Order Bilinear Groups

First of all, the concept of bilinear group is reviewed as follows. Let G and G_T be the multiplicative groups of order $N = p_1p_2p_3$, g is a generator of G, p_1, p_2, p_3 are three different prime. Then $e : G \times G \to G_T$ is a bilinear map and it has these properties as follows:

1) Bilinearity: For $\forall x, y \in Z_N$, $e\left(g^x, g^y\right) = e(g, g)^{xy}$.

2) Non-degeneracy: $e(g, g) \neq 1_{G_T}$.

3) Computability: There is an algorithm to calculate e efficiently.

Now we show the definition of the composite order bilinear groups. It is similar to bilinear groups except the order of the group is the product of two or more distinct prime numbers. That is to say, G is a composite order group, G_{p_1}, G_{p_2}, G_{p_3} are its three subgroups of order p_1, p_2, p_3, and g_i are the generators of subgroups G_{p_i} (i=1,2,3). Any element $g \in G$ can be shown as the form of $g_1^{x_1} g_2^{x_2} g_3^{x_3}$, where $x_i \in Z_{p_i}$. $g_1^{x_1}$, $g_2^{x_2}$ and $g_3^{x_3}$ are respectively called the terms of the subgroups G_{p_1}, G_{p_2} and G_{p_3}. For $\forall \alpha \in G_{p_i}$ and $\forall \beta \in G_{p_j}$, If $\alpha \neq \beta$,$e(\alpha, \beta) = 1$. Let $G_{p_i p_j}$ represent a subgroup of order $p_i p_j$ in G. For $\forall R \in G_{p_i p_j}$, we define R be the product of a member of G_{p_i} and a member of G_{p_j}. Similarly, $G_{p_1 p_3}$ and $G = G_{p_1 p_2 p_3}$ can be defined.

2.2 Complexity Hardness Assumptions

First, we show the original three complexity assumptions that are used in many constructs [12, 29].

Assumption 1 (1-SDP assumption). Given $E = (N = p_1 p_2 p_3, G, G_T, e)$, no Probabilistic Polynomial-Time (PPT) adversary A has a non-negligible probability ε such that

$$\left| \begin{array}{l} \Pr\left[A\left(E, g_1, U_3, \Gamma_0\right) = 1\right] \\ -\Pr\left[A\left(E, g_1, U_3, \Gamma_1\right) = 1\right] \end{array} \right| \leq \varepsilon,$$

where $g_1 \in G_{p_1}$, $U_3 \in G_{p_3}$, $\Gamma_0 \in G_{p_1 p_2}$, $\Gamma_1 \in G_{p_1}$.

Assumption 2 (2-SDP assumption). Given $E = (N = p_1 p_2 p_3, G, G_T, e)$, no PPT adversary A has a non-negligible probability ε such that

$$\left| \begin{array}{l} \Pr\left[A\left(E, g_1, U_1 U_2, U_3, V_2 V_3, \Gamma_0\right) = 1\right] \\ -\Pr\left[A\left(E, g_1, U_1 U_2, U_3, V_2 V_3, \Gamma_1\right) = 1\right] \end{array} \right| \leq \varepsilon,$$

where $U_3 \in G_{p_3}$, $\Gamma_0 \in G_{p_1 p_2}$, $\Gamma_1 \in G_{p_1}$.

Assumption 3 (BSDP assumption). Given $E = (N = p_1 p_2 p_3, G, G_T, e)$, no PPT adversary A has a non-negligible probability ε such that

$$\left| \begin{array}{l} \Pr\left[A\left(E, g_1, g_1^a U_2, U_3, g_1^\theta V_2, W_2, \Gamma_0\right) = 1\right] \\ -\Pr\left[A\left(E, g_1, g_1^a U_2, U_3, g_1^\theta V_2, W_2, \Gamma_1\right) = 1\right] \end{array} \right| \leq \varepsilon,$$

where $g_1 \in G_{p_1}$, $U_2 V_2 \in G_{p_2}$, $U_3 \in G_{p_3}$, $\Gamma_0 \in G_{p_1 p_3}$, $\Gamma_1 \in G$.

Now we give the three modified assumptions already been used in [22]. Since Wang *et al.* has already proved it, we will not prove its hardness. Let $[l]$ denote $\{1, \cdots, l\}$. **Assumption 4 (modified 1-SDP assumption).** Given $E = (N = p_1 p_2 p_3, G, G_T, e)$, no PPT adversary A has a non-negligible probability ε such that

$$\left| \begin{array}{l} \Pr\left[A\left(E, g_1, U_3, \Gamma_{01}\right) = 1\right] \\ -\Pr\left[A\left(E, g_1, U_3, \Gamma_{11}\right) = 1\right] \end{array} \right| \leq \varepsilon,$$

$$\vdots$$

$$\left| \begin{array}{l} \Pr\left[A\left(E, g_1, U_3, \Gamma_{0l}\right) = 1\right] \\ -\Pr\left[A\left(E, g_1, U_3, \Gamma_{1l}\right) = 1\right] \end{array} \right| \leq \varepsilon,$$

where $g_1 \in G_{p_1}$,$U_3 \in G_{p_3}$,$\Gamma_{0i} \in G_{p_1 p_2}$,$\Gamma_{1i} \in G_{p_1}$.

Assumption 5 (modified 2-SDP assumption). Given $E = (N = p_1 p_2 p_3, G, G_T, e)$, no PPT adversary A has a non-negligible probability ε such that

$$\left| \begin{array}{l} \Pr\left[A\left(E, g_1, (U_{1i} U_{2i})_{i\in[l]}, U_3, V_2 V_3, \Gamma_0\right) = 1\right] \\ -\Pr\left[A\left(E, g_1, (U_{1i} U_{2i})_{i\in[l]}, U_3, V_2 V_3, \Gamma_1\right) = 1\right] \end{array} \right| \leq \varepsilon,$$

where $g_1 \in G_{p_1}$,$U_{2i}, V_2 \in G_{p_2}$,$U_3, V_3 \in G_{p_3}$,$\Gamma_0 \in G_{p_1 p_3}$,$\Gamma_1 \in G$.

Assumption 6 (modified BSDP assumption). Given $E = (N = p_1 p_2 p_3, G, G_T, e)$, no PPT adversary A has a non-negligible probability ε such that

$$\left| \begin{array}{l} \Pr\left[A\left(\begin{array}{l} E, g_1, \left(g_1^{1/\rho_i}\right)_{i\in[l]}, (P_i^{a_i} U_2)_{i\in[l]}, \\ U_3, \left(P_i^{\theta_i} V_2\right)_{i\in[l]}, W_2, \Gamma a_0 \end{array}\right) = 1\right] \\ -\Pr\left[A\left(\begin{array}{l} E, g_1, \left(g_1^{1/\rho_i}\right)_{i\in[l]}, (P_i^{a_i} U_2)_{i\in[l]}, \\ U_3, \left(P_i^{\theta_i} V_2\right)_{i\in[l]}, W_2, \Gamma_1 \end{array}\right) = 1\right] \end{array} \right| \leqslant \varepsilon,$$

where $a_i, \theta_i, \rho_i \in Z_N$, g_1,$P_i = g_1^{\rho_i} \in G_{p_1}$, $U_2, V_2, W_2 \in G_{p_2}$, $U_3 \in G_{p_3}$, $\Gamma_0 = \prod_{i=1}^{l} e(g_1, P_i)^{a_i \theta_i}$, $\Gamma_1 \in G_T$.

