Revocable Attribute-Based Encryption With Data Integrity in Clouds

Chunpeng Ge, *Member, IEEE*, Willy Susilo, *Fellow, IEEE*, Joonsang Baek, *Member, IEEE*, Zhe Liu, *Senior Member, IEEE*, Jinyue Xia, and Liming Fang

Abstract—Cloud computing enables enterprises and individuals to outsource and share their data. This way, cloud computing eliminates the heavy workload of local information infrastructure. Attribute-based encryption has become a promising solution for encrypted data access control in clouds due to the ability to achieve one-to-many encrypted data sharing. Revocation is a critical requirement for encrypted data access control systems. After outsourcing the encrypted attribute-based ciphertext to the cloud, the data owner may want to revoke some recipients that were authorized previously, which means that the outsourced attribute-based ciphertext needs to be updated to a new one that is under the revoked policy. The integrity issue arises when the revocation is executed. When a new ciphertext with the revoked access policy is generated by the cloud server, the data recipient cannot be sure that the newly generated ciphertext guarantees to be decrypted to the same plaintext as the originally encrypted data, since the cloud server is provided by a third party, which is not fully trusted. In this article, we consider a new security requirement for the revocable attribute-based encryption schemes: integrity. We introduce a formal definition and security model for the revocable attribute-based encryption with data integrity protection (RABE-DI). Then, we propose a concrete RABE-DI scheme and prove its confidentiality and integrity under the defined security model. Finally, we present an implementation result and provide performance evaluation which shows that our scheme is efficient and practical.

Index Terms—Attribute-based encryption, data integrity, cloud computing, revocable

1 Introduction

Cloud computing has been offering cost-effective storage solutions to personal and large-scale enterprise applications. Unlike setting up in-house storage and servers, cloud computing is almost maintenance-free in terms of managing local storage. However, it becomes a potential security issue when the data owner outsources the data to the could as the cloud server usually is provided by an untrusted third party. One fundamental method to ensure data confidentiality is to provide data encryption. However, with the data being shared in a group of users, cloud computing faces a challenge of managing access control of the encrypted data. Recently, attribute-based encryption (ABE) has been considered as a promising approach to address the issue [1]. Typically, an attribute set comes along with the encryption in an ABE scheme, which is used by the authorized recipients to access the underlying data. The access policy, however, is generated when the data was encrypted and remains the same afterwards. This becomes cumbersome when some users quit the group and their access permission should be revoked.

We use the following Financial Audit System (FAS) to illustrate the aforementioned problem. A company encrypts its annual financial report with an access policy $\mathcal{T}_1$: "Audit Firm $\bigvee$ "tax office" and then uploads the ciphertext to the cloud server. An officer from the audit firm or tax office can then decrypt the ciphertext and access the financial report. Later, a new regulation was issued that only senior auditors can audit the annual financial report. Thus, the access policy needs to be updated to $\mathcal{T}_2$: ("Audit Firm $\bigvee$ "tax office") $\bigwedge$ "senior auditor". This update process indicates that the junior auditor's permission no longer exists in the original policy $\mathcal{T}_1$. A critical security requirement during such a revocation process is that the underlying data of the revoked ciphertext should be identical to the original ciphertext. The scenario is depicted in Fig. 1.

In the cloud environment, when the revocation needs to be executed in ABE, the cloud server leverages the ciphertext delegation method to revoke the access policy for the ciphertext. The delegation process, however, cannot ensure the integrity of the corresponding message. Since the ciphertext delegation process is computationally intensive, the cloud server may just return the ciphertext handled previously or output even a random ciphertext to save its computational resource. Another trivial solution is that the data owner can download the ciphertext and decrypt it to the corresponding plaintext. Then, the data owner can repeat the encryption and re-upload the encrypted data.

- *Chunpeng Ge is with the Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China, with State Key Laboratory of Cryptology, Beijing, 100878, China, with Science and Technology on Parallel and Distributed Processing Laboratory (PDL), Changsha 410000, China, and also with the University of Wollongong, Wollongong, NSW 2522, Australia. E-mail: gecp@nuaa.edu.cn.*
- *Willy Susilo and Joonsang Baek are with the University of Wollongong, Wollongong, NSW 2522, Australia. E-mail: {wsusilo, baek@uow.edu.au}@uow.edu.au.*
- *Zhe Liu and Liming Fang are with the Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China. E-mail: {zheliu, fangliming}@nuaa.edu.cn.*
- *Jinyue Xia is with the IBM, Armonk, NY 10504 USA. E-mail: jinyue.xiab@ibm.com.*

Manuscript received 28 Mar. 2020; revised 23 Feb. 2021; accepted 8 Mar. 2021. Date of publication 17 Mar. 2021; date of current version 2 Sept. 2022. (Corresponding authors: Willy Susilo and Zhe Liu.) Digital Object Identifier no. 10.1109/TDSC.2021.3065999

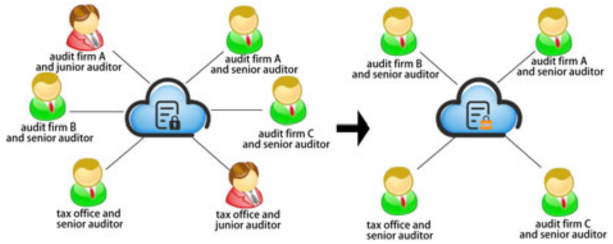


Fig. 1. Financial audit system revocation scenario. In the left part that the junior auditor from audit firm A, and the junior auditor from tax office cannot access the data from the revoked encrypted file any more.

However, such a method requires the data owner to decrypt and re-encrypt the data every time when the policy is updated, which will result in additional computational cost to the data owner. In the mean time, downloading data from the cloud and conducting computations locally bring about the data maintenance problem. What is worse, the data owner should be online during the revocation process.

1.1 Motivations

Although the existing ABE schemes with ciphertext delegation enable the revocations of access policy for the ABE ciphertext, they cannot protect the data integrity. Hence, we need a secure scheme that ensures data confidentiality as well as data integrity. All of these concerns motivate us to design an attribute-based encryption mechanism that

1) achieves revocation from the encrypted attribute-based encryption ciphertext while keeps the data integrity;
2) does not require unnecessary operations of decryption and re-encryption to the data owner;
3) the data owner is not required to be online during the revocation process.

In this paper, we propose a revocable ABE scheme with integrity protection, whereby the cloud server can directly revoke an access policy without compromising the security of the original ciphertext. Moreover, if the cloud server returns an incorrect revoked ciphertext, it will be detected.

1.2 Related Work

Attribute-Based Encryption. Attribute-based encryption (ABE) describes the user's credential as an attribute set and generates the ciphertext with another attribute set [1]. The user is able to decrypt the ciphertext only when the two attribute sets are close in a metric. Generally speaking, there exists two categories of ABE: key-policy attribute-based encryption (KP-ABE) [2] and ciphertext-policy attribute-based encryption (CP-ABE) [3]. With KP-ABE, a user's secret key is generated under an access condition and a ciphertext is encrypted with a predicate. On the contrary, in the ciphertext-policy attribute-encryption setting, a user's secret is generated with a predicate and the ciphertext is encrypted with an access condition. The user can decrypt a ciphertext only when the predicate satisfies the access condition. As illustrated in [2], KP-ABE is suitable for the scenarios where the authority decides who is the authorized users, such as the pay-TV system [2]. CP-ABE, on the other hand fits well for the cloud data sharing system because the data owner can appoint the access to the recipients [3]. Following their work, the work on attribute-based encryption have been focusing on the efficiency [4], [5], [6], [7], [8], [9], security [10], [11], [12], [13] and anonymity [14], [15], [16], [17]. At the meanwhile, Chase *et al.* [18] extended the attribute-based encryption notion to the multi authority model in which the user's attribute may be issued by multi authorities. Later, Chase *et al.* [19] enhanced the security and privacy by preventing multi authorities pooling attack. To remove the coordination among multi authorities, decentralized ABE [20] was proposed to enable any party to be an authority by issuing public keys in its domain.

