Leakage-resilient Attribute-based Encryptions with Fast Decryption: Model, Analysis and Construction[*†]

Mingwu Zhang[*,***], Wei Shi[*], Chunzhi Wang[*], Zhenhua Chen[**],Yi Mu[****‡]

May 1, 2013

Abstract

Traditionally, in attribute-based encryption (ABE), an access structure is constructed from a linear secret sharing scheme (LSSS), a boolean formula or an access tree. In this work, we encode the access structure as their minimal sets, which is equivalent to the existence of a smallest monotonic span program for the characteristic function of the same access structure. We present two leakage-resilient attribute-based encryption schemes, ciphertext-policy ABE (LR-CP-ABE) and key-policy ABE (LR-KP-ABE), that can tolerate private key and master key to be partially leaked. By using our encoding mechanism, we obtain short ciphertext in LR-CP-ABE and short key in LR-KP-ABE. Also, our schemes have higher decryption efficiency in that the decryption cost is independent to the depth of access structures. Meanwhile, our proposed schemes provide the tolerance of both master key leakage and continual leakage in the sense that there are many master keys for universal set Σ and many private keys per attribute set $\mathbb{S}$. We explicitly employ a refresh algorithm to update a (master) key while the leakage information will beyond the allowable leakage bound. The schemes are proven to be adaptively leakage-resilient secure in the standard model under the static assumptions in composite order bilinear groups.

Keywords: Leakage resilience, Attribute-based encryption, Minimal set, Monotone access structure

1 Introduction

In encryption systems, we could imagine encrypting a data under a policy which specifies under what conditions key-holder is allowed to decrypt the data. Attackers are modeled as probabilistic polynomial time machines with input/output access to the algorithm,

[*]The external abstract is in ISPEC2013. This is the full version.

[†]This work is supported by the National Natural Science Foundation of China under Grants (61272404, 61170135, 61103232), and the Guangdong Natural Science Foundation under Grant S2012010010383.

[‡]Dr Mingwu Zhang, Mr. Wei Shi and Prof. ChunZhi Wang are with School of Computer Science, Hubei University of Technology. Dr. Zhenhua Chen is with School of Computers, Shaanxi Normal University. Prof. Yi Mu is with Centre for Computer and Information Security Research, School of Computer Science and Software Engineering, University of Wollongong.

and the algorithm is considered secure if it is infeasible for any such adversary to break the system. Most existing public key encryptions allow a party to encrypt data to a particular user, but are unable to efficiently handle more expressive types of encrypted access policy. In attribute-based encryption (ABE), ciphertexts and keys are associated with sets of attributes and access policies over attributes. A key holder is able to decrypt a ciphertext if and only if the attributes satisfies the associated access policy. There are two kinds of ABE systems: cipertext-policy ABE (CP-ABE), where ciphertexts are associated with access policies and keys are associated with sets of attributes, and key-policy ABE (KP-ABE), where keys are associated with access policies and ciphertexts are associated with sets of attributes.

The original ABE construction proposed by Sahai and Waters [SW05] was limited to specify as threshold access policies, which was limited to implement formula consisting of one threshold gate. Goyal et al. [GPSW06] subsequently improved the expressibility of access policy by allowing the key to express any monotonic access structure over attributes. To achieve a more expressive access policy over many attributes, some ABE systems make use of techniques from linear secret-sharing schemes (LSSS) or boolean formulas as access policies. Recently, Hohenberger and Waters [HW13] presented a fast decryptable key-policy ABE system in which ciphertexts can be decrypted with a constant number of pairings.

Lewko et al. [LOS$^+$10] employed monotone span programs (MSPs) as access structure and then constructed a CP-ABE and a KP-ABE respectively that are proven to be adaptively secure in composite bilinear groups. However, the ciphertext in CP-ABE and the key in KP-ABE are polynomial in size of MSPs, and the decryptions are inefficient since the pairings of decryption are linearly to the number of rows in MSPs. In [Wat11], Waters introduced a new technique for realizing CP-ABE under concrete and noninteractive cryptographic assumptions, which allow any encryptor to specify access control in terms of an LSSS matrix. Goyal et al. [GJPS08] presented a *bounded* CP-ABE construction, in which they showed how to transform a KP-ABE system into a CP-ABE one. In particular, they provided a mapping onto a *universal* access tree of up to depth d formulas consisting of threshold gates of input size m. Recently, Boyen [Boy13] constructed an ABE based on lattice that the security assumptions are derived from post-quantum hardness.

Considering the attributes in access formulae or LSSS matrices, an attribute can be used once in an access policy. Although we can obtain multi-show attribute by setting a fixed bound on the maximum times of an attribute be used, however, this is inefficient since it causes the larger scale size of public key as well as the size of key in CP-ABE. Recently, Lewko and Waters [LW12] proposed a new selective proof technique to support multi-show attribute and obtains an adaptive security in CP-ABE system.

Many access policies in ABE are specified as LSSS. However, there is a close relation between LSSS and MSP. Beimel [BGP97] proved that the existence of an efficient LSSS for a specific MSP access structure is equivalent to the existence of a smallest MSP. Later, Nikova et al. [NNP05] provided a theoretical lower bound for any MSP by using some linear algebraic machineries, where the size of a MSP is at least the size of the critical set of minimal sets for the corresponding monotone access structure plus the

size of the critical set for the minimal sets of the dual of access structure minus one, i.e., the computation complexity for an access structure Γ is bounded by $|\mathcal{H}| + |\mathcal{H}^{\perp}| - 1$ where $\mathcal{H}$ and $\mathcal{H}^{\perp}$ denote the critical set of minimal sets for an access structure Γ and $\Gamma^{\perp}$ respectively. Pandit and Barua [PB12] used minimal sets to describe general access structure in ABE systems and constructed the corresponding (hierarchical) encryption schemes. By virtue of the result in [NNP05], they also indicate that there exist classes of monotone access structures for which the size of MSP is at least polynomial in the number of attributes in access structure, but the number of minimal sets in the access structure is constant.

Recent research shows that many cryptographic schemes are vulnerable to side-channel attacks on the keys by the interaction of an adversary by measuring the timing, power-consumption, temperature, radiation, acoustics and so on [AGV09, ADN10, ADW09, BG10, CDR10, DHLW10, DLWW11, YZ12, ZYT12]. The concept of leakage resilience models security of a cryptographic algorithm in the presence of an adversary who uses non-traditional way learn information about the private key. The adversary is strengthened in this model and is allowed to observe leakage from the content of private key. Leakage-resilient cryptosystems are designed to remain secure even if some information about the private key is leaked. Instead, we should take into account the key leakage in ABE system and then construct leakage-resilient ABE schemes. Also, in order to provide an efficient decryption cost, we use the minimal set to describe the monotone access structure in our leakage-resilient ABE systems.

In this work, we focus on the model of memory attacks or relative-leakage model [AGV09]. In this model, the attacker can learn any efficiently computable function of any private key, subject only to the restriction that the total amount of information learned is bounded by predetermined parameter ℓ. Our goal is to devise ABE schemes resilient to key leakage with:

(i) comparable efficiency to previously known systems,

(ii) construction and security in the standard model, and

(iii) better leakage rate.

Leakage attacks are formalized by allowing the adversary to submit leakage functions to a leakage oracle to be applied on the key with an adaptive manner, that is, the adversary can choose different leakage functions at different point of time based on its view and prior leakage. We allow the adversary to handle all key generation and key leakage queries within the dual system encryption framework, eliminating the need for a separate technique to achieve leakage resilience. This enables us to allow leakage from multiple keys which can decrypt the challenge ciphertext, as well as leakage from the master key. Also, we use the minimal sets to describe the monotone access structure in our leakage-resilient ABE systems.

To prove the security of ABE constructions, a natural proof is to use the partition technique, in which the possible key space is divided into two pieces: key space that the simulator can answer and key space of any key capable of decrypting the challenge

ciphertext falls in. Prior works rely on a weak model called *selective security* [SW05, GJPS08, GPSW06], in which the adversary must provide the challenge in advance the system public key is generated. Recently, Waters [Wat09] introduced a new technique, named *dual system encryption*, to prove the adaptive security such that the simulator can construct any key and any challenge ciphertext. In dual system encryption, there are two kinds of keys and ciphertexts: *normal* and *semi-functional*. Decryption will fail if both key and ciphertext are semi-functional. In the real construction, the key and the ciphertext are normal, but they will be transformed into semi-functional in the security proof. In the view of adversary, it has negligible advantage in distinguishing these transformations. Finally, all keys and ciphertexts are semi-functional, and the security is concluded by the incapable decryption between a semi-functional key and a semi-functional challenge ciphertext.

In our proof, we extend the semi-functional key into two types: *truly* semi-functional and *nominally* semi-functional. A truly semi-functional key can not gain non-negligible in decrypting the challenge semi-functional ciphertext, and a nominally semi-functional key can decrypt the challenge ciphertext with some probability. Eventually, by the Theorem 2, we also prove that an adversary has no advantage in transforming a truly semi-functional key into a nominally semi-functional form even the adversary can gain some leakage on the key.

2 Preliminaries

In this paper, we denote the security parameter by κ. A function $\mathsf{negl}(\cdot)$ is negligible if for every polynomial $p(\cdot)$ there exists a value κ' such that for all $\kappa > \kappa'$ it holds that $\mathsf{negl}(\kappa) < \frac{1}{p(\kappa')}$.

Definition 1 *(**Computational indistinguishability**) Let $X = \{X_n(a)\}_{n\in\mathbb{N},a\in\{0,1\}^*}$ and $Y = \{Y_n(a)\}_{n\in\mathbb{N},a\in\{0,1\}^*}$ be two distribution ensembles. We say that X and Y are computationally indistinguishable, denoted $X \approx_c Y$, if for every probabilistic polynomial-time algorithm $\mathscr{D}$, there exists a negligible function $\mathsf{negl}(\cdot)$ such that for all $a \in \{0,1\}^*$,*

$$|Pr[\mathscr{D}(X_n(a)) = 1] - Pr[\mathscr{D}(Y_n(a)) = 1]| < \mathsf{negl}(n) \tag{1}$$

Definition 2 *(**Statistical distance**) Let X_n and Y_n be random variables accepting values taken from a finite domain $\Omega \subseteq \{0,1\}^n$. The statistical distance between X_n and Y_n is*

$$SD(X_n, Y_n) = \frac{1}{2}\sum_{\delta} |Pr[X_n = \delta] - Pr[Y_n = \delta]| \tag{2}$$

We say that X_n and Y_n are ϵ-*close* if their statistical distance is at most $SD(X_n, Y_n) \leq \epsilon(n)$. We say that X_n and Y_n are *statistically close*, denoted $X_n \approx_s Y_n$, if $\epsilon(n)$ is negligible in n.