2.3 Linear Secret Sharing Scheme (LSSS) and Access Structure

Definition 1 (Access Structure). Assume that O = $\{attr_1, \cdots, attr_n\}$ is a set of attributes, $\mathcal{A} \subset 2^O$ is a non-empty subset of 2^O, where 2^O represents the set constituted by all subsets of O, that is, $\mathcal{A}$ is a non-empty set constituted by some subsets of O, We call $\mathcal{A}$ is an access structure on O. If for any P, Q satisfy the condition $P \in \mathcal{A}$ and $P \subseteq Q$, namely $Q \in \mathcal{A}$, then the set $\mathcal{A} \subseteq O$ is monotonic. Authorized set refers to the set in $\mathcal{A}$, on the contrary, the unauthorized set is not in $\mathcal{A}$.

Definition 2 (Linear Secret Sharing Scheme). Each row of the linear secret sharing matrix formed by access policy corresponds to an attribute value, that is, row vector and attribute value form a one-to-one mapping relationship. if the following two properties are satisfied, then a secret sharing scheme Σ on a set of $O = \{attr_1, \cdots, attr_n\}$ is called linear:

1) The shared secret key for each attribute is a vector formed on Z_N.

2) In scheme Σ, there is an $n \times m$ secret sharing matrix $\boldsymbol{A}$, whose row label is $b(i)$, $i \in \{1, 2, \ldots, l\}$. Given a secret sharing column vector $u = (\tau, u_2, \cdots, u_m)$, where $\tau \in Z_N$ is the secret key to be shared, $u_2, \cdots, u_m$ is selected at random, $\boldsymbol{A}u$ represents the vector of n shared secret keys according to Σ. Shared $\gamma_i = (\boldsymbol{A}u)_i$, that is the inner product $\boldsymbol{A}u$ belongs to the property $b(i)$, where b is a function that maps $i \in \{1, 2, \ldots, l\}$ to $b(i)$.

The LSSS matrix has an important feature, that is, linear reconstruction. Suppose Σ is a LSSS scheme representing access structure A, $Q \in A$ is an authorized set, then we can define $T \subset [n]$ as $T = \{i : b(i) \in Q\}$. If there has constant $\{\beta_i \in Z_N\}_{i \in T}$ that can be found in polynomial time such that $\{\gamma_i\}$ are valid shares of the secret key τ, then we have $\sum_{i \in T} \beta_i \gamma_i = \tau$. There is no such constant for any unauthorized set.

2.4 GL Theorem for Large Fields

Let q be a large prime and H be any subset of $GF(q)$, n be a positive integer. Let $h : H^n \to \{0,1\}^*$ be any function. Then choose random a vector $w \leftarrow GF(q)^n$, and randomly picks $u \leftarrow H^n$, compute $v \leftarrow h(u)$. If there exists a PPT distinguisher D runs in time δ such that

$$\left| \begin{array}{l} \Pr\left[D\left(v, w, \langle w, u \rangle\right) = 1\right] - \\ \Pr\left[z \leftarrow GF(q) : D\left(v, w, z\right) = 1\right] \end{array} \right| = \varepsilon,$$

Then exists an inverter A that runs in time $\delta' = \delta \cdot poly(n, |H|, 1/\varepsilon)$ such that

$$\Pr\left[u \leftarrow H^n, v \leftarrow f(u) : A(v) = u\right] \geqslant \frac{\varepsilon^3}{512nq^2}$$

3 CP-ABE with Post-challenge Continual Auxiliary Inputs

3.1 The Outline of CP-ABE

In our pCAI-CP-ABE, suppose $\mathcal{A}$ is a monotone access structure, Ω is a monotone attribute universe space. we define the security model of CP-ABE against post-challenge continual auxiliary inputs (pCAI-CP-ABE). First of all, we give the composition structure of CP-ABE, which is consisted of the following algorithms.

Setup $(1^k, \Omega)$***:*** This algorithm takes security parameter k and Ω as inputs, then it generates the public key *MPK* and master private key *MSK*.

KeyGen(*MSK*,$\mathbf{S}$***):*** Inputs the *MSK* and an attribute collection $\mathbf{S}$ of a user. It generates a secret key $SK_{\mathbf{S}}$.

Enc(*M*,$\mathcal{A}$***):*** Inputs a access structure $\mathcal{A}$ and a message *M*. It generates a ciphertext *C*.

Dec(*C*,$SK_{\mathbf{S}}$***):*** This algorithm takes *C* and $SK_{\mathbf{S}}$ as inputs, then it outputs *M* while $\mathbf{S}$ satisfies $\mathcal{A}$.

MSK-Update(*MPK*,*MSK* ***):*** Inputs *MPK* and *MSK*. It generates a new updated master private key MSK', where $|MSK| = |MSK'|$.

SK-Update(*MPK*,$SK_{\mathbf{S}}$***):*** Inputs *MPK* and $SK_{\mathbf{S}}$. It generates a new updated secret key $SK'_{\mathbf{S}}$, where $|SK_{\mathbf{S}}| = |SK'_{\mathbf{S}}|$.

3.2 Security Model of pCAI-CP-ABE

Based on [22], the security model of pCAI-CP-ABE is given. Let H_1 and H_2 be the polynomial-time computable function family, $\mathcal{A}^*$ is the challenge access structure. The security model of CP-ABE against the pCAI leakage model is defined by an indistinguishable game between adversary A and challenge B. A sends H_1 and H_1 to the challenge B. First, B define three lists L_{MSK}, $L_{SK} = (cnt, SK_{\mathbf{S}}, \mathbf{S})$, $L_{SK'} = (cnt', SK'_{\mathbf{S}}, \mathbf{S})$, where *cnt* and cnt' are two different counters and L_{MSK}, L_{SK} and $L_{SK'}$ are all empty at the beginning.

Setup. The Setup algorithm is first run by challenger B to generate *MPK* and *MSK*, and *MPK* is output to A.

Phase 1. A can issue the following query adaptively:

Secret Key Query: First takes an attribute set $\mathbf{S} \subset \Omega$ as input, B check the tuple L_{SK} with the form $(cnt, SK_{\mathbf{S}}, \mathbf{S})$. if there does not exist such tuple, KeyGen(MPK,MSK) is run by B to generate secret key SK_S and lets $cnt = 1$. Then, B adds $(cnt, SK_{\mathbf{S}}, \mathbf{S})$ to L_{SK}. Otherwise, it returns $SK_{\mathbf{S}}$ from the tuple $(cnt, SK_{\mathbf{S}}, \mathbf{S})$ and lets $cnt = cnt + 1$.

Pre-challenge Leakage Query: Input $h_i \in H_1$, then B returns $h_i(L_{MSK}, MSK, SK_{\mathbf{S}}, MPK, L_{SK}, \mathbf{S})$ to A.

MSK-Update Query: B first runs MSK-Update algorithm to get MSK', it then puts the MSK' into the L_{MSK}.

SK-Update Query: B first check the tuple with the form $(cnt', SK'_{\mathbf{S}}, \mathbf{S})$, if there does not exist such tuple then let $cnt' = 1$, and B runs *SK-Update* algorithm to get $SK'_{\mathbf{S}}$, it then puts the $SK'_{\mathbf{S}}$ into the $L_{SK'}$. Otherwise, B return $SK'_{\mathbf{S}}$ from $(cnt', SK'_{\mathbf{S}}, \mathbf{S})$ and let $cnt' = cnt' + 1$.