Attribute-Based Encryption With Dynamic Credentials. The dynamic credentials property that enables revoking and extending attributes is critical for attribute-based encryption to be deployed in real-world scenarios. Binding the attribute set with a time interval [3], [21] is a general idea to achieve that. However, these schemes are inefficient since new secret keys are required to be regenerated for the non-revoked parties when each new time period occurs. Moreover, the revocation mechanism in these schemes are hysteresis as only in the new time period, a user can be revoked. Later, efficient revocable CP-ABE schemes were introduced to assign an unique identifier to each attribute set [22], [23], [24]. In order to enable revocation directly from the attribute-based ciphertext, Sahai *et al.* [25] proposed an ABE that supports dynamic credentials and ciphertext delegation. In their scheme, an access policy can be directly revoked from the attribute-based ciphertext by a third party. After their work, Kim *et al.* [26] proposed a modular ciphertext delegation approach for CP-ABE. Jiang *et al.* [27] introduced an updatable ABE scheme that only supports the AND gate on attributes. Unfortunately, the previous schemes [25], [26], [27] cannot protect the data integrity during the revocation phase which is critical for dynamic credentials ABE schemes. To achieve data integrity, an extendable ciphertext ABE scheme [28] was presented to extend recipients to access the original ciphertext while protects data integrity.

Attribute-Based Proxy Re-Encryption. Attribute-based proxy re-encryption (AB-PRE) [29], [30], [31], [32] enables a proxy with a token to convert a ciphertext encrypted with an access policy to another ciphertext under a new ciphertext. Yu *et al.* [33] presented an ABE scheme with attribute revocation by leveraging the technique of attribute-based proxy re-encryption. It seems that attribute-based proxy re-encryption can be adopted to achieve extending and revocation in attribute-based encryption. However, in the attribute-based proxy re-encryption setting, the ciphertext can only be converted to a ciphertext under a certain access policy which means that the data owner needs to decide the revoked access policy beforehand. Moreover. the current AB-PRE schemes cannot protect the data integrity.

1.3 Our Contribution

Our contributions are summarized as follows:

- We consider the data integrity security requirement for a revocable ABE scheme and present a formal security model that captures the data integrity property. The data integrity ensures that the underlying plaintext cannot be altered without been detected.
- We present a concrete revocable ABE scheme that enables the cloud storage to revoke recipients

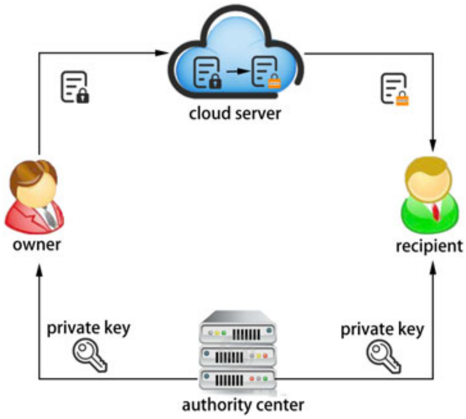


Fig. 2. System architecture of our scheme.

directly while preserves data integrity. We also prove its confidentiality and integrity under the proposed security model.

- To evaluate the performance of our proposed revocable ABE scheme, we conduct an implementation of our proposed scheme and evaluate its computation time of the key generation, encryption, revocation and decryption algorithms.

2 System Architecture and Definitions

We start with the system architecture and work flow of the proposed revocable CP-ABE scheme that provides data integrity in this section. Then we present the algorithms and security model for our scheme.

2.1 System Architecture

A revocable attribute-based encryption with data integrity (RABE-DI) system includes the following entities (Fig. 2): the original data owner, the cloud server, an authority party, and the recipients.

- The authority center (e.g., the PKG) manages the security parameters and keys for the scheme. For example, the public parameters for the system and the privates keys for the participants.
- The data owner controls the access of the shared data. To encrypt the data and upload it to the server, he encrypts the data with a ciphertext-policy attribute-based encryption.
- The cloud server (e.g., AWS) stores the ciphertexts and executes the revocation operations.
- After receiving the ciphertext, a recipient decrypts the ciphertext (original or revoked ciphertext) and also can verify the correctness of the ciphertext.

2.2 Threat Model

An adversary without a valid secret key may want to access the underlying data from the attribute-based ciphertext. A malicious cloud server may attempt to generate an incorrect revoked ciphertext that breaks the data integrity without been detected by the recipient. We refer to the former threat as data confidentiality and the latter as data integrity that will be formally described in Section 2.5. In our threat model, we assumed that the cloud server does not collude with a revoked user so that they can attempt to break the data confidentiality. Since the ciphertext is stored in the cloud server, if the cloud server collude with a revoked user by sending the revoked user an original ciphertext, the revoked user can decrypt the original ciphertext directly.

2.3 Linear Secret Sharing Scheme

A Linear secret sharing scheme (LSSS) Π over a set of parties is linear (over Z_p) if:

- every party's share is a vector over Z_p.
- There exits an $t \times k$ matrix M, and a function f, where $f(j) \in \mathcal{P}$, $j \in \{1, \ldots, t\}$. When we consider a column vector $\mu = (r, r_2, \ldots, r_k)$, where r is the secret to be shared, and $r_2, \ldots, r_k \in Z_p$ are randomly chosen, then $M \cdot \mu$ is the vector of t shares of r according to Π. The share $(M \cdot \mu)_j$ belongs to party $f(j)$.

The linear reconstruction property of LSSS scheme is defined as follows. Suppose Att be any authorized attribute set. T is the set that $T = \{j : \ f(j) \in Att\} \subset \{1, \ldots, t\}$. Then the vector $(1, 0, \ldots, 0) \in Z^k$ is in the span of vectors $\{M_j\}$ where $j \in T$, i.e., there exist constants $\{\theta_j\}_{j \in T}$, such that $\sum_{j \in T} \theta_j M_j = (1, 0, \ldots, 0)$, and $\sum_{j \in T} \theta_j M_j \cdot \mu = r$.

As illustrated in [25], an access policy (M, f) corresponds a boolean formula $\mathcal{T}$. We use $(\widetilde{M}, \widetilde{f})$ to denote the revocation access policy corresponds to $\widetilde{\mathcal{T}}$. The revoked access policy $\mathcal{T}'$ corresponding to (M', f') is $\mathcal{T}' = (\mathcal{T} \ AND \ \widetilde{\mathcal{T}})$.

