lw

作者为 6543212 6543212

提交日期: 2023年07月12日 10:30上午 (UTC-0500)
提交作业代码: 2130139945
文档名称: template.pdf (568.03K)
文字总数: 8630
字符总数: 41743

Efficient Revocable Attribute-based Encryption with Verifiable Data Integrity

IEEE Publication Technology, *Staff, IEEE,*

***Abstract*—Nowadays, cloud computing and cloud storage services that can reduce the local workload are becoming increasingly popular, allowing individual and corporate users to upload data to the cloud. Since the user's permissions in the system are not immutable, the users should have dynamic access. Revocation of users who have been granted access to data is also a strong need for cloud computing systems. In addition, we should ensure the data integrity after the cloud server performs an revocation. To address above issues, we propose a revocable attribute-based encryption scheme that protects the data integrity (RABE-DI). Our scheme is more efficient compared to existing RABE-DI scheme. In addition, we prove the semantic security and integrity of the scheme. Experimental data show that the similar scheme is not as efficient as ours.**

***Index Terms*—attribute-based encryption; full security; decisional linear assumption; data integrity;**

I. Introduction

CLOUD computing and cloud storage services have become increasingly popular among individuals and businesses in recent years because of their economical and efficient features. People store their huge data in the cloud or outsource cumbersome computing programs to the cloud while the cloud service providers charge for it. This may seem like a great give-and-take business partnership but some problems arise. In such an environment, the semantic security and integrity of the user's data are challenged. Data confidentiality is usually addressed by encrypting the data and data integrity requires verification of data. However, data on the cloud is usually shared by many users, which requires a one-to-many cryptographic primitive. Attribute-Based Encryption (ABE) is a widely known technique that solves this problem [1]. ABE has been proven to be very suitable for access control and it is widely used in many applications like paid broadcasting, cloud services, and medical data access control. ABE has undergone significant development since its initial proposal by Sahai et al. in 2005 [2]. Notably, Waters introduced the first practical version of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) in 2011 [3]. Over the past ten or so years, ABE has been extensively explored and extended with various functions besides access control, such as hidden access structures [4], dynamic credentials [5]–[7], privacy protection [8], outsourcing computation [9]–[11], etc. Numerous schemes of ABE have been put forth in recent years to improve efficiency [12]–[15]. Fast Attribute-based Message Encryption (FAME) was proposed by Agrawal et al. in 2017 [13], which is an unbounded attribute space ABE scheme with quick decryption. FAME has many advantages as one of the advanced ABE schemes. In FAME scheme, arbitrary strings are used as attributes and decryption inherently requires only 6 pairing operations. It is very efficient compared to the ABE scheme whose decryption cost is linearly related to the number of attributes. FAME is also proven to be fully secure, compared to some classical schemes [16], [17] which are only selective secure.

Another issue is that the access structure determines what attribute set can satisfy it. In CP-ABE, the plaintext is encrypted into ciphertext under a particular access structure. The access structure is generated at the time of encryption and remains unchanged. How to revoke access rights from some users by changing the access structure is a challenging problem. The individual who encrypts the data, known as the data owner, should have the authority to determine which individuals or entities are granted access to the data.

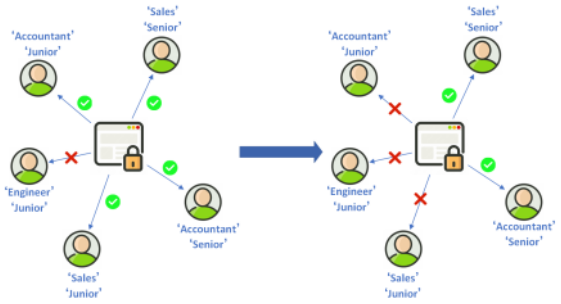

Fig. 1. Revocation process in a company

To illustrate this situation with an example, consider that in a company the annual sales data is encrypted by the access structure $\mathcal{T} = (\text{“}accountant\text{”} \vee \text{“}sales\text{”})$. The company's accountant and all sales of the marketing department have access to the report. Subsequently, the data owner, who is the manager of the company, seeks to enhance access privileges in order to safeguard privacy and mitigate the risk of malicious competition among employees. The new regulation requires that only management-level employees of the company have access to the report, that is, those with 'senior' attribute. The access structure for the encrypted report was therefore updated to the new access structure $\mathcal{T}' = (\text{“}accountant\text{”} \vee \text{“}sales\text{”}) \wedge (\text{“}senior\text{”})$. After this change, the junior sales no longer have access to this report. This process of revocation is done by a cloud server, so the data integrity after revocation needs to be guaranteed. Fig.1 depicts this example. In our model, we consider that cloud servers stores the data uploaded by users

correctly but may perform computational tasks inactively or incorrectly to save their computational resources, thus failing to make sure the integrity.

A. Motivations and Contributions

The existing revocable attribute-based encryption (RABE) schemes often fall short in ensuring data integrity. While Ge et al. [18] introduced a RABE scheme with data integrity, their scheme is not efficient enough for achieving data integrity protection. Thus, our objective is to enhance the efficiency of revocation and decryption processes while safeguarding data integrity. To accomplish this, we leverage the advantages of FAME [13], which is a more efficient scheme in terms of both encryption and decryption. Our research focuses on implementing revocation mechanisms and preserving data integrity within the framework of FAME. Following is a summary of our work's main contribution.

(1) We present an efficient RABE scheme, ensuring data integrity. The scheme includes a mechanism to detect incorrect revocation performed by the cloud, which can be identified by the data user.
(2) Our revocation process eliminates the need for the data owner to engage in decryption and encryption. Instead, the data owner can simply provide the cloud with a delegation, instructing it on how to perform the revocation.
(3) By reducing our scheme to the FAME scheme [13], we show its full security. Additionally, we prove that our scheme offers data integrity.
(4) Through experiments, we assess the execution time of various algorithms, including encryption, decryption, and revocation. We illustrate the performance of our scheme and the RABE-DI scheme presented in [18]. Our scheme has more effective revocation and decryption.

B. Related work

A lot of work has been carried out after Sahai and Waters [2] presented the idea of ABE, which requires the attribute set to meet the access structure in order to decrypt the data. ABE is divided into two types: key-policy attribute-based encryption (KP-ABE) [19], [20] and ciphertext-policy attribute-based encryption (CP-ABE) [21], [22], depending on whether the access structure belongs to the private key or ciphertext.

Revoking attributes is a significant area of research in ABE. It presents a challenging task due to the potential involvement of numerous users when updating a single attribute. Direct revocation [23]–[25], a common form of revocation, is usually implemented in two ways. One is to add a timestamp to the key and the key generation center (KGC) broadcasts periodically to update the key. Another way is to add a revocation list to the ciphertext, but faces with the problem of excessive ciphertext size. Liu et al. [23] introduced a method of revocation which is direct. This scheme incorporates the revocation list directly into the ciphertext, but this strategy has a disadvantage is that the ciphertext's length grows as time passes. They dealt this by eliminating the expired portion of the revocation list, thereby reducing the overall length of the ciphertext. Indirect revocation [26], [27] splits the user's privileges of decryption into key and update material of key. The revoked user does not receive the key update material from KGC anymore and loses the decryption privileges. Cui et al. [28] introduced a method which belongs to indirect revocation. Their method builds upon the revocation method described in [29], incorporating a combination of a binary tree and fuzzy identity-based encryption [2]. The method [29] decreases the scale of key updates from a linear to a logarithmic level. Further improvement of the method in [28] allows transferring the revocation-induced computation task to an unreliable cloud server and the data user only retains a constant-sized secret key locally. There are still some problems worth thinking about revocation. For example, how to revoke malicious users quickly, and how to decrease the computational burden during the revocation. The scheme [28] reduces the computational cost for data users with the help of auxiliary servers. Another issue is that the revoked user shouldn't have privilege to decrypt the new ciphertext after revocation, also known as revocation with forward security.

Due to the cloud server may perform revocation operations dishonestly, data integrity needs to be considered during the revocation process. It implies that it's imperative to guarantee that the encrypted data in both the previously created ciphertext from revocation and the original ciphertext are same. Some RABE schemes, such as [30] are not able to guarantee data integrity. A common solution is to verify the message being encrypted. Lai et al. [31] proposed a method to verify data integrity by giving a commitment to the message and a random message in the ciphertext. We use this verification method to ensure the data integrity of our scheme.

Proxy re-encryption (PRE) is common in cloud services and Attribute-based Proxy Re-encryption (ABPRE) is one of proxy encryption technologies [32], [33]. Data owner grants the proxy server the ability to perform re-encryption, which encrypts again on the ciphertext, achieving the effect that the original data is directly encrypted under the new access structure. Proxy servers reduce the computational pressure on users, but also bring credibility issues. Verification after the server's execution is essential. Recently, Ge et al. [33] proposed a verifiable PRE scheme that allows users to detect and refuse to pay for services if the proxy server does not perform correctly. Deng et al. [32] proposed a technique where a proxy server converts a ABE ciphertext to a ciphertext encrypted by identity-based encryption, thus reducing the decryption cost at the user end.

II. PRELIMINARIES

A. Complexity assumption

Let $(p, \mathbb{G}, \mathbb{H}, \mathbb{G}_T, e, g, h)$ be a prime order bilinear group system. The multiplicative cyclic groups $\mathbb{G}$, $\mathbb{H}$, and $\mathbb{G}_T$ have prime order p. g and h are generator of the group $\mathbb{G}$ and $\mathbb{H}$, respectively. If the subsequent conditions hold true, then $e : \mathbb{G} \times \mathbb{H} \to \mathbb{G}_T$ is a bilinear pairing.

(1) Bilinear:$e(u^x, v^y) = e(u, v)^{xy}$ for all $u \in \mathbb{G}, v \in \mathbb{H}$ and $x, y \in \mathbb{Z}_p^*$;
(2) Non-degenerate: $e(u, v) \neq 1$ whenever $u, v \neq 1_{\mathbb{G}}$;

(3) Computable: It's very efficient to caculate $e(u, v)$ for all $u \in \mathbb{G}, v \in \mathbb{H}$.

Definition 1 (Discrete Logarithm Assumption [34]). *Let $(p, \mathbb{G}, \mathbb{G}_T, e, g)$ be a bilinear group system of prime order. Given a tuple $(p, \mathbb{G}, \mathbb{G}_T, e, g, g^{\zeta})$ where $g \in \mathbb{G}, \zeta \in \mathbb{Z}_p^*$. The discrete logarithm assumption indicates that a probabilistic polynomial time (PPT) adversary $\mathcal{A}$ has a negligible advantage in finding the integer ζ. In formal terms, the advantage of such an adversary $Pr[\mathcal{A}(p, \mathbb{G}, \mathbb{G}_T, e, g, g^{\zeta}) = \zeta]$ is negligible.*

B. Access structure

The access structure [35] sometimes called a policy, requires a attribute set to be granted permissions when its requirements are met. The following statement provides the precise definition.

Definition 2. *The attribute universe dis represented by the symbol $\mathcal{U}$, $\mathbb{A}$ represents an access structure which consists of $\mathcal{U}$'s non-empty subsets, i.e., $\mathbb{A} \subseteq 2^{\mathcal{U}} \setminus \{0\}$. For any $B, C \subseteq \mathcal{U}$, if $B \subseteq C$ and $B \in \mathbb{A}$, then $C \in \mathbb{A}$, it is said to be monotone.*

From the point of comprehensibility, monotonicity suggests that a larger attribute set implies greater privileges, so adding attributes to a attribute set does not reduce its privileges but only makes it more powerful.