Challenge. First, two messages of equal length M_0 and M_1 are submitted by A, then A outputs $\mathcal{A}^*$, where any $\mathbf{S}$ does not satisfy $\mathcal{A}^*$. B samples a random bit $b \in \{0,1\}$, the ciphertext C^* is outputs to A.

Phase 2. A can issue the following query adaptively:

Secret Key Query: This query is same as the phase 1, but the attribute set that satisfies $\mathcal{A}^*$ cannot be queried by A.

Post-challenge Leakage Query: Input $h'_{i'} \in H_2$, then B samples the randomness of encryption $r' \in \{0,1\}^*$ and returns $h'_{i'}(r')$.

Guess. A submits a guess b' of b, thus we can define the advantage of A is $Adv_A^{pCAI-CPA}(\Omega) = |2\Pr[b = b] - 1|$.

A CP-ABE scheme is pCAI-CPA secure in the pCAI leakage model for H_1 and H_2 if there is no PPT adversary A with non-negligible advantage in the above game.

Auxiliary Functions. We give the definition of two families of functions H_1 and H_2. They are regarded as one-way families of $H_{ow}(f(k_e))$ and $H_{\mathcal{A}^*-ow}(f(k_e))$ functions, respectively. And we will give the definitions of $H_{ow}(f(k_e))$ and $H_{\mathcal{A}^*-ow}(f(k_e))$ later.

Let W^* represents the set of all private keys satisfying the challenge access $\mathcal{A}^*$, and W represents the set of q_s private keys such that $W \cap W^* = \emptyset$, where q_s represents the total number of times A made Secret Key Query. In order to facilitate, let $H_{ow}(f(k_e))$ and $H_{\mathcal{A}^*-ow}(f(k_e))$ are parameterized by the min-entropy k_e of the attribute secret key, where k_e is the length of key while key is random generated.

$H_{\mathcal{A}^*\text{-}ow}(f(k_e))$: The class of all polynomial time computable function, all $i \in [1, q_{pre}]$ (where q_{pre} is the total number of times A made Pre-challenge Leakage Query.) and given

$$\{MPK, \mathcal{A}^*, W, \{h_i(MSK, L_{SK'}, MPK, \mathbf{S})\}_{i\in[q_{pre}]}\},$$

where all $h_i \in H_{\mathcal{A}^*-ow}(g(k_e))$. In this case, there is no PPT algorithm can find $SK_{\mathbf{S}^*}$ with a probability greater than $f(k_e)$, where $f(k_e) \geq 2^{-k_e}$ is the hardness parameter. Hence, we have $\{h_i\}_{i\in[q_{pre}]} \subseteq H_{\mathcal{A}^*-ow}(f(k_e))$.

$H_{ow}(f(k_e))$: The class of all polynomial time computable function $h'_{i'} : \{0,1\}^* \to \{0,1\}^*$, all $i' \in [1, q_{post}]$ (where q_{post} is the total number of times A made Post-challenge Leakage Query.) and given $h'_{i'}(r')$, where all $h'_{i'} \in H_{ow}(g(k_e))$. In this case, there is no PPT algorithm can find $SK_{\mathbf{S}^*}$ with a probability greater than $f(k_e)$, where $f(k_e) \geq 2^{-k_e}$ is the hardness parameter. Hence, we have $\{h'_{i'}\}_{i\in[q_{post}]} \subseteq H_{ow}(f(k_e))$.

Definition 3 (pCAI-CPA-CP-ABE). A CP-ABE scheme is said to be $f(k_e)$-pCAI-CPA secure, if the CP-ABE scheme is CPA secure with respect to the families $(H_{ow}(f(k_e)), H_{\mathcal{A}^*-ow}(f(k_e)))$.

3.3 Strong Extractor with Hard-to-invert Auxiliary Inputs

Definition 4. Let $Ext{:}\{0,1\}^{l_1} \times \{0,1\}^{l_2} \to \{0,1\}^n$, l_1, l_2, $n \in Z_N$. If for any PPT adversary A we have that

$$\left| \begin{array}{l} \Pr\left[A\left(r, h'_{i'}(\sigma), Ext(r,\sigma)\right) = 1\right] \\ -\Pr\left[A\left(r, h'_{i'}(\sigma), \theta\right) = 1\right] \end{array} \right| < \varepsilon,$$

Ext is said to be a strong extractor with $(\varepsilon, f(k_e))$-hard-to-invert auxiliary inputs, where $0 < \varepsilon < 1$, $r \in \{0,1\}^{l_1}$, $\sigma \in \{0,1\}^{l_2}$, $\theta \in \{0,1\}^n$, $h'_{i'} \in H_{ow}(g(k_e))$, $g(k_e) \geq 2^{-k_e}$ and $i' \in [1, q_{post}]$.

Lemma 1. Let $r \in \{0,1\}^{l_1}$ be chosen uniformly random, For all $\sigma \in \{0,1\}^{l_2}$ and $h'_{i'} \in H_{ow}(g(k_e))$, given $(r, h'_{i'}(\sigma), Ext(r,\sigma))$, if no PPT adversary A has a non-negligible probability ε to find σ, then $Ext(r,\sigma)$ is a strong extractor with $(\varepsilon, f(k_e))$-hard-to-invert auxiliary inputs.

4 Construction

First each attribute is converted into a random number belonging to Z_N, where $N = p_1p_2p_3$ and p_1, p_2, p_3 are three different prime numbers, Π is a monotone universal attribute space. Then we define an injection map I_M, and for $\forall S_i \in \Pi$, we have $I_M(S_i) \in Z_N$. Then let $\Omega = I_M(\Pi)$ is a subset of Z_N and $I = |\Omega|$ denotes the cardinality of Ω, A is a monotone access structure.

Setup$(1^k, \Omega)$: Input the security parameter k, a monotone universal attribute space Ω. Then, the algorithm runs the bilinear group generator to produce $E = (N = p_1p_2p_3, G, G_T, e)$. Then, it randomly chooses generator $g_1, x_1, \cdots, x_I \in G_{p_1}$ and $g_3 \in G_{p_3}$. Let $l = (3\gamma)^{1/\varepsilon}$, where the security is with reference to 2^{-l^ε}-hard-to-invert auxiliary inputs. Then, it chooses random $\alpha, a_1, \cdots, a_l, \rho_1, \cdots, \rho_l \in Z_N$, $v_1, \cdots, v_l \in Z_{p_3}$ and $P_1 = g_1^{\rho_1}, \cdots, P_l = g_1^{\rho_l}$. Let $\sigma \in \{0,1\}^{l_2}$ and $Ext{:}\{0,1\}^{l_1} \times \{0,1\}^{l_2} \to \{0,1\}^n$, $l_1, l_2, n \in Z_N$, where the *Ext* is a strong extractor. Then, it outputs master public key is $MPK{=}\{E, g_1, g_3, (g_1^{\alpha/\rho_i})_{i\in[l]}, P_1, \cdots, P_l, x_1, \cdots, x_I, (y_i = e(g_1, P_i)^{a_i})_{i\in[l]}, \sigma\}$ and master private key is $MSK{=}(g_1^{a_i} \cdot g_3^{v_i}.)_{i\in[l]}$.