2.1 Monotone Access structure and Minimal Set

Definition 3 *(**Access structure(AS)**) Let $P_1, \cdots, P_n$ be a set of parties. A collection $\Gamma \subseteq 2^{P_1,\cdots,P_n}$ is monotonic if $\forall B \in \Gamma$ and $B \subseteq C$, then $C \in \Gamma$. An access structure is a collection Γ of non-empty subsets of $\{P_1, \cdots, P_n\}$, i.e., $\Gamma \subseteq 2^{P_1,\cdots,P_n} \backslash \{\emptyset\}$. The member in Γ is called authorized set, and the set not in Γ is called unauthorized set.*

Remark 1 *In an attribute-based encryption, the attributes will play the role of parties in set $\{P_1, \cdots, P_n\}$. In the remainder of the paper, we use $\Sigma = \{a_1, a_2, \cdots, a_n\}$ to describe a finite attribute set.*

Definition 4 *(**Minimal set of a monotonic access structure**) Let Γ be a monotonic access structure over the set of attributes $\Sigma = \{a_1, a_2, \cdots, a_n\}$. $B \in \Gamma$ is a minimal authorized set if $\forall A \in \Gamma \backslash \{B\}$, we have $A \not\subset B$. The set of all minimal sets in Γ is called the basis of Γ.*

Definition 5 *(**Dual of access structure**) The dual access structure $\Gamma^{\perp}$ of an access structure Γ over Σ is defined as the collection of sets $A \subset \Sigma$ such that $\Sigma \backslash A = A^c \notin \Gamma$.*

Definition 6 *(**Critical set of minimal sets**) [NNP05] Let $\mathcal{B} = \{X_1, \cdots, X_r\}$ be the set of minimal set of an access structure Γ, and $\mathcal{H} \subset \mathcal{B}$ be a subset of minimal sets. $\mathcal{H}$ is called a critical set of minimal sets for $\mathcal{B}$, if every $X_i \in \mathcal{H}$ contains a set $B_i \subset X_i$, $|B_i| \geq 2$, and the following conditions hold:*

1. *The set B_i uniquely determines X_i in the set $\mathcal{H}$. i.e., no other set in $\mathcal{H}$ contains B_i;*
2. *$\forall Y \subset B_i$, set $S_Y = \cup_{X_j \in \mathcal{H}, X_j \cap Y \neq \emptyset}(X_j \backslash Y)$ does not contain any element of $\mathcal{B}$.*

For example, assume that $\Sigma = \{a_1, a_2, a_3, a_4\}$ is the set of attributes, and $\mathcal{B} = \{X_1 = \{a_1, a_2\}, X_2 = \{a_3, a_4\}\}$ is the set of minimal sets for a monotone access structure Γ, then $\mathcal{H}(= \mathcal{B})$ is a critical set of minimal sets. Also, $\mathcal{B}^{\perp} = \{\{a_1, a_3\}, \{a_1, a_4\}, \{a_2, a_3\}, \{a_2, a_4\}\}$. We can find a critical set $\mathcal{H}^{\perp}$ for $\Gamma^{\perp}$ to be $\{\{a_1, a_3\}, \{a_1, a_4\}\}$. As instantiating as above, we have the following theorem that was proven in [NNP05].

Theorem 1 *Let Γ be an access structure and $\Gamma^{\perp}$ be its dual, and $\mathcal{H}$ and $\mathcal{H}^{\perp}$ be the critical set of minimal sets for Γ and $\Gamma^{\perp}$ respectively. The size of any monotone span program computing Γ is bounded by $|\mathcal{H}| + |\mathcal{H}^{\perp}| - 1$.*

Remark 2 *There existence of an efficient LSSS for a specific monotonic access structure is equivalent to the existence of a smallest monotonic span program for the characteristic function of the same access structure [BGP97].*

2.2 Random Subspaces for Leakage Resilience over Arbitrary Functions

We provide an algebraic tool that is crucial to our leakage resilient constructions. More specifically, we give an algebraic theorem and its claim that essentially say that random subspaces are resilient to continual leakage.

Theorem 2 *[BKKV10] Let $m, l, d \in \mathbb{N}$, $2d \leq l \leq m$ and p be a large prime. Let $X_1 \xleftarrow{\$} \mathbb{Z}_p^{m \times l}$ and $X_2 \xleftarrow{\$} \mathbb{Z}_p^{m \times d}$, and $T \xleftarrow{\$} Rank_d(\mathbb{Z}_p^{l \times d})$. For any function $f : \mathbb{Z}_p^{m \times d} \to \varphi$, there exists*

$$Dist((X_1, f(X_1T)), (X_1, f(X_2))) \leq \mathsf{negl}(\cdot)$$
$$|\varphi| \leq 4(1 - \frac{1}{p}) \cdot p_2^{l-2d+1} \cdot \mathsf{negl}(\cdot)^2 \tag{3}$$

We note that, if the leakage $f(X_1T)$ reveals bounded information X_1, then $(X_1, f(X_1T))$ and $(X_1, f(X_2))$ are statistically close. X_2 is a random vector and the leakage function $f(X_2)$ reveals nothing about the space X_1. By setting $d = 1$ and $l = m - 1$, we have the following claim.

Claim 1 *Let $\Delta, \vec{\mu} \xleftarrow{\$} \mathbb{Z}_p^m$ and $\vec{\mu}'$ be selected uniformly randomly from the set of vector in $\mathbb{Z}_p^m$ which are orthogonal to Δ under the dot product modulo p. For any function $f : \mathbb{Z}_p^m \to \{0,1\}^\ell$, where the function output is bounded by the length ℓ, there exists*

$$Dist((\Delta, f(\vec{\mu})), (\Delta, f(\vec{\mu}'))) \leq \mathsf{negl}(\cdot)$$
$$\ell \leq 4p^{m-3}(p-1) \cdot \mathsf{negl}(\cdot)^2 \tag{4}$$

2.3 Hardness Assumptions

Bilinear groups of composite order are groups with an efficient bilinear map where the group order is a product of two or more distinct primes. Such groups are constructed from pairing friendly curves over a finite field. The following hardness assumptions are based on the static subgroup decisional problems that have been analyzed in [LW10, LOS+10]

Definition 7 ***(1-SDP assumption)*** *1-class Subgroup Decision Problem (1-SDP) is hard relative to $\Theta = (N = p_1p_2p_3, \mathbb{G}, \mathbb{G}_T, \hat{e}) \leftarrow \pounds(\kappa)$ if for all PPT algorithm $\mathscr{A}$, there exists a negligible function negl such that*

$$|Pr[\mathscr{A}(\Theta, g_1, X_3, T_1) = 1] - Pr[\mathscr{A}(\Theta, g_1, X_3, T_2) = 1]| \leq \mathsf{negl}(\kappa)$$

where the probabilities are taken over the choices of $g_1 \in \mathbb{G}_{p_1}$, $X_3 \in \mathbb{G}_{p_3}$, $T_1 \in \mathbb{G}_{p_1p_2}$ and $T_2 \in \mathbb{G}_{p_1}$.

Definition 8 ***(2-SDP assumption)*** *2-class Subgroup Decision Problem (2-SDP) is hard relative to $\Theta = (N = p_1p_2p_3, \mathbb{G}, \mathbb{G}_T, \hat{e}) \leftarrow \pounds(\kappa)$ if for all PPT algorithm $\mathscr{A}$, there exists a negligible function negl such that*

$$|Pr[\mathscr{A}(\Theta, g_1, X_1X_2, X_3, Y_2Y_3, T_1) = 1] - Pr[\mathscr{A}(\Theta, g_1, X_1X_2, X_3, Y_2Y_3, T_2) = 1]| \leq \mathsf{negl}(\kappa)$$

where the probabilities are taken over the choices of $g_1 \in \mathbb{G}_{p_1}$, $X_2, Y_2 \in \mathbb{G}_{p_2}$, $X_3, Y_3 \in \mathbb{G}_{p_3}$, $T_1 \in \mathbb{G}_{p_1 p_2}$ *and* $T_2 \in \mathbb{G}$.

Definition 9 ***(BSDP assumption)*** *[LW10,LOS+10] Bilinear Subgroup Decision Problem (BSDP) is hard relative to* $\Theta = (N = p_1 p_2 p_3, \mathbb{G}, \mathbb{G}_T, \hat{e}) \leftarrow \mathcal{L}(\kappa)$ *if for all PPT algorithm* $\mathscr{A}$, *there exists a negligible function* negl *such that*

$$|Pr[\mathscr{A}(\Theta, g_1, g_1^{\alpha} X_2, X_3, g_1^{s} Y_2, Z_2, T_1) = 1] - Pr[\mathscr{A}(\Theta, g_1, g_1^{\alpha} X_2, X_3, g_1^{s} Y_2, Z_2, T_2) = 1]| \leq \mathsf{negl}(\kappa)$$

where $T_1 = \hat{e}(g_1^{\alpha}, g_1^{s})$ *and the probabilities are taken over the choices of* $s, \alpha \in \mathbb{Z}_N$, $g_1 \in \mathbb{G}_{p_1}$, $X_2, Y_2, Z_2 \in \mathbb{G}_{p_2}$, $X_3 \in \mathbb{G}_{p_3}$, *and* $T_2 \in \mathbb{G}_T$.

3 Leakage-resilient Attribute-based Encryption

In this section, we give the model and security defintion of leakage-resilient ciphertext-policy ABE (LR-CP-ABE), where the key is associated with an attribute set and the ciphertext is associated with an access structure. In section 6.2, we will give the model and concrete construction of leakage-resilient key-policy ABE (LR-KP-ABE).

3.1 Model of LR-CP-ABE

Definition 10 ***(LR-CP-ABE)*** *A leakage-resilient ciphertext-policy attribute-based encryption (LR-CP-ABE) for the general access structure* Γ *over the attribute universe* Σ *is comprised of five probabilistic polynomial-time algorithms.*

1. $(\mathtt{MPK}, \mathtt{MSK}) \leftarrow \mathbf{Setup}(1^{\kappa}, \Sigma, \ell)$ *The system setup algorithm takes a security parameter* κ, *a universe of attributes* Σ *and an allowable private-key leakage bound* ℓ *as inputs, and outputs system public key* $\mathtt{MPK}$ *and master key* $\mathtt{MSK}$.

   Note that the system public key can be seen by all participants in the system and will be the input in all other algorithms.

2. $\mathtt{SK}_{\mathbb{S}} \leftarrow \mathbf{KeyGen}(\mathtt{MSK}, \mathbb{S})$ *The key generation algorithm takes the master key* $\mathtt{MSK}$, *and a set of attributes* $\mathbb{S} \subseteq \Sigma$ *as inputs, and outputs a private key* $\mathtt{SK}_{\mathbb{S}}$.

3. $\mathtt{SK}'_{\mathbb{S}} \leftarrow \mathbf{KeyUpd}(\mathtt{SK}_{\mathbb{S}}, \mathbb{S})$ *The key update algorithm takes a private key* $\mathtt{SK}_{\mathbb{S}}$ *as input and outputs a updated and re-randomized key* $\mathtt{SK}'_{\mathbb{S}}$.

4. $\mathtt{CT}_{\Gamma} \leftarrow \mathbf{Enc}(M, \Gamma)$ *The encryption algorithm takes a message* M *and an access structure* Γ *as inputs, and outputs a ciphertext* $\mathtt{CT}_{\Gamma}$.

