Adaptively Secure Anonymous Identity-based Broadcast Encryption for Data Access Control in Cloud Storage Service

Liqing Chen[1, 3], Jiguo Li[1, 2, 4*] and Yichen Zhang[1, 2]

[1] College of Computer and Information, Hohai University, Nanjing 211100, Jiangsu, China

[2] College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350117, Fujian, China

[3] Faculty of Computer and Software Engineering, Huaiyin Institute of Technology, Huai'an 223003, Jiangsu, China

[4] Jiangsu Key Laboratory of Big Data Security & Intelligent Processing, Nanjing University of Posts and Telecommunications, China

Email: chenlq@hyit.edu.cn, ljg1688@163.com, zyc_718@163.com

*Corresponding author: Jiguo Li

Received March 7, 2018; revised May 13, 2018; revised October 1, 2018; accepted October 25, 2018; published March 31 2019

Abstract

Cloud computing is now a widespread and economical option when data owners need to outsource or share their data. Designing secure and efficient data access control mechanism is one of the most challenging issues in cloud storage service. Anonymous broadcast encryption is a promising solution for its advantages in the respects of computation cost and communication overload. We bring forward an efficient anonymous identity-based broadcast encryption construction combined its application to the data access control mechanism in cloud storage service. The lengths for public parameters, user private key and ciphertext in the proposed scheme are all constant. Compared with the existing schemes, in terms of encrypting and decrypting computation cost, the construction of our scheme is more efficient. Furthermore, the proposed scheme is proved to achieve adaptive security against chosen-ciphertext attack adversaries in the standard model. Therefore, the proposed scheme is feasible for the system of data access control in cloud storage service.

Keywords: identity-based cryptosystem, anonymous broadcast encryption, chosen-ciphertext attack, data access control, adaptive security, cloud computing

We would like to thank the editor and all anonymous reviewers for their valuable comments as these indeed can improve the quality of this paper. This research was supported by the National Natural Science Foundation of China (U1736112, 61772009, 61672207), Jiangsu Provincial Natural Science Foundation of China (BK20161511), Jiangsu Key Laboratory of Big Data Security & Intelligent Processing, NJUPT, and the Project of Scientific Research Innovation for College Graduate Student of Jiangsu Province (KYZZ15_0151).

http://doi.org/10.3837/tiis.2019.03.023 **ISSN : 1976-7277**

1. Introduction

Cloud computing has come into widespread adoption nowadays. Compared with the other traditional computing models, cloud computing has significant advantages in agility, scalability, flexibility, cost saving as well as energy efficiency [1,2]. Up to the present, cloud storage service is the most extensively utilized application in cloud computing. A data owner can store mass of data in cloud for saving the cost on local data management. In order to protect the data and avoid the data being compromised by cloud service provider, the data is usually encrypted by data owner before uploading to cloud service provider. However, this will bring the inconvenience of data sharing between the data owner and other designated users. Therefore, how to design both secure and efficient data access control mechanism is one of the most challenging issues in cloud storage service [3-16] and social networks [17,18].

The primitive of broadcast encryption (BE) first appeared in the literature [19], and it has become a promising mechanism for data access control which can be deployed in cloud storage service. In short, BE is an efficient cryptographic primitive for supporting a broadcaster to deliver one or more messages to a group of target receivers specified in a set through an insecure channel. In virtue of BE, a broadcaster can encrypt messages for multiple receivers within a dynamic set S and any receiver within S can decrypt the ciphertexts utilizing his/her secret key. Nevertheless, any user outside S cannot decrypt the ciphertexts. For the advantages in communication overload and computation cost, BE has received considerable both research and practical interest. Over the past decades, there has been a surge in BE application scenarios including video conference, digital rights protection, distance learning, pay cable, online database, wireless sensor networks, etc.

Two categories of BE are mainly investigated in previous studies, i.e., symmetric key BE [20] as well as public key BE (PKBE) [21]. In symmetric key BE, only the trusted authority is permitted to issue a broadcast process. Note that the trusted authority is also in charge of the distribution of users' private keys. In PKBE, any user who obtains the public parameters is permitted to send messages to a group of intended receivers. Obviously, PKBE would be more flexible for BE applications. Therefore, when speaking of BE, it generally refers to PKBE.