KeyGen$(MPK, MSK, \mathbf{S})$: Takes MPK, MSK and an attribute set $\mathbf{S}$ as input. Then it picks $y_{1,1}, \cdots, y_{1,l}, y_2, y_{3,1}, \cdots, y_{3,I}, t \in Z_N$ and outputs the secret key $SK_{\mathbf{S}} = \{(sk_{1,i})_{i\in[l]}, sk_2, (sk_{3,h})_{h\in\mathbf{S}}\} = \{(g_1^{a_i} \cdot g_1^{\alpha t/\rho_i} \cdot g_3^{y_{1,i}} \cdot g_3^{v_i})_{i\in[l]}, g_1^t \cdot g_3^{y_2}, (x_h^t \cdot g_3^{y_{3,h}})_{h\in\mathbf{S}}\}$.

Enc(M, Π, MPK): Inputs a LSSS scheme $\Sigma = (\boldsymbol{A}, b)$ for $\mathcal{A}$, MPK and a message M. Note that $\boldsymbol{A}$ is an $n \times m$ matrix. The function b maps the i-th row of A to an attribute vector $u(i)$. The algorithm chooses random $q_1, \cdots, q_n \in Z_N, r_i \in \{0,1\}^{l_1}$ and computes $\theta_i = Ext(r_i, \sigma)$, it randomly chooses a vector $u = (\sum_{i=1}^{l} \theta_i, u_2, \cdots, u_m) \in Z_N^m$. For i to 1, it computes $\gamma_i = \boldsymbol{u} \cdot \boldsymbol{A}_i$, where $\boldsymbol{A}_i$ is i-th row vector of $\boldsymbol{A}$. It creates the ciphertext $C = \{c_1 = M \cdot \prod_{i=1}^{l} y_i^{\theta_i}, (c_{2,i} = P_i^{\theta_i})_{i\in[l]}, (c_{3,i} = g_1^{\alpha\gamma_i} \cdot x_{b(i)}^{-q_i}, c_{4,i} = g_1^{q_i})_{i\in[n]}\}$.

Dec$(C, SK_{\mathbf{S}}, MPK)$: The algorithm inputs the ciphertext C of the LSSS scheme Σ on $\mathcal{A}$, the secret key of set $\mathbf{S}$ and MPK. Then let $T \subset [n]$ be defined as $T = \{i : b(i) \in \mathbf{S}\}$ while $\mathbf{S} \in \mathcal{A}$ is an authorized set.If $\{\gamma_i\}$ are valid shares of A, then the algorithm can compute a set $\{\beta_i \in Z_N\}_{i\in T}$ make $\sum_{i\in T} \beta_i\gamma_i = \sum_{i=1}^{l} \theta_i$. Finally, it calculates:

$$\frac{\prod_{i=1}^{l} e(c_{2,i}, sk_{1,i})}{\prod_{i\in T} \left(e(c_{3,i}, sk_2)e(c_{4,i}, sk_{3,b(i)})\right)^{\beta_i}} = \prod_{i=1}^{l} y_i^{\theta_i}.$$

MSK-Update(MPK,MSK): The algorithm inputs MSP, then it picks $v'_i \in Z_N$, the updated master private key $MSK' = MSK \cdot g_3^{v'_i}$.

SK-Update(MPK, $SK'_{\mathbf{S}}$): The algorithm inputs $SK_{\mathbf{S}}$, then it picks random $y'_{1,1}, \cdots, y'_{1,l}, y'_2, y'_{3,1}, \cdots, y'_{3,I}, t' \in Z_N$ and computes $sk_{1,i} = (sk_{1,i} \cdot g_1^{\alpha t'/\rho_i} \cdot g_3^{y'_{1,i}})_{i\in[l]}, sk'_2 = sk_2 \cdot g_1^{t'} \cdot g_3^{y'_2}, sk'_{3,i} = (sk_{3,i} \cdot x_h^{t'} \cdot g_3^{y'_{3,h}})_{h\in\mathbf{S}}$. Final, the updated secret key $SK'_{\mathbf{S}} = \{(sk'_{1,i})_{i\in[l]}, sk'_2, (sk'_{3,h})_{h\in\mathbf{S}}\}$.

Correctness: The correctness of the equation is verified on the next page.

5 Security Proof

We use the dual system encryption mechanism to proof the security, first of all, three semi-functional (SF) structures are defined, note that g_2 is the generator of G_{p_2}.

SF master private key: $(g_1^{a_i} \cdot g_2^{\varphi_i} \cdot g_3^{v_i})_{i\in[l]}, \varphi_1, \cdots, \varphi_l \in Z_N$.

SF attribute-based secret key: $\{(g_1^{a_i+\alpha t/\rho_i} \cdot g_2^{d_i} g_3^{y_{1,i}})_{i\in[l]}, g_1^t g_2^z g_3^{y_2}, (x_h^t g_3^{y_{3,h}})_{h\in S}\}, z, d_1, \cdots, d_l, \in Z_N$.

SF ciphertext: $\{c_1 = M \cdot \prod_{i=1}^m y_i^{\theta_i}, (c_{2,i} = P_i^{\theta_i} g_2^{\eta_i})_{i\in[l]}, (c_{3,i} = g_1^{\alpha\gamma_i} x_{b(i)}^{-q_i} g_2^{\omega_i}, c_{4,i} = g_1^{q_i})_{i\in[n]}\}, \eta_1, \cdots, \eta_l, \omega_1, \cdots, \omega_l \in Z_N$.

According to the dual system encryption, a normal secret key can decrypt SF ciphertext, and normal ciphertext can be decrypted with SF attribute-based key. If a SF attributed-based secret key is used to decrypt a SF ciphertext, we have $e(g_2, g_2)^{\sum_{i=1}^l \eta_i d_i - z\sum_{i\in T}\omega_i\beta_i}$. If $\sum_{i=1}^l \eta_i d_i = z\sum_{i\in T}\omega_i\beta_i$, decryption will succeed, and we call a SF attribute-based secret key is a nominally SF attributed-based secret key. In the same way, the attribute-based generated by a SF master private key is also SF attributed-based secret key, then we have $e(g_2, g_2)^{\sum_{i=1}^m \eta_i\varphi_i - z\sum_{i\in T}\omega_i\beta_i}$. If $\sum_{i=1}^l \eta_i\varphi_i = z\sum_{i\in T}\sigma_i\beta_i$, then decryption will succeed and the corresponding attributed-based secret key is nominally SF attributed-based secret key.

Theorem 1. *If the modified assumptions 1, 2 and 3 holds, Our CP-ABE scheme is* (2^{-l^ε})*-pCAI-CPA leakage secure.*

Proof. A series of indistinguishable games are defined to prove the theorem, $\mathcal{A}^*$ is the monotone challenge access structure.

$Game_{real}$: $Game_{real}$: is the first real, and keys and ciphertexts are normal.

$Game_{restrained}$: The difference between $Game_{restrained}$ and $Game_{real}$ is that in $Game_{restrained}$ the adversary can't ask for any attribute set in $\mathcal{A}^*$.

$Game_j$: The $Game_j$ is similar to $Game_{restrained}$, but the ciphertext for the adversary is SF. Then we defined two types attribute-based secret keys:

TypeI:$\{(g_1^{a_i+\alpha t/\rho_i} g_2^{d_i} g_3^{y_{1,i}+v_i})_{i\in[l]}, g_1^t g_2^z g_3^{y_2}, (x_h^t g_3^{y_{3,x}})_{x\in\mathbf{S}}\}$

TypeII:$\{(g_1^{a_i+\alpha t/\rho_i} g_3^{y_{1,i}+v_i})_{i\in[l]}, g_1^t g_2^z g_3^{y_2}, (x_h^t g_3^{y_{3,x}})_{x\in\mathbf{S}}\}$

For $j = 1, \cdots, q-1$ in $Game_k$, the first $j-1$ keys are SF of typeII, the j-th key is SF of typeI, and the rest keys are normal. Thus, in $Game_q$, all keys are SF of typeII. We note that the ciphertext is SF in $Game_0$, but all keys are normal. And in $Game_q$ all keys and ciphertexts are SF.