A Boolean formula $\mathcal{T}$ corresponds to an access structure $\mathbb{A} = (M, \tau)$ where M is a matrix and τ is a function. The Boolean formula $\mathcal{T}$ determines the number of rows and columns of matrix M and τ maps M's row to a specific attribute. Some simple and efficient conversion methods were proposed. For instance, in [36], Liu and Cao proposed an efficient algorithm to convert the Boolean formula into as small as possible matrix thus reducing the communication cost.

The scheme in this work does not involve the secret recovery, but only the linear secret sharing scheme's (LSSS [35]) linear reconfiguration property is used, described as follows.

Let $\mathcal{S}$ be an attribute set and $I = \{i | i \in \{1, ..., n_1\}, \tau(i) \in \mathcal{S}\}$ be the set of rows in M that corresponding to $\mathcal{S}$. If there is a way to combine the rows of matrix M such that the result is equal to $(1, 0, 0, ..., 0)$, then we describe the attribute set $\mathcal{S}$ as fulfilling the access structure (M, τ). More formally, if the attribute set $\mathcal{S}$ satisfies the access structure (M, τ), then there must exist a set of constant coefficients $\{\theta_i\}_{i \in I}$ such that the following equation holds $\sum_{i \in I} \theta_i M_i = (1, 0, 0, ..., 0)$ where M_i is the i-th row of M.

We use $(\widetilde{M}, \tilde{f})$ to denote the delegation access structure corresponds to $\widetilde{\mathcal{T}}$. The revoked boolean formula $\mathcal{T}^{'}$ corresponding to $(M^{'}, f^{'})$ is $\mathcal{T}^{'} = (\mathcal{T} AND \widetilde{\mathcal{T}})$.

III. SYSTEM ARCHITECTURE AND DEFINITIONS

A. System architecture

Our RABE system requires four entities, which are data owner (DO), data user (DU), trusted authority center (AC) and cloud server (CS).

(1) AC takes charge of setting up the entire system and generating all public parameters according to the security parameters. The authority center also uses the master private key to create private keys for the data users.
(2) DO makes the access structure and decides who can access its data accordingly. Data is encrypted under the specified access structure and transferred to the cloud.
(3) CS keeps the ciphertext that uploaded by data owner and performing the revocation operation.
(4) Data users are able to obtain the ciphertext and recover the plaintext with their own secret key. Data users also can confirm the data integrity.

B. Threat model

Threat models are used to portray adversaries. Different adversaries have different capabilities and goals, this paper deals with two adversaries in the threat model [18]. The first adversary can be any entity whose main target is to compromise the confidentiality of the data. This adversary doesn't possess a valid key, but their goal is to use the ciphertext to decipher information about the plaintext. The second adversary, typically represented by a CS, aims to tamper with the data integrity by generating incorrect revoked ciphertext. This means that they want to corrupt the data in a way that makes it unreliable or misleading. Note that the threat model assumes there is no collaboration between CS and the revoked user. In other words, CS won't share the original ciphertext with the revoked user, as doing so would allow the revoked user to decrypt it directly.

C. Syntax of Revocable FAME with Data Integrity (RFAME-DI)

Our RFAME-DI scheme is comprised of the following seven algorithms. The process of execution is depicted in Fig.2.

$\text{Setup}(1^{\lambda})$: The security parameters λ are provided as input to the authority center, which then generates the system public parameters PP and the master private key msk.

$\text{KeyGen}(msk, \mathcal{S})$: The authority center produces the private key sk for the data user by entering the master private key msk and the attribute set $\mathcal{S}$ corresponding to data user.

$\text{Encrypt}(m, \mathbb{A})$: The data owner uses the access structure $\mathbb{A}$ to encrypt the message m under t and then outputs the ciphertext CT.

$\text{Delegate}(\tilde{\mathbb{A}})$: The data owner takes the delegation access structure $\tilde{\mathbb{A}}$ as input, and then computes and takes the delegation DG based on the new attributes involved in $\tilde{\mathbb{A}}$ as output.

$\text{Revoke}(CT, \tilde{\mathbb{A}})$: The cloud server takes the original ciphertext CT and the revocation access structure $\tilde{\mathbb{A}}$ as input and takes the revoked ciphertext $CT^{'}$ whose corresponding access structure is $\mathbb{A}^{'}$ as output. The Boolean formula corresponding to $\mathbb{A}^{'}$ here is $\mathcal{T}^{'} = (\mathcal{T} AND \widetilde{\mathcal{T}})$.

$\text{Decrypt}_{\text{or}}(sk, CT)$: The data user takes their private key sk and the original ciphertext CT as input, where the private key corresponds to the attribute set $\mathcal{S}$ and the access structure contained in the ciphertext CT is $\mathbb{A}$. Then outputs the message m, when the attribute set $\mathcal{S}$ matches $\mathbb{A}$, else it outputs $\perp$.

$\text{Decrypt}_{\text{re}}(sk^{'}, CT_{csum}, CT^{'})$: The data user takes their private key $sk^{'}$ which is different from sk, a part of the original ciphertext CT_{csum} (Explicitly, it is the checksum in CT.) and

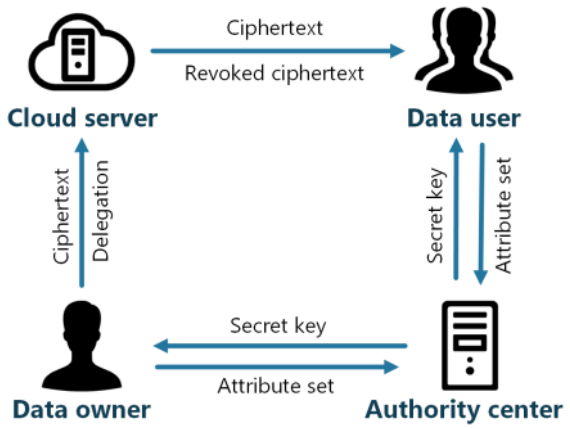

Fig. 2. Our RFAME-DI scheme's system architecture

the revoked ciphertext $CT^{'}$ downloaded from the cloud server as input if the attribute set $S^{'}$ about the private key $sk^{'}$ matches the access structure $\mathbb{A}^{'}$ in the ciphertext $CT^{'}$, then outputs the message m, else outputs $\perp$.

D. Security model

The two security models [18] required for the RFAME-DI scheme are described separately below.

IND-CPA security.

Informally, if no algorithm can distinguish between m_0 and m_1 encrypted under the chosen access structure $\mathbb{A}^*$, the scheme resists the chosen plaintext attack (CPA), as long as the algorithm is not authorized with the corresponding decryption key. Such an attack occurs at any stage of the cryptographic scheme, so the choice of the attacked access structure $\mathbb{A}^*$ depends on the private key and the public parameters possessed by the adversary. The scheme considered in this case will obtain adaptive or full security. In a less robust model referred to as selective security, the access structure $\mathbb{A}^*$ is selected before the system is deployed so as to prevent CPA, such an idealized definition is unlikely to occur in reality.

A RABE-DI scheme achieves CPA security when the $\mathcal{A}$'s advantage in the subsequent game is negligible.

Setup: The challenger $\mathcal{C}$ runs the scheme's Setup algorithm to produce public parameters and a master secret key during this phase. The public parameters are then shared by $\mathcal{C}$ and $\mathcal{A}$.

Query: $\mathcal{A}$ submits a query to obtain the secret keys $sk_{S_1}, ..., sk_{S_{q_1}}$, where S_i can't satisfy the access structure $\mathbb{A}^*$ that will be challenged for $i \in \{1, 2, ..., q_1\}$. $\mathcal{A}$ also makes delegation text query and get a series of delegation texts $dt_1, dt_2, ..., dt_{q_2}$.

Challenge: $\mathcal{A}$ chooses message m_0 and message m_1 of the same bit length. These messages are then sent to $\mathcal{C}$ by $\mathcal{A}$. $\mathcal{C}$ takes these messages and generates a challenge ciphertext CT^* by executing the algorithm $\mathrm{Enc}(m_\sigma, \mathbb{A}^*)$. Here, σ is a randomly chosen value from the set $\{0, 1\}$. $\mathcal{C}$ then sends the CT^* back to $\mathcal{A}$.

Query: This phase is the same as above.

Guess: $\mathcal{A}$'s advantage in winning the IND-CPA security game is defined by equation $Adv_{\mathcal{A}}^{IND-CPA}(\lambda) = |Pr[\sigma^{'} = \sigma] - 1/2|$, where $\sigma^{'}$ is the adversary's guess for σ.

Integrity.

The data integrity of RABE-DI scheme is captured by the game involving $\mathcal{C}$ and $\mathcal{A}$. The scheme guarantees data integrity if the advantage of an adversary $\mathcal{A}$ is negligible.

Setup: $\mathcal{C}$ runs the scheme's Setup algorithm to produce public parameters and a master secret key during this phase. The public parameters are then shared by $\mathcal{C}$ and $\mathcal{A}$.

Query: $\mathcal{A}$ submits a query to obtain the secret keys $sk_{S_1}, ..., sk_{S_q}$.

Challenge: $\mathcal{A}$ selects a message m and an access structure $\mathbb{A}$ and then transmits them to $\mathcal{C}$. $\mathcal{C}$ encrypts m by algorithm $\mathrm{Enc}(m, \mathbb{A})$ and returns it's result CT back to $\mathcal{A}$.

Query: This phase is the same as above.

Output: $\mathcal{A}$ produces an attribute set $S^{'}$ and a revoked ciphertext $CT^{'}$. $\mathcal{A}$ is considered to win if $Dec_{re}(sk_{S^{'}}, CT, CT^{'}) = m^{'}$, where $m^{'}$ is neither m nor $\perp$. We notate the $\mathcal{A}$'s advantage in winning the integrity game is $Pr[\mathcal{A}wins]$.

IV. CONSTRUCTION

In this part, we begin by presenting a revised version of the FAME construction, which includes an additional commitment to the ciphertext. Subsequently, we demonstrate that this modified version of FAME offers full security. Furthermore, we proposed the revocable FAME scheme with data integrity.

A. FAME scheme with data integrity

The scheme comprises four algorithms as follows.

$\underline{\mathrm{Setup}(1^\lambda)}$: Let $(p, \mathbb{G}, \mathbb{H}, \mathbb{G}_T, e, g, h)$ be a prime order bilinear group system. Authority center selects α_1, α_2 randomly from $\mathbb{Z}_p^*$ and selects $\gamma_1, \gamma_2, \gamma_3$ randomly from $\mathbb{Z}_p$ and computes$H_1 = h^{\alpha_1}, H_2 = h^{\alpha_2}, T_1 = e(g,h)^{\gamma_1\alpha_1+\gamma_3}, T_2 = e(g,h)^{\gamma_2\alpha_2+\gamma_3}$. Authority center also chooses two hash function $\mathcal{H} : \{0,1\}^* \to \mathbb{G}$ and H : $\mathbb{G}_T \to \mathbb{Z}_p^*$ and selects φ, ϕ randomly from $\mathbb{G}$, then authority center output public parameters $PP = (g, h, H_1, H_2, T_1, T_2, \varphi, \phi, \mathcal{H}, \mathrm{H})$. Authority center selects β_1, β_2 randomly from $\mathbb{Z}_p^*$ and output master private key $msk = (\alpha_1, \alpha_2, \beta_1, \beta_2, g^{\gamma_1}, g^{\gamma_2}, g^{\gamma_3})$.