5. $M \leftarrow \mathbf{Dec}(\mathtt{CT}_{\Gamma}, \mathtt{SK}_{\mathbb{S}})$ *The decryption algorithm takes a ciphertext* $\mathtt{CT}_{\Gamma}$ *and a key* $\mathtt{SK}_{\mathbb{S}}$ *as inputs, and outputs* M *if and only if the set of attributes* $\mathbb{S}$ *satisfies the access structure* Γ, *i.e.,* $\Gamma(\mathbb{S}) = 1$.

Let Σ and $\mathcal{M}$ be the attribute space and the message space respectively, and $\mathcal{F}$ be a polynomially computational function family that the output of a function is bounded by parameter ℓ. For all correctly generated MPK and MSK, and $\mathtt{SK}_{\mathbb{S}}$ is generated from any

attribute set over Σ. The amount leakage of $\mathtt{SK}_{\mathbb{S}}$ is bounded by ℓ, i.e., $\sum_i f_i(\mathtt{SK}_{\mathbb{S}}) \leq \ell$. The consistency of LR-CP-ABE should be guaranteed as:

$$Pr\left[\begin{array}{l|l} \mathsf{Dec}(\mathtt{CT}_{\Gamma}, \mathtt{SK}'_{\mathbb{S}}) \neq M & \begin{array}{l} \forall \mathbb{S} \subseteq \Sigma,\ \forall M \in \mathcal{M} \\ \Gamma(\mathbb{S}) = 1 \\ \forall i, f_i, h_i \in \mathcal{F} \\ \mathtt{CT}_{\Gamma} \leftarrow \mathsf{Enc}(M, \Gamma) \\ \mathtt{SK}_{\mathbb{S}} \leftarrow \mathsf{KeyGen}(\mathtt{MSK}, \mathbb{S}) \\ \mathtt{SK}'_{\mathbb{S}} \leftarrow \mathsf{KeyUpd}(\mathtt{SK}_{\mathbb{S}}, \mathbb{S}) \\ \sum_i f_i(\mathtt{SK}_{\mathbb{S}}) \leq \ell \\ \sum_i h_i(\mathtt{SK}'_{\mathbb{S}}) \leq \ell \end{array} \end{array}\right] \leq \mathsf{negl}(\kappa) \tag{5}$$

3.2 Security Properties in the Presence of Leakage

We follow the natural leakage-resilient security definition from [AGV09], which roughly states that an encryption is ℓ-leakage-resilient if it remains secure despite the fact that an adversary can learn up to ℓ bits of arbitrary information on the private key of being attacked.

An attribute-based encryption scheme is key-leakage resilient if it is semantically secure when the adversary obtain partial information on the key. We model the key leakage by providing the adversary a function that taking the private key as input and obtaining the output of the key. In order to record the queried and leaked keys, we set two initially empty lists: $\mathcal{R} = \langle hd, \mathbb{S} \rangle$, $\mathcal{Q} = \langle hd, \mathbb{S}, \mathtt{SK}_{\mathbb{S}}, lb \rangle$ to store the records, where all records are associated with a handle hd.

Definition 11 *(**Leakage-resilient experiment**) The leakage-resilient experiment $\mathsf{Game}_R(1^{\kappa}, \Sigma, \ell)$ works between a challenger $\mathscr{C}$ and an adversary $\mathscr{A}$ as follows.*

***Setup**. The challenger $\mathscr{C}$ runs setup algorithm to generate public key $\mathtt{MPK}$ and master key $\mathtt{MSK}$, and starts the interaction with $\mathscr{A}$ by providing the public key $\mathtt{MPK}$.*

***Lunch query**. In this stage, adversary $\mathscr{A}$ can perform the following queries:*

- *Key extraction query (Ω_E): $\mathscr{A}$ provides an attribute set $\mathbb{S}$ to request a key $\mathtt{SK}_{\mathbb{S}}$, and $\mathscr{C}$ answers with $\mathtt{SK}_{\mathbb{S}} \leftarrow \mathsf{KeyGen}(\mathtt{MSK}, \mathbb{S})$, and adds $(hd, \mathbb{S}, \mathtt{SK}_{\mathbb{S}}, 0)$ into queue $\mathcal{Q}$.Notice that in this query, the leaked bit of extracted key $\mathtt{SK}_{\mathbb{S}}$ is 0, which means that a new created key has no leakage.*

- *Key leakage query (Ω_L): $\mathscr{A}$ issues a key leakage query for $\mathtt{SK}_{\mathbb{S}}$ with a function $f : \mathtt{SK} \rightarrow \{0,1\}^*$. $\mathscr{C}$ at first seeks the record in $\mathcal{Q}$, and responds with $f(\mathtt{SK}_{\mathbb{S}})$ if $lb + f(\mathtt{SK}_{\mathbb{S}}) \leq \ell$, and updates lb with $lb + f(\mathtt{SK}_{\mathbb{S}})$; Outputs ϕ otherwise.*

- *Key update query (Ω_U): $\mathscr{A}$ issues a key update query for $\mathtt{SK}_{\mathbb{S}}$. $\mathscr{C}$ finds the record in $\mathcal{Q}$. If not found, $\mathscr{C}$ returns the key with key extraction oracle Ω_E and sets $lb = 0$. Otherwise, $\mathscr{C}$ returns with $\mathtt{SK}'_{\mathbb{S}} \leftarrow \mathsf{KeyUpd}(\mathtt{SK}_{\mathbb{S}}, \mathbb{S})$ and updates the corresponding lb with 0.*

Challenge. *$\mathscr{A}$ outputs two messages $(M^{(0)}, M^{(1)})$ and an access structure Γ such that for all $\mathbb{S} \in \mathcal{R}$ $\Gamma(\mathbb{S}) = 0$. $\mathscr{C}$ at random picks a bit $b \in \{0,1\}$ and then returns the challenge ciphertext $\mathsf{CT}^{(b)} = \mathsf{Enc}(M^{(b)}, \Gamma)$.*

Supper query. *$\mathscr{A}$ continues to issues the queries like in Lunch query.*

Response. *Finally, $\mathscr{A}$ outputs a bit $b' \in \{0,1\}$ as the guess for the random coin b in the challenge phase. Adversary $\mathscr{A}$'s advantage in experiment $\mathsf{Game}_R(1^\kappa, \Sigma, \ell)$ is defined as $\mathsf{Adv}_{\mathscr{A}}(1^\kappa, \Sigma, \ell) = |2Pr[(b = b')] - 1|$.*

Definition 12 *(**Adaptively leakage-resilient security**) Suppose that the leakage bound is ℓ and a polynomial-time adversary has at most Q queries for keys. An attribute-based encryption scheme is adaptively $(Q, \ell, \frac{\ell}{|\mathsf{SK}|})$-leakage-resilient secure if the advantage of the adversary in winning $\mathsf{Game}_R(\kappa, \Sigma, \ell)$ is less than $\mathsf{negl}(\kappa)$ in security parameter κ and leakage bound ℓ.*

Definition 13 *(**Selectively leakage-resilient security**) An attribute-based encryption scheme is selectively $(Q, \ell, \frac{\ell}{|\mathsf{SK}|})$-leakage-resilient secure, if in experiment $\mathsf{Game}_R(\kappa, \Sigma, \ell)$ the challenge pair had to provide before the system public key and master key build, and the advantage of the adversary in the experiment is less than $\mathsf{negl}(\kappa)$ in security parameter κ and leakage bound ℓ.*

Definition 14 *(**Leakage rate**) The leakage rate $\gamma = \ell/|\mathsf{SK}|$ is defined as the relative leakage of a private key SK, where ℓ is an allowable leakage bound and $|\mathsf{SK}|$ is the number of bits needed to efficiently store private key SK.*

4 Construction of LR-CP-ABE

Let Σ be an attribute set, we denote the cardinality of set Σ by $|\Sigma|$. Let vectors $\vec{\rho} = (\rho_1, \rho_2, \cdots, \rho_n)$ and $\vec{\sigma} = (\sigma_1, \sigma_2, \cdots, \sigma_n)$, we denote the inner product of vectors $\vec{\rho}$ and $\vec{\sigma}$ by $\langle \vec{\rho}, \vec{\sigma} \rangle$ and the bilinear group inner product by $\hat{e}_n(g^{\vec{\rho}}, g^{\vec{\sigma}})$. i.e., $\langle \vec{\rho}, \vec{\sigma} \rangle = \sum_{i \in [n]} \rho_i \sigma_i$, and $\hat{e}_n(g^{\vec{\rho}}, g^{\vec{\sigma}}) = \prod_{i \in [n]} \hat{e}(g^{\rho_i}, g^{\sigma_i}) = \hat{e}(g, g)^{\langle \vec{\rho}, \vec{\sigma} \rangle}$.

LR-CP-ABE.Setup$(1^\kappa, \Sigma, \ell)$ On input a security parameter κ, an attribute set Σ and a leakage bound ℓ, this algorithm generates system public key MPK and master key MSK as follows:

1. Run the bilinear group generator to produce $\Theta = (N = p_1 p_2 p_3, \mathbb{G}, \mathbb{G}_T, \hat{e})$, where p_1, p_2 and p_3 are distinct primes;
2. Define $\mathsf{negl} = p_2^{-\tau}$ as the allowable maximum probability in succeeding in leakage guess[1], and compute $\omega = \lceil 1 + 2\tau + \frac{\ell}{\log_2 p_2} \rceil$[2];
3. Select random generators $g_1 \in \mathbb{G}_{p_1}$ and $g_3 \in G_{p_3}$;
4. For each attribute $i \in \Sigma$, pick $t_i \in \mathbb{Z}_N$ and set $T_i = g_1^{a_i t_i}$;

[1] We can denote this probability as the entropy loss when the private key leaks.

[2] As τ is a small positive constant, in practice we can eliminate this parameter in ω, i.e., $\omega \approx \lceil 1 + \frac{\ell}{\log_2 p_2} \rceil$.

5. At random choose $\alpha \in \mathbb{Z}_N$ and set $Y = \hat{e}(g_1, g_1)^{\alpha}$;

6. Select $a, t, y_2, y_3 \in \mathbb{Z}_N$, for $i = 1, \cdots, \omega$, select $\rho_i, y_{1,i} \in \mathbb{Z}_N$, and for $j = 1, \cdots, |\Sigma|$, select $y_{4,j} \in \mathbb{Z}_N$ randomly;

7. Set the master key

$$\begin{aligned} \mathtt{MSK} &= \langle \Sigma, \vec{w}_1, w_2, w_3, \vec{w}_4 \rangle \\ &= \langle \Sigma, g_1^{\vec{\sigma}} g_3^{\vec{y}_1}, g_1^{\alpha+at+\langle \vec{\rho}, \vec{\sigma} \rangle} g_3^{y_2}, g_1^t g_3^{y_3}, \forall i \in \Sigma \ T_i^t g_3^{y_{4,i}} \rangle \end{aligned} \tag{6}$$

8. Publish the system public key

$$\mathtt{MPK} = \langle \Theta, g_1, g_3, g_1^a, g_1^{\vec{\rho}}, Y, (T_i)_{i \in \Sigma} \rangle \tag{7}$$

The parameter ω, mainly decided by ℓ, can be varied to achieve desired (master) key leakage tolerance and size of keys and ciphertexts.