2.4 Revocable CP-ABE With Data Integrity (RABE-DI)

Definition 1. *A RABE-DI scheme is composed of the following steps.*

- $Setup(\lambda, U)$: $Setup$ is executed by the authority party. And this the first step for the system initialization. A security parameter λ and the attribute universe U are the input to $Setup$. It outputs the system public parameter PP and a master secret key msk.
- $KeyGen(msk, Att)$: $KeyGen$ is also executed by the authority party. This step outputs the secret keys for participants. The master secret key msk and an attribute set Att are the input. For the outputs, it is the generated secret key sk for Att.
- $Enc(m, (M, f))$: This algorithm encrypts a message m with an access policy (M, f) and it is the step outputs a ciphertext CT.
- $Revoke(CT, (\widetilde{M}, \widetilde{f}))$: The $Revoke$ algorithm is completed by the cloud server. With the input of a ciphertext CT under access policy (M, f), a revocation access policy $(\widetilde{M}, \widetilde{f})$. The cloud server returns an revoked ciphertext CT' under access policy (M', f'). Here (M', f') corresponds to a boolean formula $\mathcal{T}' = (\mathcal{T} \ AND \ \widetilde{\mathcal{T}})$ where $\mathcal{T}$ and $\widetilde{\mathcal{T}}$ correspond to (M, f) and $(\widetilde{M}, \widetilde{f})$, respectively.
- $Dec_{or}(sk, CT)$: The Dec_{or} algorithm uses a secret key sk for the attribute set Att to decrypt a ciphertext CT under (M, f) and returns the plaintext M if $R(Att, (M, f)) = 1$.[1] If $R(Att, (M, f)) = 0$, outputs $\perp$.

[1] $R(Att, (M, f)) = 1$ means Att satisfies (M, f), while $R(Att, (M, f)) = 0$ means Att doesn't satisfy (M, f).

- $Dec_{re}(sk', CT, CT')$: The Dec_{re} algorithm takes as input a secret key sk', a ciphertext CT and a revoked ciphertext CT'. Outputs a message m if CT' is a valid revoked ciphertext. Else, outputs $\perp$.

Note that, in the definition of [25], [26], the Dec_{re} algorithm only includes sk and CT' as input. While in our scheme, the original ciphertext CT is included in the input of Dec_{re} algorithm. This is because it is impossible to construct a RABE-DI scheme without involving the original ciphertext, since the cloud server can encrypt a random message and then set it as the revoked ciphertext. One may think that, including the original ciphertext will leads a revoked recipient to decrypt the ciphertext. However, in our scheme, not the total original ciphertext CT is included in the Dec_{re} algorithm. Only a part of CT that does not contain any information about the plaintext m is included. This part is used to verify the validity of the revoked ciphertext. Moreover, as the access policy is revoked in the revoked ciphertext, the revoked recipient will not satisfy the revoked access policy. Another problem one may think is that, the cloud server may generate a ciphertext itself and then send it the recipient. This is the reason that the original ciphertext CT need to be included in the Dec_{re} algorithm. This mechanism may introduce the problem that how the recipient can get the original ciphertext since the data owner may offline. To avoid this problem, the data owner can generate a signature for each ciphertext. Thus, the cloud server cannot forge a ciphertext itself. To simplify the system model, we add the original ciphertext as input of the Dec_{re} algorithm.

2.5 Security Definitions

The security of RABE-DI requires semantic security and integrity.

Semantic Security. A RABE-DI scheme is semantic secure in the selective model if the advantage of an adversary $\mathcal{A}$ in the following game is negligible.

- Init. The attacker $\mathcal{A}$ chooses a challenge access policy (M^*, f^*).
- Setup. In this step, the challenger C generates public parameters and master secret key by executing the $Setup$ algorithm. Then, C passes public parameters to $\mathcal{A}$.
- Query. $\mathcal{A}$ makes the secret key query and gets the secret keys $sk_{Att_1}, \ldots sk_{Att_q}$, where $R(Att_j, (M^*, f^*) = 0$ for $j \in \{1, \ldots, q\}$.
- Challenge. Two plaintext (m_0, m_1) with equal length are selected by $\mathcal{A}$ and then $\mathcal{A}$ sends them to the challenger $\mathcal{C}$. $\mathcal{C}$ computes the challenge ciphertext $CT^* = Enc(m_\sigma, (M^*, f^*))$ where $\sigma \in \{0, 1\}$, and returns it to $\mathcal{A}$.
- Query. $\mathcal{A}$ continues to make the secret key query as before.
- Guess. $\mathcal{A}$ outputs its guess σ'.

The adversary $\mathcal{A}'$ advantage to win the semantic security game is defined as

$$Adv_{\mathcal{A}}^{Semantic}(\lambda) = |Pr[\sigma' = \sigma] - 1/2|.$$

Note that, the above semantic security definition requires that even an adversary $\mathcal{A}$ can obtain q private keys for different attribute sets, he cannot decrypt the challenge ciphertext that each individual private key cannot decrypt. To achieve this, in our scheme, a random value is introduced when generating a private key. Thus, even an adversary can get q private keys, it cannot decrypt the challenge ciphertext as each of the q private keys are generated with different random values. The details will be shown later in the construction Section 4.1.

Integrity. A RABE-DI scheme achieve the data integrity of the original ciphertext and the revoked ciphertext if the advantage of an adversary $\mathcal{A}$ in the following game is negligible.

- Setup. In this step, the challenger C generates public parameters and master secret key by executing the $Setup$ algorithm. Then, C passes public parameters to $\mathcal{A}$.
- Query. $\mathcal{A}$ makes the secret key query and gets the secret keys $sk_{Att_1}, \ldots sk_{Att_q}$.
- Challenge. $\mathcal{A}$ chooses a message m and access policy (M, f) and then sends them to the challenger $\mathcal{C}$. $\mathcal{C}$ sets $CT = Enc(m, (M, f))$ and sends it back to $\mathcal{A}$.
- Query. $\mathcal{A}$ can continue to make the secret key query as before.
- Output. The adversary $\mathcal{A}$ outputs a revoked ciphertext CT' and an attribute set Att'. The adversary wins if $Dec_{re}(sk_{Att'}, CT, CT') \notin \{m, \perp\}$.

The adversary $\mathcal{A}'$ advantage to win the integrity game is defined as $Pr[\mathcal{A}\ wins]$.

3 Preliminaries

3.1 Negligible Function

If for $\forall c > 0$, there exists a x_c such that $f(x) < 1/x^c$ for $\forall x > x_c$, the $f(x)$ is a negligible function.

3.2 Bilinear Pairing

A tuple (e, G, G_T, g, p) is a bilinear pairing if

(1) $e(x^u, y^v) = e(x, y)^{uv}$ for all $x, y \in G$ and $u, v \in Z_p^*$,
(2) $e(x, y) \neq 1$,
(3) $e(x, y)$ can be efficiently computed for all $x, y \in G$,

where G and G_T are multiplicative cyclic groups with order p, g is a generator of group G.

3.3 Complex Assumption

Discrete Logarithm Assumption. Let (e, G, G_T, g, p) a bilinear pairing. Given a tuple $(e, G, G_T, p, g, g^\delta)$ where $g \in G, \delta \in Z_p^*$, the discrete logarithm assumption means that the advantage of a probability polynomial time (PPT) adversary $\mathcal{A}$ to find the integer δ is negligible. Formally, the advantage of a PPT adversary $\mathcal{A}$

$$Pr[\mathcal{A}(e, G, G_T, p, g, g^\delta) = \delta],$$

is negligible.

4 Proposed RABE-DI Construction

Our RABE-DI scheme is constructed based on the expressive CP-ABE construction [11] that is semantic secure in the selective model. This section first illustrates a modified CP-

ABE construction by adding a commitment for the underlying plaintext. Second, we demonstrate that the modified CP-ABE construction is selective semantic secure. Then, we present the revocable CP-ABE with data integrity scheme.