$Game_{final}$: It is similar to $Game_q$, but the message is not M_0 and M_1, but is blinded with a random value in G_T. □

Lemma 1. Suppose there is an adversary A such that $Adv_A^{Game_{real}} - Adv_A^{Game_{real2}} \geq \varepsilon$, then there is an algorithm B that has advantage to break the Assumption 2.

Proof. $\mathcal{A}^*$ is the challenge monotone access structure. For $S^* = \{S_1^*, \cdots, S_n^*\} \in A^*$, where S^* has n attributes. Then, let $\mathcal{S}^* = \{\mathcal{S}'_1 | \mathcal{S}'_1 = S_1 \bmod p_2\} \bigcup \cdots \bigcup \{S'_n | S'_n = S_n \bmod p_2\}$ and Φ^* be the set of all $\mathcal{S}^*$, where $\mathcal{S}^*$ is a superset of S^*.

If adversary A wants to make key query on $\Omega^* \notin \mathcal{A}^*$, for $\forall S'_i \in \Omega^*$, the B's answer is as follows:

1) If $S'_i \notin \mathcal{S}^*$, for $\forall \mathcal{S}^* \in \Phi^*$. In this case, C runs the KeyGen and uses MSK as responses.

2) If $S'_i \in \mathcal{S}^*$, for $\exists \mathcal{S}^* \in \Phi^*$. Then we have $S'_i \neq S_i$ and $S'_i = S_i \bmod p_2$, C will computes $\alpha = \gcd(S_i - S'_i, N)$, then we can define $\beta = N/\alpha$, where $N = p_1p_2p_3$. Finally, we can get a tuple $(g, U_1U_2, U_3, V_2V_3, \Gamma)$, note that it is an example of the 2-SDP assumption.

   a. If $\alpha = p_1p_2$ and $\beta = p_3$, then B will verify whether $\alpha = p_1p_2$ from $(U_1U_2)^\alpha = 1$. If the equation is satisfied, B will continue to verify $e(U_2U_3, \Gamma)^{\beta \stackrel{?}{=}} 1$ to distinguish between $\Gamma \in G_{p_1p_3}$ and $\Gamma \in G$;

   b. If $\alpha = p_2p_3$ and $\beta = p_1$, then B will verify whether $\alpha = p_2p_3$ from $(V_2V_3)^\alpha = 1$. If the equation is satisfied, B will continue to verify $e(U_1U_2, \Gamma)^{\beta \stackrel{?}{=}} 1$ to distinguish between $\Gamma \in G_{p_1p_3}$ and $\Gamma \in G$;

   c. If $\alpha = p_2$ and $\beta = p_1p_3$, B will continue to verify $\Gamma^{\beta \stackrel{?}{=}} 1$ to distinguish between $\Gamma \in G_{p_1p_3}$ and $\Gamma \in G$.

□

Lemma 2. Suppose there is an adversary A such that $Adv_A^{Game_{restrained}} - Adv_A^{Game_{real0}} \geq \varepsilon$, then there is an algorithm B that has advantage to break the modified 1-SDP Assumption.

Proof. Input a tuple $(N, g_1, U_3, G, G_T, (\Gamma_i)_{i\in[l]})$, which is an example of the modified 1-SDP assumption.

Setup. B constructs MPK=$\{g_1, U_3, (g_1^{\alpha t/\rho_i})_{i\in[l]}, P_1, \cdots, P_l, x_1, \cdots, x_I, (y_i = e(g_1, P_i)^{a_i})_{i\in[l]}\}$,$MSK$=$(g_1^{a_i} U_3^{v_i})_{i\in[l]}$,

$$\frac{\prod_{i=1}^{l} e(c_{2,i}, sk'_{1,i})}{\prod_{i\in T}\left(e(c_{3,i}, sk'_2)\cdot e(c_{4,i}, sk'_{3,b(i)})\right)^{\beta_i}} = \frac{\prod_{i=1}^{l} e(P_i^{\theta_i}, g_1^{a_i} g_1^{\alpha t/\rho_i} g_3^{y_{1,i}} g_3^{v_i} \cdot g_1^{\alpha t'/\rho_i} g_3^{y'_{1,i}})}{\prod_{i\in T}\left(e(g_1^{\alpha\gamma_i} x_{b(i)}^{-q_i}, g_1^t g_3^{y_2}\cdot g_1^{t'} g_3^{y'_2})\cdot e(g_1^{q_i}, x_{b(i)}^t g_3^{y_{3,b(i)}} x_{b(i)}^{t'} g_3^{y'_{3,b(i)}})\right)^{\beta_i}}$$

$$= \frac{(\prod_{i=1}^{l} e(P_i, g_1)^{a_i\theta_i})\cdot e(g_1,g_1)^{\alpha t\cdot\sum_{i=1}^{l}\theta_i}\cdot e(g_1,g_1)^{\alpha t'\cdot\sum_{i=1}^{l}\theta_i}}{\prod_{i\in T}\left(e(g_1^{\alpha\gamma_i}, g_1^t)\cdot e(g_1^{\alpha\gamma_i}, g_1^{t'})\cdot e(x_{b(i)}^{-q_i}, g_1^t)\cdot e(x_{b(i)}^{-q_i}, g_1^{t'})\cdot e(g_1^{q_i}, x_{b(i)}^t)\cdot e(g_1^{q_i}, x_{b(i)}^{t'})\right)^{\beta_i}}$$

$$= \frac{(\prod_{i=1}^{l} e(P_i, g_1)^{a_i\theta_i})\cdot e(g_1,g_1)^{\alpha t\cdot\sum_{i=1}^{l}\theta_i}\cdot e(g_1,g_1)^{\alpha t'\cdot\sum_{i=1}^{l}\theta_i}}{e(g_1,g_1)^{\alpha t\cdot\sum_{i=1}^{l}\theta_i}\cdot e(g_1,g_1)^{\alpha t'\cdot\sum_{i=1}^{l}\theta_i}} = \prod_{i=1}^{l} e(P_i, g_1)^{a_i\theta_i} = \prod_{i=1}^{l} {y_i}^{\theta_i}$$

$a, \alpha_i, \rho_i \in Z_N$. Then, B send MPK to A.

Phase 1. A can issue the Secret Key Query, Pre-challenge Leakage Query, MSK-Update Query and SK-Update Query to B, and B will answer respectively.

Challenge. Two messages M_0 and M_1 with the same length and $\mathcal{A}^*$ are sent by A to B, then B picks random $\tilde{\gamma}_1, \cdots, \tilde{\gamma}_n$, $q_1, \cdots, q_n \in Z_N$ and outputs $C^* = \{c_1 = M_b \cdot \prod_{i=1}^{l} e(g_1^{a_i}, \Gamma_i), c_{2,i} = (\Gamma_i)_{i\in[l]}, (c_{3,i} = \Gamma_i^{\alpha\tilde{\gamma}_i} x_{b(i)}^{-q_i}, c_{4,i} = g_1^{q_i})_{i\in[n]}\}$ to A.