LR-CP-ABE.KeyGen($\mathtt{MSK}, \mathbb{S}$) On input an attribute set $\mathbb{S}$ and the master key $\mathtt{MSK} = \langle \Sigma, \vec{w}_1, w_2, w_3, \vec{w}_4 \rangle$, this algorithm selects $\triangle t, \triangle y_2, \triangle y_3 \in \mathbb{Z}_N$, and selects $y_{1,i} \in \mathbb{Z}_N$ for $i \in [\omega]$, and picks $y_{4,j} \in \mathbb{Z}_N$ for $j \in [|\mathbb{S}|]$ randomly, and returns the key $\mathtt{SK}_{\mathbb{S}}$ as:

$$\begin{aligned} \mathtt{SK}_{\mathbb{S}} &= \langle \mathbb{S}, \vec{k}_1, k_2, k_3, \vec{k}_4 \rangle \\ &= \begin{pmatrix} \mathbb{S}, \\ \vec{w}_1 * g_1^{\triangle \vec{\sigma}} * g_3^{\vec{\triangle} y_1}, \\ w_2 * g_1^{a \triangle t + \langle \vec{\rho}, \triangle \vec{\sigma} \rangle} * g_3^{\triangle y_2}, \\ w_3 * g_1^{\triangle t} * g_3^{\triangle y_3}, \\ \forall i \in \mathbb{S} \ \ w_{4,i} * T_i^{\triangle t} * g_3^{\triangle y_{4,i}} \end{pmatrix}^{\top} = \begin{pmatrix} \mathbb{S}, \\ g_1^{\vec{\sigma} + \triangle \vec{\sigma}} g_3^{\vec{y}_1 + \triangle \vec{y}_1}, \\ g_1^{\alpha + a(t+\triangle t) + \langle \vec{\rho}, \vec{\sigma} + \triangle \vec{\sigma} \rangle} g_3^{y_2 + \triangle \vec{y}_2}, \\ g_1^{t+\triangle t} g_3^{y_3 + \triangle y_3}, \\ \forall i \in \mathbb{S} \ \ T_i^{t+\triangle t} g_3^{y_{4,i} + \triangle y_{4,i}} \end{pmatrix}^{\top} \end{aligned} \tag{8}$$

Note that the components of private key are $\omega + |\mathbb{S}| + 2$ elements in subgroup $\mathbb{G}_{p_1 p_3}$.

LR-CP-ABE.KeyUpd($\mathtt{SK}_{\mathbb{S}}, \mathbb{S}$) Let a private key $\mathtt{SK}_{\mathbb{S}} = \langle \mathbb{S}, \vec{k}_1, k_2, k_3, \vec{k}_4 \rangle = \langle \mathbb{S}, g_1^{\vec{\sigma}} g_3^{\vec{y}_1}, g_1^{\alpha+at+\langle \vec{\rho}, \vec{\sigma} \rangle} g_3^{y_2}, g_1^t g_3^{y_3}, (T_i^t g_3^{y_{4,i}})_{i \in \mathbb{S}} \rangle$. The key update algorithm at random selects $\triangle t, \triangle y_2, \triangle y_3 \in \mathbb{Z}_N$, and selects $y_{1,i} \in \mathbb{Z}_N$ for $i \in [\omega]$, and $y_{4,j} \in \mathbb{Z}_N$ for $j \in [|\mathbb{S}|]$, and outputs a new key $\mathtt{SK}'_{\mathbb{S}}$:

$$\begin{aligned} \mathtt{SK}'_{\mathbb{S}} &= \langle \mathbb{S}, \vec{k}'_1, k'_2, k'_3, \vec{k}'_4 \rangle \\ &= \begin{pmatrix} \mathbb{S}, \\ \vec{k}_1 * g_1^{\triangle \vec{\sigma}} * g_3^{\vec{\triangle} y_1}, \\ k_2 * g_1^{a \triangle t + \langle \vec{\rho}, \triangle \vec{\sigma} \rangle} * g_3^{\triangle y_2}, \\ k_3 * g_1^{\triangle t} * g_3^{\triangle y_3}, \\ \forall i \in \mathbb{S} \ \ k_{4,i} * T_i^{\triangle t} * g_3^{\triangle y_{4,i}} \end{pmatrix}^{\top} = \begin{pmatrix} \mathbb{S}, \\ g_1^{\vec{\sigma}'} g_3^{\vec{y}'_1}, \\ g_1^{\alpha + at' + \langle \vec{\rho}, \vec{\sigma}' \rangle} g_3^{y'_2}, \\ g_1^{t'} g_3^{y_3}, \\ (T_i^{t'} g_3^{y_{4,i}})_{i \in \mathbb{S}} \end{pmatrix}^{\top} \end{aligned} \tag{9}$$

where $t' = t + \triangle t$, $\vec{\sigma}' = \vec{\sigma} + \triangle \vec{\sigma}$, $\vec{y}'_1 = y_1 + \triangle \vec{y}_1$, $y'_2 = y_2 + \triangle y_2$, $y'_3 = y_3 + \triangle y_3$, and $\vec{y}_4 = \vec{y}_4 + \triangle y_4$.

Remark 3 *If $\mathbb{S} = \Sigma$ and $\mathtt{SK}_{\Sigma} = \mathtt{MSK}$, then the update algorithm can refresh the master key that generates a same distributed master key. Thus, we can consider the master key $\mathtt{MSK}$ as a special private key for universal set Σ.*

Remark 4 *In our scheme, we allow many private keys per attribute set $\mathbb{S}$ and many master keys for universal attribute set Σ.*

LR-CP-ABE.Enc(M, Γ) At first, this algorithm converts the monotone access structure Γ to the set of minimal sets $\mathcal{B} = \{B_1, B_2, \cdots, B_m\}$, where $B_i \subset \Sigma$ for $i = 1, \cdots, m$. The algorithm also at random selects $s, s_1, \cdots, s_m \in \mathbb{Z}_N$, and outputs the ciphertext $\mathtt{CT}_\Gamma$:

$$\begin{aligned}\mathtt{CT}_\Gamma &= \langle \mathcal{B}, c_0, \vec{c}_1, c_2, \vec{c}_3, \vec{c}_4 \rangle \\ &= \langle \mathcal{B}, MY^s, g_1^{s\vec{\rho}}, g_1^{-s}, g_1^{as}(\prod_{j\in B_i} T_j)_{i\in[m]}^{s_i}, (g_1^{s_i})_{i\in[m]} \rangle \end{aligned} \tag{10}$$

LR-CP-ABE.Dec$(\mathtt{CT}_\Gamma, \mathtt{SK}_\mathbb{S})$ If attributes set $\mathbb{S}$ satisfies the access structure Γ specified by $\mathcal{B}$, then $\mathbb{S}$ must be a superset of a minimal set in $\mathcal{B}$. Let $S_k \subset \mathbb{S}$ for some $k \in [m]$. This algorithm calculates:

$$M \leftarrow c_0 \frac{\hat{e}_\omega(c_1, k_1)\hat{e}(c_2, k_2)\hat{e}(c_{3,k}, k_3)}{\hat{e}(c_{4,k}, \prod_{i\in B_k} k_{4,i})} \tag{11}$$

Remark 5 *In our scheme, we are equipped with an update algorithm* KeyUpd *that takes in a (master) private key and outputs a new and re-randomized key from the same distribution generated by a fresh call to* KeyGen *algorithm, then the security will yield resilience to continual leakage "for free". In particular, the many master keys for universal set Σ and the many private keys per attribute set $\mathbb{S}$ allow to leak can be interpreted as refreshed versions of corresponding master/private keys.*

Correctness. The correctness is described as follows:

$$(1)\ \hat{e}(c_1, k_1) = \hat{e}(g_1^{s\vec{\rho}}, g_1^{\vec{\sigma}} g_3^{y_1}) = \hat{e}(g_1^{s\vec{\rho}}, g_1^{\vec{\sigma}}) = \hat{e}(g_1, g_1)^{s\langle\vec{\rho},\vec{\sigma}\rangle} \tag{12}$$

$$(2)\ \hat{e}(c_2, k_2) = \hat{e}(g_1^{-s}, g_1^{\alpha+at+\langle\vec{\rho},\vec{\sigma}\rangle} g_3^{y_2}) = \hat{e}(g_1, g_1)^{-s\alpha-ast-s\langle\vec{\rho},\vec{\sigma}\rangle} \tag{13}$$

$$(3)\ \hat{e}(c_{3,k}, k_3) = \hat{e}(g_1^{as}(\prod_{j\in B_k} T_j)^{s_k}, g_1^t g_3^{y_3}) = \hat{e}(g_1, g_1)^{ast}\hat{e}(\prod_{j\in B_k} T_j, g_1)^{s_k t} \tag{14}$$

$$(4)\ \hat{e}(c_{4,k}, \prod_{j\in B_k} k_{4,j}) = \hat{e}(g_1^{s_k}, \prod_{j\in B_k} T_j^t g_3^{y_{4,j}}) = \hat{e}(g_1, \prod_{j\in B_k} T_j)^{s_k t} \tag{15}$$

Then, the blind factor is calculated by

$$\frac{\hat{e}(c_1, k_1)\hat{e}(c_2, k_2)\hat{e}(c_{3,k}, k_3)}{\hat{e}(c_{4,k}, \prod_{j\in B_k} k_{4,j})} = \hat{e}(g_1, g_1)^{-s\alpha} = Y^{-s} \tag{16}$$

Remark 6 *In the decryption, the algorithm only performs ω+3 pairing operations, which is more efficient than the construction that uses LSSS to specify the access structure in [LRW11]. We will discuss and compare the decryption performance in section 6.2.*

5 Security

We will prove the adaptive security of LR-CP-ABE with the technique of dual system encryption. Our analysis of leakage resilience of our system will rely on Theorem 2 in [BKKV10], which is proven using the techniques in [BFO08].

5.1 Key Refresh and Continual Leakage

As our schemes are equipped with a update algorithm that takes input a private key and outputs a new re-randomized key from the same distribution, we can obtain continual leakage tolerance. We can specify the leakage parameter ℓ as the entropy loss that a private key can tolerate, and update the private key when the entropy loss of that private key will draw near the threshold.

In the update algorithm, it explicitly updates the randomness in the key. That is, the new randomness in the key are described as follows:

$$\begin{pmatrix} t' \\ \vec{\sigma}' \\ \vec{y}_1' \\ y_2' \\ y_3' \\ \vec{y}_4' \end{pmatrix} = \begin{pmatrix} t \\ \vec{\sigma} \\ \vec{y}_1 \\ y_2 \\ y_3 \\ \vec{y}_4 \end{pmatrix} + \begin{pmatrix} \triangle t \\ \triangle \vec{\sigma} \\ \triangle \vec{y}_1 \\ \triangle y_2 \\ \triangle y_3 \\ \triangle \vec{y}_4 \end{pmatrix} \tag{17}$$

Here the randomness with $\triangle$ is randomly picked from $\mathbb{Z}_N$, and the new randomness have the same distribution with the previous one.