Shamir [22] first raised the conception of identity-based cryptosystem (IBC) in Crypto 1984. However, the first identity-based encryption (IBE) construction was put forward in the literature [23] until 2001. Subsequently, many IBE schemes were proposed [24,25]. By leveraging the idea of IBE, Delerablée [26] raised identity-based broadcast encryption (IBBE), which can be deemed as a special type of PKBE. Specifically, in IBBE, a user's public key can be denoted by a unique identity of the user, e.g. identity card number, cell-phone number, etc.

In most BE application scenarios, anonymity is a paramount security requirement, which means the identities of target receivers cannot be revealed by the receivers in the same group or by the unintended users who are not in the target group. Specifically, for achieving privacy preservation, the intended receivers' identities also need to be protected in the broadcast process. In pay cable, for example, those subscribers who are watching sensitive or adult programs certainly do not wish to reveal their identities. More concretely, they may hope their identities are anonymous not only to the users outside the program channel but also even to the users who subscribe the same program channel. Another example is that the commercial websites or brokerage companies usually do not wish to reveal their customers' identities when pushing information via broadcast. Otherwise, the competitors may take advantage of these revealed identities for precision advertising or attracting customers. However, in general PKBE/IBBE schemes [26-31], the set of intended receivers' identities is usually deemed as a default part when outputting broadcast ciphertext. Then in the decryption phase, each user

should first examine whether he/she is authorized to decrypt according to the target receiver set. Obviously, the user can naturally obtain the other target receivers' identities in the same set. Meanwhile, as the transmission of ciphertext adopts public channel, the intended receivers' identities are more easily intercepted. Hence, it is imperative that the receivers' identities are kept anonymous for protecting privacy of receivers.

Consequently, the PKBE (IBBE) schemes with anonymity or privacy preservation were proposed. To be specific, in privacy-preserving or anonymous PKBE, a user is restricted to only examine whether himself/herself is an intended receiver. In the whole broadcast process, however, the user obtains none information about the identities of the other intended receivers. Be different with general PKBE, for anonymous PKBE, the broadcast ciphertext does not involve the target receiver set. Furthermore, in anonymous PKBE, the target receiver set should not be as input of decryption algorithm. In fact, over the past decade, many studies concentrated on constructing both secure and efficient anonymous PKBE schemes.

1.1 Related Work

Barth et al. [32] first considered the privacy preservation requirement in BE and proposed two concrete PKBE schemes with sublinear ciphertext length. For protecting the receivers' identities, they introduced private broadcast encryption. The two PKBE schemes they presented can guarantee the anonymity of the target receivers in the broadcast process. Thereafter, an extensive body of literature related to privacy-preserving or anonymous PKBE existed. A receiver anonymous BE scheme with sublinear ciphertext length was proposed in the literature [33]. However, the scheme only achieved the anonymity to the outside users, but not to the intended receivers within the same set. In the literature [34], Libert et al. claimed that the property of anonymity given in [33] cannot satisfy the requirement of real-world applications. In consideration of the case that an adversary may corrupt adaptively, they gave a formal security definition for anonymous broadcast encryption. Their scheme was not efficient, because multiple ciphertext components were used as the broadcast body for achieving anonymity. The anonymous IBBE scheme raised by Hur et al. [35] achieved static security. In the decryption phase of their scheme, an intended receiver may need to try multiple times before decrypting successfully. In the literature [36], a privacy-preserving IBBE scheme was put forward while the scheme achieved adaptive security without random oracles. The anonymous IBBE scheme proposed in the literature [37] was constructed via asymmetric bilinear groups. Xie and Ren [38] proposed an IBBE scheme which only achieved anonymity to outsiders, and their scheme can resist chosen-plaintext attack (CPA) adversaries. For hiding the identities of intended receivers, the privacy-preserving PKBE scheme put forward in the literature [39] adopted Lagrange interpolation polynomial. Their scheme did not achieve security against adaptive chosen-ciphertext attack (CCA2) adversaries. More precisely, in the second phase of the security game defined in [39], the adversary is forbidden to issue decryption queries. He et al. [40] proposed an anonymous IBBE construction with CCA2 security. However, the security model defined in their paper was weak. In the same year, He et al. [41] provided a generic method for constructing anonymous IBBE schemes based on anonymous identity-based encryption (IBE). Similar with the scheme in [40], the security of generic construction was also proved under the foregoing weak security model. The security of the two privacy-preserving IBBE constructions given in the literature [42] was proved under the random oracle as well as standard model, respectively. The two schemes both achieved CPA security. Lai et al. [43] raised an anonymous IBBE construction with revocation. The decryption cost grew linearly with the amount of revoked users. Their scheme achieved CPA security. Recently, Li et al. [44] brought forward a privacy-preserving