Phase 2. A can perform the Secret Key Query, Post-challenge Leakage Query, MSK-Update Query and SK-Update Query to B, and B will answer respectively.

1) If $\Gamma_i = g_1^{\rho_i\theta_i} g_2^{z_i} \in G_{p_1p_2}$, then $C^* = \{M_b \cdot \prod_{i=1}^{l} e(g_1^{a_i}, P_i^{\theta_i}), (P_i^{\theta_i} g_2^{\eta_i})_{i\in[l]}, (g_1^{\alpha\gamma_i} g_2^{\omega_i} x_{b(i)}^{-q_i}, g_1^{q_i})_{i\in[n]}\}$, where $\omega_i = ac_i \cdot \tilde{\gamma}_i$, η_i=ci, $\gamma_i = \rho_i \cdot \theta_i \cdot \tilde{\gamma}_i$ and C^* is a SF ciphertext. Hence B can simulate $Game_0$.

2) If $\Gamma_i \in G_{p_1}$, then C^* is normal. Hence an normal ciphertext game $Game_{restrained}$ can be simulated by B.

Thus, if A can distinguish between $Game_0$ and $Game_{restrained}$ with a non-negligible advantage ε, then B can break the modified 1-SDP Assumption with non-negligible advantage. □

Lemma 3. Suppose there is an adversary A such that $Adv_A^{Game_{j+1}} - Adv_A^{Game_j} \geq \varepsilon$, then there is an algorithm B that has advantage to break the modified 2-SDP Assumption.

Proof. Input a tuple $(g_1, (U_{1i}U_{2i})_{i\in[m]}, U_3, V_2V_3, \Gamma)$, which is an example of the modified 2-SDP assumption.

Setup. B constructs $MPK = \{E, g_1, g_2, (g_1^{\alpha t/\rho_i})_{i\in[l]}, P_1, \cdots, P_l, x_1, \cdots, x_I, (y_i = e(g_1, P_i)^{a_i})_{i\in[l]}\}$ and $MSK = (g_1^{a_i} g_3^{v_i})_{i\in[l]}$. Then, B send the MPK to A.

Phase 1. A can issue kth Secret Key Query, Pre-challenge Leakage Query, MSK-Update Query and SK-Update Query to B, where $k \in N$.

- **Key Query:**

  If $k < j$, where $k \in [0, q]$, B answers with $\{(g_1^{a_i+\alpha t/\rho_i} g_3^{y_{1,i}+v_i})_{i\in[l]}, g_1^t (V_2V_3)^x g_3^{y_2}, (x_h^t g_3^{y_{3,h}})_{h\in\mathbf{S}}\}$, which is a typeII SF key.

  If $k = j$, then There are two different situations:

  1) B answers with $\{(g_1^{a_i} \cdot \Gamma^{\alpha} \cdot g_3^{y_{1,i}+v_i})_{i\in[l]}, \Gamma \cdot g_3^{y_2}, (x_h^t g_3^{y_{3,h}})_{h\in\mathbf{S}}\}$. If $\Gamma = g_1^a g_2^b g_3^c \in G$, the j-th is a typeI SF. If $\Gamma = g_1^a g_3^c \in G_{p_1p_3}$, the j-th key is normal.
  2) B answers with $\{(g_1^{a_i} \cdot \Gamma^{\alpha} \cdot g_3^{y_{1,i}+v_i})_{i\in[l]}, \Gamma \cdot g_3^{y_2}(V_2V_3)^x, (x_h^t g_3^{y_{3,h}})_{h\in\mathbf{S}}\}$. If $\Gamma = g_1^a g_2^b g_3^c \in G$, the j-th is a typeI SF key. If $\Gamma = g_1^a g_3^c \in G_{p_1p_3}$, the j-th key is a typeII SF key.

  If $k > j$, then B will answer with normal keys.

- **Pre-challenge Leakage Query:** A issue the Pre-challenge Leakage Query, B returns $h_i(MSK, L_{MSK}, MPK, L_{SK}, \mathbf{S})$.

- **MSK-Update Query and SK-Update Query:**

  B answers the MSK-Update Query from A with MSK-Update algorithm, B returns MSK' and adds $(MSK', \cdot)$ to L_{MSK}, where MSK' is a SF key.

  B answers the SK-Update Query from A with SK-Update algorithm, B returns $SK'_{\mathbf{S}}$ and update cnt', then adds $(cnt', SK'_{\mathbf{S}}, \mathbf{S})$ to $L_{SK'}$, where $SK'_{\mathbf{S}}$ is a typeII SF key.

Challenge. B picks random $\tilde{\gamma}_1, \cdots, \tilde{\gamma}_n \in Z_N$, then it outputs the ciphertext $C = \{c_1 = M_b \cdot \prod_{i=1}^{l} e(g_1^{a_i}, U_{1i}U_{2i}), c_{2,i} = (U_{1i}U_{2i})_{i\in[l]}, (c_{3,i} = U_{1i}U_{2i}{}^{\alpha\tilde{\gamma}_i} x_{b(i)}^{-q_i}, c_{4,i} = g_1^{q_i})_{i\in[n]}\}$ to A.

Phase 2. A can perform the Secret Key Query, Post-challenge Leakage Query to B, where Key Query are simulated as before. If we let $U_{1i}U_{2i} = g_1^{\rho_i\theta_i} g_2^{z_i}$, then we have that $c_1 = M_b \cdot \prod_{i=1}^{l} e(g_1^{a_i}, B_i^{\theta_i})$, $c_{2,i} = (B_i^{\theta_i} g_2^{\varphi_i})_{i\in[l]}$,$(c_{3,i} = g_1^{\alpha\gamma_i} g_2^{\omega_i} x_{b(i)}^{-q_i}, c_{4,i} = g_1^{q_i})_{i\in[n]}$, where $\omega_i = ac_i \cdot \tilde{\gamma}_i$, $\gamma_i = \rho_i \cdot \theta_i \cdot \tilde{\gamma}_i$, $\eta_i = ci$. Note that this is a SF ciphertext.

In conclusion, if $\Gamma \in G$, B simulates $Game_{j+1}$ correctly. If $\Gamma \in G_{p_1p_3}$, then B simulates $Game_j$ correctly. Thus, if A can distinguish between $Game_{j+1}$ and $Game_j$ with a non-negligible advantage ε, then B can break the

Table 1: Performance comparison with other schemes

Schemes	Ciphertext size	Secret key size	Encrypt cost	Decrypt cost
[12]	$(\tilde{k}+2l+1)\|G\|+\|G_T\|$	$(\tilde{k}+2+\|S\|)\|G\|$	$(3l+\tilde{k}+1)Ep+Ep_T$	$(2n+\tilde{k}+1)Pa$
[15]	$(\tilde{k}+3l+1)\|G\|+\|G_T\|$	$3(\tilde{k}+l+2+\|S\|)\|G\|$	$(3l+\tilde{k}+\tilde{p}l+1)Ep+Ep_T$	$(3n+\tilde{k}+1)Pa$
[27]	$(\tilde{k}+2l+2)\|G\|+\|G_T\|$	$(\tilde{k}+2+\|S\|)\|G\|$	$(3l+\tilde{k}+1)Ep+Ep_T$	$(2n+\tilde{k}+1)Pa$
[29]	$(\tilde{k}+2\tilde{m}+1)\|G\|+\|G_T\|$	$(\tilde{k}+2+\|S\|)\|G\|$	$(2\tilde{m}+\tilde{k}+2)Ep+Ep_T$	$(\tilde{k}+3)Pa$
ours	$(2n+l)\|G\|+\|G_T\|$	$(l+1+\|S\|)\|G\|$	$(2n+l)Ep+lEp_T$	$(2n+l)Pa$

modified 2-SDP Assumption with non-negligible advantage. □

Lemma 4. Suppose there is an adversary A such that $Adv_A^{Game_q} - Adv_A^{Game_{final}} \geq \varepsilon$, then there is an algorithm B that has advantage to break the modified BSDP Assumption.