We can tolerate leakage on the key generation and update procedures in the continual leakage model. More detail, we can tolerate leakage which is logarithmic in the security parameter κ by guessing a value for the leakage and observing whether the adversary's advantage distinctly decreases. In continual leakage models in [DKL09,BKKV10], there are only one master key and one private key per user at any time, but in our scheme we design to provide master key and private key from arbitrary number of keys. When a master key or a private key is updated, the entropy of the key will sustain the maximum entropy that the key provides in the presence of non-leakage model, and as a result a new leakage session on the updated key is allowed. We can achieve the continual leakage tolerance when we assume keys are periodically updated and no leakage is allowed during the update process.

5.2 Leakage-resilient Semantic Security

Our security employs the dual system encryption mechanism of [Wat09, LW10]. Let Q be the number of key queries that the adversary makes, then our proof considers a sequence of $2Q + 4$ games between an adversary $\mathscr{A}$ and a challenger $\mathscr{C}$. By means of dual system encryption, we at first give the semi-functional ciphertext/key generation algorithms and convert the challenge ciphertext and queried keys into semi-functional form. We also define two types of semi-functional key. The semi-functional key and ciphertext algorithms are presented as follows:

- **KeyGenSF**. Let $\mathtt{SK}_{\mathbb{S}} = \langle \mathbb{S}, \vec{k}_1, k_2, k_3, \vec{k}_4 \rangle$ be a normal key, a semi-functional key is constructed as:

  1. Type 1: $\overline{\mathtt{SK}}_{\mathbb{S}} = \langle \mathbb{S}, \vec{k}_1 * g_2^{\vec{d}_1}, k_2 * g_2^{d_2}, k_3 * g_2^{d_3}, \vec{k}_4 * g_2^{\vec{d}_4} \rangle$, where g_2 is a random generator of $\mathbb{G}_{p_2}$ and $d_i (i = 1, \ldots, 4)$ is randomly picked from $\mathbb{Z}_N$.
  2. Type 2: $\overline{\mathtt{SK}}_{\mathbb{S}} = \langle \mathbb{S}, \vec{k}_1, k_2 * g_2^{d_2}, k_3, \vec{k}_4 \rangle$.

- **EncSF**. Let $\mathtt{CT}_{\Gamma} = \langle \mathcal{B}, c_0, \vec{c}_1, c_2, \vec{c}_3, \vec{c}_4 \rangle$ be a normal ciphertext, a semi-functional ciphertext is converted as: $\overline{\mathtt{CT}}_{\Gamma} = \langle \mathcal{B}, c_0, \vec{c}_1 * g_2^{\vec{e}_1}, c_2 * g_2^{e_2}, \vec{c}_3 * g_2^{\vec{e}_3}, \vec{c}_4 \rangle$, where $\vec{e}_1, e_2, \vec{e}_3$ are random elements in $\mathbb{Z}_N$.

Obviously, if we use a type-1 semi-functional key to decrypt a semi-functional ciphertext, we will obtain extra term $\hat{e}(g_2, g_2)^{\langle \vec{d}_1, \vec{e}_1 \rangle + d_2 e_2 + d_3 e_{3,k}}$. If $\langle \vec{d}_1, \vec{e}_1 \rangle + d_2 e_2 + d_3 e_{3,k} = 0$, we call the semi-functional key is a nominally semi-functional key w.r.t the ciphertext, otherwise we call the semi-functional key is truly semi-functional.

Our security proof has two steps: At first we use a series of indistinguishable games to prove that the scheme is adaptively secure in non-match key/ciphertext situation, which is derived from the idea of dual system encryption [Wat09,LW10,LW12]. We do so by proving that, in the view of the adversary, the valid private keys are indistinguishable from keys that are random in the subgroup in which the message is embedded. Secondly, we prove that, even the adversary has at most ℓ bits leakage on each match key, he also has only negligible advantage to decrypt the challenge ciphertext. We give the following theorem:

Theorem 3 *If a dual system*

$$\prod_{D} = (\mathit{Setup}, \mathit{KeyGen}, \mathit{KeyUpd}, \mathit{Enc}, \mathit{Dec}, \mathit{KeyGenSF}, \mathit{EncSF})$$

has semi-functional ciphertext invariance, semi-functional key invariance, and semi-functional security under the leakage bound ℓ, then the LR-CP-ABE scheme $\prod = (\mathit{Setup}, \mathit{KeyGen}, \mathit{KeyUpd}, \mathit{Enc}, \mathit{Dec})$ is an $(Q, \ell, \frac{\ell}{|SK|})$-leakage secure attribute-based encryption scheme.

Proof. We prove this theorem by a series of claims listed in Tab.1. The key and the ciphertext in real construction in Section 4 are normal forms. At first we show that the update procedure can be considered as a special key extraction procedure, and then we only consider key extraction oracle instead of update oracle. Next we convert the challenge ciphertext into semi-functional form, and then convert the keys into semi-functional forms one by one. By these conversions, all ciphertexts and keys are semi-functional. We also give a Claim 5 to demonstrate that an adversary has no advantage in changing a truly semi-functional key (can not decrypt a semi-functional ciphertext) to a nominally semi-functional key (can decrypt a semi-functional ciphertext). Finally, we also show that the message is indistinguishable from a random message in the challenge ciphertext, which means that the challenge message is fully hidden in the ciphertext. We provide the security by Claim 1 – Claim 6 and hybrid argument over

Table 1: Lemmas from indistinguishable games

Lemma	Result	Functionality
Lem 1	Ω_U can be answered by Ω_E	Update invariance
Lem 2	$\mathsf{Adv}_{\mathscr{A}}^{Game_R} - \mathsf{Adv}_{\mathscr{A}}^{Game_1} \leq \epsilon_1$	
Lem 3	$\mathsf{Adv}_{\mathscr{A}}^{Game_2} - \mathsf{Adv}_{\mathscr{A}}^{Game_1} \leq \epsilon_2$	Semi-functional ciphertext invariance
Lem 4	$\mathsf{Adv}_{\mathscr{A}}^{Game_{3,k+1}} - \mathsf{Adv}_{\mathscr{A}}^{Game_{3,k}} \leq \epsilon_{3,k}$	Semi-functional key invariance
Lem 5	$\mathsf{Adv}_{\mathscr{A}}^{Game_{3,k}^L} - \mathsf{Adv}_{\mathscr{A}}^{Game_{3,k}} \leq \epsilon_{3,k}^L$	Truly/nominally semi-functional inconvertibility
Lem 6	$\mathsf{Adv}_{\mathscr{A}}^{Game_4} - \mathsf{Adv}_{\mathscr{A}}^{Game_{3,Q}} \leq \epsilon_4$	Message hiding

the sequence of games to demonstrate the real security game Game_R is computationally indistinguishable from Game_4, in which the challenge message $M^{(b)}$ is masked with a random element in $\mathbb{G}_T$. We leave the detail proof in the full version. □

Lemma 1 ***Update invariance.*** *All queries on Ω_U oracle can be answered by Ω_E oracle.*

Proof. In remark 3, we show that Ω_U is a special kind of key extraction Ω_E. Any query to Ω_U can be answered by Ω_E by setting the input $\texttt{MSK}$ as $\texttt{SK}_{\mathbb{S}}$. □

Lemma 2 *The key space defined in $\mathbb{G}_{p_1p_3}$ is indistinguishable to the definition in $\mathbb{G}_{p_1p_2p_3}$ (i.e., $\mathbb{G}$).*

Proof. If the query is a leakage oracle Ω_L, the simulator $\mathscr{C}$ simply uses the master key to answer the query. If the query is key extraction query Ω_E or a key update query Ω_U, $\mathscr{C}$ answers as follows:

1. If $S_i = S_i^*$ and $p_2 \nmid (S_i - S_i^*)$, $\mathscr{C}$ answers by using $\texttt{MSK}$;
2. If $S_i \neq S_i^*$ and $p_2 | (S_i - S_i^*)$, then $\mathscr{C}$ can obtain a non-trivial factor of N as $a = gcd(S_i - S_i^*, N$. We denote $b = N/a$, as $N = p_1p_2p_3$ and p_is are distinct primes, then
   (a) Case $a = p_1p_2$ and $b = p_3$: given $(g, X_1X_2, X_3, Y_2Y_3, T)$ from 2-SDP assumption, $\mathscr{C}$ check whether $a = p_1p_2$ by testing $(X_1X_2)^a = 1$. If the equation holds, concludes $T \in p_1p_3$ if $\hat{e}(Y_2Y_3, T)^b = 1$ and $T \in \mathbb{G}$ otherwise.
   (b) Case $a = p_2p_3$ and $b = p_1$: Similar to above case, $\mathscr{C}$ checks $a = p_2p_3$ by testing $(Y_2Y_3)^a = 1$ and concludes $T \in \mathbb{G}_{p_1p_3}$ if $\hat{e}(X_1X_2, T)^b = 1$ and $T \in \mathbb{G}$ otherwise.
   (c) Case $a = p_2$ and $b = p_1p_3$: $\mathscr{C}$ determines that this case occurs when above two cases fail. Given $(g, X_1X_2, X_3, Y_2Y_3, T)$, $\mathscr{C}$ concludes $T \in \mathbb{G}_{p_1p_3}$ if $T^b = 1$ and $T \in \mathbb{G}$ otherwise.

□

Lemma 3 ***Semi-functional ciphertext invariance.*** *A semi-functional ciphertext* $\overline{\mathtt{CT}}_\Gamma$ *is indistinguishable from a normal ciphertext* $\mathtt{CT}_\Gamma$.

Proof. Suppose that an adversary can distinguish between a semi-functional ciphertext $\widehat{\mathtt{CT}}_\Gamma$ and a normal ciphertext $\mathtt{CT}_\Gamma$, we can construct an algorithm to solve the hardness assumption 1-SDP.

Receiving the instance $(\Omega = (N = p_1p_2p_3, g_1, X_3, \mathbb{G}, \mathbb{G}_T, \hat{e}), T)$ of 1-SDP, $\mathscr{C}$ constructs the system public key $\mathtt{MPK} = \langle g_1, g_3 = X_3, g_1^a, g_1^{\vec{\rho}}, Y = \hat{e}(g_1, g_1)^\alpha, \forall i \in \Sigma\ T_i = g_1^{t_i}\rangle$ where $a, \alpha, t_i \leftarrow \mathbb{Z}_N$. Knowing the master key, $\mathscr{C}$ can answer all key extraction queries and leakage queries.

In the challenge stage, $\mathscr{C}$ receives the challenger pair $(M^{(0)}, M^{(1)}, \Gamma^*)$ provided by adversary $\mathscr{A}$, and then generates the challenger ciphertext as follows: convert the access structure Γ^* into the set of minimal set $\mathcal{B}^* = \{B_1, B_2, \cdots, B_m\}$ where $B_i \subseteq \Sigma$; at random pick $b \leftarrow \{0, 1\}$ and output the ciphertext $\mathtt{CT}^*_\Gamma = \langle \mathcal{B}^*, M^{(b)}\hat{e}(g_1^\alpha, T), T^{\vec{\rho}}, T^{-1}, T^a(\prod_{j\in B_i} T_j)_{i\in[m]}^{s_i}, (g_1^{s_i})_{i\in[m]}\rangle$.

