2020

Improving the Leakage Rate of Ciphertext-Policy Attribute-Based Encryption for Cloud Computing

Leyou Zhang

Xiaoxu Gao

Fuchun Guo
University of Wollongong, fuchun@uow.edu.au

Gongcheng Hu

Recommended Citation

Zhang, Leyou; Gao, Xiaoxu; Guo, Fuchun; and Hu, Gongcheng, "Improving the Leakage Rate of Ciphertext-Policy Attribute-Based Encryption for Cloud Computing" (2020). *Faculty of Engineering and Information Sciences - Papers: Part B*. 4135.
https://ro.uow.edu.au/eispapers1/4135

Improving the Leakage Rate of Ciphertext-Policy Attribute-Based Encryption for Cloud Computing

Abstract

© 2013 IEEE. A Leakage-Resilient Ciphertext-Policy Attribute-based Encryption (LR-CP-ABE) not only supports the fine-grained access control to encrypted data but also guarantees the security of the data under the side-channel attacks. However, the leakage rate in the existing schemes is low or related to the number of attributes. It will make these schemes suffer from continual attacks. In addition, all of them almost not consider the leakage of the users' privacy and rely on the composite order groups which will threaten the privacy security of the users and depress the users in practice. In this paper, we aim at solving the above problems and propose a scheme with the improving leakage rate in the prime order group. In the proposed scheme, an extension of the lattice-based trapdoor is used to make it achieve the maximum leakage rate 1-o(1). Moreover, it achieves the anonymity which can protect the privacy of the receivers. The proposed scheme can be reduced to the standard assumption-Decision Linear (DLIN) assumption in the selective security model and resist the Chosen Plaintext Attacks (CPA security). At last, the performance comparisons are given to confirm the efficiency and security of the proposed scheme.

Disciplines

Engineering | Science and Technology Studies

Publication Details

Zhang, L., Gao, X., Guo, F. & Hu, G. (2020). Improving the Leakage Rate of Ciphertext-Policy Attribute-Based Encryption for Cloud Computing. IEEE Access, 8 94033-94042.

IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received May 5, 2020, accepted May 12, 2020, date of publication May 19, 2020, date of current version June 2, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2995480

Improving the Leakage Rate of Ciphertext-Policy Attribute-Based Encryption for Cloud Computing

LEYOU ZHANG[1], XIAOXU GAO[1], FUCHUN GUO[2], AND GONGCHENG HU[1]
[1]School of Mathematics and Statistics, Xidian University, Xi'an 710126, China
[2]Centre for Computer and Information Security Research, University of Wollongong, Wollongong, NSW 2522, Australia

Corresponding authors: Leyou Zhang (lyzhang@mail.xidian.edu.cn) and Xiaoxu Gao (gxx_xidian@126.com)

This work was part supported in part by the National Cryptography Development Fund under Grant MMJJ20180209, in part by the International S&T Cooperation Program of Shaanxi Province under Grant 2019KW-056, and in part by the Key Foundation of National Natural Science Foundation of China under Grant U19B2021.

ABSTRACT A Leakage-Resilient Ciphertext-Policy Attribute-based Encryption (LR-CP-ABE) not only supports the fine-grained access control to encrypted data but also guarantees the security of the data under the side-channel attacks. However, the leakage rate in the existing schemes is low or related to the number of attributes. It will make these schemes suffer from continual attacks. In addition, all of them almost not consider the leakage of the users' privacy and rely on the composite order groups which will threaten the privacy security of the users and depress the users in practice. In this paper, we aim at solving the above problems and propose a scheme with the improving leakage rate in the prime order group. In the proposed scheme, an extension of the lattice-based trapdoor is used to make it achieve the maximum leakage rate $1 - o(1)$. Moreover, it achieves the anonymity which can protect the privacy of the receivers. The proposed scheme can be reduced to the standard assumption-Decision Linear (DLIN) assumption in the selective security model and resist the Chosen Plaintext Attacks (CPA security). At last, the performance comparisons are given to confirm the efficiency and security of the proposed scheme.

INDEX TERMS Leakage rate, anonymity, ciphertext-policy ABE, the maximum leakage rate, CPA security.

I. INTRODUCTION

Cloud computing [1]–[4] is favored by users and enterprises for its high speed, flexibility, low investment and reliable service. However, its dynamics and openness also lead to security problems, such as data security and privacy protection. Data leakage incidents have occurred frequently in recent years. For example, on March 18, 2018, it was revealed that during the 2016 presidential election, a company called Cambridge's Analytica illegally used the personal data of 50 million users obtained from Facebook to create archives. Later, Facebook found that up to 87 million people's information had been improperly shared by the company. And on May 20, 2019, TechCrunch reported that a database of Facebook's photo-sharing website called Instagram was leaked on the Internet, which contained private information such as phone numbers and email addresses of nearly 50 million users, including some stars and internet celebrities. Such leakage incidents are fatal.

In dealing with the data leakage and privacy information leakage of the users, public key cryptography technique has occupied a decisive position in the information security system. However, the general constructions from the Public Key Infrastructure (PKI) and an Identity-based Encryption (IBE) [5] are often not realistic or secure in practice. One of the reasons is their one-to-one design principle. And the more complex system which was called Attribute-based Encryption (ABE) [6] came into being in 2005 as a one-to-many encryption mechanism. It not only ensures data security but also supports expressive access control policies because attributes acts as public keys and associate them with ciphertexts and users secret keys. An ABE has mainly been classified into two categories: Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE) [7]. The other comes from the side-channel attacks, where the adversaries can obtain the limited additional information about secret keys and other internal states. These leakage information may make the existing works be easily broken. Naturally, the Leakage-Resilient Encryption mechanism was introduced, which ensured the security of scheme under the key leakage attacks. To describe

The associate editor coordinating the review of this manuscript and approving it for publication was Petros Nicopolitidis.

TABLE 1. Definitions of leakage models.

Leakage Model	Definition
OCL model	A model that the leakage occurs only in the memory part processing the calculations
BML model	A model that the amount of leakage bits is bounded by a value set in advance
BRL model	A model that the leakage parameter is independent of the system and can be arbitrarily increased without affecting the size of the public key
CML model	A model that the amount of leakage bits is bounded between two consecutive updates while unbounded in the liftstyle of the system
AI model	A model that the leakage function is one-way and irreversible
CAI model	A combination model of CMLM and AIM

[1] OCL: Only Computation Leakage. BML: Bounded Memory Leakage. BRL: Bounded Retrieval Leakage. CML: Continual Memory Leakage. AI: Auxiliary Input. CAI: Continual Auxiliary Input.

the amount of leakage bits that the adversaries can know under these attacks, various leakage models are designed, such as Only Computation Leakage (OCL) model, the Continuous Memory Leakage (CML) model and so on. The concrete information of the various models are shown in Table 1. Now the Leakage-Resilient (LR) cryptosystem especially the LR-ABE has become a research hotspot.

LR-ABE schemes give stronger security guarantees to the sharing data than general constructions, but most of them rarely pay attention to protecting the privacy of recipients from access policies. After an encryptor uploads the specified access policy to the cloud platform along with the encrypted data, the adversaries can obtain the attribute information contained in the access policy directly or through DDH test, thus obtaining the sensitive information of the receivers, which really poses a great threat to the privacy of the users. For the purpose of better protecting users' privacy and data security, the concept of Anonymous ABE (ANON-ABE) was introduced in [8], [9]. In ANON-ABE, the adversaries cannot grasp the meaningful information of the corresponding attributes embedded in an access policy through testing and other means.

A. RELATED WORKS

1) LEAKAGE-RESILIENT CRYPTOGRAPHY

Akavia *et al.* [10] firstly presented the BML model and defined an attack model called ''memory attack'' that solved the problem of [11], where they considered the amount of leaked bits that the trapdoor one-way function outputted. Subsequently, Naor and Segev [12] constructed a Leakage-Resilient Public Key Encryption (LR-PKE) scheme by utilizing Hash Proof System (HPS) that was not related to other complexity assumptions and was as efficient as the underlying scheme. They also built two complementary schemes based on Decisional Diffie-Hellman (DDH) and K-Linear assumptions whose leakage bits could be approach the bit length of private keys. Moreover, they constructed two LR-PKE schemes which came from Cramer-Shoup cryptosystem [13]. The corresponding leakage rates are $1/4$ and $1/6$ respectively.

In [14], Alwen *et al.* showed the details of LR-PKE/IBE schemes under the Bounded Retrieval Leakage (BRL) model. Additionally, a novel concept of IB-HPS was proposed. Then, they showed that a LR-IBE scheme was derived from their IB-HPS. Afterwards, Chow *et al.* [15] introduced the Leakage-Resilient IBE (LR-IBE) systems under static assumptions in the standard model. Their proposals were derived from applying the hash proof technique to IBE schemes of Boneh-Boyen, Waters and Lewko-Waters. And their three schemes achieves the leakage rate $1/3$, $1/3$ and $1/9$ respectively in the CPA security model. Lewko *et al.* [16] provided IBE, ABE and Hierarchical IBE (HIBE) schemes under the Continual Memory Leakage (CML) model described in [17] and [18]. All of their constructions achieve the leakage-resilience on the master secret keys and private keys simultaneously.