4.1 Modified CP-ABE Construction

The modified CP-ABE construction is composed of the following four steps:

- $Setup(\lambda, U)$: The authority center generates a bilinear pairing tuple (e, G, G_T, g, p). Chooses random value $g, h_1, \dots, h_U, \phi, \varphi \in G$, $\alpha, a \in Z_p^*$ and a hash function $H : G_T \rightarrow Z_p^*$. Sets the master secret key $msk = g^{\alpha}$ and public parameters $PP = (e, G, G_T, g, h_1, \dots, h_U, \phi, \varphi, g^a, e(g, g)^{\alpha}, H)$.
- $KeyGen(msk, Att)$: The authority center chooses a random value $s \in Z_p^*$, and computes
$$sk = (Att,\ K = g^{\alpha} g^{as},\ K_0 = g^s,\ \forall x \in Att\ K_x = h_x^s).$$
- $Enc(m, (M, f))$: On input a message m and an access policy (M, f), M is an $t \times k$ matrix and f associates each row of M to an attribute. The algorithm selects two random vectors $\vec{\mu} = (r, y_2, \dots, y_k) \in Z_p^k$ and $\vec{v} = (\overline{r}, \overline{y_2}, \dots, \overline{y_k}) \in Z_p^k$. For each row M_j of M, computes $\lambda_j = \vec{\mu} \cdot M_j$ and $\overline{\lambda_j} = \vec{v} \cdot M_j,\ \ j \in [1, t]$. Randomly chooses $r_j, \overline{r_j} \in Z_p$ for each $j \in [1, t]$ and $m' \in G_T$. Then computes
$$C_1 = m \cdot e(g, g)^{\alpha r}, \quad C_2 = g^r,$$
$$C_{3,j} = g^{a\lambda_j} h_{f(j)}^{-r_j}, \quad C_{4,j} = g^{r_j}\ \forall j \in [1, t],$$
$$D_1 = m' \cdot e(g, g)^{\alpha \overline{r}}, \quad D_2 = g^{\overline{r}},$$
$$D_{3,j} = g^{a\overline{\lambda_j}} h_{f(j)}^{-\overline{r_j}}, \quad D_{4,j} = g^{\overline{r_j}}\ \forall j \in [1, t],$$
$$\overline{C} = \phi^{H(m)} \varphi^{H(m')}.$$
Outputs the ciphertext as $CT = ((M, f), C_1, C_2, C_{3,j}, C_{4,j}, D_1, D_2, D_{3,i}, D_{4,j}, \overline{C}), j \in [1, t]$.
- $Dec(sk, CT)$: On input a secret key $sk = (Att, K, K_0, K_x)$ and a ciphertext $CT = ((M, f), C_1, C_2, C_{3,j}, C_{4,j}, D_1, D_2, D_{3,j}, D_{4,j}, \overline{C})$, the recipient first checks whether $R(Att, (M, f)) = 1$. If $R(Att, (M, f)) \neq 1$, outputs an error symbol $\perp$. Otherwise, finds the set $T \subset \{1, \dots t\}$ and $T = \{j : f(j) \in Att\}$. Computes constant element $\theta_j \in Z_p^*$, such that $\sum_{j \in T} \theta_j \cdot M_j = (1, 0, \dots, 0)$. Then the recipient computes
$$m = C_1 / \frac{e(K, C_2)}{\left(\prod_{j \in T} e(K_0, C_{3,j}) \cdot e(K_{f(j)}, C_{4,j})\right)^{\theta_j}}$$
and
$$m' = D_1 / \frac{e(K, D_2)}{\left(\prod_{j \in T} e(K_0, D_{3,j}) \cdot e(K_{f(j)}, D_{4,j})\right)^{\theta_j}}.$$
Checks if $\overline{C} = \phi^{H(m)} \varphi^{H(m')}$, outputs m. Otherwise outputs an error symbol $\perp$.

Correctness. In the decryption algorithm, we have
$$\begin{aligned} &\frac{e(K, C_2)}{\left(\prod_{j \in T} e(K_0, C_{3,j}) \cdot e(K_{f(j)}, C_{4,j})\right)^{\theta_j}} \\ =&\frac{e(g^{\alpha} g^{as}, g^r)}{\left(\prod_{j \in T} e(g^s, g^{a\lambda_j} h_{f(j)}^{-r_j}) \cdot e(h_{f(j)}^s, g^{r_j})\right)^{\theta_j}} \\ =&\frac{e(g^{\alpha}, g^r) \cdot e(g^{as}, g^r)}{e(g^s, g^a)^{\sum_{j \in T} \lambda_j \theta_j}} \\ =& e(g, g)^{\alpha r}, \end{aligned}$$
and $C_1 / e(g, g)^{\alpha r} = m \cdot e(e, g)^{\alpha r} / e(g, g)^{\alpha r} = m$.

Further, the correctness of m' can be verified in the same manner.

The above modified CP-ABE scheme is selective semantic secure if the underlying Water's CP-ABE scheme [11] is semantic secure. Intuitively, the $Setup$ and $KeyGen$ algorithms is identical to that in the Water's scheme. The ciphertext consists of three part, the message ciphertext $(C_1, C_2, C_{3,j}, C_{4,j})$ which is the same as [11], a ciphertext of a random message $(D_1, D_2, D_{3,j}, D_{4,j})$, and checksum vale $\overline{C}$. The random message ciphertext part is independent to the message ciphertext, and the checksum value is a random value in G from an adversary's view that doesn't know the value m and m'.

Theorem 1. *The above modified CP-ABE scheme is semantic secure in the selective model if Water's CP-ABE scheme [11] is semantic secure in the selective model.*

Proof. Suppose an adversary $\mathcal{A}$ can break the selective semantic security of our scheme, then there exists a simulator $\mathcal{B}$ that can break the selective semantic security of the CP-ABE scheme [11] by interacting with a challenger $\mathcal{C}$. □

- Init. The simulator $\mathcal{B}$ calls adversary $\mathcal{A}$ to get a challenge access policy (M^*, f^*), and then sends (M^*, f^*) as the challenge policy to the $\mathcal{C}$.
- Setup. Simulator $\mathcal{B}$ call $\mathcal{C}$ to get $e, G, G_T, g, h_1, \dots, h_U, g^a, e(g, g)^{\alpha}$. $\mathcal{B}$ randomly chooses $\phi, \varphi \in G$ and hash function H. $\mathcal{B}$ returns the public parameters $PP = (e, G, G_T, g, h_1, \dots, h_U, g^a, e(g, g)^{\alpha}, \phi, \varphi, H)$ to $\mathcal{A}$.
- Query. When $\mathcal{A}$ issues a private key query for an attribute set Att. $\mathcal{B}$ set makes a private key query to $\mathcal{C}$ and sends the result to $\mathcal{A}$.
- Challenge. $\mathcal{A}$ submits two equal length plaintext m_0, m_1 to $\mathcal{B}$. $\mathcal{B}$ forwards m_0, m_1 to challenger $\mathcal{C}$. $\mathcal{C}$ selects a random value $\sigma \in \{0, 1\}$ and returns the challenge ciphertext of m denote as $((M^*, f^*), C_1, C_2, C_{3,j}, C_{4,j})$ to $\mathcal{B}$. The simulator $\mathcal{B}$ randomly chooses $m' \in G_T, Q \in G$ and a vector $\vec{\mu}' = (r', y_2', \dots, y_k') \in Z_p^k$. Then $\mathcal{B}$ computes $\lambda_j' = \vec{\mu}' \cdot M_j$ for each row M_j of M. $\mathcal{B}$ randomly chooses $r_j' \in Z_p$ for each $j \in [1, t]$ and computes
$$D_1 = m' \cdot e(g, g)^{\alpha r'}, \quad D_2 = g^{r'},$$
$$D_{3,j} = g^{a\lambda_j'} h_{f(j)}^{-r_j'}, \quad D_{4,j} = g^{r_j'}\ \forall j \in [1, t],$$

$\mathcal{B}$ sets $CT = ((M^*, f^*), C_1, C_2, C_{3,j}, C_{4,j}, D_1, D_2, D_{3,j}, D_{4,j}, Q)$ $j \in [1, t]$, and sends it to $\mathcal{A}$ as the challenge ciphertext.