If $T = g_1^{c_1}g_2^{c_2} \in \mathbb{G}_{p_1p_2}$ for some $c_1, c_2 \in \mathbb{Z}_N$, then we implicitly set the semi-functional factor of challenge ciphertext as $\langle c_2\vec{\rho}, -c_2, 0, ac_2\rangle$. In this case, $\mathtt{CT}^*_\Gamma$ is a properly distributed semi-functional ciphertext and successfully simulates a semi-functional game. If $T \in \mathbb{G}_{p_1}$, $\mathscr{C}$ can successfully simulate a normal ciphertext game as there is no $\mathbb{G}_{p_2}$ part in the created challenge ciphertext $\mathtt{CT}^*_\Gamma$.

If the adversary $\mathscr{A}$ can distinguish between a semi-functional ciphertext $\overline{\mathtt{CT}}_\Gamma$ and a normal ciphertext $\mathtt{CT}_\Gamma$ with a non-negligible advantage, then we can use the output of $\mathscr{A}$ to break 1-SDP assumption with the same advantage. Thus we conclude the proof of the lemma. □

Lemma 4 ***Semi-functional key invariance.*** *Let Q be the number of queries that the adversary issues and the challenge ciphertext is a semi-functional form* $\overline{\mathtt{CT}}_\Gamma$. *For $k = 1, \ldots, Q-1$, the first $k-1$ keys are semi-functional of type 2, the k-th key is semi-functional of type 1, and rest keys are normal, then* $\epsilon = Adv_{\mathscr{A}}^{Game_{k+1}} - Adv_{\mathscr{A}}^{Game_k}$ *is negligible.*

Proof. We establish a PPT algorithm $\mathscr{C}$ that takes a $(g, X_1X_2, X_3, Y_2Y_3, T)$ of 2-SDP assumption instance as input and decides $T \in \mathbb{G}_{p_1p_3}$ or $T \in \mathbb{G}$.

At first, $\mathscr{C}$ constructs the system public key $\mathtt{MPK}$ as: take input (κ, ℓ) and output group description Θ and set $\omega = 1 + \frac{\ell}{\log p_2}$; at random select $\alpha, a, t, \vec{y}_1, y_2, y_3, \vec{y}_4, \vec{\rho}, \vec{\sigma} \in \mathbb{Z}_N$ and set $\mathtt{MPK} = \langle g_1, g_3, g_1^a, g_1^{\vec{\rho}}, Y, (T_i)_{i\in\Sigma}\rangle$ and $\mathtt{MSK} = \langle g_1^{\vec{\sigma}}g_3^{\vec{y}_1},\ g_1^{\alpha+at+\langle\vec{\rho},\vec{\sigma}\rangle}g_3^{y_2}, g_1^t g_3^{y_3}, \forall i \in \Sigma\ T_i^t g_3^{y_{4,i}}\rangle$, where $T_i = g_1^{t_i}$ and $Y = \hat{e}(g_1, g_1)^\alpha$.

To respond the first $k-1$ key query, $\mathscr{C}$ answers the query as a semi-functional key of type 2: $\overline{\mathtt{SK}}_{\mathbb{S}} = \langle \mathbb{S}, \vec{k}_1 = g_1^{\vec{\sigma}}g_3^{\vec{y}_1}, k_2 = g_1^{\alpha+at}(Y_2Y_3)^h g_3^{y_2}, k_3 = g_1^t g_3^{y_3}, \forall i \in \mathbb{S}\ T_i^t g_3^{y_{4,i}}\rangle$. It is easy to see that these keys are semi-functional of type 2.

To respond a k-th key query, $\mathscr{C}$ considers two cases: type 1 and type 2. $\mathscr{C}$ uses the term T in 2-SDP instance to answer the query as:

$$\overline{\mathtt{SK}}_\Gamma = \begin{cases} \langle \mathbb{S}, \vec{k}_1 = g_1^{\vec{\sigma}} g_3^{\vec{y}_1}, k_2 = g_1^{\alpha} T^a g_3^{y_2}, k_3 = T g_3^{y_3}, \forall i \in \mathbb{S}\ T^{t_i} g_3^{y_{4,i}} \rangle & (i) \\ \langle \mathbb{S}, \vec{k}_1 = g_1^{\vec{\sigma}} g_3^{\vec{y}_1}, k_2 = g_1^{\alpha} T^a g_3^{y_2} (Y_2 Y_3)^d, k_3 = T g_3^{y_3}, \forall i \in \mathbb{S}\ T^{t_i} g_3^{y_{4,i}} \rangle & (ii) \end{cases} \tag{18}$$

For the rest key queries, $\mathscr{C}$ answers a normal key. We now further discuss the k-th key in Eq.18.

Case (i), if $T \in \mathbb{G} = g_1^t g_2^r g_3^s$, $\mathtt{SK}_\mathbb{S}$ is a semi-functional key of type 1 for the k-th key. However, if $T \in \mathbb{G}_{p_1 p_3}$, $\mathtt{SK}_\mathbb{S}$ is a normal key since it has not $\mathbb{G}_{p_2}$ part.

Case (ii), the $\mathbb{G}_{p_2}$ part of component k_2 is randomized by $(Y_2 Y_3)^d$. It is easy to demonstrate that the k-th key is type 1 semi-functional if $T \in \mathbb{G}$, and is type 2 semi-functional if $T \in \mathbb{G}_{p_1 p_3}$.

In the challenge phase, $\mathscr{C}$ at first converts the challenge access structure Γ to $\mathcal{B} = \{B_1, \ldots, B_m\}$ where each $B_i \subseteq \Sigma$. $\mathscr{C}$ returns the challenge ciphertext $\mathtt{CT}_\Gamma = \langle \Gamma, c_0 = M^{(b)} \hat{e}(g_1^\alpha, X_1 X_2), \vec{c}_1 = (X_1 X_2)^{\vec{\rho}}, c_2 = X_1 X_2, (c_{3,i} = (X_1 X_2)^a (\prod_{j \in B_i} T_j)^{s_i})_{i \in [m]}, (c_{4,i} = g_1^{s_i})_{i \in [m]} \rangle$. If $T \in \mathbb{G}$ then $\mathscr{C}$ simulates Game_{k+1}, and if $T \in \mathbb{G}_{p_1 p_3}$ $\mathscr{C}$ simulates Game_k. When the k-th key is created in case (i), we indicate that the adversary can not distinguish a type 1 semi-functional key and a normal key. When the k-th key is created in case (ii), we indicate the adversary can not distinguish a type 2 semi-functional key and a type 1 semi-functional key. If an adversary has the negligible advantage $\epsilon = Adv_{\mathscr{A}}^{Game_{k+1}} - Adv_{\mathscr{A}}^{Game_k}$, then we can use algorithm $\mathscr{C}$ in breaking 2-SDP assumption. □

Lemma 5 ***Truly/norminal semi-functional inconvertibility***. *Let the allowable leakage bit of a key be bounded by parameter $\ell = 2 + (\omega - 1 - 2\tau) \log p_2$, where p_2 is the order of $\mathbb{G}_{p_2}$ and τ is a constant s.t. $p_2^{-\tau}$ is negligible in security parameter κ. For $Game_{3,k+1}$, if the $k+1$ query is a leakage oracle or update oracle for $\Gamma(\mathbb{S}) = 1$, any adversary $\mathscr{A}$ can distinguish the reply of that query is calculated from nominally semi-functional keys or truly semi-functional keys is $p_2^{-\tau}$.*

Proof. We use this lemma to show that, even the adversary $\mathscr{A}$ can obtain at most ℓ bits key leakage about set $\mathbb{S}$ that satisfies the challenge access structure Γ^* and then $\mathscr{A}$ has $p_2^{-\tau}$ probability to decrypt the challenge ciphertext $\mathtt{CT}_\Gamma^*$. If $p_2^{-\tau}$ is negligible, then $\mathscr{A}$ has only negligible advantage to successfully perform the decryption, that is, $\mathscr{A}$ can not convert a truly semi-functional key (has no ability in decrypting the challenge ciphertext) to a nominally semi-functional key (can decrypt the challenge ciphertext).

We use Theorem 2 and its claim 1 to prove this lemma. If there exists an algorithm in converting a truly semi-functional key into a nominally semi-functional one, we can construct an algorithm $\mathscr{C}$ that uses $\mathscr{A}$ as a subroute to distinguish two distributions in claim 1. In this simulation, we consider the match key $\mathtt{SK}_\mathbb{S}$ such that $\mathbb{S}$ satisfies the challenge access structure Γ^* (all non-match keys had been considered in Lemma 4). Actually, in non-leakage model, any adversary is unable to query any information about the match key. In our model, we allow the adversary obtain at most ℓ bits information about the match key.

Receiving an instance $(\Delta, f(\lambda))$ in claim 1 where λ is either distributed as $\vec{\mu}$ or $\vec{\mu}'$, $\mathscr{C}$ will use $f(\lambda)$ to answer $\mathscr{A}$'s leakage query: at first create a normal key $\texttt{SK}_{\mathbb{S}}$ by calling KeyGen algorithm; at random choose $r, d_3 \in \mathbb{Z}_N$, and create a semi-functional key $\overline{\texttt{SK}_{\mathbb{S}}}$ by setting the $\mathbb{G}_{p_2}$ part of $\texttt{SK}_{\mathbb{S}}$ to be $g_2^{\vec{\lambda}'}$ where $\vec{\lambda}' = \langle \lambda_1, \cdots, \lambda_\omega, \lambda_{\omega+1} + r, d_3 \rangle$. Obviously, $\vec{\lambda}'$ is the semi-functional factor of key $\overline{\texttt{SK}}_{\mathbb{S}}$. For any leakage query launched by a function f, $\mathscr{C}$ returns $f(\texttt{SK}_{\mathbb{S}})$ if $lb \leq \ell$ and updates lb with $lb + |f(\texttt{SK})|$.

In the challenge phase, the adversary provides two challenge messages $(M^{(0)}, M^{(1)})$ and an access structure Γ^*. $\mathscr{C}$ answers the challenge as follows: (1) at first create a normal ciphertext by calling $\mathsf{Enc}(M^{(b)}, \Gamma^*)$ algorithm; (2) select $e_3 \in \mathbb{Z}_N$ s.t. $\lambda_{\omega+1} + r + d_3 e_3 = 0 \bmod p_2$ where r and d_3 are the values in key extraction query; (3) create a semi-functional ciphertext $\overline{\texttt{CT}_\Gamma^*}$ by setting $\langle \underbrace{1, \cdots, 1}_{\omega}, 1, e_3 \rangle$ as semi-functional factor; (4) send the semi-functional ciphertext $\overline{\texttt{CT}}_\Gamma^*$ to $\mathscr{A}$.

Obviously, if λ is not orthogonal to Δ, then the key is truly semi-functional. Otherwise, if λ is orthogonal to Δ, then the key is nominally semi-functional. Thus we successfully simulate two distributions in claim 1. That is, if there exists an adversary can change a truly semi-functional key into nominally semi-functional form, then we can distinguish the distributions between $(\Delta, f(\vec{\mu}))$ and $(\Delta, f(\vec{\mu}'))$ with the same probability. We can conclude the lemma since this lemma holds for $k = 0, \ldots, Q-1$. □

Lemma 6 ***Message hiding***. *Suppose that in Game$_4$, all keys are semi-functional of type 2 and ciphertexts are semi-functional, and the message is masked with a random element in $\mathbb{G}_T$. If an adversary can distinguish Game$_4$ from Game$_{3,Q}^L$ with advantage ϵ, then we can construct an algorithm with advantage ϵ in breaking BSDP assumption.*

Proof. After receiving an instance of BSDP assumption $(\Theta, g_1, g_1^\alpha X_2, X_3, g_1^s Y_2, Z_2, T)$, $\mathscr{C}$ sets $g_3 = X_3$, $g_2 = Z_2$, $Y = e(g_1, g_1^\alpha X_2) = \hat{e}(g_1, g_1)^\alpha$.