In 2013, a new LR-PKE scheme was put forward by Liu *et al.* [19] to solve the shortcoming of [20] that the leakage parameter λ is linearly correlated with the length of the plaintext l_m. Specifically, the relationship between λ and l_m is described as $\lambda + l_m \leq \log p - \omega(\log \kappa)$, while the number of leakage bits is $\lambda \leq \log p - \omega(\log \kappa)$ in the scheme [19], where κ represents the security parameter and p is a big prime that denotes the order of the fundamental group. Then Zhang *et al.* [21] put forward two schemes which tolerated the continual leakage in the standard model. Both constructions of LR-CP-ABE and LR-KP-ABE schemes achieve fast decryption and the cost of decryption has nothing to do with the depth of the access structures. In 2017, the improved LR-CP-ABE and LR-KP-ABE were introduced by Zhang *et al.* [22] by employing the HPS to ABE which were proved to be adaptively secure. In addition, these two schemes overcome the shortcomings of most of schemes that the leakage rate is not only related to the size of the dependent group, but also depends on the leakage parameter of $\tilde{n}$. To protect the privacy of the receivers, the anonymous LR-ABE was considered in the design process of [23]. The recent works due to Li *et al.* [24], [25] were still not given an ideal leakage rate since the best rate of them was 1/3 when the depth of the hierarchy was 1.

2) ANONYMOUS ABE

Kapadia *et al.* [8] defined an ANON-ABE for the first time which has the following four characteristics: (1) Realize the data sharing between the data owner with multiple recipients through a semi-trusted server, which avoids the connection between the sender and the receiver. (2) Hide the plaintext

TABLE 2. Performance analyses.

ABE schemes	Assumption	Leakage model	Leakage bound	Leakage ratio	Composite order group
[16]	SD	CML	$(\tilde{n}-1-2c)\log p_2$	$\frac{\tilde{n}-1-2c}{\tilde{n}+2+\lvert S\rvert}\cdot\frac{1}{1+c_1+c_3}$	✓
[21]	SD	CML	$(\tilde{n}-1-2c)\log p_2$	$\frac{\tilde{n}-1-2c}{\tilde{n}+2+\lvert S\rvert}\cdot\frac{1}{1+c_1+c_3}$	✓
[22]	SD	BML	$\log p_1$	$\frac{c_1}{(3+\lvert S\rvert)(1+c_1+c_3)}$	✓
[23]	SD	CML	$(\tilde{n}-1-2c)\log p_2$	$\frac{\tilde{n}-1-2c}{\tilde{n}+2+\lvert S\rvert}\cdot\frac{1}{1+c_1+c_3}$	✓
[25]	SD	CML	$(\tilde{n}-1-2c)\log p_2$	$\frac{\hat{n}-2c-1}{3(\tilde{n}+\lvert S\rvert+l+2)}$	✓
Our scheme	DLIN	BML	$(2\tilde{l}-3)\log p-2\zeta$	$1-o(1)$	×

[1] SD: Subgroup decisional.

messages and access policies. (3) Any recipients cannot know the information of the access policies. (4) Support the non-monotonic boolean access policies. Subsequently, Yu *et al*. [9] designed a scheme whose security could be reduced to the Symmetric External Diffie-Hellman (SXDH) assumption, in which the anonymity was achieved by hiding access policy. Then two anonymous schemes were given in [26]. But both schemes are based on inflexible AND gates and only achieved partially hidden. The [27] solved the problem of illegal sharing the keys among users, which could support user accountability by embedding additional information specified by users. However, users must calculate again and again to test whether they are legitimate users specified by the encryptor in these schemes. It will greatly increase the cost of decryption. So Zhang *et al*. [28] proposed a scheme with decryption test in 2013, namely, adding a matching operation with less computation before decryption phase. The [29] proposed an anonymous scheme based on a prime order group. In 2016, the [30] extended the ANON-CP-ABE to the electronic medical record system to protect the users privacy, in which the access structure was more expressive. In 2017, the idea of Hidden Vector Encryption (HVE) was used to detect whether the attribute met the requirements of legal decryption in scheme [31], where the calculation of decryption was performed by the cloud server. Additionally, the obvious difference between this solution and the previous solution was that the list of coefficients $\{\omega_x\}$ was embedded into the ciphertexts without evaluation. The [32] proposed an ANON-CP-ABE scheme that supports fast decryption for Personal Health Record (PHR). The core technology of [29], [30], [32] is to disclose the index of attribute names and the attribute values are embed into access structures, so these schemes only can partially hide the access policies.

B. OUR CONTRIBUTIONS

Following the above trend, we aim to solve the problems of low leakage rate and recipient anonymity in the existing LR-ABE and proposed a LR-CP-ABE scheme. The detail contributions are as follows.

1) *Higher leakage rate*
Technically, the proposed scheme is based on the Bounded Memory Leakage (BML) model (or Relative Leakage model), in which the arbitrary information of the private keys can be obtained and there is a restriction that the total number of leaked bits cannot exceed λ. From the viewpoint of security reduction, we are motivated by the LWE-based IBE [33] and the extensions of it [34], [35]. Select randomly matrices $\boldsymbol{A}_0, \boldsymbol{A}_1 \in_R \mathbb{Z}_p^{2\times\tilde{l}}$ and set masker keys as $msk = \langle \boldsymbol{A}_0, \boldsymbol{A}_1\rangle$. The system public parameters are set as $pp = \langle g^{\boldsymbol{A}_0}, g^{\boldsymbol{A}_1}, \boldsymbol{B}, g^{\boldsymbol{D}}\rangle$ where $\boldsymbol{B} \in_R \mathbb{Z}_p^{\tilde{l}\times\tilde{l}}$ and $\boldsymbol{D} \in_R \mathbb{Z}_p^{2\times 1}$. The *pp* are different from LWE-based constructions. In addition, the private keys and ciphertexts are set as $\boldsymbol{sk}_{v_{i,x_i}} = g^{\boldsymbol{v}_{v_{i,x_i}}}$ and $\boldsymbol{c}_{i'} = g^{\check{\boldsymbol{A}}_{i'}\cdot\boldsymbol{\omega}\cdot\boldsymbol{z}\cdot\boldsymbol{F}(\rho(i'))}$ where $i \in I$ and $v()$ is attributes. These differences make the proposed LR-CP-ABE realize the maximum leakage rate $1-o(1)$ based the DLIN assumption. Table 2 shows some comparisons with others.

2) *Recipient-anonymity*
Anonymous encryption is an effective method to protect the privacy of the recipient. It requires the adversaries cannot obtain the information of the private keys from the ciphertexts under the premise of possessing the public keys. In most LR-ABE schemes, the sensitive information about attributes in access policies can be capture by DDH test when the adversary obtains the ciphertexts, which will lead to the disclosure of the user's privacy. To address this dilemma, we consider the implementation of the anonymity in the proposed scheme.

3) *High efficiency on prime-order groups*
According to the recent articles, a pairing computation on prime-order groups is more fast than that on composite ones, where "a Tate pairing on a 1024-bit composite-order elliptic curve is roughly 50 times slower than the same pairing on a comparable prime-order curve". In addition, the decryption cost in schemes over prime-order groups decreases more than that over composite-order ones. The proposed scheme is based on prime order groups which is more efficient than the available (refer to the Table 5).

C. ORGANIZATION

Arrange the remaining sections according to the following way. The 2^{nd} part describes some preliminaries, such as basic notations, LSSS and DLIN assumption. The definitions

TABLE 3. Meaning of symbols.

Symbol	Meaning	Symbol	Meaning
$\hat{e}$	bilinear map	$\mathbb{G}, \mathbb{G}_T$	cyclic groups
g	a generator of $\mathbb{G}$	p	a large prime number
$\mathcal{A}$	adversary	$\mathcal{C}$	challenger
$\mathcal{B}$	simulator	ϵ	advantage
pp	public parameters	msk	master secret keys
v_{i,x_i}	an attribute value	$sk_{v_{i,x_i}}$	private keys
m	a message	$\Gamma(\check{\boldsymbol{A}}, \rho)$	a access policy
$\lvert\mathbb{A}\rvert$	order of the set $\mathbb{A}$	$\mathbb{Z}_p^{m\times n}$	a matrice of size $m \times n$ over $\mathbb{Z}_p$
$Rk_r(\mathbb{Z}_p^{m\times n})$	a matrice of rank r in $\mathbb{Z}_p^{m\times n}$	$0 < \rho_m < 1$	leakage rate
$g^{\dot{\boldsymbol{A}}} = (g^{\dot{\boldsymbol{A}}[i,j]})$	a matrix over $\mathbb{G}$	$span(\dot{\boldsymbol{A}})$	$[\boldsymbol{z}\dot{\boldsymbol{A}} : \boldsymbol{z} \in \mathbb{Z}_p^{1\times m}]$
$ker(\dot{\boldsymbol{A}})$	$[\boldsymbol{x} \in \mathbb{Z}_p^{n\times 1} : \dot{\boldsymbol{A}} \cdot \boldsymbol{x} = \boldsymbol{0}]$	$U_{\mathbb{Y}}$	uniform distribution on $\mathbb{Y}$
$a \in_R \mathbb{A}$	a select randomly from a set $\mathbb{A}$	Pr	probability
$[l]$	the set $\{1, 2, ..., l\}$	κ	security parameter

and security model of CP-ABE under the BML model are elaborated in the 3rd part. The 4th portion of article provides the specific constructions and security proofs. The detailed analyses are presented in the 5th section. The conclusion is given at last.

II. PRELIMINARIES

A. NOTATIONS

In order to facilitate understanding the specific meaning of symbols, a summary is given in Table 3.