$\underline{\mathrm{KeyGen}(msk, S)}$: Authority center selects r_1, r_2 randomly from $\mathbb{Z}_p$, and uses β_1, β_2 to compute $sk_0 = (h^{\beta_1 r_1}, h^{\beta_2 r_2}, h^{r_1+r_2})$. We use $sk_{0,1}, sk_{0,2}, sk_{0,3}$ to represent the three subterms of sk_0. Authority center selects $\sigma_y, \sigma^{'}$ randomly from $\mathbb{Z}_p$. For $z = 1, 2$ and all $y \in \mathcal{S}$, authority center computes

$$sk_{y,z} = \mathcal{H}(y1z)^{\frac{\beta_1 r_1}{\alpha_z}} \cdot \mathcal{H}(y2z)^{\frac{\beta_2 r_2}{\alpha_z}} \cdot \mathcal{H}(y3z)^{\frac{r_1+r_2}{\alpha_z}} \cdot g^{\frac{r_1+r_2}{\alpha_z}},$$
$$sk_z^{'} = g^{d_z} \cdot \mathcal{H}(011z)^{\frac{\beta_1 r_1}{\alpha_z}} \cdot \mathcal{H}(012z)^{\frac{\beta_2 r_2}{\alpha_z}} \cdot \mathcal{H}(013z)^{\frac{r_1+r_2}{\alpha_z}} \cdot g^{\frac{\sigma^{'}}{\alpha_z}}.$$

Authority center let $sk_y = (sk_{y,1}, sk_{y,2}, g^{-\sigma_y})$, $sk^{'} = (sk_1^{'}, sk_2^{'}, g^{\gamma_3 - \sigma^{'}})$ and output secret key $sk = (\mathcal{S}, sk_0, \{sk_y\}_{y \in \mathcal{S}}, sk^{'})$ for attribute set $\mathcal{S}$.

$\underline{\mathrm{Encrypt}(m, \mathbb{A} = (M, \tau))}$: Data owner selects s_1, s_2 and $\hat{s_1}, \hat{s_2}$ from $\mathbb{Z}_p$ randomly, computes $c_0 = (H_1^{s_1}, H_2^{s_2}, h^{s_1+s_2})$

and $e_0 = (H_1^{\hat{s_1}}, H_2^{\hat{s_2}}, h^{\hat{s_1}+\hat{s_2}})$. We use $c_{0,1}, c_{0,2}, c_{0,3}$ to represent the three subterms of c_0, the same for e_0. Suppose that M is a matrix of $n_1 \times n_2$ and $M_{i,j}$ is an element of M, where i and j represent the row and column number, respectively. For $k = 1, 2, 3$ and $i = 1, ..., n_1$, the data owner computes

$$c_{i,k} = \mathcal{H}(\tau(i)k1)^{s_1} \cdot \mathcal{H}(\tau(i)k2)^{s_2} \cdot \prod_{j=1}^{n_2} [\mathcal{H}(0jk1)^{s_1} \cdot \mathcal{H}(0jk2)^{s_2}]^{M_{i,j}},$$

Data owner lets $c_i = (c_{i,1}, c_{i,2}, c_{i,3})$ and computes $ct^{'} = T_1^{s_1} \cdot T_2^{s_2} \cdot m$, where message m belongs to group $\mathbb{G}_T$, and then data owner selects $m^{'}$ from $\mathbb{G}_T$ randomly. For $k = 1, 2, 3$ and $i = 1, ..., n_1$, the data owner computes

$$e_{i,k} = \mathcal{H}(\tau(i)k1)^{\hat{s_1}} \cdot \mathcal{H}(\tau(i)k2)^{\hat{s_2}} \cdot \prod_{j=1}^{n_2} [\mathcal{H}(0jk1)^{\hat{s_1}} \cdot \mathcal{H}(0jk2)^{\hat{s_2}}]^{M_{i,j}},$$

Data owner lets $e_i = (e_{i,1}, e_{i,2}, e_{i,3})$ and computes $ct^{''} = T_1^{\hat{s_1}} \cdot T_2^{\hat{s_2}} \cdot m^{'}$, $csum = \varphi^{\mathrm{H}(m)} \phi^{\mathrm{H}(m')}$.

Data owner outputs ciphertext $CT = (\mathbb{A}, c_0, c_1, ..., c_{n_1}, ct^{'}, e_0, e_1, ..., e_{n_1}, ct^{''}, csum)$.

$\underline{\mathrm{Decrypt}_{\mathrm{or}}}(sk, CT)$: Data user checks whether the private key's attribute set $\mathcal{S}$ matches the ciphertext's access structure $\mathbb{A} = (M, \tau)$. If not, the algorithm aborts after printing the error symbol $\perp$. Otherwise, data user perform the following operations. Data owner finds the set $I \subset \{1, 2, ..., n_1\}$ and $I = \{j : \tau(j) \in \mathcal{S}\}$ and then finds a constant set $\{\theta_i\}_{i \in I}$ that satisfy $\sum_{i \in I} \theta_i \cdot M_i = (1, 0, ..., 0)$. Data owner computes

$$num = ct^{'} \cdot e(\prod_{i \in I} c_{i,1}^{\theta_i}, sk_{0,1}) \cdot e(\prod_{i \in I} c_{i,2}^{\theta_i}, sk_{0,2}) \cdot e(\prod_{i \in I} c_{i,3}^{\theta_i}, sk_{0,3}),$$

$$den = e(sk_1^{'} \cdot \prod_{i \in I} sk_{\tau(i),1}^{\theta_i}, ct_{0,1}) \cdot e(sk_2^{'} \cdot \prod_{i \in I} sk_{\tau(i),2}^{\theta_i}, ct_{0,2}) \cdot e(sk_3^{'} \cdot \prod_{i \in I} sk_{\tau(i),3}^{\theta_i}, ct_{0,3}),$$

and output $m = num/den$. A similar calculation can be performed for $(e_0, e_1, ..., e_{n_1}, ct^{''})$ and output $m^{'}$. At last, if $csum = \varphi^{\mathrm{H}(m)} \phi^{\mathrm{H}(m')}$ holds, the data user outputs m, otherwise outputs $\perp$.

Correctness. Here we demonstrate that when the private key sk includes the necessary attributes in $\mathbb{A}$ of a valid FAME ciphertext, our decryption algorithm will always recover the correct message with a certainty of 1.

From the $ct^{'}$ we know that if we wish to get m, the essence is that we need to compute $T_1^{s_1} \cdot T_2^{s_2}$. For $k = 1, 2, 3$, using the equation $\sum_{i \in I} \theta_i M_i = (1, 0, 0, ..., 0)$, we can calculate $\prod_{i \in I} c_{i,k}^{\theta_i}$.

$$\begin{aligned}
\prod_{i \in I} c_{i,k}^{\theta_i} &= \prod_{i \in I} (\mathcal{H}(\tau(i)k1)^{\theta_i s_1} \cdot \mathcal{H}(\tau(i)k2)^{\theta_i s_2} \cdot \prod_{j=1}^{n_2} [\mathcal{H}(0jk1)^{s_1} \cdot \mathcal{H}(0jk2)^{s_2}]^{\theta_i M_{i,j}}) \\
&= \prod_{j=1}^{n_2} [\mathcal{H}(0jk1)^{s_1} \cdot \mathcal{H}(0jk2)^{s_2}]^{\sum_{i \in I} \theta_i M_{i,j}} \cdot (\prod_{i \in I} (\mathcal{H}(\tau(i)k1)^{\theta_i s_1} \cdot \mathcal{H}(\tau(i)k2)^{\theta_i s_2}) \\
&= [\mathcal{H}(01k1)^{s_1} \cdot \mathcal{H}(01k2)^{s_2}]^{\sum_{i \in I} \theta_i M_{i,j}} \cdot (\prod_{i \in I} (\mathcal{H}(\tau(i)k1)^{\theta_i s_1} \cdot \mathcal{H}(\tau(i)k2)^{\theta_i s_2})
\end{aligned}$$

This allows us to compute the last three pairing operations in num except for the $ct^{'}$ involving the encrypted message m. The results are as follows.

$$\begin{aligned}
&num/ct^{'} = \\
&\prod_{t \in \{1,2\}} [e(\mathcal{H}(011t), h)^{\beta_1 r_1 s_t} \cdot e(\mathcal{H}(012t), h)^{\beta_2 r_2 s_t} \cdot \\
&e(\mathcal{H}(013t), h)^{(r_1+r_2)s_t} \cdot \prod_{i \in I} (e(\mathcal{H}(\tau(i)1t)^{\theta_i}, h)^{\beta_1 r_1 s_t} \cdot \\
&e(\mathcal{H}(\tau(i)2t)^{\theta_i}, h)^{\beta_2 r_2 s_t} \cdot e(\mathcal{H}(\tau(i)3t)^{\theta_i}, h)^{(r_1+r_2)s_t})]
\end{aligned}$$

When the above $num/ct^{'}$ and the related term in dem are eliminated, we get the inverse of

$$(\prod_{t \in \{1,2\}} e(g^{d_t} \cdot g^{\frac{\sigma^{'}}{a_t}} \cdot \prod_{i \in I} g^{\frac{\theta_i \sigma_{\tau(i)}}{a_t}}, h^{a_t s_t})) \cdot e(g^{\gamma_3} \cdot g^{-\sigma^{'}} \cdot \prod_{i \in I} g^{-\theta_i \sigma_{\tau(i)}}, h^{s_1+s_2})$$

Simply organizing the above term we get $e(g, h)^{\gamma_1 \alpha_1 s_1 + \gamma_2 \alpha_2 s_2 + \gamma_3 (s_1+s_2)}$, it is evident that this is the $T_1^{s_1} \cdot T_2^{s_2}$ we want. Hence, the message m is recovered successfully. Similarly, we can obtain $m^{'}$.

B. RFAME-DI scheme

The RFAME-DI scheme is a further improvement on the FAME scheme with data integrity. The Setup, KeyGen, Encrypt, $\mathrm{Decrypt}_{\mathrm{or}}$ of our RFAME-DI scheme is the same as the scheme above. To achieve revocation, we add three algorithms Delegate, Revoke and $\mathrm{Decrypt}_{\mathrm{re}}$ as described below.

To perform a revocation of a file, the cloud needs a delegation DG provifded by the data owner of this file and the cloud performs the revocation algorithm based on the DG. To implement the delegation, the data owner randomly selects s_1, s_2 and saves s_1, s_2 as a file identifier for that file during the encryption phase. In the delegation phase, the data owner needs to use s_1, s_2 to generate the dt which is a part of DG.

$\underline{\mathrm{Delegate}}(\widetilde{\mathbb{A}})$: The data owner specifies an access structure $\widetilde{\mathbb{A}} = (\widetilde{M}, \widetilde{\tau})$, where $\widetilde{M}$ is a $\widetilde{n_1} \times \widetilde{n_2}$ matrix and $\widetilde{\tau}$ is a function that converts a row from the matrix $\widetilde{M}$ into an attribute. Then the following calculation is done for the new attributes contained in the access structure $\widetilde{\mathbb{A}}$ and $k = 1, 2, 3$.

$$dt_k = \prod_{i=1}^{\widetilde{n_1}} \mathcal{H}(\widetilde{\tau}(i)k1)^{s_1} \cdot \mathcal{H}(\widetilde{\tau}(i)k1)^{s_2}$$

Data owner lets $dt = (dt_1, dt_2, dt_3)$ and outputs delegation $DG = (dt, \widetilde{\mathbb{A}} = (\widetilde{M}, \widetilde{\tau}))$ for the could server.