In the key extraction phase, $\mathscr{C}$ can answer all queries: $\texttt{SK}_{\mathbb{S}} = \langle \mathbb{S}, \vec{k}_1 = g_1^t g_3^{\vec{y}_1}, k_2 = (g_1^\alpha X_2) g_1^{at\langle \vec{\rho}, \vec{\sigma} \rangle} g_3^{y_2}, k_3 = g_1^t g_3^{y_3}, \forall i \in \mathbb{S}\ k_{4,i} = T_i^t g_3^{y_{4,i}} \rangle$.

$\mathscr{C}$ receives two challenge messages $(M^{(0)}, M^{(1)})$ and a challenge access structure Γ in the challenge phase, and then at random selects $M^{(b)} \in \{M^{(0)}, M^{(1)}\}$. Then, $\mathscr{C}$ converts the access structure Γ into the set of minimal set $\mathcal{B}^* = \{B_1, B_2, \cdots, B_m\}$, where $B_i \subset \Sigma$ for $i = 1, \cdots, m$, and returns the challenge ciphertext $\texttt{CT}_\Gamma^* = \langle \mathcal{B}^*, M^{(b)} T, (g_1^s Y_2)^{\vec{\rho}}$, $(g_1^s Y_2)^{-1}$, $(g_1^s Y_2)^a (\prod_{j \in B_i} T_j)^{s_i}_{i \in [m]}$, $(g_1^{s_i})_{i \in [m]} \rangle$, where $g_1^s Y_2$ is derived from the instance of BSDP assumption, T is the assumption term and s_i $(1 \leq i \leq m)$ is chosen from $\mathbb{Z}_N$ randomly.

Intuitively, if $T = \hat{e}(g_1, g_1)^{s\alpha}$, $\texttt{CT}_\Gamma^*$ is a semi-functional ciphertext and in this case $\mathscr{C}$ can simulate Game$_{3,Q}^L$. Otherwise, if T is a random element from $\mathbb{G}_T$ then $\mathscr{C}$ can simulate Game$_4$. If the adversary can distinguish Game$_4$ and Game$_{3,Q}^L$ with non-negligible advantage ϵ, then we can break the BSDP assumption with the same advantage. □

6 Performance and Discussion

6.1 Master Key Leakage Tolerance

In our construction, we design the same key structure of master key $\mathtt{MSK}$ and user private key $\mathtt{SK}_{\mathbb{S}}$. Actually, the master key $\mathtt{MSK}$ can be considered as a special key of universal attribute set Σ. Implicitly, we can call KeyUpd algorithm to update and refresh the master key that takes the master key $\mathtt{MSK}$ and attribute set Σ as inputs. As we only re-randomize the randomness in the master key, the refreshed master key does not impact on the previous user key generated by it.

6.2 Leakage-resilient Key-policy ABE

In this section, we give the construction of key-policy attribute-based encryption with leakage resilience ($\mathsf{LR\text{-}KP\text{-}ABE}$), which uses the same technique in section 4, i.e., using the set of minimal sets to describe the monotone access structure. In key-policy ABE, a key is associated with access structure and a ciphertext is associated with a set of attributes. The construction has the similar security proof method with $\mathsf{LR\text{-}CP\text{-}ABE}$.

$\mathsf{LR\text{-}KP\text{-}ABE.Setup}$ $(1^\kappa, \Sigma, \ell)$ Like in section 4, this algorithm generates the description of composite-order bilinear group Θ, and selects randomness and then sets the master key and the master public key as:

$$\mathtt{MPK} = \langle \Theta, g_1, g_3, g_1^a, g_1^{\vec{\rho}}, Y, (T_i)_{i\in\Sigma} \rangle \tag{19}$$

$$\begin{aligned}\mathtt{MSK} &= \langle \vec{w}_1, w_2, \vec{w}_3, \vec{w}_4 \rangle \\ &= \langle g_1^\sigma g_3^{\vec{y}_1}, g_1^{-t} g_3^{y_2}, (g_1^{\alpha+at+\langle\vec{\rho},\vec{\sigma}\rangle}(\prod_{j=[|\Sigma|]} T_j)^{t_i} g_3^{y_{3,i}})_{i\in[|\Sigma|]}, (g_1^{t_i} g_3^{y_{4,i}})_{i\in[|\Sigma|]} \rangle \end{aligned} \tag{20}$$

$\mathsf{LR\text{-}KP\text{-}ABE.KeyGen}$ $(\mathtt{MSK}, \Gamma)$ Let $\mathtt{MSK} = \langle \vec{w}_1, w_2, \vec{w}_3, \vec{w}_4 \rangle$. This algorithm first converts the monotone access structure Γ to the set of minimal sets $\mathcal{B} = \{B_1, B_2, \cdots, B_m\}$, where $B_i \subset \Sigma$ for $i = 1, \cdots, m$, and then generates the private key $\mathtt{SK}_\Gamma$ as

$$\begin{aligned}\mathtt{SK}_\Gamma &= \langle \mathcal{B}, \vec{k}_1, k_2, \vec{k}_3, \vec{k}_4 \rangle \\ &= \langle \mathcal{B}, \vec{w}_1 * g_1^{\triangle\sigma} * g_3^{\triangle\vec{y}_1}, \\ &\quad w_2 * g_1^{-\triangle t} * g_3^{\triangle y_2}, \\ &\quad (w_{3,i} * g_1^{a\triangle t+\langle\vec{\rho},\triangle\vec{\sigma}\rangle}(\prod_{j\in B_i} T_j)^{\triangle t_i} * g_3^{\triangle y_{3,i}})_{i\in[m]}, \\ &\quad (w_{4,i} * g_1^{\triangle t_i} * g_3^{\triangle y_{4,i}})_{i\in[m]} \rangle \\ &= \begin{pmatrix} \mathcal{B}, g_1^{\sigma+\triangle\sigma} g_3^{\vec{y}_1+\triangle\vec{y}_1}, \\ g_1^{-t-\triangle t} * g_3^{y_2+\triangle y_2}, \\ (g_1^{\alpha+a(t+\triangle t)+\langle\vec{\rho},\vec{\sigma}+\triangle\vec{\sigma}\rangle}(\prod_{j\in B_i} T_j)^{t_i+\triangle t_i} * g_3^{y_{3,i}+\triangle y_{3,i}})_{i\in[m]} \\ (g_1^{t_i+\triangle t_i} g_3^{y_{4,i}+\triangle t_{4,i}})_{i\in[m]} \end{pmatrix}^\top \end{aligned} \tag{21}$$

where $\triangle t, \triangle\vec{\sigma}, \triangle t_i, \triangle\vec{y}_1, \cdots, \triangle\vec{y}_4$ are picked from $\mathbb{Z}_N$ randomly.

Table 2: Performance

schemes	LRW11 [LRW11]	LR-CP-ABE	LR-KP-ABE
Encrypt	$2(\omega+2n_1)Mu$	$(\omega+2m)Mu$	$(\omega+\lvert\mathbb{S}\rvert+2)Mu$
Decrypt	$(\omega+2n_1+1)Pr+1Ex$	$(\omega+3)Pr$	$(\omega+3)Pr$
KeyUpdate	$2(\omega+\lvert\mathbb{S}\rvert+2)Mu$	$2(\omega+\lvert\mathbb{S}\rvert+2)Mu$	$2(\omega+2m+1)Mu$
# of $\mathtt{MSK}$	$(\omega+\lvert\Sigma\rvert+2)\lvert\mathbb{G}\rvert$	$(\omega+\lvert\Sigma\rvert+2)\lvert\mathbb{G}\rvert$	$(\omega+2\lvert\Sigma\rvert+1)\lvert\mathbb{G}\rvert$
# of $\mathtt{SK}_{\mathbb{S}}$	$(\omega+\lvert\mathbb{S}\rvert+2)\lvert\mathbb{G}\rvert$	$(\omega+\lvert\mathbb{S}\rvert+2)\lvert\mathbb{G}\rvert$	$(\omega+2m+1)\lvert\mathbb{G}\rvert$
# of $\mathtt{CT}_{\Gamma}$	$(\omega+2n_1+1)\lvert\mathbb{G}\rvert+\lvert\mathbb{G}_T\rvert$	$(\omega+2m+1)\lvert\mathbb{G}\rvert+\lvert\mathbb{G}_T\rvert$	$(\omega+\lvert\mathbb{S}\rvert+2)\lvert\mathbb{G}\rvert+\lvert\mathbb{G}_T\rvert$
Master key leakage	$\surd$	$\surd$	$\surd$
User key leakage	$\surd$	$\surd$	$\surd$
Continual leakage	$\surd$	$\surd$	$\surd$
Multi-show attr	X	$\surd$	$\surd$
Leakage bound ℓ	$2+(\omega-1-2\tau)\log p_2$	$2+(\omega-1-2\tau)\log p_2$	$2+(\omega-1-2\tau)\log p_2$
Allowable probability	$p_2^{-\tau}$	$p_2^{-\tau}$	$p_2^{-\tau}$
Leakage rate γ	$\frac{\omega-1-2\tau}{(1+\beta_1+\beta_3)(\omega+2+\lvert\mathbb{S}\rvert)}$	$\frac{\omega-1-2\tau}{(1+\beta_1+\beta_3)(\omega+2+\lvert\mathbb{S}\rvert)}$	$\frac{\omega-1-2\tau}{(1+\beta_1+\beta_3)(\omega+2m+1)}$

ω: leakage parameter; τ: allowable leakage probability parameter; ℓ: leakage bound of a key; γ: leakage rate, i.e., $\gamma=\ell/|\mathtt{SK}|$; Pr: computation cost of pairing; Ex: exponent cost in $\mathbb{G}_T$; Mu: point multiplication; $|\mathbb{G}|$: size of an element in $\mathbb{G}$; $|\mathbb{G}_T|$: size of an element in $\mathbb{G}_T$; Σ: universal attribute set; $\mathbb{S}$: attribute set; $\mathcal{I}$: minimum #rows labeled by user's attributes to compute target vector in LSSS matrix with n_1 rows and n_2 columns; β_1,β_3: value of $|\mathbb{G}_{p_1}|/|\mathbb{G}|$ and $|\mathbb{G}_{p_3}/|\mathbb{G}|$;

LR-KP-ABE.KeyUpd$(\mathtt{SK}_{\Gamma},\Gamma)$ This algorithm at random selects $\triangle\vec{\sigma},\triangle t,\triangle y_1,\triangle y_2,\triangle y_3,\triangle y_4$ from Z_N, and performs the refresh procedure like in LR-KP-ABE.$\mathsf{KeyGen}(\mathtt{MSK},\Gamma)$.