certificate-based BE construction. Their scheme is efficient for its constant decryption cost. Furthermore, their scheme achieved anonymity and confidentiality against CCA2 adversaries simultaneously under standard assumption.

For most of the existing anonymous or privacy-preserving PKBE/IBBE schemes, the lengths of user private key, public parameters as well as ciphertext either grew linearly with the maximal number of intended receivers in the system or grew linearly with the number of current intended receivers. Besides, for some existing schemes, the amount of user private keys in the system was also linear with the maximal number of intended receivers.

1.2 Motivation

As mentioned previously, cloud computing is now a widespread and economical solution when data owners need to outsource or share their data. With the aid of cloud storage service, the data owners can expediently upload their data to the cloud or distribute their data to the designated authorized users. Benefit from the advantage of IBC, anonymous IBBE can be an efficient option for designing mechanism of data access control in cloud storage service.

Fig. 1 illustrates the system framework of data access control adopting anonymous IBBE in cloud storage service. Four entities are involved in the system framework, including data owner (DO), data users (DUs), cloud storage server (CSS) and private key generator (PKG). The data owner encrypts his/her data with a session key and then stores the encrypting result on the cloud storage server. In virtue of anonymous IBBE, the session key is broadcasted to a target set of data users by the data owner. More specifically, the data users register at the private key generator with their identities and request for authorization of access. The private key generator generates private keys for all the data users on the basis of their identities and publishes the system public parameters to the data owner as well as data users simultaneously. Then the data owner takes the authorized data users as the receivers in a target set and encrypts the session key by anonymous IBBE. The target data users can successfully decrypt the broadcast ciphertext by their own secret keys and then obtain the session key. Finally, these target data users can access and further decrypt the encrypted data with the session key. It is worth noting that, in this procedure, a target data user is unable to obtain the identities of other target data users. In other words, the anonymity of target data users can be guaranteed.

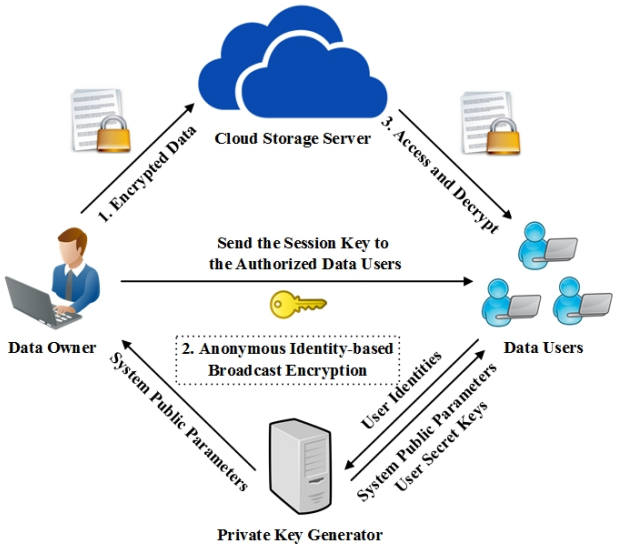

Fig. 1. System framework of data access control adopting anonymous IBBE in cloud storage service

However, in the aspect of the lengths for system public parameters, user private key as well as ciphertext, the existing anonymous PKBE/IBBE were infeasible for building data access control mechanism in cloud storage service. Besides, to achieve anonymity, most of the previous schemes adopted the technique of hiding the receivers' identities into the ciphertext. This technique would lead to high cost of decryption, because the target receivers need to find the right part in the whole ciphertext when decrypting. In other words, the target receivers may need multiple times of decryption attempts to locate their corresponding part in the whole ciphertext and output the proper broadcast message. Furthermore, it is extremely challenging to achieve CCA2 security for anonymous IBBE schemes. Therefore, our motivation is to design an efficient CCA2-secure anonymous IBBE scheme which is more suitable for constructing data access control mechanism in cloud storage service.