$\underline{\mathrm{Revoke}}(CT, DG)$: The cloud server inputs a ciphertext $CT = (\mathbb{A}, c_0, c_1, ..., c_{n_1}, ct^{'}, e_0, e_1, ..., e_{n_1}, ct^{''}, csum)$ and a

delegation $DG = (dt, \widetilde{\mathbb{A}} = (\widetilde{M}, \widetilde{\tau}))$. M is a matrix with n_1 rows and n_2 columns and $\widetilde{M}$ is a matrix with $\widetilde{n_1}$ rows and $\widetilde{n_2}$ columns. The cloud server produces a revoked ciphertext under access structure $\mathbb{A}^{'} = (M^{'}, \tau^{'})$. The cloud server constructs $(M^{'}, \tau^{'})$ as

$$M^{'} = \left(\begin{array}{c|c|c} M & -col_1 & \mathbf{0} \\ \hline \mathbf{0} & & \widetilde{M} \end{array}\right),$$

$$\tau^{'} = \begin{cases} \tau(j) & j \leq n_1 \\ \widetilde{\tau}(j - n_1) & j > n_1 \end{cases}$$

where col_1 is first column of M. $M^{'}$ is a $n_1^{'} \times n_2^{'}$ matrix, where $n_1^{'} = n_1 + \widetilde{n_1}, n_2^{'} = n_2 + \widetilde{n_2}$. The cloud selects $s_1^{'}, s_2^{'}$ from $\mathbb{Z}_p$ randomly and computes revoked ciphertext

$\bar{ct}^{'} = ct^{'} \cdot T_1^{'s_1} \cdot T_2^{'s_2}, \bar{c}_0 = (c_{0,1} \cdot H_1^{'s_1}, c_{0,2} \cdot H_2^{'s_2}, c_{0,3} \cdot h^{s_1^{'} + s_2^{'}})$,

$\bar{c}_{i,k}^{'} = c_{i,k} \cdot \mathcal{H}(\tau(i)k1)^{'s_1} \cdot \mathcal{H}(\tau(i)k2)^{'s_2} \cdot \prod_{j=1}^{n_2^{'}} [\mathcal{H}(0jk1)^{'s_1} \cdot \mathcal{H}(0jk2)^{'s_2}]^{M_{i,j}^{'}}$, where $i \in [1, n_1]$.

$\bar{c}_{i,k}^{'} = dt_l \cdot \mathcal{H}(\tau(i)k1)^{'s_1} \cdot \mathcal{H}(\tau(i)k2)^{'s_2} \cdot \prod_{j=1}^{n_2^{'}} [\mathcal{H}(0jk1)^{'s_1} \cdot \mathcal{H}(0jk2)^{'s_2}]^{M_{i,j}^{'}}$, where $i \in [n_1 + 1, n_1^{'}]$.

The cloud server lets $\bar{c}_i = (\bar{c}_{i,1}, \bar{c}_{i,2}, \bar{c}_{i,3})$ for i from 1 to $n_1^{'}$ and $\overline{csum} = csum$. The $\bar{e}_0, \bar{e}_1, ..., \bar{e}_{n_1}$ can be gotten in the same way as above.

The revoked ciphertext is $CT^{'} = (\mathbb{A}^{'}, \bar{c}_0, \bar{c}_1, ..., \bar{c}_{n_1^{'}}, \bar{ct}^{'}, \bar{e}_0, \bar{e}_1, ..., \bar{e}_{n_1^{'}}, \bar{ct}^{''}, \overline{csum})$.

$\mathrm{Decrypt}_{\mathrm{re}}(sk^{'}, CT_{csum}, CT^{'})$: The data user enters the private key $sk^{'}$, which corresponds to the attribute set $\mathcal{S}^{'}$. The data owner also enters the checksum in original ciphertext CT_{csum} and revoked ciphertext $CT^{'}$. First, the data user verify whether $\overline{csum}$ is equal to CT_{csum}. If not, the data user outputs an error symbol $\perp$ and abort. The second step, the data user checks if the attribute set $\mathcal{S}^{'}$ meets the access structure $(M^{'}, \tau^{'})$. If it doesn't satisfy, the algorithm aborts after printing $\perp$. Otherwise, the data user finds a set $I^{'} \subset \{1, 2, ..., n_1^{'}\}$ where $I^{'} = \{j : \tau^{'}(j) \in \mathcal{S}^{'}\}$ and a set of constants $\{\theta_i^{'}\}_{i \in I^{'}}$ which elements belong to $\mathbb{Z}_p^*$. Such that $\sum_{i \in I^{'}} \theta_i^{'} \cdot M_i^{'} = (1, 0, 0, ..., 0)$. Then, the data user calculates m and $m^{'}$ in the same way as in $\mathrm{Decrypt}_{\mathrm{or}}$. At last, the data user checks whether $\overline{csum} = \varphi^{\mathrm{H}(m)} \phi^{\mathrm{H}(m^{'})}$. If the equation holds, the algorithm exports m, else prints $\perp$.

Correctness. Algorithm $\mathrm{Decrypt}_{\mathrm{re}}$ is the equivalent of the original decryption algorithm $\mathrm{Decrypt}_{\mathrm{or}}$ except for the first step, the fourth part of the original ciphertext CT_{csum} is compared with the checksum in the revoked ciphertext $CT^{'}$. Therefore, as long as $CT^{'}$ is a valid ciphertext under the access structure $(M^{'}, \tau^{'})$, algorithm $\mathrm{Decrypt}_{\mathrm{re}}$ naturally satisfies the correctness. In the following, we show that the $CT^{'}$ produced through Revoke is correct by lemma 1.

Lemma 1. *If the above M and $\widetilde{M}$ are valid LSSS access structures, then $M^{'}$ is a valid LSSS access structure, and vice versa.*

proof: Due to the fact that both (M, τ) and $(\widetilde{M}, \widetilde{\tau})$ are valid, there are two sets of constants $\{\theta_i\}_{i \in [1, n_1]}$ and $\{\widetilde{\theta_i}\}_{i \in [1, \widetilde{n_1}]}$ which elements both belong to $\mathbb{Z}_p^*$, such that $\sum_{i \in [1, n_1]} \theta_i \cdot M_i = (1, 0, 0, ..., 0) \in \mathbb{Z}_p^{n_1}$ and $\sum_{i \in [1, \widetilde{n_1}]} \widetilde{\theta_i} \cdot \widetilde{M_i} = (1, 0, 0, ..., 0) \in \mathbb{Z}_p^{\widetilde{n_1}}$, respectively. We can then use $\{\theta_i\}_{i \in [1, n_1]}$ and $\{\widetilde{\theta_i}\}_{i \in [1, \widetilde{n_1}]}$ to construct $\{\theta_i^{'}\}_{i \in [1, n_1^{'}]}$ in the following way, where $n_1^{'} = n_1 + \widetilde{n_1}$.

$$\theta_i^{'} = \begin{cases} \theta_i & , i \in [1, n_1] \\ \widetilde{\theta}_{i - n_1} & , i \in [n_1 + 1, n_1^{'}] \end{cases}$$

It is easy to deduce from the formula that,

$$\begin{aligned} \sum_{i \in [1, n_1^{'}]} \theta_i^{'} \cdot M_i^{'} &= \sum_{i \in [1, n_1]} \theta_i \cdot M_i^{'} + \sum_{i \in [1, \widetilde{n_1}]} \widetilde{\theta_i} \cdot M_{i + n_1}^{'} \\ &= (\overbrace{1, 0, ..., 0}^{n_1}, \overbrace{-1, 0, ..., 0}^{\widetilde{n_1}}) + (\overbrace{0, ..., 0, 1, 0, ..., 0}^{n_1 \quad \widetilde{n_1}}) \\ &= (1, 0, 0, ..., 0) \in \mathbb{Z}_p^{n_1^{'}} \end{aligned}$$

Thus, $(M^{'}, \tau^{'})$ is valid LSSS access structures.

Conversely, if $(M^{'}, \tau^{'})$ is valid, there exists a set of constants $\{\theta_i^{'}\}_{i \in [1, n_1^{'}]}$ which elements both belong to $\mathbb{Z}_p^*$, such that $\sum_{i \in [1, n_1^{'}]} \theta_i^{'} \cdot M_i^{'} = (1, 0, 0, ..., 0) \in \mathbb{Z}_p^{n_1^{'}}$. We can construct $\{\theta_i = \theta_i^{'}\}_{i \in [1, n_1]}$ and $\{\widetilde{\theta_i} = \theta_{i + n_1}\}_{i \in [1, \widetilde{n_1}]}$

$$\begin{aligned} \sum_{i \in [1, n_1^{'}]} \theta_i^{'} \cdot M_i^{'} &= (1, 0, 0, ..., 0) \\ &= (\overbrace{1, 0, ..., 0}^{n_1}, \overbrace{-1, 0, ..., 0}^{\widetilde{n_1}}) + (\overbrace{0, ..., 0, 1, 0, ..., 0}^{n_1 \quad \widetilde{n_1}}) \\ &= \sum_{i \in [1, n_1]} \theta_i \cdot M_i^{'} + \sum_{i \in [1, \widetilde{n_1}]} \widetilde{\theta_i} \cdot M_{i + n_1}^{'} \\ &= (\sum_{i \in [1, n_1]} \theta_i \cdot M_i, \sum_{i \in [1, n_1]} \theta_i \cdot (\overbrace{-col_{1,i}, 0, ..., 0}^{\widetilde{n_1}})) \\ &+ (\sum_{i \in [1, \widetilde{n_1}]} \widetilde{\theta_i} \cdot (\overbrace{0, ..., 0}^{n_1}), \sum_{i \in [1, \widetilde{n_1}]} \widetilde{\theta_i} \cdot \widetilde{M_i}) \end{aligned}$$

From the above equation it can be inferred that $\sum_{i \in [1, n_1]} \theta_i \cdot M_i = (1, 0, 0, ..., 0) \in \mathbb{Z}_p^{n_1}$ and $\sum_{i \in [1, \widetilde{n_1}]} \widetilde{\theta_i} \cdot \widetilde{M_i} = (1, 0, 0, ..., 0) \in \mathbb{Z}_p^{\widetilde{n_1}}$. Thus, the LSSS access structures M and $\widetilde{M}$ are both valid.

V. SECURITY ANALYSIS

First, we prove the confidentiality of the modified FAME scheme by reducing it to the original FAME scheme. We then demonstrate the semantic security of the proposed revocable FAME with data integrity scheme. Finally, we give a data integrity proof of our formal scheme by reducing to the discrete logarithm assumption.

Theorem 1. *The FAME with data integrity scheme is fully IND-CPA secure if Shashank's FAME scheme [13] is fully IND-CPA secure.*

Proof: The simulator $\mathcal{B}$ can be built to breach the underlying FAME scheme's full security by communicating with the

challenger $\mathcal{C}$, if a $\mathcal{A}$ exists that can breach the security of FAME-DI scheme.

• Setup. $\mathcal{B}$ obtains the basic parameters $(p, \mathbb{G}, \mathbb{H}, \mathbb{G}_T, e, H_1, H_2, T_1, T_2, \mathcal{H})$ by calling $\mathcal{C}$, where $H_1 = h^{\alpha_1}, H_2 = h^{\alpha_2}, T_1 = e(g,h)^{\gamma_1\alpha_1+\gamma_3}, T_2 = e(g,h)^{\gamma_2\alpha_2+\gamma_3}$. $\mathcal{B}$ first selects a hash H that maps from $\mathbb{G}_T$ to $\mathbb{Z}_p^*$, and then randomly selects two elements ϕ, φ from the group $\mathbb{G}$. Then $\mathcal{B}$ adds these to the base parameters to form the public parameters $PP = (\phi, \varphi, H_1, H_2, T_1, T_2, \mathcal{H}, \mathrm{H})$ to $\mathcal{A}$, and sends them to $\mathcal{A}$.