- Query. $\mathcal{A}$ can continue to issues queries as in the previous query phase. $\mathcal{B}$ answers the queries as before in the previous query phase.
- When the adversary $\mathcal{A}$ outputs its guess σ', $\mathcal{B}$ outputs σ' as its guess.

Analysis. The simulation is perfect except that during the challenge phase. In the challenge phase, $\mathcal{B}$ returns a random value $Q \in G$ instead of the value of $\overline{C} = \phi^{H(m_\sigma)}\varphi^{H(m')}$. However, the random value Q is identical to the distribution of $\overline{C}$. Since the adversary $\mathcal{A}$ doesn't know the value of m', thus $\phi^{H(m_\sigma)}\varphi^{H(m')}$ is identical to a random value from its view.

4.2 Our RABE-DI Construction

In our revocable CP-ABE with data integrity scheme, the $Setup$, $KeyGen$, Enc and Dec_{or} algorithms are identical to the modified CP-ABE in Section 4.1. The remaining $Revoke$ and Dec_{re} algorithms are as follows.

- $Revoke(CT, (\widetilde{M}, \widetilde{f}))$: On input a ciphertext $CT = ((M, f), C_1, C_2, C_{3,j}, C_{4,j}, D_1, D_2, D_{3,j}, D_{4,j}, \overline{C})$ and a revocation access policy $(\widetilde{M}, \widetilde{f})$, where M and $\widetilde{M}$ are $t \times k$ and $\widetilde{t} \times \widetilde{k}$ matrixes, outputs a revoked ciphertext for access policy (M', f'). Sets (M', f') as

$$M' = \left(\begin{array}{c|c|c} M & -\boldsymbol{c_1} & \mathbf{0} \\ \hline \mathbf{0} & \multicolumn{2}{c}{\widetilde{M}} \end{array}\right), \quad f'(j) = \begin{cases} f(j) & j \le t \\ \widetilde{f}(j-l) & j > t \end{cases}, \tag{1}$$

where $\boldsymbol{c_1}$ is the first column of M. Note that M' is an $t' \times k'$ matrix, where $t' = t + \widetilde{t}$, $k' = k + \widetilde{k}$. Computes $C''_1 = C_1, C''_2 = C_2$,

$$\begin{cases} C''_{3,j} = C_{3,j}, & C''_{4,j} = C_{4,j} \quad j \in [1, t] \\ C''_{3,j} = 1_G, & C''_{4,j} = 1_G \quad\;\; j \in [t+1, t'] \end{cases},$$

where 1_G is the identity element of group G.

Then selects a random vector $\vec{\mu}''' = (r''', y'''_2, \ldots, y'''_{k'}) \in Z_p^{k'}$. For each row M'_j of M', computes $\lambda'''_j = \vec{\mu}''' \cdot M'_j$, $j \in [1, t']$. Randomly chooses $r'''_j \in Z_p$ for each $j \in [1, t']$. Then computes a random ciphertext CT''' as

$$C'''_1 = e(g, g)^{\alpha r'''}, \quad C'''_2 = g^{r'''},$$

$$C'''_{3,j} = g^{a\lambda'''_j} h_{f(j)}^{-r'''_j}, \quad C'''_{4,j} = g^{r'''_j} \ \forall j \in [1, t'].$$

Then, computes

$$C'_1 = C''_1 \cdot C'''_1, \quad C'_2 = C''_2 \cdot C'''_2,$$

$$C'_{3,j} = C''_{3,j} \cdot C'''_{3,j} \quad C'_{4,j} = C''_{4,j} \cdot C'''_{4,j} \ \forall j \in [1, t'].$$

The value $D'_1, D'_2, D'_{3,j}, D'_{4,j}, j \in [1, t']$ can be computed in the same manner. Sets $\overline{C}' = \overline{C}$. Finally, outputs the revoked ciphertext $CT' = ((M', f'), C'_1, C'_2, C'_{3,j}, C'_{4,j}, D'_1, D'_2, D'_{3,j}, D'_{4,j}, \overline{C}'), j \in [1, t']$).

- $Dec_{re}(sk', CT, CT')$: On input a secret sk' of attribute set Att', an original ciphertext $CT = ((M, f), C_1, C_2, C_{3,j}, C_{4,j}, D_1, D_2, D_{3,j}, D_{4,j}, \overline{C})$ and a revoked ciphertext $CT' = ((M', f'), C'_1, C'_2, C'_{3,j}, C'_{4,j}, D'_1, D'_2, D'_{3,j}, D'_{4,j}, \overline{C}')$, it verifies whether $\overline{C}' = \overline{C}$. If not, outputs an error symbol $\perp$ and abort. Then, it checks whether $R(Att', (M', f')) = 1$. If $R(Att', (M', f')) \ne 1$, outputs an error symbol $\perp$ and abort. Otherwise, finds the set $T' \subset \{1, \ldots t'\}$ and $T' = \{j : f'(j) \in Att'\}$. Computes constant element $\theta'_j \in Z_p^*$, such that $\sum_{j \in T'} \theta'_j \cdot M'_j = (1, 0, \ldots, 0)$. Then, it computes

$$m = C'_1 / \frac{e(K, C'_2)}{\left(\prod_{j \in T'} e(K_0, C'_{3,j}) \cdot e(K_{f'(j)}, C'_{4,j})\right)^{\theta'_j}}$$

and

$$m' = D'_1 / \frac{e(K, D'_2)}{\left(\prod_{j \in T'} e(K_0, D'_{3,j}) \cdot e(K_{f'(j)}, D'_{4,j})\right)^{\theta'_j}}.$$

Checks if $\overline{C}' = \phi^{H(m)}\varphi^{H(m')}$, outputs m. Otherwise outputs an error symbol $\perp$.

Correctness. The Dec_{re} algorithm is identical to that in the modified CP-ABE scheme. Thus, the Dec_{re} scheme achieves correctness if the revoked ciphertext CT' is a valid ciphertext. Next we will present that the ciphertext CT' generated in $Revoke$ algorithm is a valid ciphertext-policy attribute-based ciphertext through the following two lemmas.