B. LINEAR SECRET SHARING scheme (LSSS)

The specific meaning of linearity in the linear secret sharing scheme Γ composed of attribute sets S is explained as follows:

- *Secret sharing*: $\check{A}$ is matrix whose number of rows and columns are l and n respectively, and this matrix also named sharing-generating matrix. The i'^{th} row of $\check{A}$ is connected with an attribute value $\rho(i')$ for $i' \in [l]$ by a function ρ. Select a random vector $\boldsymbol{\omega} = (s, \omega_2, \ldots, \omega_n)^T \in \mathbb{Z}_p^n$, where s stands for the secret that the data owner wants to share, the l shares of the secret s are expressed as $\check{A}\boldsymbol{\omega}$. $(\check{A}\omega)_{i'} \in \mathbb{Z}_p$ is the share for attribute value $\rho(i')$.
- *Secret reconstruction*: $\mathbb{C} \in \Gamma$ represents any authorization set, I be defined as $I = \{i' : \rho(i') \in \mathbb{C}\} \subset \{1, 2, \ldots, n\}$. In polynomial time, such a collection $\{\mu_{i'}\}_{i' \in I}$ can be solved that satisfies $\sum_{i' \in I} \mu_{i'}\lambda_{i'} = s$ if $\{\lambda_{i'}\}_{i' \in I}$ are indeed valid shares of secret s.

C. DLIN ASSUMPTION

The original decision linear assumption says that given g_1^x and g_2^y, it is difficult to distinguish g^{x+y} from $\mathbb{G}_T$, in which x, $y \in_R \mathbb{Z}_p$ and $g_1, g_2, g \in_R \mathbb{G}$. For our purpose, the assumption described in [34] is converted to given the matrix $g^{\boldsymbol{A}}$ where $\boldsymbol{A} \in \mathbb{Z}_p^{3\times\tilde{l}}$ whose rank is 2 or 3 and the number of columns satisfies the condition $\tilde{l} \geq 3$, it is hard to decide the rank of $\boldsymbol{A}$. That is to say, under the DLIN assumption, the advantage $|Pr[b' = b : \boldsymbol{A_0} \in_R Rk_2(\mathbb{Z}_p^{3\times\tilde{l}}), \boldsymbol{A_1} \in_R Rk_3(\mathbb{Z}_p^{3\times\tilde{l}}), b \in_R \{0, 1\}, b' \leftarrow \mathcal{D}(g, g^{\boldsymbol{A_b}})] - \frac{1}{2}|$ of distinguisher $\mathcal{D}$ is negligible.

Definition 1 (Universal Hash Function): If for any $x \neq x' \in \mathbb{X}$, there is

$$Pr_{h \overset{\$}{\leftarrow} \mathcal{H}_{\tilde{l}}}[h(x) = h(x')] = \frac{1}{|\mathbb{Y}|},$$

where $\mathcal{H}_{\tilde{l}} = \{h : \mathbb{X} \rightarrow \mathbb{Y}\}$ is a family of hash functions, then we say it is universal.

Lemma 1 (Generalized Leftover Hash Lemma [33]): $\mathcal{H}_{\tilde{l}} = \{h : \mathbb{X} \rightarrow \mathbb{Y}\}$ means a family of universal hash functions and $f : \mathbb{X} \rightarrow \mathbb{Z}$ is a family of leakage functions. The statistical distance

$$SD((h, h(\mathbb{T}), f(\mathbb{T})); (h, U_{\mathbb{Y}}, f(\mathbb{T}))) \leq \frac{1}{2}\sqrt{\gamma(\mathbb{T}) \cdot |\mathbb{Y}| \cdot |\mathbb{Z}|},$$

for $\mathbb{T} \in_R \mathbb{X}$, $\gamma(\mathbb{T}) = \max_t Pr[\mathbb{T} = t]$. That is, if the right-side of the inequality is negligible, $h(\mathbb{T})$ is still random even if h and $f(\mathbb{T})$ are given.

Lemma 2 (Leakage-Resilience Random Subspaces [17]): Let $\mathbf{m} \geq \mathbf{l} \geq 4$, p is a large prime, $\boldsymbol{X} \in_R \mathbb{Z}_p^{\mathbf{m}\times\mathbf{l}}$, $\boldsymbol{T} \in_R \mathbb{Z}_p^{\mathbf{l}\times 2}$, $\boldsymbol{Y} \in_R \mathbb{Z}_p^{\mathbf{m}\times 2}$ and $f : \mathbb{Z}_p^{\mathbf{m}\times 2} \rightarrow \mathbb{Z}$. As long as $|\mathbb{Z}| \leq q^{\mathbf{l}-3}\epsilon^2$ is satisfied, then there is

$$SD((\boldsymbol{X}, f(\boldsymbol{X} \cdot \boldsymbol{T}); (\boldsymbol{X}, f(\boldsymbol{Y}))) \leq \epsilon.$$

D. DEFINITIONS AND SECURITY MODEL FOR LR-CP-ABE UNDER THE BML MODEL

A CP-ABE scheme which is resilient to bounded memory leakage attacks uses the four algorithms (**Setup, KeyGen, Encryption, Decryption**) as constituents. A security parameter κ and a description of attribute universe set U are used as inputs in the **Setup** algorithm, the corresponding outputs are system public parameters pp and master secret keys msk. pp is the common input of four algorithms. The **KeyGen** algorithm inputs msk and an attribute value $v_{i,x_i} \in S$ and outputs a secret key $\boldsymbol{sk}_{v_{i,x_i}}$. The **Encryption** algorithm takes a message m, and an access structure $\Gamma(\check{A}, \rho)$ over the universe of attributes as input and the ciphertexts CT as output.

We assume that $(\check{\boldsymbol{A}}, \{I_{i'}\}_{i' \in [l]})$ is implicitly included in CT, where $I_{i'}$ is the attribute name of the $\rho(i')$. In the **Decryption** algorithm, the inputs are ciphertexts CT and the private keys $\boldsymbol{sk}_{v_{i,x_i}}$ for $v_{i,x_i} \in S$, the output is a message m on the understanding that the attribute set S corresponding to the private keys sk_S satisfies the access structure $\Gamma(\check{\boldsymbol{A}}, \rho)$ embedded the ciphertexts CT.

Next, a CP-ABE scheme with LR-IND-sAP-CPA security and a scheme with ANON-LR-IND-sAP-CPA security can be modeled as the following games completed by an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$ interaction respectively. The specific process of games are described as follows:

Definition 2 (LR-IND-sAP-CPA Security): A CP-ABE scheme is LR-IND-sAP-CPA secure with leakage rate ρ_m if there is only a negligible advantage in the following game for $\mathcal{A}$.

- **Initialize**: $\mathcal{A}$ sends the challenge access policy $\Gamma^*(\boldsymbol{A}^*, \rho^*)$ to $\mathcal{C}$. Then (pp, msk) are generated by $\mathcal{C}$ running **Setup**, the pp is sent to $\mathcal{A}$.
- **KeyGen**: $\mathcal{C}$ runs $sk_{v^*_{i,x_i}}$ $\leftarrow$**KeyGen**(msk, v^*_{i,x_i}) for $v^*_{i,x_i} \in \{\rho^*(i')\}_{i' \in [l]}$.
- **Phase 1**: $\mathcal{A}$ adaptively performs the following queries.
  - *KeyGen queries* $v_{i,x_i} \notin \{\rho^*(i')\}_{i' \in [l]}$: $\mathcal{C}$ returns $sk_{v_{i,x_i}}$ =**KeyGen**(msk, v_{i,x_i}) to $\mathcal{A}$.
  - *Leakage queries* $(leak, \check{v}_{i,x_i}, f)$: $\mathcal{C}$ returns $f(sk_{\check{v}_{i,x_i}})$ to $\mathcal{A}$ with the restriction that $|f(sk_{\check{v}_{i,x_i}})| \leq \rho_m$ $|sk_{\check{v}_{i,x_i}}|$, where $\check{v}_{i,x_i} \in \{\rho^*(i')\}_{i' \in [l]}$ maybe hold in this queries, and f is a leakage function family.
- **Challenge**: $\mathcal{A}$ sends two messages m_0, m_1 $(|m_0| = |m_1|)$ to $\mathcal{C}$, then $\mathcal{C}$ sends back CT^*_b $\leftarrow$**Encryption**$(m_b, \Gamma^*$ $(\boldsymbol{A}^*, \rho^*))$ for $b \in_R \{0, 1\}$.
- **Phase 2**: $\mathcal{A}$ asks $\mathcal{C}$ some additional *KeyGen queries* about v_{i,x_i}, where $v_{i,x_i} \notin \{\rho^*(i')\}_{i' \in [l]}$. Then $\mathcal{C}$ answers in the same manner as above.
- **Guess**: $\mathcal{A}$ finally outputs a guess b' about b. If b' and b are equal, $\mathcal{A}$ is successful.

Definition 3 (ANON-LR-IND-sAP-CPA Security): A CP-ABE scheme is ANON-IND-sAP-CPA secure with leakage rate ρ_m if $\mathcal{A}$ has only negligible advantage.