Proof. Input a tuple $(g_1, (g_1^{1/\rho_i})_{i\in[l]}, (P_i^{a_i}U_2)_{i\in[m]}, U_3, (P_i^{a_i}V_2)_{i\in[m]}, W_2, \Gamma)$, which is an example of the modified BSDP assumption.

Setup. B sets $g_3 = U_3$, $g_2 = W_2$, $y_i = e(g_1, P_i^{a_i}U_2) = e(g_1, P_i)^{a_i}$, then constructs the MPK and the MSK=$(P_i^{a_i}U_2 g_3^{v_i})_{i\in[l]}$.

Phase 1. A can perform the Secret Key Query, Pre-challenge Leakage Query, MSK-Update Query and SK-Update Query to B.

For all queries of Key Query, B answers as $SK_{\mathbf{S}} = \{(sk_{1,i})_{i\in[l]}, sk_2, (sk_{3,h})_{h\in\mathbf{S}}\} = \{((P_i^{a_i}U_2)\cdot g_1^{\alpha t/\rho_i}\cdot g_3^{y_{1,i}+v_i})_{i\in[l]}, g_1^t g_3^{y_2}, (x_h^t g_3^{y_{3,h}})_{h\in\mathbf{S}}\}$.

Challenge. B picks random $\tilde{\gamma}_1, \cdots, \tilde{\gamma}_n, q_1, \cdots, q_n \in Z_N$, then it returns $C^* = \{c_1 = M_b \cdot \Gamma, c_{2,i} = (P_i^{\theta_i}V_2)_{i\in[l]}, (c_{3,i} = (P_i^{\theta_i}V_2)^{\alpha\tilde{\gamma}_i} x_{b(i)}^{-q_i}, c_{4,i} = g_1^{q_i})_{i\in[n]}\}$.

Phase 2. A can perform the Secret Key Query, Post-challenge Leakage Query to B.

1) If we let $P_i^{\theta_i}V_2 = P_i^{\theta_i} g_2^{z_i}$, $C^* = \{c_1, c_{2,i}, c_{3,i}, c_{4,i}\} = \{M_b\cdot\Gamma, (P_i^{\theta_i} g_2^{\eta_i})_{i\in[l]}, (g_1^{\alpha\gamma_i} x_{b(i)}^{-q_i} g_2^{\omega_i}, g_1^{q_i})_{i\in[n]}\}$, where $\omega_i = ac_i\cdot\tilde{\gamma}_i, \eta_i = ci, \gamma_i = \rho_i\cdot\theta_i\cdot\tilde{\gamma}_i$.
2) If $\Gamma = \prod_{i=1}^m e(g_1, P_i)^{a_i\theta_i}$, then C^* is SF, B simulates $Game_q$ correctly.
3) If $\Gamma \in G_T$ is a random value, B simulates $Game_{final}$ correctly. In conclusion, if A can distinguish between $Game_q$ and $Game_{final}$ with a non-negligible advantage ε, then B can break the modified BSDP Assumption with non-negligible advantage.

□

6 Performance Comparison

The performance of other related scheme [12,15,27,29] is compared with this scheme in this section. Let Ep and Ep_T denote exponential operation in G and G_T, Pa denotes pairing operation. $|G|$ and $|G_T|$ respectively denotes the length of G and G_T, $|S|$ is the number of elements in S. For convenience, let $\tilde{m}$ denotes the number of minimal sets, let the LSSS matrix with l rows and n columns, $\tilde{k}$ denotes the leakage parameter and $\tilde{p}$ denotes the number of elements in attribute vectors. Table 1 shows the efficiency analysis and comparison of each scheme.

From the data in Table 1, the leakage parameter is the decisive factor in the performance efficiency of the scheme [12, 15, 27, 29], that is, the size of the leakage parameter determines whether the scheme is efficient. However, our scheme is independent of the leakage parameters, but only depends on the scale of the LSSS matrix.

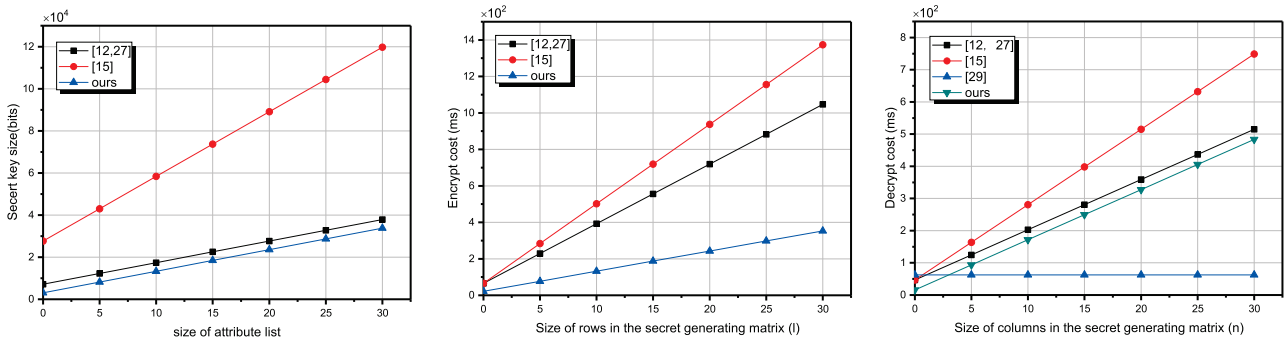
We use JPBC library version 2.0.0 for related experiments. The experiment was simulated on Windows system with an Intel(R) Core (TM) i5 CPU 3.20GHz and 8.00GB RAM to approximate the actual operation. We have obtained the measured values of exponentiation and pairing operations. The operating times of Ep, Ep_T and Pa are 10.9ms, 7.8ms and 0.15ms, respectively.

According to the above data, in order to achieve better leakage-resilient performance, We set N to be a 1024-bit number in the scheme [12, 15, 27, 29], we let $n = 1$ and $l = 2$ in the simulation of encrypt cost and decrypt cost respectively. Figure 1 shows the running time of different algorithms in these schemes.

Obviously, our scheme is more effective than [12,15,27, 29]. The efficiency of the scheme [15] is related to both the leakage parameters and the LSSS matrix. Although the minimum set used in [29] can improve the decryption time, LSSS is more flexible and can be applied in a variety of scenarios. What's more, our scheme is not affected by the leakage parameters. Therefore, from the above analysis, our scheme has certain advantages.

7 Conclusion

We propose an ABE scheme which resilient to post-challenge continuous auxiliary input leakage, and proved that the scheme is secure under the three modified static assumptions. Our scheme can tolerate auxiliary input and continuous leakage. In addition, if there is an adversary who can query the secret key information after the



(a) Secret key size (b) Encrypt time (c) Decrypt time

Figure 1: Efficiency comparison

challenge phase, our solution can tolerate post-challenge leakage. It may be even more interesting to construct certain KP-ABE schemes that can against pCAI.