Lemma 1. *If (M, f) and $(\widetilde{M}, f)$ described as above are valid access structures correspond to LSSS schemes, then (M', f') is also a valid access structure corresponds to an LSSS scheme.*

Proof. Since (M, f) and $(\widetilde{M}, f)$ are valid access structures, there exist two vectors $\theta = (\theta_1, \ldots, \theta_t) \in Z_p^t$ and $\widetilde{\theta} = (\widetilde{\theta}_1, \ldots, \widetilde{\theta}_{\widetilde{t}}) \in Z_p^{\widetilde{t}}$ that satisfy $\sum_{j \in [1,t]} \theta_j \cdot M_j = (1, 0, \ldots, 0) \in Z_p^k$ and $\sum_{j \in [1, \widetilde{t}]} \widetilde{\theta}_j \cdot \widetilde{M}_j = (1, 0, \ldots, 0) \in Z_p^{\widetilde{k}}$. Then, we can construct a vector $\theta' = (\theta'_1, \ldots, \theta'_{t'}) = (\theta_1, \ldots, \theta_t, \widetilde{\theta}_1, \ldots, \widetilde{\theta}_{\widetilde{t}}) \in Z_p^{t'}$ that satisfies $\sum_{j \in [1,t']} \theta'_j M'_j = (1, 0, \ldots, 0)$. It can be verified as

$$\begin{aligned} &\sum_{j \in [1,t']} \theta'_j M'_j \\ =&\sum_{j \in [1,t]} \theta_j M'_j + \sum_{j \in [1,\widetilde{t}]} \widetilde{\theta}_j M'_{t+j} \\ =&(\overbrace{1, 0, \ldots, 0}^{k}, \overbrace{-1, 0, \ldots, 0}^{\widetilde{k}}) + (\overbrace{0, \ldots, 0}^{k}, \overbrace{1, \ldots, 0}^{\widetilde{k}}) \\ =&(1, 0, \ldots, 0). \end{aligned}$$

□

Lemma 2. *If (M', f') described as in Equation (1) is valid access structure corresponds to an LSSS scheme, then (M, f) and $(\widetilde{M}, \widetilde{f})$ as in (1) are valid access structures correspond to LSSS schemes.*

Proof. Since (M', f') is a valid access structure, there exists a vector $\theta' = (\theta'_1, \ldots, \theta'_{t'}) \in Z_p^{t'}$ that satisfies $\sum_{j \in [1,t']} \theta'_j M'_j =$

$(1, 0, \ldots, 0) \in Z_p^{k'}$. Denote c'_j as the jth column of M' and $\theta' = (\theta, \widetilde{\theta})$, where $\theta \in Z_p^t$ and $\widetilde{\theta} \in Z_p^{t'}$. □

$$\begin{aligned} \theta' \cdot M' &= (\theta, \widetilde{\theta}) \cdot \left(\begin{array}{c|c|c} M & -\boldsymbol{c}_1 & \boldsymbol{0} \\ \hline \boldsymbol{0} & \multicolumn{2}{c}{\widetilde{M}} \end{array} \right) \\ &= (\overbrace{\theta \cdot M}^{k}, \overbrace{-e + \widetilde{\theta} \cdot \widetilde{M}}^{\widetilde{k}}) \\ &= (\overbrace{1, 0, \ldots, 0}^{k + \widetilde{k}}), \end{aligned}$$

where $e \in Z_p^{\widetilde{k}}$ is a vector whose first element is the first element of vector $\theta \cdot M$ and 0 of the left $\widetilde{k} - 1$ elements.

Since $\theta' \cdot M' = (1, 0, \ldots, 0) \in Z_p^{k'}$, then we have $\theta \cdot M = (1, 0, \ldots, 0) \in Z_p^k$ and $e = (1, 0, \ldots, 0) \in Z_p^k$. Furthermore, we can get $\widetilde{\theta} \cdot \widetilde{M} = (1, 0, \ldots, 0) \in Z_p^k$. Thus, (M, f) and $(\widetilde{M}, \widetilde{f})$ are valid access structures correspond to LSSS schemes.

Theorem 2. *The above revocable ciphertext-policy attribute-based encryption scheme is selective semantic secure if the modified CP-ABE scheme is selective semantic secure.*

Proof. In our scheme, since the original ciphertext is identical to that in the modified CP-ABE scheme, the original ciphertext achieves the semantic security as the modified CP-ABE scheme. Now we will present that the revoked ciphertext for an access policy (M', f') is identically distributed as a ciphertext generated by the $Enc((M', f'), m)$. In our RABE-DI scheme, the ciphertext CT''' is valid ciphertext for the identity element in G_T by choosing random elements $\vec{\mu}'''$, r'''_j. As $\vec{\mu}'''$, r'''_j are randomly chosen, then $\vec{\mu}' = \vec{\mu}''' + \vec{\mu}$ and $r'_j = r'''_j + r_j$ are also random values from the adversary's view. Thus the revoked ciphertext CT' is identically distributed as the ciphertext generated by the $Enc((M', f'), m')$ algorithm during which the random elements are set as $\vec{\mu}'$ and r'_j. □

Theorem 3. *The above revocable ciphertext-policy attribute-based encryption scheme achieves the data integrity if the discrete logarithm assumption holds.*

Proof. Suppose there is an adversary $\mathcal{A}$ who can break the integrity of the RABE-DI scheme, then a simulator $\mathcal{B}$, that can solve the discrete logarithm problem, can be built. The simulator's input is a discrete logarithm instance $(e, G, G_T, p, g, g^\delta)$, and his aim is to output the value δ. □

- Setup. Simulator $\mathcal{B}$ sets a bilinear pairing e, G, G_T, g, p and chooses $\alpha, a, \eta \in Z_p$, $h_1, \ldots, h_U \in G$ and a collusion resistant hash function $H : G_T \to Z_p$. $\mathcal{B}$ sets $\phi = g^\delta$, $\varphi = g^\eta$. $\mathcal{B}$ returns the public parameters $PP = (e, G, G_T, g, h_1, \ldots, h_U, g^a, e(g, g)^\alpha, \phi, \varphi, H)$ to $\mathcal{A}$.
- Query. When $\mathcal{A}$ issues a private key query for an attribute set S. Since $\mathcal{B}$ knows the mast secret key α, $\mathcal{B}$ can generate the private key and then returns it to the adversary $\mathcal{A}$.
- Challenge. $\mathcal{A}$ chooses a message m and access policy (M, f) and sends them to the challenger. The simulator $\mathcal{B}$ executes the $Enc((M, f), m)$ algorithm to get the ciphertext $CT = ((M, f), C_1, C_2, C_{3,j}, C_{4,j}, D_1, D_2, D_{3,j}, D_{4,j}, \overline{C})$, where $\overline{C} = \phi^{H(m)} \varphi^{H(m')}$. $\mathcal{B}$ returns CT to the adversary $\mathcal{A}$.
- Query. $\mathcal{A}$ can continue to issues queries as in the previous query phase. $\mathcal{B}$ answers the queries as before in the previous query phase.
- Output. The adversary $\mathcal{A}$ outputs a revoked ciphertext $CT' = ((M', f'), C'_1, C'_2, C'_{3,j}, C'_{4,j}, D'_1, D'_2, D'_{3,j}, D'_{4,j}, \overline{C}')$.

Simulator $\mathcal{B}$ chooses an attribute set Att' where $R(Att', (M', f') = 1)$. Then generates a secret key $sk_{Att'}$ using the mast secret key, and decrypts CT' with the secret key $sk_{Att'}$ to get the plaintext. Denote the plaintext as $\overline{m} = Dec_{re}(sk_{Att'}, CT, CT')$, and the random message as $\overline{m}'$. If $\mathcal{A}$ wins the integrity game, which means $\overline{m} \notin \{m, \perp\}$, i.e., $\overline{m} \neq m$ and $\overline{C} = \overline{C}'$. Then $\mathcal{B}$ can ensure that

$$\begin{aligned} \overline{C} = \overline{C}' &\Leftrightarrow \phi^{H(m)} \varphi^{H(m')} = \phi^{H(\overline{m})} \varphi^{H(\overline{m}')} \\ &\Leftrightarrow g^{\delta \cdot H(m) + \eta \cdot H(m')} = g^{\delta \cdot H(\overline{m}) + \eta \cdot H(\overline{m}')} \\ &\Leftrightarrow \delta \cdot (H(m) - H(\overline{m})) = \eta \cdot (H(\overline{m}') - H(m')). \end{aligned}$$

Finally, $\mathcal{B}$ computes $\delta = \frac{\eta \cdot (H(\overline{m}') - H(m'))}{H(m) - H(\overline{m})}$, and returns δ as its answer.