- **Initialize**: $\mathcal{A}$ sends the challenge access policy $\Gamma^*_0(\boldsymbol{A}^*_0, \rho^*_0)$, $\Gamma^*_1(\boldsymbol{A}^*_1, \rho^*_1)$ to $\mathcal{C}$. Then $\mathcal{C}$ generates (pp, msk) through **Setup**, $\mathcal{A}$ gets pp sent by $\mathcal{C}$.
- **KeyGen**: $\mathcal{C}$ runs $sk_{v^*_{i,x_i}}$ $\leftarrow$**KeyGen**(msk, v^*_{i,x_i}) for any $v^*_{i,x_i} \in \{\rho^*_0(i')\}_{i' \in [l]}$ and $v^*_{i,x_i} \in \{\rho^*_1(i')\}_{i' \in [l]}$.
- **Phase 1**: The following queries are performed adaptively by $\mathcal{A}$.
  - *KeyGen queries* $(v_{i,x_i} \notin \{\rho^*_0(i')\}_{i' \in [l]}) \wedge (v_{i,x_i} \notin \{\rho^*_1(i')\}_{i' \in [l]})$: $\mathcal{C}$ returns $sk_{v_{i,x_i}}$ =**KeyGen**(msk, v_{i,x_i}) to $\mathcal{A}$.
  - *Leakage queries* $(leak, \check{v}_{i,x_i}, f)$: $\mathcal{C}$ returns $f(sk_{\check{v}_{i,x_i}})$ to $\mathcal{A}$. It is restrict that $|f(sk_{\check{v}_{i,x_i}})| \leq \rho_m |sk_{\check{v}_{i,x_i}}|$, where $\check{v}_{i,x_i} \in \{\rho^*_0(i')\}_{i' \in [l]}$ or $\check{v}_{i,x_i} \in \{\rho^*_1(i')\}_{i' \in [l]}$ maybe hold in this queries.
- **Challenge**: Two messages m_0, m_1 which has same length selected by $\mathcal{A}$ are transmitted to $\mathcal{C}$, then $\mathcal{C}$ sends back CT^*_b $\leftarrow$**Encryption**$(m_b, \Gamma^*_b(\boldsymbol{A}^*_b, \rho^*_b))$ for $b \in_R \{0, 1\}$.
- **Phase 2**: $\mathcal{A}$ makes additional *KeyGen queries* about v_{i,x_i}, where $(v_{i,x_i} \notin \{\rho^*_0(i')\}_{i' \in [l]}) \wedge (v_{i,x_i} \notin \{\rho^*_1(i')\}$ $\{\rho^*_1(i')\}$. Then $\mathcal{C}$ answers in the same manner as above.
- **Guess**: Eventually, $\mathcal{A}$ outputs his guess b' about b. $\mathcal{A}$ will succeed if $b' = b$.

The advantage of $\mathcal{A}$ in the above two games is defined as $Adv = |Pr[b' = b] - \frac{1}{2}|$.

III. CONCRETE CONSTRUCTIONS

A. LR-CP-ABE WITH LEAKAGE RATE $1 - o(1)$

The LR-CP-ABE consists of four algorithms: Setup, KeyGen, Encryption and Decryption. These algorithms are given as follows.

Algorithm 1 Setup

```
Input: $\kappa$
Output: $pp$ and $msk$
Fix $\tilde{l} \geq 3$
Choose a collision-resistent hash function
    $$H : \{0, 1\}^* \rightarrow \mathbb{Z}_p$$
and define
    $$\boldsymbol{F}(v_{i,j}) = [\boldsymbol{A}_0|\boldsymbol{A}_1 + H(v_{i,j}) \cdot \boldsymbol{A}_0\boldsymbol{B}] \in \mathbb{Z}_p^{2\times 2\tilde{l}}$$
for each attribute value $v_{i,j} \in \{0, 1\}^*$
Keep the system master secret keys
    $$msk = \langle \boldsymbol{A}_0, \boldsymbol{A}_1 \rangle$$
where the matrices $\boldsymbol{A}_0, \boldsymbol{A}_1 \in_R \mathbb{Z}_p^{2\times\tilde{l}}$
Return the system public parameters
    $$pp = \langle g^{\boldsymbol{A}_0}, g^{\boldsymbol{A}_1}, \boldsymbol{B}, g^{\boldsymbol{D}} \rangle$$
where $\boldsymbol{B} \in_R \mathbb{Z}_p^{\tilde{l}\times\tilde{l}}$ and $\boldsymbol{D} \in_R \mathbb{Z}_p^{2\times 1}$
```

Algorithm 2 KeyGen

```
Input: $pp$, $msk$ and $S$
Output: private keys $sk_S$
for $v_{i,x_i} \in S$ do
    Choose a random vector $\boldsymbol{v}_{v_{i,x_i}} \in \mathbb{Z}_p^{2\tilde{l}\times 1}$ such that
        $$\boldsymbol{F}(v_{i,x_i}) \cdot \boldsymbol{v}_{v_{i,x_i}} = \boldsymbol{D} \quad (1)$$
    Compute
        $$\boldsymbol{sk}_{v_{i,x_i}} = g^{\boldsymbol{v}_{v_{i,x_i}}}$$
end for
Return the private keys $sk_S$ as follows
    $$sk_S = \langle \{\boldsymbol{sk}_{v_{i,x_i}}\}_{v_{i,x_i} \in S} \rangle$$
```

Algorithm 3 Encryption

```
**Input:** $pp$, $\Gamma(\check{\boldsymbol{A}}, \rho)$ and $m$
**Output:** the ciphertexts $CT$
Select $\boldsymbol{\omega} = (s, \omega_2, \omega_3, \dots, \omega_n)^T \in \mathbb{Z}_p^n, \boldsymbol{z} \in \mathbb{Z}_p^{1\times 2}$ at random
Compute $e = \hat{e}(g, g)^{s\boldsymbol{z}\cdot\boldsymbol{D}} \cdot m$
**for** $i' \in [l]$ **do**
    Compute
        $$\boldsymbol{c}_{i'} = g^{\check{\boldsymbol{A}}_{i'}\cdot\boldsymbol{\omega}\cdot\boldsymbol{z}\cdot\boldsymbol{F}(\rho(i'))}$$
**end for**
Return the ciphertexts $CT$ of the message $m$
    $$CT = \langle \check{\boldsymbol{A}}, \{I_{i'}\}_{i'\in[l]}, e, \{\boldsymbol{c}_{i'}\}_{i'\in[l]} \rangle$$
```

Algorithm 4 Decryption

```
**Input:** $pp$, $CT$ and $\boldsymbol{sk}_{\rho(i')}$ for $\rho(i') \in S$
**Output:** a symbol " $\perp$" or a message $m$
Compute the constant coefficient list $\{\mu_{i'}\}_{i'\in I}$ that $\sum_{i'\in I} \mu_{i'}\check{\boldsymbol{A}}_{i'} = (1, 0, \dots, 0)$ and the index set $I$
**for** $i' \in I$ **do**
    Compute $k_{i'} = \hat{e}(\boldsymbol{c}_{i'}, \boldsymbol{sk}_{\rho(i')}) = \hat{e}(g, g)^{\check{\boldsymbol{A}}_{i'}\cdot\boldsymbol{\omega}\cdot\boldsymbol{z}\cdot\boldsymbol{D}}$
**end for**
Compute
    $$k = \prod_{i'\in I} k_{i'}^{\mu_{i'}} = \hat{e}(g, g)^{s\boldsymbol{z}\cdot\boldsymbol{D}}$$
Compute $m = e/k$
Return the message $m$ or " $\perp$"
```

1) TRAPDOOR

After receiving the challenge access policy $\Gamma^*(\boldsymbol{A}^*, \rho^*)$, $\mathcal{B}$ generates the matrice $\boldsymbol{A}_1$ instead of as above, suppose that

$$\boldsymbol{A}_1 = \boldsymbol{A}_0\boldsymbol{R}_{v_{i,x_i}^*} - H(v_{i,x_i}^*)\boldsymbol{A}_0\boldsymbol{B},$$

where $v_{i,x_i}^* \in \{\rho^*(i')\}_{i'\in[l]}$, $\boldsymbol{R}_{v_{i,x_i}^*} \in_R \mathbb{Z}_p^{\tilde{l}\times\tilde{l}}$ is the trapdoor used in the security proofs. $\boldsymbol{A_1}$ is also random because $\boldsymbol{R}_{v_{i,x_i}^*}$ is random. Then we can compute $\boldsymbol{sk}_{v_{i,x_i}} = g^{\boldsymbol{v}_{v_{i,x_i}}}$ from pp and $\boldsymbol{R}_{v_{i,x_i}^*}$ for any attribute values $(v_{i,x_i} \neq v_{i,x_i}^*) \wedge (v_{i,x_i} \notin \{\rho^*(i')\}_{i'\in[l]})$ as follows: choose a random matrice $\boldsymbol{w} \in \mathbb{Z}_p^{\tilde{l}\times 1}$ and a random vector $\boldsymbol{y} \in \mathbb{Z}_p^{\tilde{l}\times 1}$ such that

$$(H(v_{i,x_i}) - H(v_{i,x_i}^*))\boldsymbol{A}_0\boldsymbol{B}\boldsymbol{y} = -\boldsymbol{A}_0\boldsymbol{w} + \boldsymbol{D}. \tag{2}$$