• Query. $\mathcal{A}$ query a private key, then $\mathcal{B}$ query a private key to $\mathcal{C}$ on the attribute set $\mathcal{S}$ which is the same as the query of $\mathcal{A}$. Then $\mathcal{B}$ forwards the return of $\mathcal{C}$ to $\mathcal{A}$. $\mathcal{A}$ can also initiate a delegation query to access structure $\widetilde{\mathbb{A}} = (\widetilde{M}, \widetilde{\tau})$. $\mathcal{B}$ randomly selects two random numbers s_a and s_b and computes $dt_l = \prod_{i=1}^{\widetilde{n_1}} \mathcal{H}(\widetilde{\tau}(i)k1)^{s_a} \cdot \mathcal{H}(\widetilde{\tau}(i)k1)^{s_b}$, set $dt = (dt_1, dt_2, dt_3)$, then $\mathcal{B}$ forwards dt to $\mathcal{A}$.

• Challenge. $\mathcal{A}$ sends message m_0 and message m_1 of the same bit length and the access structure $\mathbb{A}^* = (M^*, \tau^*)$ intended to be challenged to $\mathcal{B}$. $\mathcal{B}$ forwards m_0, m_1 and $\mathbb{A}^*$ to $\mathcal{C}$. $\mathcal{C}$ tosses a random coin to determine the value of $\sigma \in \{0,1\}$ based on its tails and sends the challenge ciphertext about m_σ encrypted with $\mathbb{A}^*$ to $\mathcal{B}$, denote as $(\mathbb{A}^*, c_0, c_1, ..., c_{n_1}, ct^{'})$. $\mathcal{B}$ selects $m^{'} \in \mathbb{G}, Q \in \mathbb{G}_T$ and $\hat{s_1}, \hat{s_2}$ from $\mathbb{Z}_p$ randomly. The simulator $\mathcal{B}$ computes $e_0 = (H_1^{\hat{s_1}}, H_2^{\hat{s_2}}, h^{\hat{s_1}+\hat{s_2}})$ and for $k = 1, 2, 3$ and $i = 1, ..., n_1$, $\mathcal{B}$ computes $e_{i,k} = \mathcal{H}(f(i)k1)^{\hat{s_1}} \cdot \mathcal{H}(f(i)k2)^{\hat{s_2}} \cdot \prod_{j=1}^{n_2}[\mathcal{H}(0jk1)^{\hat{s_1}} \cdot \mathcal{H}(0jk2)^{\hat{s_2}}]^{(M^*)_{i,j}}$. $\mathcal{B}$ sets $e_i = (e_{i,1}, e_{i,2}, e_{i,3})$. Then $\mathcal{B}$ computes $ct^{''} = T_1^{\hat{s_1}} \cdot T_2^{\hat{s_2}} \cdot m^{'}$ and sets $csum = Q$. Eventually $\mathcal{B}$ sets challenge ciphertext $CT = ((M^*, f^*), c_0, c_1, ..., c_{n_1}, ct^{'}, e_0, e_1, ..., e_{n_1}, ct^{''}, csum)$ and forwards it to $\mathcal{A}$.

• Query. This phase is the same as above.

• Output. $\mathcal{A}$ gives its guess $\sigma^{'}$ on σ, $\mathcal{B}$ also guesses σ as $\sigma^{'}$.

Analysis. If $\mathcal{A}$ can break our modified scheme, $\mathcal{B}$ has same advantage to compromise the FAME scheme. The simulation in the game works perfectly, except that during the challenge phase, instead of providing the calculated check value $csum = \varphi^{\mathrm{H}(m)}\phi^{\mathrm{H}(m')}$, $\mathcal{B}$ returns a random value Q from the group $\mathbb{G}_T$. The important point is that $\mathcal{A}$ is unaware of the value of m', so the random value Q has the same statistical distribution as the calculated check value $csum$. This means that the computed $csum$ and the random value Q look the same from $\mathcal{A}$'s perspective.

Theorem 2. *The revocable FAME with data integrity scheme is fully IND-CPA secure if the modified FAME scheme is fully IND-CPA secure.*

Proof: First, in the revocable FAME with data integrity scheme, the ciphertext generated by encryption algorithm Encrypt before revocation is the same as the ciphertext in the modified FAME scheme. We call the ciphertext generated by Encrypt the original ciphertext, so the original ciphertext generated by encryption in RFAME-DI achieves the same full security as the modified FAME scheme. Second, we show that the revoked ciphertext generated by the revocation Revoke and the ciphertext produced during encryption are identically distributed, i.e., these two are indistinguishable from the adversary's view. In our RFAME-DI scheme, the ciphertext generated by the Revoke is the elements in the $\mathbb{G}_T$ generated by the value $s_1 + s_1^{'}$ and $s_2 + s_2^{'}$. Where $s_1^{'}, s_2^{'}$ are chosen randomly and s_1, s_2 are in the original ciphertext. So in the adversary's view $s_1 + s_1^{'}$ and $s_2 + s_2^{'}$ are also chosen randomly. Thus the revocation ciphertext generated with random value $s_1 + s_1^{'}, s_2 + s_2^{'}$ and the ciphertext generated by directly encrypting under the access structure $(M^{'}, \tau^{'})$ with randomly selected value $s_1^{''}, s_2^{''}$ are identically distributed, i.e., indistinguishable from the adversary's viewpoint.

Theorem 3. *If the discrete logarithm assumption holds, the revocable FMAE scheme captures the data integrity.*

Proof: If a malicious $\mathcal{A}$ attempts to compromise the RFAME-DI scheme's integrity, it implies the existence of simulator $\mathcal{B}$ to address the discrete logarithm problem. Simulator $\mathcal{B}$ inputs a discrete logarithm instance, represented by the parameters $(p, \mathbb{G}, \mathbb{G}_T, e, g, g^\zeta)$. Its objective is to get the ζ as the output.

• Setup. $\mathcal{B}$ sets a bilinear group system of prime order $(p, \mathbb{G}, \mathbb{G}_T, e, g)$. $\mathcal{B}$ selects $\alpha_1, \alpha_2, \beta_1, \beta_2$ randomly from $\mathbb{Z}_p^*$ and select $\gamma_1, \gamma_2, \gamma_3, \mu$ randomly from $\mathbb{Z}_p$, then chooses two hash function $\mathrm{H} : \mathbb{G}_T \to \mathbb{Z}_p^*$ and $\mathcal{H} : \{0,1\}^* \to \mathbb{G}_T$. $\mathcal{B}$ lets $\varphi = g^\zeta, \phi = g^\mu$ and computes $H_1 = h^{\alpha_1}, H_2 = h^{\alpha_2}, T_1 = e(g,h)^{\gamma_1\alpha_1+\gamma_3}, T_2 = e(g,h)^{\gamma_2\alpha_2+\gamma_3}$. Then $\mathcal{B}$ sends the public parameters $PP = (\varphi, \phi, H_1, H_2, T_1, T_2, \mathcal{H}, \mathrm{H})$ to $\mathcal{A}$.

• Query. $\mathcal{A}$ query a private key on the attribute set $\mathcal{S}$. As $\mathcal{B}$ holds the master private key $msk = (g, h, \alpha_1, \alpha_2, \beta_1, \beta_2, g^{\gamma_1}, g^{\gamma_2}, g^{\gamma_3})$, $\mathcal{B}$ can generate the $sk_\mathcal{S}$ and provide it to $\mathcal{A}$.

• Challenge. $\mathcal{A}$ selects an access structure $\mathbb{A} = (M, f)$ and a message m and provides them to the $\mathcal{B}$. Note that here $\mathcal{B}$ is both the simulator and the challenger. The simulator $\mathcal{B}$ runs the $\mathrm{Encrypt}(m, (M, \tau))$ to obtain $CT = (\mathbb{A}, c_0, c_1, ..., c_{n_1}, ct^{'}, e_0, e_1, ..., e_{n_1}, ct^{''}, csum)$, where $csum = \varphi^{\mathrm{H}(m)}\phi^{\mathrm{H}(m^{'})}$ and $m^{'}$ is randomly selected during the encryption process. $\mathcal{B}$ sends CT to the $\mathcal{A}$.

• Query. This phase is the same as above.

• Output. $\mathcal{A}$ gives a revoked ciphertext under the revoked access structure $CT^{'} = (\mathbb{A}^{'} = (M^{'}, \tau^{'}), \bar{c}_0, \bar{c}_1, ..., \bar{c}_{n_1^{'}}, \bar{ct^{'}}, \bar{e}_0, \bar{e}_1, ..., \bar{e}_{n_1^{'}}, \bar{ct^{''}}, \overline{csum})$.

At this point, simulator $\mathcal{B}$ can choose a attribute set $\mathcal{S}^{'}$ that satisfy the revoked access structure $M^{'}$ and then use the master private key to generate the corresponding private key$sk_{\mathcal{S}^{'}}$, which is then used to decrypt $CT^{'}$ to obtain the encrypted message. Denote the decrypted real message and random message be $\bar{m}$ and $\bar{m^{'}}$ respectively. If $\mathcal{A}$ can break data integrity, then it means $\bar{m} \neq m$ and $\bar{m^{'}} \neq m^{'}$ but $\overline{csum} = csum$. So that $\mathcal{B}$ can calculate ζ by the following computation and return ζ as its answer for discrete logarithm assumption.

$$
\begin{aligned}
csum = \overline{csum} &\Leftrightarrow \varphi^{\mathrm{H}(m)}\phi^{\mathrm{H}(m^{'})} = \varphi^{\mathrm{H}(\bar{m})}\phi^{\mathrm{H}(\bar{m^{'}})} \\
&\Leftrightarrow g^{\zeta\cdot\mathrm{H}(m)+\mu\cdot\mathrm{H}(m^{'})} = g^{\zeta\cdot\mathrm{H}(\bar{m})+\mu\cdot\mathrm{H}(\bar{m^{'}})} \\
&\Leftrightarrow \zeta \cdot (\mathrm{H}(m) - \mathrm{H}(\bar{m})) = \mu \cdot (\mathrm{H}(\bar{m^{'}}) - \mathrm{H}(m^{'}))
\end{aligned}
$$

$$
\Rightarrow \zeta = \frac{\mu\cdot(\mathrm{H}(\bar{m^{'}}) - \mathrm{H}(m^{'}))}{\mathrm{H}(m) - \mathrm{H}(\bar{m})}.
$$

Analysis. The simulation of $\mathcal{B}$ in the game is flawless, and the $\mathcal{B}$'s advantage in solving the discrete logarithmic hard problem is identical to the adversary $\mathcal{A}$'s advantage in winning the above game.

VI. IMPLEMENTATION & EVALUATION

We put our scheme into action and assess its feasibility by considering the computational expenses involved, we also compare it with other RABE scheme.

To implement our scheme, we experimented on a laptop with AMD's CPU. It's Ryzon 7 5800H @3.2GHz with 4GB RAM. Both the client and cloud server utilize the Linux Ubuntu 20.04 operating system. We use the library charm 0.5.0 in python to write the code and run it with version 2.7.15 of python. It is possible to carry our scheme on type III curves, such as MNT and BN curves, but some MNT and BN curves are known to be insecure in some parameters, so be sure to choose elliptic curves carefully when implementing cryptographic schemes. We implement our scheme on the type III curve MNT224 in PBC, which is widely acknowledged for its exceptional balance between security and efficiency.