1.3 Our Contribution

With the aid of the composite order bilinear groups [45], we bring forward an efficient anonymous IBBE scheme which is feasible for implementing data access control mechanism in cloud storage service. In virtue of the conversion technique [46,47], the proposed scheme achieves CCA2 security under general subgroup decision assumption in the standard model. In the regard of efficiency, compared with existing anonymous PKBE/IBBE schemes, the lengths for public parameters, user private key as well as ciphertext in the proposed scheme are all constant. Further, our scheme has advantages for its low cost of encryption and decryption.

The remainder of this paper is structured as follows. Section 2 first briefs the preliminaries on composite order bilinear groups as well as general subgroup decision assumption. Then, the formal definition and security model for anonymous IBBE are provided. Section 3 presents our scheme combined its application to construct data access control mechanism in cloud storage service. The scheme's correctness is also analyzed. Section 4 discusses the scheme's security. Subsequently, the scheme's security is converted from CPA to CCA2 in Section 5. Section 6 analyzes our scheme's performance and Section 7 concludes this paper.

2. Preliminaries

2.1 Composite Order Bilinear Groups

Composite order bilinear groups first appeared in the literature [45]. Given the security parameter λ as input, the algorithm $\mathcal{G}$ generates composite order bilinear groups $(p,\mathbb{G},\mathbb{G}_T,e)$. Specifically, p denotes the product of three disparate and large primes p_1, p_2, and p_3, namely $p=p_1p_2p_3$. The two multiplicative cyclic groups $\mathbb{G}$ and $\mathbb{G}_T$ have the same order p. $e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$ denotes a bilinear map while g denotes the group $\mathbb{G}$'s generator. For a bilinear map e, the following three properties should be satisfied:

(1) Bilinearity: $e(u^a,v^b)=e(u^b,v^a)=e(u,v)^{ab}$, where $u,v\in\mathbb{G}$ and $a,b\in\mathbb{Z}_p^*$.

(2) Non-degeneracy: $e(g,g)\neq 1$.

(3) Computability: $e(u,v)$ can be computed efficiently for all $u,v\in\mathbb{G}$.

Orthogonality. Besides the above properties, the three subgroups $\mathbb{G}_{p_1}$, $\mathbb{G}_{p_2}$ as well as $\mathbb{G}_{p_3}$ in the group $\mathbb{G}$, which has order p_1, p_2 and p_3, respectively, would satisfy the additional property called orthogonality: $\forall u_i\in\mathbb{G}_{p_i}$, $\forall v_j\in\mathbb{G}_{p_j}$, $e(u_i,v_j)=1$, where $i\neq j$. Note that, this property is crucial for constructing and proving security of our proposed scheme.

2.2 General Subgroup Decision Assumption

The security of our scheme relies on the general subgroup decision (GSD) assumption [48], which consists of three static hardness assumptions. These assumptions hold based on the intractability for large integer factorization problem. Specifically, for a group order defined above, it is difficult to find its nontrivial factors. As previously mentioned, inputting the security parameter λ, the algorithm $\mathcal{G}$ generates composite order bilinear groups $(p = p_1 p_2 p_3, \mathbb{G}, \mathbb{G}_T, e)$. Hereinafter, we use $\mathbb{G}_{p_i p_j}$ to represent the subgroup with order $p_i p_j$.

Assumption 1. Let g be a randomly selected generator for the subgroup $\mathbb{G}_{p_1}$, X_3 be a randomly chosen element in the subgroup $\mathbb{G}_{p_3}$, T_0 be a randomly selected element in the subgroup $\mathbb{G}_{p_1 p_2}$, and T_1 be a randomly selected element in the subgroup $\mathbb{G}_{p_1}$. Given the tuple $D = (p, \mathbb{G}, \mathbb{G}_T, e, g, X_3)$, it is difficult to distinguish T_0 from T_1. An algorithm $\mathcal{B}$'s advantage could be defined as follows:

$$\mathrm{Adv1}_{\mathcal{B}}(\lambda) = \left|\Pr[\mathcal{B}(D, T_0) = 1] - \Pr[\mathcal{B}(D, T_1) = 1]\right|.$$

Definition 1. If for arbitrary probabilistic polynomial-time (PPT) algorithm $\mathcal{B}$, $\mathrm{Adv1}_{\mathcal{B}}(\lambda)$ is negligible, Assumption 1 holds.