Obviously, it is not difficult to calculate $g^{\boldsymbol{y}}$ from $\boldsymbol{B}$, $g^{\boldsymbol{A_0}}$ and $g^{\boldsymbol{D}}$ contained in public parameters pp. We set $\boldsymbol{v}_{v_{i,x_i}} = \begin{bmatrix}\boldsymbol{w} - \boldsymbol{R}_{v_{i,x_i}^*}\boldsymbol{y} & \boldsymbol{y}\end{bmatrix}^T$ and use $g^{\boldsymbol{y}}$ to compute $g^{\boldsymbol{v}_{v_{i,x_i}}}$. This $\boldsymbol{v}_{v_{i,x_i}}$ meets requirements because there are

$$\begin{aligned}
&\boldsymbol{F}(v_{i,x_i})\boldsymbol{v}_{v_{i,x_i}} \\
&= \begin{bmatrix}\boldsymbol{A_0}|\boldsymbol{A_0}\boldsymbol{R}_{v_{i,x_i}^*} + (H(v_{i,x_i}) - H(v_{i,x_i}^*))\boldsymbol{A_0}\boldsymbol{B}\end{bmatrix} \\
&\quad \cdot \begin{bmatrix}\boldsymbol{w} - \boldsymbol{R}_{v_{i,x_i}^*}\boldsymbol{y} \\ \boldsymbol{y}\end{bmatrix} \\
&= \boldsymbol{A_0}(\boldsymbol{w} - \boldsymbol{R}_{v_{i,x_i}^*}\boldsymbol{y}) + (\boldsymbol{A_0}\boldsymbol{R}_{v_{i,x_i}^*} + (H(v_{i,x_i}) - H(v_{i,x_i}^*)) \\
&\quad \boldsymbol{A_0}\boldsymbol{B})\boldsymbol{y} \\
&= \boldsymbol{A_0}\boldsymbol{w} + (H(v_{i,x_i}) - H(v_{i,x_i}^*))\boldsymbol{A_0}\boldsymbol{B}\boldsymbol{y} \\
&= \boldsymbol{D}.
\end{aligned}$$

It can be seen from above that the $\boldsymbol{v}_{v_{i,x_i}}$ is correctly distributed whose dimension is $2\tilde{l} - 2$. Furthermore, the dimension of $\boldsymbol{w}$ is $\tilde{l}$ and the freedom of solution space is $\tilde{l} - 2$ in Eq.(2) since $\boldsymbol{A_0}\boldsymbol{B} \in \mathbb{Z}_p^{2\times\tilde{l}}$. Therefore, the set of above $\boldsymbol{v}_{v_{i,x_i}}$ and the solution space of Eq.(1) are equal in practice since there is $\tilde{l} + (\tilde{l} - 2) = 2\tilde{l} - 2$.

Theorem 1: The scheme is IND-sAP-CPA secure based on the DLIN assumption, which is leakage-resilient with rate $1 - \frac{3}{2\tilde{l}} - \frac{\zeta}{\tilde{l}\log p}$ for ζ-bits. The overhead of private keys and ciphertexts are $2\tilde{l}|S|$ and $2l\tilde{l}$ respectively.

Proof: Let $Game_0$ be the real attack game described in **Definition 3**. However, some conceptual changes have been made to generate the public parameters

$$pp = (g^{\boldsymbol{A_0}}, g^{\boldsymbol{A_1}}, \boldsymbol{B}, g^{\boldsymbol{D}}).$$

Set $\boldsymbol{A}_1$ as follows:

$$\boldsymbol{A_1} = \boldsymbol{A_0}\boldsymbol{R}_{v_{i,x_i}^*} - H(v_{i,x_i}^*)\boldsymbol{A_0}\boldsymbol{B}, \tag{3}$$

in which $\boldsymbol{A_0} \in_R \mathbb{Z}_p^{2\times\tilde{l}}$ and $\boldsymbol{B}, \boldsymbol{R}_{v_{i,x_i}^*} \in_R \mathbb{Z}_p^{\tilde{l}\times\tilde{l}}$. Next, set

$$\boldsymbol{D} = \boldsymbol{F}(\rho^*(i')) \cdot \boldsymbol{v}_{\rho^*(i')} \in \mathbb{Z}_p^{2\times 1},$$

where

$$\boldsymbol{F}(\rho^*(i')) = \begin{bmatrix}\boldsymbol{A_0}|\boldsymbol{A_0}\boldsymbol{R}_{v_{i,x_i}^*} + (H(\rho^*(i')) - H(v_{i,x_i}^*))\boldsymbol{A_0}\boldsymbol{B}\end{bmatrix}.$$

As a result, $\boldsymbol{D}$ is also uniformly distributed, where $\boldsymbol{v}_{\rho^*(i')} \in_R \mathbb{Z}_p^{2\tilde{l}\times 1}$.

$Game_1$ and $Game_0$ are similar except that the ciphertext component $\boldsymbol{c}_{i'}^*$ is randomly chosen. Then we prove the theorem by the following three lemmas.

Lemma 3: $Game_1$ and $Game_0$ are indistinguishable under the DLIN assumption, ignoring leakage queries.

Proof: Suppose the ABE scheme can be broken by an adversary $\mathcal{A}$, then there is a simulator $\mathcal{B}$ who uses $g^{\boldsymbol{A}}$ as input to tell the rank of $\boldsymbol{A} \in \mathbb{Z}_p^{3\times\tilde{l}}$ is 2 or 3. After $\mathcal{A}$ announces the challenge access structure $\Gamma^*(\boldsymbol{A}^*, \rho^*)$, $\mathcal{B}$ sets the public parameters as follows:

$$pp = (g^{\boldsymbol{A_0}}, g^{\boldsymbol{A_1}}, \boldsymbol{B}, g^{\boldsymbol{D}}),$$

where $\boldsymbol{A_0} \in_R \mathbb{Z}_p^{2\times\tilde{l}}$ consists of the first two rows of $\boldsymbol{A}$, $\boldsymbol{B}$ and $\boldsymbol{R}_{v_{i,x_i}^*}$ are randomly selected from $\mathbb{Z}_p^{\tilde{l}\times\tilde{l}}$ and $\boldsymbol{A_1}$ as in (3). It is obvious that $g^{\boldsymbol{A_1}}$ can be computed from $g^{\boldsymbol{A_0}}$. Take note of

$$\begin{aligned}
\boldsymbol{F}(v_{i,x_i}) &= [\boldsymbol{A_0}|\boldsymbol{A_1} + H(v_{i,x_i})\boldsymbol{A_0}\boldsymbol{B}] \\
&= \begin{bmatrix}\boldsymbol{A_0}|\boldsymbol{A_0}\boldsymbol{R}_{v_{i,x_i}^*} + (H(v_{i,x_i}) - H(v_{i,x_i}^*))\boldsymbol{A_0}\boldsymbol{B}\end{bmatrix}.
\end{aligned}$$

In particular, $\boldsymbol{F}(v_{i,x_i}^*) = \begin{bmatrix}\boldsymbol{A_0}|\boldsymbol{A_0}\boldsymbol{R}_{v_{i,x_i}^*}\end{bmatrix}$. $\mathcal{B}$ chooses $\boldsymbol{v}_{v_{i,x_i}^*}$ from $\mathbb{Z}_p^{2\tilde{l}\times 1}$ and sets $\boldsymbol{D}$ as in (3), so that $g^{\boldsymbol{D}}$ can be calculated from

$g^{\boldsymbol{A}_0}$ easily. When $\mathcal{A}$ makes the *KeyGen queries* of v_{i,x_i} that $v_{i,x_i} \notin \{\rho^*(i')\}_{i'\in[l]}$, $\mathcal{B}$ computes and returns $g^{\boldsymbol{v}_{v_{i,x_i}}}$.

In the challenge phase, $\mathcal{A}$ sends two messages m_0, m_1 ($|m_0| = |m_1|$) to $\mathcal{B}$, in response, $\mathcal{B}$ randomly chooses b from $\{0, 1\}$ and sets $\boldsymbol{y}'$ as the third row of $\boldsymbol{A}$, and returns the ciphertexts $CT^* = \langle \boldsymbol{A}^*, \{I_{i'}\}_{i'\in[l]}, \{\boldsymbol{c}^*_{i'}\}_{i'\in[l]}, e^*\rangle$ as follows. To simplify the formula description, the matrice

$$\left[\boldsymbol{y}'|\boldsymbol{y}'\boldsymbol{R}_{v^*_{i,x_i}} + (H(\rho^*(i')) - H(v^*_{i,x_i}))\boldsymbol{y'B}\right]$$

is labeled by $\boldsymbol{C}$, then

$$\begin{aligned} \boldsymbol{c}^*_{i'} &= g^{\boldsymbol{A}^*_{i'}\boldsymbol{\omega C}}, \\ e^* &= m_b \cdot \hat{e}(g, g)^{s\boldsymbol{v}_{\rho^*(i')}\boldsymbol{C}}. \end{aligned}$$

Finally, $\mathcal{A}$ outputs the guess b' of b. If $b' = b$, $\mathcal{B}$ thinks the rank of $\boldsymbol{A}$ is 2. Otherwise, it guesses the rank of $\boldsymbol{A}$ is 3. We can prove that $\mathcal{B}$ simulates the $Game_0$ if $\mathsf{rank}(\boldsymbol{A}) = 2$; $Game_1$ is simulated when the $\mathsf{rank}(\boldsymbol{A}) = 3$.

Suppose that $\mathsf{rank}(\boldsymbol{A}) = 2$, then $\boldsymbol{y'}$ and the first two rows of $\boldsymbol{A}$ are linearly related, that is to say, there exist $\boldsymbol{z}^* \in \mathbb{Z}_p^{1\times 2}$ that makes $\boldsymbol{y'} = \boldsymbol{z}^*\boldsymbol{A}_0$ hold. Therefore

$$\begin{aligned} &\left[\boldsymbol{y}'|\boldsymbol{y}'\boldsymbol{R}_{v^*_{i,x_i}} + (H(\rho^*(i')) - H(v^*_{i,x_i}))\boldsymbol{y'B}\right] \\ &= \left[\boldsymbol{z}^*\boldsymbol{A}_0|\boldsymbol{z}^*\boldsymbol{A}_0\boldsymbol{R}_{v^*_{i,x_i}} + (H(\rho^*(i')) - H(v^*_{i,x_i}))\boldsymbol{z}^*\boldsymbol{A}_0\boldsymbol{B}\right] \\ &= \boldsymbol{z}^*\left[\boldsymbol{A}_0|\boldsymbol{A}_0\boldsymbol{R}_{v^*_{i,x_i}} + (H(\rho^*(i')) - H(v^*_{i,x_i}))\boldsymbol{A}_0\boldsymbol{B}\right] \\ &= \boldsymbol{z}^* \cdot \boldsymbol{F}(\rho(i')), \end{aligned}$$

it shows that $(e^*, \{\boldsymbol{c}^*_{i'}\}_{i'\in[l]})$ are the ciphertext components in $Game_0$.