Since there are AND-gates and OR-gates in the randomly generated access structure, how many attributes are used in decryption is not determined by the access structure size, and only some attributes are needed to participate in the calculation to complete the decryption. Therefore, the access structure we generate for testing only contains AND-gates, the goal is to ensure that the amount of attributes needed for decryption matches the access structure size. We also did the same test 50 times and averaged the results to get more realistic and accurate time data. Specifically in the experiment, for the three algorithms $\mathrm{Encrypt}$, $\mathrm{Decrypt}_{\mathrm{or}}$, and Revoke, the attribute set and access structure were adjusted in increments of 10, ranging from a minimum of 10 to a maximum of 100. The horizontal coordinates of the experimental images of Revoke represent the size of $\mathbb{A}^{'}$. For the algorithm $\mathrm{Decrypt}_{\mathrm{re}}$, the access structure size is from 20 to 200 with a step of 20. In fact, there is no difference between the two algorithms $\mathrm{Decrypt}_{\mathrm{or}}$ and $\mathrm{Decrypt}_{\mathrm{re}}$, but $\mathrm{Decrypt}_{\mathrm{re}}$ does one more equation verification operation than $\mathrm{Decrypt}_{\mathrm{or}}$, i.e., verifying whether the CT_{csum} item from the original ciphertext is equal to $\overline{csum}$ in the revoked ciphertext, and this operation is very light and its time consumption is negligible. We can see from the Fig.4 and Fig.6 that the performance of the $\mathrm{Decrypt}_{\mathrm{re}}$ algorithm is almost the same as that of the $\mathrm{Decrypt}_{\mathrm{or}}$ algorithm in the set size range from 10 to 100.

We compare with the scheme [18]. From Fig.6-9, we see that our scheme outperforms the the scheme [18] in all four phases: encryption, decryption, revocation, and decryption of the revoked ciphertext. Especially in decryption phases, where the time consumed in our scheme for decryption is independent of the set size, which is stable at about 36ms regardless of the set size. This is because the decryption process of FAME only needs 6 pairing operations. Our scheme has acceptable disadvantages and very large advantages in practical applications. Because the KGC, which has adequate computational capability, manages key generation and the algorithm is usually executed only once for one user. The client device handles both encryption and decryption tasks, so it's crucial for the computational load to be as minimal as possible. Since ABE is a one-to-many encryption technique, so decryption occurs more frequently than encryption in practical scenarios. Our scheme happens to exactly has a significant advantage in decryption.

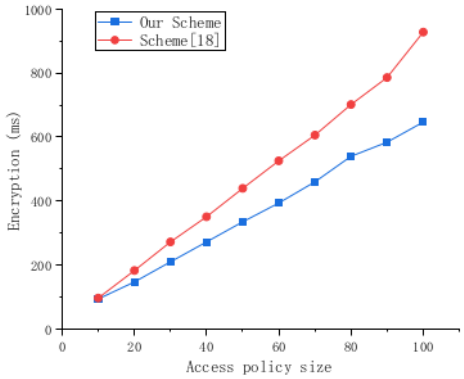

Fig. 3. Encryption time of RFAME-DI scheme and compared scheme

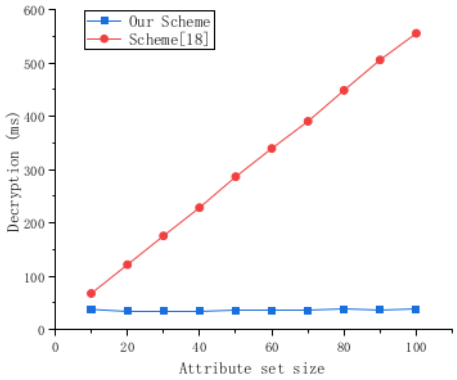

Fig. 4. Decryption time of RFAME-DI scheme and compared scheme

The outcomes of the experiment show the effectiveness and feasibility of our revocation scheme in ensuring the data integrity.

VII. CONCLUSION

In this study, we introduced a practical and effective RABE scheme designed to safeguard the data integrity on the cloud, thereby minimizing performance limitations both for the data users and cloud. We reduced our scheme to the FAME scheme to show its full security and we also demonstrated the data integrity of our scheme in adaptive model under discrete

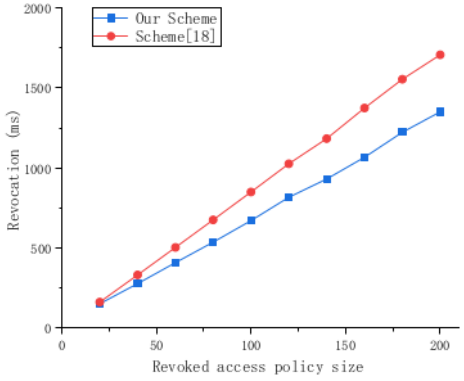

Fig. 5. Revocation time of RFAME-DI scheme and compared scheme

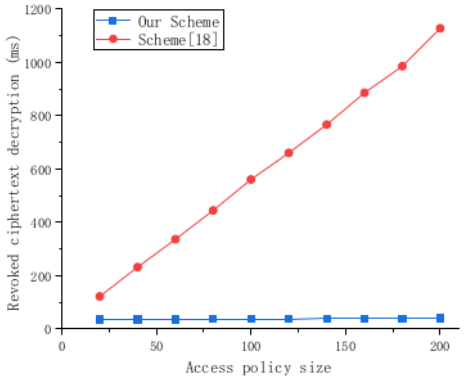

Fig. 6. Revoked ciphertext decryption time of RFAME-DI scheme and compared scheme

logarithm assumption. Furthermore, we have conducted simulation experiments and experimental analysis indicates that our scheme's efficiency surpasses the comparison scheme in encryption, decryption and revocation algorithms. However, our scheme achieves efficient attribute-based revocation while protecting data integrity, but the essence of revocation is an update of the access structure. It will affect the access of some data user to the file. Upcoming efforts will concentrate on how to implement more fine-grained revocation, enabling data owners to withdraw access to a single file for a specific user.

REFERENCES

[1] L. Zhang, H. Xiong, Q. Huang, J. Li, K. R. Choo, and J. Li, "Cryptographic solutions for cloud storage: Challenges and research opportunities," *IEEE Trans. Serv. Comput.*, vol. 15, no. 1, pp. 567–587, 2022.

[2] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, vol. 3494. Springer, 2005, pp. 457–473.

[3] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011. Proceedings*, ser. Lecture Notes in Computer Science, D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, Eds., vol. 6571. Springer, 2011, pp. 53–70.

[4] K. B. Frikken, M. J. Atallah, and J. Li, "Attribute-based access control with hidden policies and hidden credentials," *IEEE Trans. Computers*, vol. 55, no. 10, pp. 1259–1270, 2006.

[5] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, vol. 7417. Springer, 2012, pp. 199–217.

[6] R. Zhang, J. Li, Y. Lu, J. Han, and Y. Zhang, "Key escrow-free attribute based encryption with user revocation," *Inf. Sci.*, vol. 600, pp. 59–72, 2022.

[7] J. Li, R. Zhang, Y. Lu, J. Han, Y. Zhang, W. Zhange, and X. Dong, "Multi-authority attribute-based encryption for assuring data deletion," *IEEE Systems Journal*, 2022.

[8] J. Li, Y. Zhang, J. Ning, X. Huang, G. S. Poh, and D. Wang, "Attribute based encryption with privacy protection and accountability for cloudiot," *IEEE Trans. Cloud Comput.*, vol. 10, no. 2, pp. 762–773, 2022.

[9] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," *IEEE Trans. Parallel Distributed Syst.*, vol. 22, no. 7, pp. 1214–1221, 2011.

[10] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," *IEEE Trans. Parallel Distributed Syst.*, vol. 25, no. 8, pp. 2201–2210, 2014.

[11] J. Li, Y. Wang, Y. Zhang, and J. Han, "Full verifiability for outsourced decryption in attribute based encryption," *IEEE Trans. Serv. Comput.*, vol. 13, no. 3, pp. 478–487, 2020.

[12] N. Chen, J. Li, Y. Zhang, and Y. Guo, "Efficient CP-ABE scheme with shared decryption in cloud storage," *IEEE Trans. Computers*, vol. 71, no. 1, pp. 175–184, 2022.

[13] S. Agrawal and M. Chase, "FAME: fast attribute-based message encryption," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*. ACM, 2017, pp. 665–682.

[14] D. Riepel and H. Wee, "FABEO: fast attribute-based encryption with optimal security," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, Los Angeles, CA, USA, November 7-11, 2022*, H. Yin, A. Stavrou, C. Cremers, and E. Shi, Eds. ACM, 2022, pp. 2491–2504.

[15] M. Ambrona, G. Barthe, R. Gay, and H. Wee, "Attribute-based encryption in the generic group model: Automated proofs and new constructions," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*. ACM, 2017, pp. 647–664.

[16] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA, October 28-31, 2007*. ACM, 2007, pp. 195–203.

[17] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in *Automata, Languages and Programming, 35th International Colloquium, ICALP 2008, Reykjavik, Iceland, July 7-11, 2008, Proceedings, Part II - Track B: Logic, Semantics, and Theory of Programming & Track C: Security and Cryptography Foundations*, vol. 5126. Springer, 2008, pp. 579–591.

[18] C. Ge, W. Susilo, J. Baek, Z. Liu, J. Xia, and L. Fang, "Revocable attribute-based encryption with data integrity in clouds," *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 5, pp. 2864–2872, 2022.

[19] N. Attrapadung, B. Libert, and E. de Panafieu, "Expressive key-policy attribute-based encryption with constant-size ciphertexts," in *Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011. Proceedings*, vol. 6571. Springer, 2011, pp. 90–108.

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

[21] J. Li, W. Yao, J. Han, Y. Zhang, and J. Shen, "User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1767–1777, 2018.

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

[23] J. K. Liu, T. H. Yuen, P. Zhang, and K. Liang, "Time-based direct revocable ciphertext-policy attribute-based encryption with short revocation list," in *Applied Cryptography and Network Security - 16th International Conference, ACNS 2018, Leuven, Belgium, July 2-4, 2018, Proceedings*, vol. 10892. Springer, 2018, pp. 516–534.

[24] Y. Shi, Q. Zheng, J. Liu, and Z. Han, "Directly revocable key-policy attribute-based encryption with verifiable ciphertext delegation," *Inf. Sci.*, vol. 295, pp. 221–231, 2015.

[25] H. Wang, Z. Zheng, L. Wu, and P. Li, "New directly revocable attribute-based encryption scheme and its application in cloud storage environment," *Clust. Comput.*, vol. 20, no. 3, pp. 2385–2392, 2017.

[26] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, vol. 7417. Springer, 2012, pp. 199–217.

[27] Y. Yang, J. K. Liu, K. Liang, K. R. Choo, and J. Zhou, "Extended proxy-assisted approach: Achieving revocable fine-grained encryption of cloud data," in *Computer Security - ESORICS 2015 - 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, 2015, Proceedings, Part II*, vol. 9327. Springer, 2015, pp. 146–166.

[28] H. Cui, R. H. Deng, Y. Li, and B. Qin, "Server-aided revocable attribute-based encryption," in *Computer Security - ESORICS 2016 - 21st European Symposium on Research in Computer Security, Heraklion, Greece, September 26-30, 2016, Proceedings, Part II*, vol. 9879. Springer, 2016, pp. 570–587.

[29] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proceedings of the 2008 ACM Conference on Computer and Communications Security, CCS 2008, Alexandria, Virginia, USA, October 27-31, 2008*. ACM, 2008, pp. 417–426.