Acknowledgments

This paper is supported by the National Natural Science Foundation of China under Grant No. 61902140, the Anhui Provincial Natural Science Foundation under Grant No. 1908085QF288, the Nature Science Foundation of Anhui Higher Education Institutions under Grant No.KJ2021A0527, No.KJ2019A0605, No.KJ2020A0032, No. KJ2020A0034.

References

[1] M. Bayat, M. Doostari, and S. Rezaei, "A lightweight and efficient data sharing scheme for cloud computing," *International Journal of Electronics and Information Engineering*, vol. 9, no. 2, pp. 115–131, 2018.

[2] S. Belguith, N. Kaaniche, M. Laurent, A. Jemai, and R. Attia, "Phoabe: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted iot," *Computer Networks*, vol. 133, pp. 141–156, 2018.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE Symposium on Security and Privacy (SP)*, pp. 321–334, Berkeley, CA, USA, 2007.

[4] Z. Cao, L. Liu, and Z. Guo, "Ruminations on attribute-based encryption," *International Journal of Electronics and Information Engineering*, vol. 8, no. 1, pp. 9–19, 2018.

[5] Y. Dodis, S. Goldwasser, Y. T. Kalai, and C. Peikert, "Public-key encryption schemes with auxiliary inputs," in *Theory of Cryptography Conference (TCC)*, pp. 361–381, Zurich, Switzerland, 2010.

[6] A. Faonio, J. B. Nielsen, and D. Venturi, "Fully leakage-resilient signatures revisited: Graceful degradation, noisy leakage, and construction in the bounded-retrieval model," *Theoretical Computer Science*, vol. 660, pp. 23–56, 2018.

[7] X. Gao and L. Zhang, "Efficient anonymous ciphertext-policy attribute-based encryption for general structures supporting leakage-resilience," *International Journal of Network Security*, vol. 22, no. 5, pp. 763–774, 2020.

[8] 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)*, pp. 89–98, Alexandria, VA, USA, 2006.

[9] S. Halevi and H. Lin, "After-the-fact leakage in public-key encryption," in *Theory of Cryptography Conference (TCC)*, pp. 107–124, Providence, RI, USA, 2011.

[10] M. S. Hwang, T. H. Sun, and C. C. Lee, "Achieving dynamic data guarantee and data confidentiality of public auditing in cloud storage service," *Journal of Circuits Systems and Computers*, vol. 26, no. 5, 2017.

[11] C. C. Lee, P. S. Chung, and M. S. Hwang, "A survey on attribute-based encryption schemes of access control in cloud environments," *International Journal of Network Security*, vol. 15, no. 4, pp. 231–240, 2013.

[12] A. Lewko, Y. Rouselakis, and B. Waters, "Achieving leakage resilience through dual system encryption," in *Theory of Cryptography Conference (TCC)*, pp. 70–88, Providence, RI, USA, 2010.

[13] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 62–91, Riviera, FrenchA, 2010.

[14] J. Li, Y. Wang, Y. Zhang, and J. Han, "Full verifiability for outsourced decryption in attribute based encryption," *IEEE Transactions on Services Computing*, vol. 13, no. 3, pp. 478–487, 2020.

[15] J. Li, Q. Yu, and Y. Zhang, "Hierarchical attribute based encryption with continuous leakage-resilience," *Information Sciences*, vol. 484, pp. 113–134, 2019.

[16] J. Li, Q. Yu, Y. Zhang, and J. Shen, "Key-policy attribute-based encryption against continual auxiliary input leakage," *Information Sciences*, vol. 470, pp. 175–188, 2019.

[17] H. Ma, Z. Wang, J. Wang, and Z. Guan, "Multi-authority attribute-based encryption resilient against auxiliary-input leakage," *Journal of Computers*, vol. 31, no. 1, pp. 134–147, 2020.

[18] S. Micali and L. Reyzin, "Physically observable cryptography," in *Theory of Cryptography Conference (TCC)*, pp. 278–296, Cambridge, MA, USA, 2004.

[19] P. K. Premkamal and S. K. Pasupuleti, "Dynamic traceable cp-abe with revocation for outsourced big data in cloud storage," *International Journal of Communication Systems*, vol. 34, no. 2, p. e4351, 2021.

[20] J. Ren, L. Zhang, and B. Wang, "Decentralized multi-authority attribute-based searchable encryption scheme," *International Journal of Network Security*, vol. 23, no. 2, pp. 332–342, 2021.

[21] A. Sahai and B. R. Waters, "Fuzzy identity-based encryption," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, pp. 457–473, Aarhus, Denmark, 2004.

[22] Z. Wang and S. M. Yiu, "Attribute-based encryption resilient to auxiliary input," in *The International Conference on Provable Security (ProvSec)*, p. 371–390, Kanazawa, Japan, 2015.

[23] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *International Workshop on Public Key Cryptography Springer Berlin Heidelberg (PKC)*, pp. 53–70, Taormina, Italy, 2008.

[24] B. Waters, "Dual system encryption: Realizing fully secure ibe and hibe under simple assumptions," in *Annual International Cryptology Conference*, pp. 619–636, Santa Barbara, CA, USA, 2009.

[25] T. H. Yuen, S. S. M. Chow, Y. Zhang, and S. M. Yiu, "Identity-based encryption resilient to continual auxiliary leakage," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, pp. 117–134, Cambgridge, UK, 2012.

[26] T. H. Yuen, Y. Zhang, and S. M. Yiu, "Identity-based encryption with post-challenge auxiliary inputs for secure cloud applications and sensor networks," in *European Symposium on Research in Computer Security(ESORICS)*, pp. 130–147, Wroclaw, Poland, 2014.

[27] J. Zhang and L. Zhang, "Anonymous cp-abe against side-channel attacks in cloud computing," *Journal of Information Science and Engineering*, vol. 33, no. 3, p. 789–805, 2017.

[28] L. Zhang and Y. Shang, "Leakage-resilient attribute-based encryption with cca2 security," *International Journal of Network Security*, vol. 21, no. 5, pp. 819–827, 2019.

[29] M. Zhang, S. Wei, and C. Wang, "Leakage-resilient attribute-based encryption with fast decryption: Models, analysis and constructions," in *International Conference on Information Security Practice and Experience (ISPEC)*, pp. 75–90, Lanzhou, China, May 2013.

[30] M. Zhang, Y. Zhang, Y. Su, Q. Huang, , and Y. Mu, "Attribute-based hash proof system under learning-with-errors assumption in obfuscator-free and leakage-resilient environments," *IEEE Systems Journal*, vol. 11, no. 2, pp. 1018–1026, 2017.

Biography

Yuyan Guo Associate professor in the School of Computer Science and Technology, Huaibei Normal University. She received her Ph.D. degree in computer science from Hohai University, Nanjing, China in 2016. Her research interests include cryptography and information security, cloud computing and trusted computing etc. She has published over 10 research papers in refereed international conferences and journals.

Zhenhua Lu MS. of Huaibei Normal University. His research interests include information security and cryptography.

Mingming Jiang Associate professor in the School of Computer Science and Technology, Huaibei Normal University. He received his PhD in cryptography from Xidian University in 2014, and received his MS and BS in cryptography from Huaibei Normal University in 2010 and 2007, respectively. His research interests include public key cryptography based on lattice and provable security.

Dongbing Zhang Born in 1974, Master. Now, he is an associate professor in Huaibei Normal University. His main research interests include algorithm optimization and information security.