If $\mathsf{rank}(\boldsymbol{A}) = 3$, $\boldsymbol{y'}$ is a random element in $\mathbb{Z}_p^{1\times\tilde{l}}$, namely, $\boldsymbol{d} = \boldsymbol{y'R}_{v^*_{i,x_i}} + (H(\rho(i')) - H(v_{i,x_i}))\boldsymbol{y'B}$ is also a random element in $\mathbb{Z}_p^{1\times\tilde{l}}$ even given $\boldsymbol{A_0}$, $\boldsymbol{U} = \boldsymbol{A_0R}_{v^*_{i,x_i}} + (H(\rho(i')) - H(v^*_{i,x_i}))\boldsymbol{A}_0\boldsymbol{B}$ and $\boldsymbol{y'}$. It is easy to find that

$$\boldsymbol{A} \cdot (\boldsymbol{R}_{v^*_{i,x_i}} + (H(\rho(i')) - H(v^*_{i,x_i}))\boldsymbol{B}) = \begin{bmatrix} \boldsymbol{U} \\ \boldsymbol{d} \end{bmatrix}.$$

Therefore, the rank of $\boldsymbol{A}$ is full, if $v^*_{i,x_i} \in \{\rho(i')\}_{i'\in[l]}$ is selected for any $\boldsymbol{d}$, there will be a unique $\boldsymbol{R}_{v^*_{i,x_i}}$ which makes the equation true (the probability is negligible). That is to say, $\boldsymbol{d}$ is as random as $\boldsymbol{R}_{v^*_{i,x_i}}$. Same with $\boldsymbol{c}^*_{i'}$. As a result, under the DLIN problem, it is impossible to make a distinction between $Game_0$ and $Game_1$.

Lemma 4: The advantage of $\mathcal{A}$ against the ABE scheme is negligible under the DLIN assumption.

Proof: Let p_i represent the probability $Pr[b' = b]$ of $\mathcal{A}$ in $Game_i$ for $i = 0, 1$, so that $|p_0 - p_1|$ is computationally negligible. Moreover, $|p_1 - \frac{1}{2}| \leq \frac{1}{p^{2\tilde{l}}}$.

First of all, there is $\boldsymbol{c}^*_{i'} = g^{\boldsymbol{A}^*_{i'}\boldsymbol{\omega}\cdot\boldsymbol{c}_{\rho(i')}}$ for some $\boldsymbol{c}_{\rho(i')} \in \mathbb{Z}_p^{1\times 2\tilde{l}}$. Next

$$e^* = \hat{e}(g, g)^{s\boldsymbol{c}_{\rho(i')}\cdot\boldsymbol{v}_{\rho(i')}}m_b$$

Let $\alpha = \boldsymbol{c}_{\rho(i')} \cdot \boldsymbol{v}_{\rho(i')}$ and there is $\boldsymbol{D} = \boldsymbol{F}_{\rho(i')} \cdot \boldsymbol{v}_{\rho(i')}$, then we have

$$\begin{bmatrix} \alpha \\ \boldsymbol{D} \end{bmatrix} = \begin{bmatrix} \boldsymbol{c}_{\rho(i')} \\ \boldsymbol{F}(\rho(i')) \end{bmatrix} \cdot \boldsymbol{v}_{\rho(i')}.$$

In $Game_1$, $\boldsymbol{c}_{\rho(i')}$ is a random element since $\boldsymbol{c}^*_{i'}$ is random, so that $\boldsymbol{c}_{\rho(i')} \in \mathbb{Z}_p^{1\times 2\tilde{l}}$ and the two rows of $\boldsymbol{F}_{\rho(i')}$ are linearly independent with a non-negligible probability $1/p^{2\tilde{l}}$. In other words, α is a random value even provided $\boldsymbol{c}_{\rho(i')}, \boldsymbol{D}$ and $\boldsymbol{F}_{\rho(i')}$ because of $\boldsymbol{v}_{\rho(i')}$ is random. So $e^* = \hat{e}(g, g)^{s\alpha}m_b$ is random and $|p_1 - \frac{1}{2}| \leq \frac{1}{p^{2\tilde{l}}}$. Hence, the advantage of $\mathcal{A}$ attack the ABE scheme successfully

$$|p_0 - \frac{1}{2}| \leq |p_0 - p_1| + |p_1 - \frac{1}{2}| \leq |p_0 - p_1| + \frac{1}{p^{2\tilde{l}}}$$

is negligible under the DLIN assumption.

Lemma 5: The proposed scheme is leakage-resilient.

Proof: Let $f : \mathbb{Z}_p^{2\tilde{l}} \rightarrow \mathbb{Z}$ represent all leakage functions of *Leakage queries* from $\mathcal{A}$, for the set $\mathbb{Z}$. The purpose is to prove the distributions $(\boldsymbol{c}_{\rho(i')}, \boldsymbol{c}_{\rho(i')}\boldsymbol{v}_{\rho(i')}, f(\boldsymbol{v}_{\rho(i')}))$ and $(\boldsymbol{c}_{\rho(i')}, U_{\mathbb{Z}_p}, f(\boldsymbol{v}_{\rho(i')}))$ are statistically indistinguishable, it means that $\alpha = \boldsymbol{c}_{\rho(i')}\boldsymbol{v}_{\rho(i')}$ is indistinguishable with a randomly distributed on the condition that $\boldsymbol{c}_{\rho(i')} = \frac{\log_g \boldsymbol{c}^*_{i'}}{\boldsymbol{A}^*_{i'}\boldsymbol{\omega}}$ and the leakage information $f(\boldsymbol{v}_{\rho(i')})$.

Now reconsider the indiscernibility of the two games with *leakage queries*. Because $\mathcal{B}$ in the DLIN assumption can generate $\boldsymbol{v}_{\rho(i')}$, $Game_0$ and $Game_1$ are still indistinguishable even given $f(\boldsymbol{v}_{\rho(i')})$. Moreover, $\boldsymbol{c}_{\rho(i')}$ in $Game_1$ is random over $\mathbb{Z}_p^{1\times 2\tilde{l}}$. Set $h_{\boldsymbol{c}_{\rho(i')}}(\boldsymbol{r}) = \boldsymbol{c}_{\rho(i')}\boldsymbol{r}$ maps $\boldsymbol{r} \in \mathbb{Z}_p^{2\tilde{l}\times 1}$ to $\mathbb{Z}_p$. The function $h_{\boldsymbol{c}_{\rho(i')}}$ is universal due to $Pr_{\boldsymbol{c}_{\rho(i')}}[h_{\boldsymbol{c}_{\rho(i')}}(\boldsymbol{r}) = h_{\boldsymbol{c}_{\rho(i')}}(\boldsymbol{r'})] = \frac{1}{p}$ for $\boldsymbol{r} \neq \boldsymbol{r'}$. According to the **Lemma 1**, the statistical distance of the above two distributions is at most $\frac{1}{2}\sqrt{\gamma(\boldsymbol{v}_{\rho(i')}) \cdot p \cdot |\mathbb{Z}|}$ where $\gamma(\boldsymbol{v}_{\rho(i')}) = \max_{\boldsymbol{u}\in\mathbb{Z}_p^{2\tilde{l}}} Pr[\boldsymbol{v}_{\rho(i')} = \boldsymbol{u}]$.

2) ANONYMITY OF THE SELECTIVELY SECURE ABE

Theorem 2: The ABE scheme above mentioned is ANON-IND-sAP-CPA secure under the DLIN assumption.

Proof: The proof is similar to **Theorem 1** and its specific description is as follows.

$Game_0$ be the real attack game as given in **Definition 3**, $Game_1$ is identical with $Game_0$ except that $\boldsymbol{c}^*_{i'}$ of the challenge ciphertexts is a random value. The definition of $Game_2$ is as same as that of $Game_1$ besides e^* in the challenge ciphertexts is random. So the challenge ciphertexts of $Game_2$ becomes random under the DLIN assumption, realizing ANON-IND-sAP-CPA security. The concrete proof process will be explained by the next two lemmas.

Lemma 6: $Game_0$ and $Game_1$ are indistinguishable under the DLIN assumption.

Proof: $\mathcal{B}$ is similar to that of **Theorem 1** except that

$$\boldsymbol{A}_1 = \boldsymbol{A}_0\boldsymbol{R}_{v^*_{i,x_i,b}} - H(v^*_{i,x_i,b})\boldsymbol{A}_0\boldsymbol{B}.$$

TABLE 4. Efficiency comparisons.