LR-KP-ABE.Enc$(M,\mathbb{S})$ Output the ciphertext for attribute set $\mathbb{S}$ as

$$\mathtt{CT}_{\mathbb{S}}=\langle\mathbb{S},c_0,\vec{c}_1,c_2,c_3,\vec{c}_4\rangle=\langle\mathbb{S},\ MY^s,\ g_1^{s\vec{\rho}},\ g_1^{as},\ g_1^s,\ \forall i\in\mathbb{S}\ \ T_i^s\rangle \tag{22}$$

where s is picked from $\mathbb{Z}_N$ randomly.

LR-KP-ABE.Dec$(\mathtt{CT}_{\mathbb{S}},\mathtt{SK}_{\Gamma})$ If $\mathbb{S}$ satisfies Γ specified by $\mathcal{B}$, then $\mathbb{S}$ must be a superset of a minimal set in $\mathcal{B}$. Find $S_k\subset\mathbb{S}$ for some $k\in[m]$, and calculate:

$$M\leftarrow c_0\frac{\hat{e}_{\omega}(c_1,k_1)\hat{e}(c_{4,k},\prod_{i\in B_k}k_{4,i})}{\hat{e}(c_2,k_2)\hat{e}(c_{3,k},k_3)} \tag{23}$$

6.3 Leakage Performance

In this section, we give the performance analysis and comparison between [LRW11] and ours schemes, which are listed in Tab. 2.

[LRW11] and our LR-CP-ABE are all ciphertext-policy attribute-based encryption schemes in the presence of key leakage model. [LRW11] uses LSSS to denote the access structure, but it does not support attribute multi-show functionality [LW12]. Our schemes use the minimal set to denote the access structure and support attribute multi-show ability.

We evaluate the computation cost in decryption since it mainly depends on the bilinear pairing operation in this algorithm but the pairing operation is very time-consuming compared to the other operations such as point multiplication, exponent and so on. To express an access structure, row number n_1 in LSSS has the approximate size with the number of set m in minimal set method. However, as far as the decryption in our two schemes, they need constant $\omega + 3$ pairing operation which is independent to the scale of access structure Γ and are more efficient than [LRW11] that describes the access structure as LSSS.

On the side of leakage resilience, all schemes support master key leakage, user private key leakage and continual leakage. Also, the schemes have the same leakage bound $\ell = 2 + (\omega - 1 - 2\tau) \log p_2$ and allowable probability $p = p_2^{-\tau}$. Thus, the leakage rate of our LR-CP-ABE and [LRW11] are

$$\gamma = \frac{\omega - 1 - 2\tau}{(1 + \beta_1 + \beta_3)(\omega + 2 + |\mathbb{S}|)} \tag{24}$$

The leakage rate of LR-KP-ABE is

$$\frac{\omega - 1 - 2\tau}{(1 + \beta_1 + \beta_3)(\omega + 2m + 1)} \tag{25}$$

Obviously, higher values of ω give a better leakage rate, but leads to larger public parameters, private keys, and ciphertexts. Smaller values of β_1 and β_3 provide a better leakage rate, but also give fewer bits of security in subgroup $\mathbb{G}_{p_1}$ and $\mathbb{G}_{p_3}$. We must choose the security parameter κ so that $\beta_1\kappa$ and $\beta_3\kappa$ are sufficiently large.

In the setup algorithm, we set

$$\omega = \lceil 1 + 2\tau + \frac{\ell}{\log p_2} \rceil \tag{26}$$

In particular, if $\omega = 1$ then $\ell = 0$ and $\tau = 0$. In this case, the scheme is simplified to be a fully secure non-leakage attribute-based encryption like in [LW12], which is straightforward to see that allowable leakage is zero.

7 Conclusions

We proposed two leakage-resilient attribute-based encryptions that can tolerate leakage on the master key, as well as leakage on several keys for each attribute set. We explicitly employ a update algorithm to periodically update the master/private key so that it tolerates continual (master) key leakage. In our schemes, the access structures are converted as the minimal set, which can provide fast decryption ability. We can give our construction in prime order groups by using the transformation mechanism from [Lew12] and [Fre10].

References

[AGV09] Akavia A, Goldwasser S and Vaikuntanathan V. *"Simultaneous hardcore bits and cryptography against memory attacks"*. TCC'09, LNCS 5444, pp. 474–495, Berlin: Springer-Verlag, 2009.

[ADN10] Alwen J, Dodis Y, Naor M. *"Public-key encryption in the bounded-retrieval model"*. EUROCRYPT'10, LNCS 6110, pp. 113–134, Berlin: Springer-Verlag, 2010.

[ADW09] Alwen J, Dodis Y, Wichs D. *"Leakage-resilient public-key in the bounded-retrieval model"*. CRYPTO'09, LNCS 5677, pp. 36–54, Berlin: Springer-Verlag, 2009.

[BGP97] Beimel A, Gal A, Paterson M. *"Lower bounds for monotone span programs"*. Computational Complexity, vol.6, no.1, pp. 29–45, 1997.

[BFO08] Boldyreva A, Fehr S, and O'Neill A. *"On notions of security for deterministic encryption, and efficient constructions without random oracles"*. CRYPTO'08, pp. 335–359, Berlin: Springer-Verlag, 2008.

[BSW06] Boneh D, Sahai A, Waters B. *"Fully collusion resistant traitor tracing with short ciphertexts and private keys"*. EUROCRYPT'06, pp. 573–592, Berlin: Springer-Verlag, 2006.

[Boy13] Boyen X. *"Attribute-based functional encryption on lattices."* TCC'13, LNCS 7785, pp. 122–142, Berlin: Springer-Verlag, 2013.

[BG10] Brakerski Z and Goldwasser S. *"Circular and leakage resilient public-Key encryption under subgroup indistinguishability"*. CRYPTO'10, LNCS 6223, pp. 1–20, Berlin: Springer-Verlag, 2010.

[BKKV10] Brakerski Z, Kalai Y T, Katz J, and Vaikuntanathan V. *"Overcoming the hole in the bucket: Publickey cryptography resilient to continual memory leakage"*. FOCS'10, pp. 501–510, 2010.

[CDR10] Chow S, Dodis Y, Rouselakis Y, Waters B. *"Practical leakage-resilient identity-based encryption from simple assumptions"*. ACM-CCS'10, pp.152–161, 2010.

[DHLW10] Dodis Y, Haralambiev K, López-Alt K and Wichs D. *"Efficient public-key cryptography in the presence of key leakage"*. ASIACRYPT'10, pp. 613–631, Berlin: Springer-Verlag, 2010.

[DKL09] Dodis Y, Kalai Y, and Lovett S. *"On cryptography with auxiliary input"*. STOC'09, pp. 621–630, 2009.

[DLWW11] Dodis Y, Lewko A, Waters B, Wichs D. *"Storing secrets on continually leaky devices"*. FOCS'11, pp. 688–697, 2011.

[Fre10] Freeman D M. *"Converting pairing-based cryptosystems from composite-order groups to prime-order groups."* EUROCRYPT'10, LNCS, pp. 44–61, 2010.

[GJPS08] Goyal V, Jain A, Pandey O, and Sahai A. "Bounded ciphertext policy attribute-based encryption". Proceedings of the 35th international colloquium on Automata, Languages and Programming (ICALP'08), 579—591, Berlin: Springer-Verlag, 2008.

[GPSW06] Goyal V, Pandey O, Sahai A, and Waters B. *"Attribute-based encryption for fine-grained access control of encrypted data"*. ACM-CCS'06, pp. 89-98, 2006.

[HW13] Hohenberger S and Waters B. *"Atribute-based encryption with fast decryption"*. PKC'13, LNCS 7778, pp. 162-179, 2013.

[KSW08] Katz J, Sahai A, and Waters B. *"Predicate encryption supporting disjunction, polynomial equations, and inner products"*. EUROCRYPT'08, LNCS 4956, pp. 146-162, Berlin: Springer-Verlag, 2008.

[Lew12] Lewko A. *"Tools for simulating features of composite order bilinear groups in the prime order setting"*. EUROCRYPT'12, pp. 318-335, Berlin: Springer-Verlag, 2012.

[LW12] Lewko A, Waters B. *"New proof methods for attribute-based encryption: achieving full security through selective techniques"*. CRYPTO'12, pp. 180-198, Berlin: Springer-Verlag, 2012.

[LOS+10] Lewko A, Okamoto T, Sahai A, Takashima T, and Waters B. *"Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption"*. EUROCRYPT'10, LNCS 6110, pp. 62-91, Berlin: Springer-Verlag, 2010.

[LRW11] Lewko A, Rouselakis Y and Waters B. *"Achieving leakage resilience through dual system encryption"*. TCC'11, LNCS 6597, pp. 70-88, Berlin: Springer-Verlag, 2011.

[LW10] Lewko A and Waters B. *"New techniques for dual system encryption and fully secure hibe with short ciphertexts"*. TCC'10, LNCS 5978, 2010, pp. 455-479, Berlin: Springer-Verlag, 2010.

[LY13] Libert B and Yung M. *" Adaptively secure non-interactive threshold cryptosystems"*. Theoretical Computer Science, doi:10.1016/j.tcs.2013.01.001, 2013.

[NS09] Naor M, Segev G. *"Public-key cryptosystems resilient to key leakage"*. CRYPTO'09, LNCS 5677, pp. 18-35, Berlin: Springer-Verlag, 2009.

[NNP05] Nikov V, Nikova S, Preneel B. *"On the size of monotone span programs"*. SCN'04, LNCS 3352, pp. 249-262, Berlin: Springer-Verlag, 2005.

[PB12] Pandit T and Barua R. *"Efficient fully secre attribute-based encryption schemes for general access structures"*. ProvSec'12, LNCS 7496, pp. 193-214, Berlin: Springer-Verlag, 2012.

[SW05] Sahai A and Waters B. *"Fuzzy identity based encryption"*. EUROCRYPT'05, LNCS 3494, pp. 457-473, Berlin: Springer-Verlag, 2005.

[SSW09] Shen E, Shi E and Waters B. *"Predicate privacy in encryption systems"*. TCC'09, LNCS 5444, pp.457-473, Berlin: Springer-Verlag, 2009.

[Wat09] Waters B. *"Dual system encryption: realizing fully secure ibe and hibe under simple assumptions"*. CRYPTO'09, LNCS 5677, pp. 619-636, Berlin: Springer-Verlag, 2009.

[Wat11] Waters B. *"Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization."* PKC'11, LNCS 6571, pp. 53-70, Berlin: Springer-Verlag, 2011.

[YZ12] Yang B and Zhang M. *"LR-UESDE: A continual-leakage resilient encryption with unbounded extensible set delegation"*, ProvSec'12, LNCS 7496, pp.125-142, Berlin: Springer-Verlag, 2012.

[YCZY12] Yuen TH, Chow SSM, Zhang Y and Yiu SM. *"Identity-based encryption resilient to continual auxiliary leakage"*. EUROCRYPT'12, LNCS 7237, pp. 117-134, Berlin: Springer-Verlag, 2012.

[ZYT12] Zhang M, Yang B, Takagi T. *"Bounded leakage-resilient funtional encryption with hidden vector predicate"*. The Computer Journal, Oxford, 56(4): 464–477,2013.