[30] Y. Jiang, W. Susilo, Y. Mu, and F. Guo, "Ciphertext-policy attribute-based encryption supporting access policy update and its extension with preserved attributes," *Int. J. Inf. Sec.*, vol. 17, no. 5, pp. 533–548, 2018.

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

[32] H. Deng, Z. Qin, Q. Wu, Z. Guan, and Y. Zhou, "Flexible attribute-based proxy re-encryption for efficient data sharing," *Inf. Sci.*, vol. 511, pp. 94–113, 2020.

[33] C. Ge, W. Susilo, J. Baek, Z. Liu, J. Xia, and L. Fang, "A verifiable and fair attribute-based proxy re-encryption scheme for data sharing in clouds," *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 5, pp. 2907–2919, 2022.

[34] A. Sadeghi and M. Steiner, "Assumptions related to discrete logarithms: Why subtleties make a real difference," in *Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding*, vol. 2045. Springer, 2001, pp. 244–261.

[35] A. Beimel, "Secure schemes for secret sharing and key distribution," Ph.D. dissertation, Technion - Israel Institute of Technology, Israel, 1996.

[36] Z. Liu and Z. Cao, "On efficiently transferring the linear secret-sharing scheme matrix in ciphertext-policy attribute-based encryption," *IACR Cryptol. ePrint Arch.*, p. 374, 2010.

lw

原创性报告

30%	23%	29%	14%
相似指数	网际网络来源	出版物	学生文稿

主要来源

1	kresttechnology.com 网际网络来源	1%
2	www.researchgate.net 网际网络来源	1%
3	Chunpeng Ge, Willy Susilo, Joonsang Baek, Zhe Liu, Jinyue Xia, Liming Fang. "Revocable Attribute-Based Encryption with Data Integrity in Clouds", IEEE Transactions on Dependable and Secure Computing, 2021 出版物	1%
4	Binanda Sengupta, Yingjiu Li, Yangguang Tian, Robert H Deng, Zheng Yang. "Policy-Based Editing-Enabled Signatures: Authenticating Fine-Grained and Restricted Data Modification", The Computer Journal, 2021 出版物	1%
5	core.ac.uk 网际网络来源	1%
6	eprint.iacr.org 网际网络来源	1%

7	Yuyan Guo, Zhenhua Lu, Hui Ge, Jiguo Li. "Revocable Blockchain-Aided Attribute-Based Encryption With Escrow-Free in Cloud Storage", IEEE Transactions on Computers, 2023 出版物	1 %
8	Zhenzhen Guo, Gaoli Wang, Yingxin Li, Jianqiang Ni, Runmeng Du, Miao Wang. "Accountable Attribute-Based Data Sharing Scheme Based on Blockchain for Vehicular Ad Hoc Network", IEEE Internet of Things Journal, 2022 出版物	1 %
9	www.thefreelibrary.com 网际网络来源	1 %
10	Submitted to National Sun Yat-sen University 学生文稿	1 %
11	www.eurchembull.com 网际网络来源	<1 %
12	downloads.hindawi.com 网际网络来源	<1 %
13	Jingwei Wang, Xinchun Yin, Jianting Ning, Shengmin Xu, Guowen Xu, Xinyi Huang. "Secure Updatable Storage Access Control System for EHRs in the Cloud", IEEE Transactions on Services Computing, 2022 出版物	<1 %

14	Liqing Chen, Jiayi Li, Jiguo Li. "Towards Forward and Backward Private Dynamic Searchable Symmetric Encryption Supporting Data Deduplication and Conjunctive Queries", IEEE Internet of Things Journal, 2023 出版物	<1%
15	Jianfei Sun, Guowen Xu, Tianwei Zhang, Xuehuan Yang, Mamoun Alazab, Robert H. Deng. "Verifiable, Fair and Privacy-Preserving Broadcast Authorization for Flexible Data Sharing in Clouds", IEEE Transactions on Information Forensics and Security, 2023 出版物	<1%
16	academic.oup.com 网际网络来源	<1%
17	Hui Cui, Zhiguo Wan, Xinlei Wei, Surya Nepal, Xun Yi. "Pay as You Decrypt: Decryption Oursoucing for Functional Encryption Using Blockchain", IEEE Transactions on Information Forensics and Security, 2020 出版物	<1%
18	www.yunzhan365.com 网际网络来源	<1%
19	Lucas Schabhuser, Denise Demirel, Johannes Buchmann. "An unconditionally hiding auditing procedure for computations over distributed data", 2016 IEEE Conference on	<1%

	Communications and Network Security (CNS), 2016 出版物	
20	software.imdea.org 网际网络来源	<1 %
21	Jun Feng, Hu Xiong, Jinhao Chen, Yang Xiang, Kuo-Hui Yeh. "Scalable and Revocable Attribute-based Data Sharing with Short Revocation List for IIoT", IEEE Internet of Things Journal, 2022 出版物	<1 %
22	arxiv.org 网际网络来源	<1 %
23	Marco Rasori, Michele La Manna, Pericle Perazzo, Gianluca Dini. "A Survey on Attribute-Based Encryption Schemes Suitable for the Internet of Things", IEEE Internet of Things Journal, 2022 出版物	<1 %
24	Yangguang Tian, Atsuko Miyaji, Koki Matsubara, Hui Cui, Nan Li. "Revocable Policy-Based Chameleon Hash for Blockchain Rewriting", The Computer Journal, 2022 出版物	<1 %
25	ijeecs.iaescore.com 网际网络来源	<1 %

26	Zhaoman Liu, Lei Wu, Weizhi Meng, Hao Wang, Wei Wang. "Accurate Range Query With Privacy Preservation for Outsourced Location-Based Service in IoT", IEEE Internet of Things Journal, 2021 出版物	<1%
27	Xixi Yan, Xu He, Jinxia Yu, Yongli Tang. "White-Box Traceable Ciphertext-Policy Attribute-Based Encryption in Multi-Domain Environment", IEEE Access, 2019 出版物	<1%
28	ijns.jalaxy.com.tw 网际网络来源	<1%
29	ijsrcseit.com 网际网络来源	<1%
30	Guoyan Zhang, Shaohui Wang. "A Certificateless Signature and Group Signature Schemes against Malicious PKG", 22nd International Conference on Advanced Information Networking and Applications (aina 2008), 2008 出版物	<1%
31	Kotoko YAMADA, Nuttapong ATTRAPADUNG, Keita EMURA, Goichiro HANAOKA, Keisuke TANAKA. "Generic Constructions for Fully Secure Revocable Attribute-Based Encryption", IEICE Transactions on	<1%

Fundamentals of Electronics, Communications and Computer Sciences, 2018
出版物

---

32 Yinbin Miao, Feng Li, Xinghua Li, Jianting Ning, Hongwei Li, Kim-Kwang Raymond Choo, Robert H. Deng. "Verifiable Outsourced Attribute-Based Encryption Scheme for Cloud-Assisted Mobile E-health System", IEEE Transactions on Dependable and Secure Computing, 2023 <1 %
出版物

---

33 Yinbin Miao, Jianfeng Ma, Ximeng Liu, Xinghua Li, Qi Jiang, Junwei Zhang. "Attribute-Based Keyword Search over Hierarchical Data in Cloud Computing", IEEE Transactions on Services Computing, 2017 <1 %
出版物

---

34 Kaiqing Huang. "Accountable and Revocable Large Universe Decentralized Multi-Authority Attribute-Based Encryption for Cloud-Aided IoT", IEEE Access, 2021 <1 %
出版物

---

35 Shashank Agrawal, Melissa Chase. "FAME", Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017 <1 %
出版物

---

36 igbquickload.org

网际网络来源

<1%

37 Shengmin Xu, Xinyi Huang, Jiaming Yuan, Yingjiu Li, Robert H. Deng. "Accountable and Fine-Grained Controllable Rewriting in Blockchains", IEEE Transactions on Information Forensics and Security, 2022
出版物

<1%

38 docksci.com
网际网络来源

<1%

39 Hu Xiong, Xin Huang, Minghao Yang, Lili Wang, Shui Yu. "Unbounded and Efficient Revocable Attribute-based Encryption with Adaptive Security for Cloud-Assisted Internet of Things", IEEE Internet of Things Journal, 2021
出版物

<1%

40 Submitted to University of Hong Kong
学生文稿

<1%

41 Yinbin Miao, Jianfeng Ma, Ximeng Liu, Jian Weng, Hongwei Li, Hui Li. "Lightweight Fine-Grained Search Over Encrypted Data in Fog Computing", IEEE Transactions on Services Computing, 2019
出版物

<1%

42 pure.royalholloway.ac.uk
网际网络来源

<1%

43	www.mdpi.com 网际网络来源	<1 %
44	"Computer Security – ESORICS 2016", Springer Nature, 2016 出版物	<1 %
45	Yinghui Zhang, Dong Zheng, Xiaofeng Chen, Jin Li, Hui Li. "Efficient attribute-based data sharing in mobile clouds", Pervasive and Mobile Computing, 2016 出版物	<1 %
46	ink.library.smu.edu.sg 网际网络来源	<1 %
47	tojqi.net 网际网络来源	<1 %
48	Lecture Notes in Computer Science, 2015. 出版物	<1 %
49	Shangping Wang, Duqiao Zhao, Yaling Zhang. "Searchable attribute-based encryption scheme with attribute revocation in cloud storage", PLOS ONE, 2017 出版物	<1 %
50	Tsz Hon Yuen, Willy Susilo, Yi Mu. "Towards a cryptographic treatment of publish/subscribe systems1", Journal of Computer Security, 2014 出版物	<1 %
51	discovery.researcher.life	

网际网络来源

<1%

52	ir.cwi.nl 网际网络来源	<1%
53	isrc.ccs.asia.edu.tw 网际网络来源	<1%
54	"Computer Security – ESORICS 2021", Springer Science and Business Media LLC, 2021 出版物	<1%
55	Lecture Notes in Computer Science, 2013. 出版物	<1%
56	Pengshou xie, Haoxuan Yang, Tao Feng, Yan Yan. "Implementing efficient attribute encryption in IoV under cloud environments", Computer Networks, 2022 出版物	<1%
57	Rui Guo, Chaoyuan Zhuang, Huixian Shi, Yinghui Zhang, Dong Zheng. "A lightweight verifiable outsourced decryption of attribute-based encryption scheme for blockchain-enabled wireless body area network in fog computing", International Journal of Distributed Sensor Networks, 2020 出版物	<1%
58	Submitted to University of Wollongong 学生文稿	<1%

59	Chunpeng Ge, Willy Susilo, Joonsang Baek, Zhe Liu, Jinyue Xia, Liming Fang. "A Verifiable and Fair Attribute-based Proxy Re-encryption Scheme for Data Sharing in Clouds", IEEE Transactions on Dependable and Secure Computing, 2021 出版物	<1%
60	Leyou Zhang, Jian Su, Yi Mu. "Outsourcing Attributed-Based Ranked Searchable Encryption With Revocation for Cloud Storage", IEEE Access, 2020 出版物	<1%
61	Ma Zhuo, Jiawei Zhang. "Efficient, Traceable and Privacy-Aware Data Access Control in Distributed Cloud-based IoD Systems", IEEE Access, 2023 出版物	<1%
62	Qutaibah M. Malluhi, Abdullatif Shikfa, Viet Cuong Trinh. "A Ciphertext-Policy Attribute-based Encryption Scheme With Optimized Ciphertext Size And Fast Decryption", Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security - ASIA CCS '17, 2017 出版物	<1%
63	Rui Guo, Geng Yang, Huixian Shi, Yinghui Zhang, Dong Zheng. "O-R-CP-ABE: An Efficient and Revocable Attribute-Based Encryption	<1%