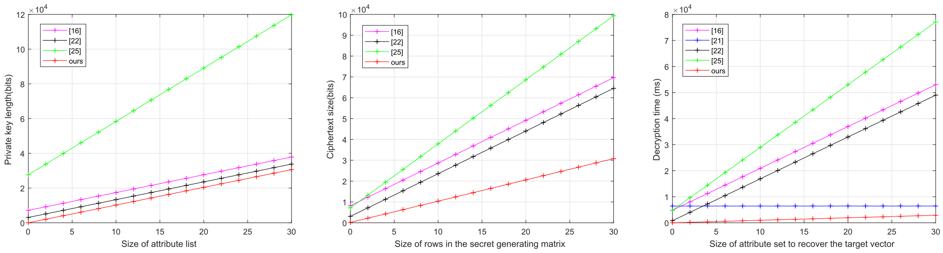
ABE schemes	Private key length	Ciphertext length
[16]	$(\tilde{n}+2+\|S\|)\|\mathbb{G}\|$	$(\tilde{n}+2+2l)\|\mathbb{G}\|+\|\mathbb{G}_T\|$
[21]	$(\tilde{n}+2+\|S\|)\|\mathbb{G}\|$	$(\tilde{n}+1+2\check{m})\|\mathbb{G}\|+\|\mathbb{G}_T\|$
[22]	$(3+\|S\|)\|\mathbb{G}\|$	$(1+2l)\|\mathbb{G}\|+2\|\mathbb{G}_T\|$
[23]	$(\tilde{n}+2+\|S\|)\|\mathbb{G}\|$	$(\tilde{n}+2+2l)\|\mathbb{G}\|+\|\mathbb{G}_T\|$
[24]	$l[2(3\kappa)^{\frac{1}{\varepsilon}}+l(\|S\|-l))]\|\mathbb{G}\|$	$[2(3\kappa)^{\frac{1}{\varepsilon}}+\|S\|]\|\mathbb{G}\|+\|\mathbb{G}_T\|$
[25]	$3(\tilde{n}+\|S\|+l+2)\|\mathbb{G}\|$	$(\tilde{n}+1+3l)\|\mathbb{G}\|+\|\mathbb{G}_T\|$
The proposed scheme	$(2\tilde{l}\|S\|)\|\mathbb{G}\|$	$2l\tilde{l}\|\mathbb{G}\|+\|\mathbb{G}_T\|$

[1] $\|\mathbb{G}\|$: the length of group $\mathbb{G}$. $\|\mathbb{G}_T\|$: the length of group $\mathbb{G}_T$. $|S|$: the number of elements in S. $|I|$: the minimum number of attributes to resconstruct the target vector.

TABLE 5. Efficiency comparsions.

ABE schemes	KeyGen	Encryption	Decryption
[16]	$(3\tilde{n}+4+2\|S\|)Exp$	$(\tilde{n}+2+3l)Exp$	$(2\|I\|+\tilde{n}+1)P$
[21]	$(2\tilde{n}+4+2\|S\|)Exp$	$(\tilde{n}+3+2\check{m})Exp$	$(\tilde{n}+3)P$
[22]	$(4+\|S\|)Exp$	$(3+3l)Exp$	$(2\|I\|+1)P$
[23]	$(3\tilde{n}+4+2\|S\|)Exp$	$(\tilde{n}+2+3l)Exp$	$(2\|I\|+\tilde{n}+1)P$
[24]	$[(2+\|S\|)l+(3\kappa)^{\frac{1}{\varepsilon}}]Exp$	$(2+\|S\|)(3\kappa)^{\frac{1}{\varepsilon}}Exp$	$2(3\kappa)^{\frac{1}{\varepsilon}}P$
[25]	$[3\tilde{n}+5+(2l+3-k)\|S\|]Exp$	$(\tilde{n}+2+3l+kl)Exp$	$(3\|I\|+\tilde{n}+1)P$
The proposed scheme	$(2\tilde{l}\|S\|)Exp$	$(1+2l\tilde{l})Exp$	$(2\tilde{l}\|I\|)P$

[1] Exp : the exponential operation in group. P: the pairing operation in group $\mathbb{G}_T$.



(a) Private key length (b) Ciphertext length (c) Decryption time

FIGURE 1. Evaluation of efficiency.

in which $v^*_{i,x_i,b} \in_R \{\rho^*_b(i')\}_{i'\in[l]}$ and $b \in_R \{0, 1\}$. Correspondingly,

$$\begin{aligned}\boldsymbol{F}(v_{i,x_i}) &= \left[\boldsymbol{A_0}|\boldsymbol{A_1}+H(v_{i,x_i})\boldsymbol{A_0}\boldsymbol{B}\right]\\ &= \left[\boldsymbol{A_0}|\boldsymbol{A_0}\boldsymbol{R}_{v^*_{i,x_i,b}}+(H(v_{i,x_i})-H(v^*_{i,x_i,b}))\boldsymbol{A_0}\boldsymbol{B}\right],\end{aligned}$$

and as before $\boldsymbol{v} \in_R \mathbb{Z}_p^{2\tilde{l}\times 1}$ and

$$\boldsymbol{D} = \left[\boldsymbol{A}_0|\boldsymbol{A}_0(H(v_{i,x_i})-H(v^*_{i,x_i,b}))\boldsymbol{B}\right]\cdot\boldsymbol{v}.$$

For all *KeyGen queries* on v_{i,x_i} such that $(v_{i,x_i} \neq v^*_{i,x_i,b}) \wedge (v_{i,x_i} \notin \{\rho^*_0(i')\}_{i'\in[l]}) \wedge (v_{i,x_i} \notin \{\rho^*_1(i')\}_{i'\in[l]})$ from $\mathcal{A}$, $\mathcal{B}$ answered basing on the following equation

$$(H(v_{i,x_i})-H(v^*_{i,x_i,b}))\boldsymbol{A}_0\boldsymbol{B}\boldsymbol{y} = -\boldsymbol{A}_0\boldsymbol{w}+\boldsymbol{D},$$

where $H(v_{i,x_i})-H(v^*_{i,x_i,b}) \neq 0$. Besides, since

$$\boldsymbol{F}(\rho^*_b(i')) = \left[\boldsymbol{A}_0|\boldsymbol{A}_0\boldsymbol{R}_{v^*_{i,x_i,b}}+(H(v_{\rho^*_b(i')})-H(v^*_{i,x_i,b}))\boldsymbol{A}_0\boldsymbol{B}\right]$$

is unchanged, $\mathcal{B}$ is identical with that of **Theorem 2**. Therefore, it will not be described here.

Lemma 7: Game$_1$ and *Game*$_2$ are information-theoretically indistinguishable.

Proof: From the proof of **Theorem 1**, we can know that $e^* = \hat{e}(g, g)^{\boldsymbol{sc}_{\rho^*_b(i')}\cdot\boldsymbol{v}_{\rho^*_b(i')}}m_b$ is random owing to the randomness of $\boldsymbol{v}_{\rho^*_b(i')}$ and

$$\begin{bmatrix}\alpha\\ \boldsymbol{D}\end{bmatrix} = \begin{bmatrix}\boldsymbol{c}_{\rho^*_b(i')}\\ \boldsymbol{F}(\rho^*_b(i'))\end{bmatrix}\cdot\boldsymbol{v}_{\rho^*_b(i')}.$$

In order to simplify the explanation, let **DEPEND** be express the matrix

$$\begin{bmatrix}\boldsymbol{c}_{\rho^*_b(i')}\\ \boldsymbol{F}(\rho^*_b(i'))\end{bmatrix} \in \mathbb{Z}_p^{3\times 2\tilde{l}}$$

whose rank is 2, this means that there is $\hat{u} \in \mathbb{Z}_p$ such that $\boldsymbol{c}_{\rho_b(i')} = \hat{u}\boldsymbol{F}(\rho_b(i'))_{\tilde{k}}$, where $\boldsymbol{F}(\rho_b(i'))_{\tilde{k}}$ denotes the $\tilde{k}^{th}$ row of $\boldsymbol{F}(\rho^*_b(i'))$. Because of $\boldsymbol{c}_{\rho_b(i')} \in \mathbb{Z}_p^{1\times 2\tilde{l}}$ of *Game*$_1$ and *Game*$_2$ is random,

$$Pr[DEPEND] = Pr[\boldsymbol{c}_{\rho^*_b(i')} = \hat{u}\boldsymbol{F}(\rho^*_b(i'))_{\tilde{k}}] = \frac{1}{p^{2\tilde{l}}}.$$

Lemma 7 can be proved, since *Game*$_1$ and *Game*$_2$ can be distinguishable only when **DEPEND** occurs.

IV. ANALYSES

A. PERFORMANCE ANALYSES

In this section, analyses on efficiency are given in Table 4 and 5.

Let the order of $\mathbb{G}$ and $\mathbb{G}_T$ in scheme [16], [21], [22], [24], [25] be $N = \prod_{\mathrm{i}=1}^{3} p_{\mathrm{i}}$, where p_{i} ($\mathrm{i} \in \{1, 2, 3\}$) is large primes of d_{i} ($d_{\mathrm{i}} = c_{\mathrm{i}}\kappa$) bits. c, c_{i} ($\mathrm{i} = 1, 2, 3$) are any positive constants. $\tilde{n}$ denotes the leakage parameter. ε is a constant satisfied with $0 < \varepsilon < 1$. $\breve{m}$ denotes the number of minimal sets. The number of elements in attribute vectors is represented by k. Comparing our scheme with schemes [16], [21]–[25] in terms of the length of private keys and ciphertexts, the time of key generation, encryption and decryption in Table 4 and 5, one can find that our scheme has advantage in private key length and ciphertext length over the others. In addition, our scheme has lower cost in decryption. From the analyses above mentioned, our scheme is more practical than the rest of the table.

B. EXPERIMENTS ANALYSES

We will analyze the experimental results by using the PBC library. The experiment is on a 64-bits PC with Intel Core i5-6300 CPU(2.4GHz) and 8GB of RAM. To achieve better performance of leakage resilience, we set N in schemes [16], [21], [22], [25] is a number of 1024-bits, the order p of the proposed scheme is a number of 170-bits. To achieve the balance of efficiency and leakage rate, we set $\tilde{n} = 5$ and $\tilde{l} = 3$ respectively. And set $l = 2$ in the simulation of private key length.