Analysis. The above simulation is perfect, the advantage of $\mathcal{B}$ to solve the discrete logarithm assumption is identical to the advantage of an adversary $\mathcal{A}$ to win in the integrity security game.

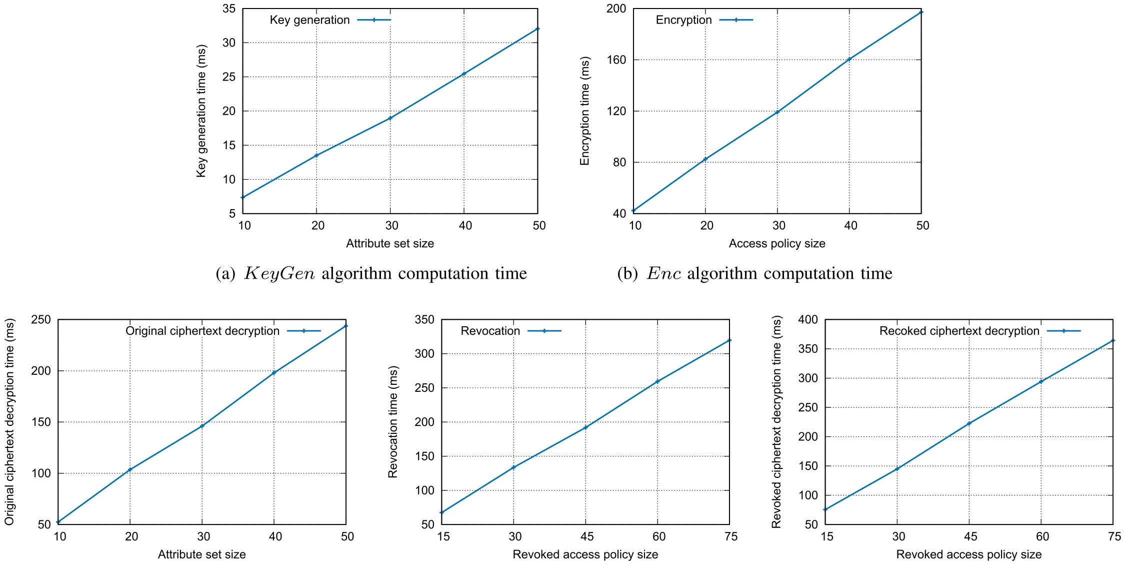
5 Performance and Evaluation

Now we illustrate the conducted evaluation of the introduced RABE-DI scheme in the perspective of computation cost. After that, we demonstrate the practicality of our scheme.

To implement our scheme, we leverage the Java Pairing-based cryptography package [34] which supports a wrapper of a C library of Pairing-based cryptography [35]. The hardware we used are two laptops with Intel(R) Core(TM) CPUs. One is i5-8520U @1.60 GHZ 1.80 GHZ with a 8 GB RAM and the other one is Intel(R) Core(TM) i7-7700HQ @2.80 GHZ 2.81 GHZ with a 16 GB RAM. The first one is used to initialize the client and the second one is for the cloud server. The operating system of the client and cloud server server are both Linux Mint 18.1 Serena. We use the type A elliptic curve $Y^2 = X^3 + X$ and the group order is 160 bit. The hash function *SHA*-256 is adopted as the hash function H of our scheme.

Implementation. In our experiment, the universal attribute set size is set to be $|U| = 1000$. We set the attribute set sized varied from 10 to 50 with a step 10 and the access policy $\mathcal{T}$ is set as the AND gate of the selected attributes during the generation of the original ciphertext. In the $Revoke$ algorithm, the size of access policy $\widetilde{T}$ in the revocation is set from 5 to 25 with a step of 5. Thus, the size of revoked access policy $\mathcal{T}' = \mathcal{T}\ AND\ \widetilde{T}$ varied form 15 to 75 with a step of 15. To get a more accurate execution time, we execute each experiment 100 times to get an average time.

Fig. 3 shows the execution time of the $Setup$, $KeyGen$, $Revoke$, Dec_{or} and Dec_{re} algorithms. It is obvious that the execution time of the algorithms are almost linear with the size of access policy/attribute set. The encryption and decryption operations under an access policy with size 50 take about only 200ms 250ms respectively. At the mean while the revocation and decryption for revoked ciphertext under an access policy sized 75 take about only 320 ms 370 ms respectively. The



(a) $KeyGen$ algorithm computation time

(b) Enc algorithm computation time

(c) Dec_{or} algorithm computation time

(d) $Revoke$ algorithm computation time

(e) Dec_{re} algorithm computation time

Fig. 3. Computation time of our proposed RABE-DI scheme.

implementation shows that the algorithms in the proposed RABE-DI scheme are efficient and practical.

6 Conclusion

In this work, we investigated the integrity requirement for revocable CP-ABE and put forward a notion of revocable CP-ABE scheme with data integrity (RABE-DI), which ensures data integrity during the revocation process. We presented a concrete RABE-DI scheme and proved its semantic security and integrity. We also conducted an implementation to demonstrate the practicality of the proposed RABE-DI scheme.

This work opens many interesting problems. One of them is to design a revocable attribute-based encryption scheme with data integrity, which achieves the replayable chosen-ciphertext security.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (Grant No. 62032025, 62076125, 61702236, 61872181), and National Key R&D Program of China (Grant No. 2020YFB1005902). This work was also supported in part by the Australian Research Council Discovery Project (DP180100665).

References

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*, 2005, pp. 457–473.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2006, pp. 89–98.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 321–334.

[4] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," in *Proc. Int. Conf. Inf. Secur. Pract. Experience*, 2009, pp. 13–23.

[5] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in *Proc. Int. Workshop Public Key Cryptogr.*, 2013, pp. 162–179.

[6] N. Attrapadung, B. Libert, and E. De Panafieu, "Expressive key-policy attribute-based encryption with constant-size ciphertexts," in *Proc. Int. Workshop Public Key Cryptogr.*, 2011, pp. 90–108.

[7] J. Herranz, F. Laguillaumie, and C. Ràfols, "Constant size ciphertexts in threshold attribute-based encryption," in *Proc. Int. Workshop Public Key Cryptogr.*, 2010, pp. 19–34.

[8] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. De Panafieu, and C. Ràfols, "Attribute-based encryption schemes with constant-size ciphertexts," *Theor. Comput. Sci.*, vol. 422, pp. 15–38, 2012.

[9] C. Chen, Z. Zhang, and D. Feng, "Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost," in *Proc. Int. Conf. Provable Secur.*, 2011, pp. 84–101.

[10] A. Lewko and B. Waters, "New proof methods for attribute-based encryption: Achieving full security through selective techniques," in *Proc. Annu. Cryptol. Conf.*, 2012, pp. 180–198.