Scheme in the Cloud-Assisted IoMT System", IEEE Internet of Things Journal, 2021
出版物

---

64 Wu, Shengyan, Changlu Lin, and Li Xu. "Fully Distributed Multi-authority Cloud Storage Model", 2013 International Conference on Cloud Computing and Big Data, 2013.
出版物 <1%

---

65 iacr.org
网际网络来源 <1%

---

66 Sana Belguith, Nesrine Kaaniche, Mohammad Hammoudeh. "Analysis of attribute_based cryptographic techniques and their application to protect cloud services", Transactions on Emerging Telecommunications Technologies, 2019
出版物 <1%

---

67 Syh-Yuan Tan, Swee-Huay Heng, Bok-Min Goi. "Chapter 22 On the Security of an Attribute-Based Signature Scheme", Springer Science and Business Media LLC, 2009
出版物 <1%

---

68 eprints-phd.biblio.unitn.it
网际网络来源 <1%

---

69 hal.science
网际网络来源 <1%

---

vdoc.pub

70	网际网络来源	<1%
71	www.astesj.com 网际网络来源	<1%
72	Haiyan Wang, yuan li, shulan wang, Lianguan Hang, Fucai Luo. "FFH-ABE: Fast File-Hierarchy Attribute-Based Encryption Scheme for the Internet of Things", Institute of Electrical and Electronics Engineers (IEEE), 2023 出版物	<1%
73	Lei Zhang, Hu Xiong, Qiong Huang, Jiguo Li, Kim-Kwang Raymond Choo, Jiangtao LI. "Cryptographic Solutions for Cloud Storage: Challenges and Research Opportunities", IEEE Transactions on Services Computing, 2019 出版物	<1%
74	journalofcloudcomputing.springeropen.com 网际网络来源	<1%
75	"Innovations in Computer Science and Engineering", Springer Science and Business Media LLC, 2019 出版物	<1%
76	Jianchang Lai, Yi Mu, Fuchun Guo, Rongmao Chen. "Fully Privacy-Preserving ID-Based Broadcast Encryption with Authorization", The Computer Journal, 2017 出版物	<1%

77	Jiang, Rui, Xianglong Wu, and Bharat Bhargava. "SDSS-MAC: secure data sharing scheme in multi-authority cloud storage systems", Computers & Security, 2016. 出版物	<1 %
78	Jiguo Li, Ruyuan Zhang, Yang Lu, Jinguang Han, Yichen Zhang, Wenzheng Zhang, Xinfeng Dong. "Multiauthority Attribute-Based Encryption for Assuring Data Deletion", IEEE Systems Journal, 2022 出版物	<1 %
79	Q.M. Malluhi, A. Shikfa, V.D. Tran, V.C. Trinh. "Decentralized ciphertext-policy attribute-based encryption schemes for lightweight devices", Computer Communications, 2019 出版物	<1 %
80	Shangping Wang, Shasha Jia, Yaling Zhang. "Verifiable and Multi-Keyword Searchable Attribute-Based Encryption Scheme for Cloud Storage", IEEE Access, 2019 出版物	<1 %
81	Yadav, Umesh Chandra, and Syed Taqi Ali. "Ciphertext policy-hiding attribute-based encryption", 2015 International Conference on Advances in Computing Communications and Informatics (ICACCI), 2015. 出版物	<1 %

82	pt.scribd.com 网际网络来源	<1%
83	"Advances in Information and Computer Security", Springer Science and Business Media LLC, 2011 出版物	<1%
84	"Wireless Algorithms, Systems, and Applications", Springer Science and Business Media LLC, 2019 出版物	<1%
85	Danan Thilakanathan, Shiping Chen, Surya Nepal, Rafael Calvo. "SafeProtect: Controlled Data Sharing With User-Defined Policies in Cloud-Based Collaborative Environment", IEEE Transactions on Emerging Topics in Computing, 2016 出版物	<1%
86	Hua Deng, Jixin Zhang, Zheng Qin, Qianhong Wu, Hui Yin, Aniello Castiglione. "Policy-based Broadcast Access Authorization for Flexible Data Sharing in Clouds", IEEE Transactions on Dependable and Secure Computing, 2021 出版物	<1%
87	Jie Cui, Bei Li, Hong Zhong, Yan Xu, Lu Liu. "Achieving Revocable Attribute Group-Based Encryption for Mobile Cloud Data: A Multi-	<1%

Proxy Assisted Approach", IEEE Transactions on Dependable and Secure Computing, 2022
出版物

88	Jing Li, Zhitao Guan, Xiaojiang Du, Zijian Zhang, Jun Wu. "An efficient encryption scheme with verifiable outsourced decryption in mobile cloud computing", 2017 IEEE International Conference on Communications (ICC), 2017 出版物	<1%
89	Lecture Notes in Computer Science, 2010. 出版物	<1%
90	Submitted to Monash University 学生文稿	<1%
91	Sascha Muller, Stefan Katzenbeisser, Claudia Eckert. "ON MULTI-AUTHORITY CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION", Bulletin of the Korean Mathematical Society, 2009 出版物	<1%
92	Shengmin Xu, Guomin Yang, Yi Mu. "Revocable attribute-based encryption with decryption key exposure resistance and ciphertext delegation", Information Sciences, 2019 出版物	<1%

93	Xi Sun, Hao Wang, Xiu Fu, Hong Qin, Mei Jiang, Likun Xue, Xiaochao Wei. "Substring-searchable attribute-based encryption and its application for IoT devices", Digital Communications and Networks, 2020 出版物	<1 %
94	dlibra.itl.waw.pl 网际网络来源	<1 %
95	innoovatum.com 网际网络来源	<1 %
96	mdpi-res.com 网际网络来源	<1 %
97	www.indusedu.org 网际网络来源	<1 %
98	www.karger.com 网际网络来源	<1 %
99	"Advances in Cryptology – CRYPTO 2018", Springer Science and Business Media LLC, 2018 出版物	<1 %
100	"Information Security and Privacy", Springer Science and Business Media LLC, 2017 出版物	<1 %
101	"Information and Communications Security", Springer Science and Business Media LLC, 2015	<1 %

出版物

102	Changsong Yang, Yueling Liu, Feng Zhao, Shubin Zhang. "Provable data deletion from efficient data integrity auditing and insertion in cloud storage", Computer Standards & Interfaces, 2022 出版物	<1%
103	Deli Jiang, Xuegeng Chen, Limin Yan, Haixiao Gou, Jiacheng Yang, Ying Li. "Parameter Calibration of Discrete Element Model for Cotton Rootstalk–Soil Mixture at Harvest Stage in Xinjiang Cotton Field", Agriculture, 2023 出版物	<1%
104	Hamed Arshad, Christian Johansen, Olaf Owe, Pablo Picazo-Sanchez, Gerardo Schneider. "Semantic Attribute-Based Encryption: A framework for combining ABE schemes with semantic technologies", Information Sciences, 2022 出版物	<1%
105	Heyi Tang, Yong Cui, Chaowen Guan, Jianping Wu, Jian Weng, Kui Ren. "Enabling Ciphertext Deduplication for Secure Cloud Storage and Access Control", Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security - ASIA CCS '16, 2016 出版物	<1%

106	Jiguo Li, Wei Yao, Yichen Zhang, Huiling Qian, Jinguang Han. "Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing", IEEE Transactions on Services Computing, 2017 出版物	<1 %
107	Kaiqing Huang. "Secure Efficient Revocable Large Universe Multi-Authority Attribute-Based Encryption for Cloud-Aided IoT", IEEE Access, 2021 出版物	<1 %
108	Lecture Notes in Computer Science, 2014. 出版物	<1 %
109	Lewis Nkenyereye, S.M. Riazul Islam, Muhammad Bilal, M. Abdullah-Al-Wadud, Atif Alamri, Anand Nayyar. "Secure crowd-sensing protocol for fog-based vehicular cloud", Future Generation Computer Systems, 2021 出版物	<1 %
110	Shardha Porwal, Sangeeta Mittal. "A Secure Key Delegation Mechanism for Fog Networking", 2019 Twelfth International Conference on Contemporary Computing (IC3), 2019 出版物	<1 %
111	Ti Wang, Yongbin Zhou, Hui Ma, Rui Zhang. "Flexible and Controllable Access Policy	<1 %

	Update for Encrypted Data Sharing in the Cloud", The Computer Journal, 2023 出版物	
112	Yudi Zhang, Fuchun Guo, Willy Susilo, Guomin Yang. "Balancing Privacy and Flexibility of Cloud-based Personal Health Records Sharing System", IEEE Transactions on Cloud Computing, 2022 出版物	<1 %
113	Yuyan Guo, Zhenhua Lu, Hui Ge, Jiguo Li. "Revocable blockchain-aided attribute-based encryption with escrow-free in cloud storage", IEEE Transactions on Computers, 2023 出版物	<1 %
114	d-nb.info 网际网络来源	<1 %
115	ijcert.org 网际网络来源	<1 %
116	jit.ndhu.edu.tw 网际网络来源	<1 %
117	jwcn-eurasipjournals.springeropen.com 网际网络来源	<1 %
118	link.springer.com 网际网络来源	<1 %
119	translateyar.ir 网际网络来源	<1 %

120	www.dcs.bbk.ac.uk 网际网络来源	<1%
121	www.ijaerd.com 网际网络来源	<1%
122	"Applied Cryptography and Network Security", Springer Science and Business Media LLC, 2018 出版物	<1%
123	"Information Security and Privacy", Springer Science and Business Media LLC, 2019 出版物	<1%
124	"Public Key Cryptography – PKC 2011", Springer Science and Business Media LLC, 2011 出版物	<1%
125	Alberto Fachechi. "PDE/Statistical Mechanics Duality: Relation Between Guerra's Interpolated p-Spin Ferromagnets and the Burgers Hierarchy", Journal of Statistical Physics, 2021 出版物	<1%
126	Hui Cui, Xun Yi, Surya Nepal. "Achieving Scalable Access Control Over Encrypted Data for Edge Computing Networks", IEEE Access, 2018 出版物	<1%

127	Jiguo Li, Fengjie Sha, Yichen Zhang, Xinyi Huang, Jian Shen. "Verifiable Outsourced Decryption of Attribute-Based Encryption with Constant Ciphertext Length", Security and Communication Networks, 2017 出版物	<1 %
128	Jiguo Li, Yichen Zhang, Jianting Ning, Xinyi Huang, Geong Sen Poh, Debang Wang. "Attribute Based Encryption with Privacy Protection and Accountability for CloudIoT", IEEE Transactions on Cloud Computing, 2020 出版物	<1 %
129	Steven D. Galbraith. "References", Cambridge University Press (CUP), 2012 出版物	<1 %
130	Zechao Liu, Zoe L. Jiang, Xuan Wang, S.M. Yiu, Chunkai Zhang, Xiaomeng Zhao. "Dynamic Attribute-Based Access Control in Cloud Storage Systems", 2016 IEEE Trustcom/BigDataSE/ISPA, 2016 出版物	<1 %
131	orca.cardiff.ac.uk 网际网络来源	<1 %
132	"Recent Advances in Information and Communication Technology 2019", Springer Science and Business Media LLC, 2020 出版物	<1 %

133 Yinbin Miao, Jian Weng, Ximeng Liu, Kim-Kwang Raymond Choo, Zhiquan Liu, Hongwei Li. "Enabling verifiable multiple keywords search over encrypted cloud data", Information Sciences, 2018

出版物

<1%

不含引文	关闭	不含相符结果	关闭
排除参考书目	关闭		