V. CONCLUSIONS

As an important encryption primitive, CP-ABE has attracted much attention in the setting of key leakage attacks. However, the leakage rate of most of the existing schemes is low and dependent on the number of attributes. It is a challenge to design a scheme with high leakage rate at present. In this paper, we proposed a scheme with the leakage rate about $1-o(1)$ by using the trapdoor technique. The scheme is based on DLIN assumption in the selective access policy model and achieves anonymity which can protect the privacy of users. In addition, our scheme is built in a group of prime order that more efficient than the construction of composite order. How to design a more efficient scheme is left as the future work.

REFERENCES

[1] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, "Flexible and fine-grained attribute-based data storage in cloud computing," *IEEE Trans. Services Comput.*, vol. 10, no. 5, pp. 785–796, Sep. 2017.

[2] J. Li, N. Chen, and Y. Zhang, "Extended file hierarchy access control scheme with attribute based encryption in cloud computing," *IEEE Trans. Emerg. Topics Comput.*, early access, Mar. 12, 2019, doi: 10.1109/TETC.2019.2904637.

[3] M. Bouchaala, C. Ghazel, L. A. A. Saidane "Toward ciphertext policy attribute based encryption model: A revocable access control solution in cloud computing," in *Proc. CRiSIS*. Berlin, Germany: ResearchGate, Oct. 2020, pp. 193–207.

[4] R. Ahuja, and S K. Mohanty, "A scalable attribute-based access control scheme with flexible delegation cum sharing of access privileges for cloud storage," *IEEE Trans. Cloud Comput.*, vol. 8, no. 1, pp. 32–44, May 2020.

[5] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Adv. Cryptol. (CRYPTO)*, vol. 196. Berlin, Germany: Springer, Aug. 1984, pp. 47–53.

[6] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Adv. Cryptol. (CRYPTO)*, vol. 3494. Berlin, Germany: Springer, May 2005, pp. 457–473.

[7] J. Li, Y. Wang, Y. Zhang, and J. Han, "Full verifiability for outsourced decryption in attribute based encryption," *IEEE Trans. Services Comput.*, early access, May 31, 2017, doi: 10.1109/TSC.2017.2710190.

[8] A. Kapadia, P. Tsang, and S. Smith, "Attribute-based publishing with hidden credentials and hidden policies," in *Proc. NDSS*, 2007, pp. 179–192.

[9] S. Yu, K. Ren, and W. Lou, "Attribute-based content distribution with hidden policy," in *Proc. 4th Workshop Secure Netw. Protocols*, Oct. 2008, pp. 39–44.

[10] A. Akavia, S. Goldwasser, and V. Vaikuntanathan, "Simultaneous hardcore bits and cryptography against memory attacks," in *Proc. TCC*, vol. 5444. Berlin, Germany: Springer, Feb. 2009, pp. 474–495.

[11] J. Halderman, S. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten, "Lest we remember: Cold-boot attacks on encryption keys," in *Proc. SS*, Jul. 2008, pp. 45–60.

[12] M. Naor and G. Segev, "Public-key cryptosystems resilient to key leakage," in *Proc. Adv. Cryptol. (CRYPTO)*, vol. 5677. Berlin, Germany: Springer, Aug. 2009, pp. 18–35.

[13] R. Cramer and V. Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack," in *Proc. Adv. Cryptol. (CRYPTO)*, vol. 1462. Berlin, Germany: Springer, Aug. 1998, pp. 13–25.

[14] J. Alwen, Y. Dodis, M. Naor, G. Segev, and S. Walfish, "Public-key encryption in the bounded-retrieval model," in *Proc. EUROCRYPT*, vol. 6110. Berlin, Germany: Springer, May 2010, pp. 113–134.

[15] S. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, "Practical leakage-resilient identity-based encryption from simple assumptions," in *Proc. CCS*, Oct. 2010, pp. 152–161.

[16] A. Lewko, Y. Rouselakis, and B. Waters, "Achieving leakage resilience through dual system encryption," in *Proc. TCC*, vol. 6597. Berlin, Germany: Springer, Mar. 2011, pp. 70–88.

[17] Z. Brakerski, Y. T. Kalai, J. Katz, and V. Vaikuntanathan, "Overcoming the hole in the bucket: Public-key cryptography resilient to continual memory leakage," in *Proc. IEEE 51st Annu. Symp. Found. Comput. Sci.*, Oct. 2010, pp. 501–510.

[18] Y. Dodis, K. Haralambiev, A. Lopez-Alt, and D. Wichs, "Cryptography against continuous memory attacks," in *Proc. IEEE 51st Annu. Symp. Found. Comput. Sci.*, Oct. 2010, pp. 511–520.

[19] S. Liu, J. Weng, and Y. Zhao, "Efficient public key cryptosystem resilient to key leakage chosen ciphertext attacks," in *Proc. CT-RSA*, vol. 7779. Berlin, Germany: Springer, 2013, pp. 84–100.

[20] M. Naor and M. Yung, "Public-key cryptosystems provably secure against chosen ciphertext attacks," in *Proc. 22nd Annu. ACM Symp. Comput. (STOC)*, May 1990, pp. 427–437.

[21] M. Zhang, W. Shi, C. Wang, Z. Chen, and Y. Mu, "Leakage-resilient attribute-based encryption with fast decryption: Models, analysis and constructions," in *Proc. ISPEC*, vol. 7863. Berlin, Germany: Springer, 2013, pp. 75–90.

[22] L. Zhang, J. Zhang, and Y. Mu, "Novel leakage-resilient attribute-based encryption from hash proof system," *Comput. J.*, vol. 60, no. 4, pp. 541–554, Mar. 2017.

[23] J.-X. Zhang and L.-Y. Zhang, "Anonymous CP-ABE against side-channel attacks in cloud computing," *J. Inf. Sci. Eng.*, vol. 33, no. 3, pp. 789–805, 2017.

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

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

[26] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in *Proc. ACNS*, vol. 5037. Berlin, Germany: Springer, 2008, pp. 111–129.

[27] J. Li, K. Ren, B. Zhu, and Z. Wan, "Privacy-aware attribute-based encryption with user accountability," in *Proc. ISC*, vol. 5735. Berlin, Germany: Springer, 2009, pp. 347–362.

[28] Y. Zhang, X. Chen, J. Li, D. S. Wong, and H. Li, "Anonymous attribute-based encryption supporting efficient decryption test," in *Proc. 8th ACM SIGSAC Symp. Inf., Comput. Commun. Secur. (ASIA CCS)*, May 2013, pp. 511–516.

[29] H. Cui, R. H. Deng, J. Lai, X. Yi, and S. Nepal, "An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures, revisited," *Comput. Netw.*, vol. 133, pp. 157–165, Mar. 2018.

[30] L. Liu, J. Lai, R. H. Deng, and Y. Li, "Ciphertext-policy attribute-based encryption with partially hidden access structure and its application to privacy-preserving electronic medical record system in cloud environment," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 4897–4913, Dec. 2016.

[31] F. Khan, H. Li, L. Zhang, and J. Shen, "An expressive hidden access policy CP-ABE," in *Proc. IEEE 2nd Int. Conf. Data Sci. Cyberspace (DSC)*, Jun. 2017, pp. 474–495.

[32] L. Zhang, G. Hu, Y. Mu, and F. Rezaeibagha, "Hidden ciphertext policy attribute-based encryption with fast decryption for personal health record system," *IEEE Access*, vol. 7, pp. 33202–33213, 2019.

[33] S. Agrawal, D. Boneh, and X. Boyen, "Efficient lattice (H) IBE in the standard model," in *Proc. EUROCRYPT*, vol. 6110. Berlin, Germany: Springer, 2010, pp. 553–572.

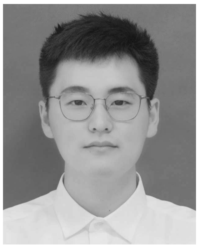
[34] K. Kurosawa and L. T. Phong, "Anonymous and leakage resilient IBE and IPE," *Designs, Codes Cryptogr.*, vol. 85, no. 2, pp. 273–298, Nov. 2017.

[35] D. Boneh, A. Raghunathan, and G. Segev, "Function-private identity-based encryption: Hiding the function in functional encryption," in *Proc. Adv. Cryptol. (CRYPTO)*, vol. 8043. Berlin, Germany: Springer, 2013, pp. 461–478.

LEYOU ZHANG received the M.S. and Ph.D. degrees from Xidian University, in 2002 and 2009, respectively. He is currently a Professor with Xidian University. His current research interests include cryptography, network security, cloud security, and computer security.

XIAOXU GAO received the B.S. degree in mathematics from Taiyuan Normal University, China, in 2017. She is currently pursuing the M.S. degree in applied mathematics with Xidian University, China. Her current interests include applied cryptography and cloud security.

FUCHUN GUO received the B.S. and M.S. degrees from Fujian Normal University, China, in 2005 and 2008, respectively, and the Ph.D. degree from the University of Wollongong, Australia, in 2013. He is currently an Associate Research Fellow with the School of Computing and Information Technology, University of Wollongong. His primary research interests include the public key cryptography, in particular protocols, encryption and signature schemes, and security proof.



GONGCHENG HU received the B.S. degree in mathematics from Xinxiang University, China, in 2017. He is currently pursuing the M.S. degree in applied mathematics with Xidian University, China. His current interests include applied cryptography and cloud security.