[11] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," *Lecture Notes Comput. Sci.*, vol. 2008, pp. 321–334, 2011.

[12] J. Chen and H. Wee, "Semi-adaptive attribute-based encryption and improved delegation for Boolean formula," in *Proc. Int. Conf. Secur. Cryptogr. Netw.*, 2014, pp. 277–297.

[13] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn.*, 2010, pp. 62–91.

[14] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.*, 2008, pp. 111–129.

[15] T. V. X. Phuong, G. Yang, and W. Susilo, "Hidden ciphertext policy attribute-based encryption under standard assumptions," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, pp. 35–45, Jan. 2016.

[16] H. Cui, R. H. Deng, G. Wu, and J. Lai, "An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures," in *Proc. Int. Conf. Provable Secur.*, 2016, pp. 19–38.

[17] A. Kapadia, P. P. Tsang, and S. W. Smith, "Attribute-based publishing with hidden credentials and hidden policies," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2007, vol. 7, pp. 179–192.

[18] M. Chase, "Multi-authority attribute based encryption," in *Proc. Theory Cryptog. Conf.*, 2007, pp. 515–534.

[19] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *Proc. 16th ACM Conf. Comput. Commun. Secur.*, 2009, pp. 121–130.

[20] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn.*, 2011, pp. 568–588.

[21] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems," *J. Comput. Secur.*, vol. 18, no. 5, pp. 799–837, 2010.

[22] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Ciphertext policy attribute based encryption with efficient revocation," Univ. Waterloo, Waterloo, Canada, 2010, pp. 1–14.

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

[24] X. Xie, H. Ma, J. Li, and X. Chen, "New ciphertext-policy attribute-based access control with efficient revocation," in *Proc. Inf. Commun. Technol.-EurAsia Conf.*, 2013, pp. 373–382.

[25] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in *Proc. Annu. Cryptol. Conf.*, 2012, pp. 199–217.

[26] J. Kim, W. Susilo, J. Baek, S. Nepal, and D. Liu, "Ciphertext-delegatable CP-ABE for a dynamic credential: A modular approach," in *Proc. Australas. Conf. Inf. Secur. Privacy*, 2019, pp. 3–20.

[27] 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. Secur.*, vol. 17, no. 5, pp. 533–548, 2018.

[28] W. Susilo, P. Jiang, F. Guo, G. Yang, Y. Yu, and Y. Mu, "EACSIP: Extendable access control system with integrity protection for enhancing collaboration in the cloud," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 12, pp. 3110–3122, Dec. 2017.

[29] K. Liang, L. Fang, W. Susilo, and D. S. Wong, "A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security," in *Proc. 5th Int. Conf. Intell. Netw. Collaborative Syst.*, 2013, pp. 552–559.

[30] C. Ge, W. Susilo, J. Wang, Z. Huang, L. Fang, and Y. Ren, "A key-policy attribute-based proxy re-encryption without random oracles," *The Comput. J.*, vol. 59, no. 7, pp. 970–982, 2016.

[31] K. Liang, M. H. Au, W. Susilo, D. S. Wong, G. Yang, and Y. Yu, "An adaptively CCA-secure ciphertext-policy attribute-based proxy re-encryption for cloud data sharing," in *Proc. Int. Conf. Inf. Secur. Pract. Experience*, 2014, pp. 448–461.

[32] C. Ge, W. Susilo, L. Fang, J. Wang, and Y. Shi, "A CCA-secure key-policy attribute-based proxy re-encryption in the adaptive corruption model for DropBox data sharing system," *Des. Codes Cryptography*, vol. 86, no. 11, pp. 2587–2603, 2018.

[33] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *Proc. 5th ACM Symp. Inf. Comput. Commun. Secur.*, 2010, pp. 261–270.

[34] Nik-U, "PBC package," 2015. [Online]. Available: https://github.com/Nik-U/pbc

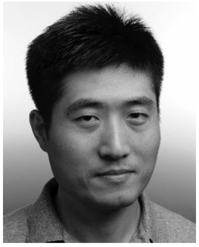
[35] B. Lynn *et al.*, "PBC library," 2006. [Online]. Available: http://crypto.stanford.edu/pbc

Chunpeng Ge (Member, IEEE) received the PhD degree in computer science from the Nanjing University of Aeronautics and Astronautics, China, in 2016. He is currently a research fellow at the University of Wollongong, Australia, and an associate professor with the Nanjing University of Aeronautics and Astronautics, China. His current research interests include cryptography, information security, and privacy preserving for blockchain. His recent work has focused on the topics of public key encryption with keyword search, proxy re-encryption, and identity-based encryption.

Willy Susilo (Fellow, IEEE) received the PhD degree in computer science from the University of Wollongong, Australia. He is currently a senior professor, the head of the School of Computing and Information Technology, and the director of the Institute of Cybersecurity and Cryptology, University of Wollongong, Australia. He has published more than 400 research papers in the area of cybersecurity and cryptology. His main research interests include cybersecurity, cryptography, and information security. He was a recipient of the prestigious Australian Research Council (ARC) Future fellow and the Researcher of the Year Award by the University of Wollongong, Australia, in 2016. He is the editor-in-chiefs of the Elsevier's Computer Standards and Interface and MDPI's Information Journal. He has served as a program committee member in dozens of international conferences. His work has been cited more than 16 000 times in Google Scholar.

Joonsang Baek (Member, IEEE) received the PhD degree from Monash University, Australia, in 2004. He is a senior lecturer with the School of Computer Science and Information Technology and a member of the Institute of Cybersecurity and Cryptology, University of Wollongong, Australia. He was a research scientist with the Institute for Infocomm Research, Singapore, and an assistant professor with the Khalifa University of Science and Technology, United Arab Emirates. His PhD thesis was on security analysis of signcryption, and has received great attention from the research community. He has published his work in numerous reputable journals and conference proceedings. His current research interests are in the field of applied cryptography and cybersecurity. He has also served as a program committee member and the chair for a number of renowned conferences on information security and cryptography.

Zhe Liu (Senior Member, IEEE) received the BS and MS degrees from Shandong University, China, in 2008 and 2011, respectively, and the PhD degree from the University of Luxembourg, Luxembourg, in 2015. He is a professor with the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, China. His research interests include security, privacy and cryptography solutions for the Internet of Things. He has co-authored more than 80 research peer-reviewed journal and conference papers. He was a recipient of the prestigious FNR Awards-Outstanding PhD Thesis Award, in 2016, ACM CHINA SIGSAC Rising Star Award, in 2017, as well as DAMO Academy Young Fellow, in 2019. He serves as program committee member in more than 60 international conferences, including program chairs in INSCRYPT 2019, CRYPTOIC 2019, and ACM CHINA SIGSAC 2020.



Jinyue Xia received the PhD degree in computer science from the University of North Carolina at Charlotte, Charlotte, North Carolina, in 2017. His current research interests include data security, cryptography and information security. His recent work has focused on the topics of public key encryption with proxy re-encryption and identity-based encryption.

Liming Fang (Member, IEEE) received the PhD degree in computer science from the Nanjing University of Aeronautics and Astronautics, China, in 2012, and has been a postdoctor in the information security from the City University of Hong Kong, Hong Kong. He is the associate professor with the School of Computer Science, Nanjing University of Aeronautics and Astronautics, China. Currently, he is a visiting scholar with the Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, New Jersey. His current research interests include cryptography and information security. His recent work has focused on the topics of public key encryption with keyword search, proxy re-encryption, and identity-based encryption.