Assumption 2. Let g be a randomly chosen generator for the subgroup $\mathbb{G}_{p_1}$, X_1 be a randomly chosen element in the subgroup $\mathbb{G}_{p_1}$, X_2, Y_2 be two randomly chosen elements in the subgroup $\mathbb{G}_{p_2}$, X_3, Y_3 be two randomly chosen elements in the subgroup $\mathbb{G}_{p_3}$, T_0 be a randomly selected element in the group $\mathbb{G}$, and T_1 be a randomly selected element in the subgroup $\mathbb{G}_{p_1 p_3}$. Given the tuple $D = (p, \mathbb{G}, \mathbb{G}_T, e, g, X_1 X_2, X_3, Y_2 Y_3)$, it is difficult to distinguish T_0 from T_1. An algorithm $\mathcal{B}$'s advantage could be defined as follows:

$$\mathrm{Adv2}_{\mathcal{B}}(\lambda) = \left|\Pr[\mathcal{B}(D, T_0) = 1] - \Pr[\mathcal{B}(D, T_1) = 1]\right|.$$

Definition 2. If for arbitrary PPT algorithm $\mathcal{B}$, $\mathrm{Adv2}_{\mathcal{B}}(\lambda)$ is negligible, Assumption 2 holds.

Assumption 3. Let g be a randomly chosen generator for the subgroup $\mathbb{G}_{p_1}$, X_2, Y_2, Z_2 be three randomly chosen elements from the subgroup $\mathbb{G}_{p_2}$, X_3 be a randomly chosen element from the subgroup $\mathbb{G}_{p_3}$, α, s be two randomly chosen elements in $\mathbb{Z}_p^*$, $T_0 = e(g, g)^{\alpha s}$, and T_1 be a randomly selected element in the group $\mathbb{G}_T$. Given the tuple $D = (p, \mathbb{G}, \mathbb{G}_T, e, g, X_3)$, it is difficult to distinguish T_0 from T_1. An algorithm $\mathcal{B}$'s advantage could be defined as follows:

$$\mathrm{Adv3}_{\mathcal{B}}(\lambda) = \left|\Pr[\mathcal{B}(D, T_0) = 1] - \Pr[\mathcal{B}(D, T_1) = 1]\right|.$$

Definition 3. If for arbitrary PPT algorithm $\mathcal{B}$, $\mathrm{Adv3}_{\mathcal{B}}(\lambda)$ is negligible, Assumption 3 holds.

2.3 Formal Definition

Let N be the maximum size of target receiver set. An anonymous IBBE scheme includes four algorithms as follows.

Setup(1^{λ}). After inputting the security parameter λ, the algorithm generates the public parameters *params* and system master key *MK*. The system master key *MK* is secretly held by the PKG while the system public parameters *params* are publicly released.

KeyGen$(params, MK, ID_i)$. After inputting *params*, *MK* and a user identity ID_i, where

$i \in [1, N]$, the PKG outputs the user ID_i's private key SK_i.

Encrypt$(params, S, M)$. After inputting $params$ as well as an intended receiver set $S \subseteq \{ID_1, ID_2, ..., ID_N\}$, the algorithm produces (Hdr, K), in which Hdr is often called as broadcast header while K is a session key used in a symmetric encryption algorithm. For broadcasting a certain message M to the receivers within the set S, the broadcaster first generates (Hdr, K), then calculates the ciphertext C_M on M with K, and lastly, outputs the pair (Hdr, C_M). C_M is usually called as broadcast body. The algorithm outputs final broadcast ciphertext $CT = (Hdr, C_M)$. It is worth noting that, unlike the final broadcast ciphertext in general IBBE, the set of intended receiver cannot be taken as a default part.

Decrypt$(params, CT, ID_i, SK_i)$. The input of this algorithm includes $params$, a ciphertext CT, a user's identity ID_i as well as secret key SK_i. The algorithm outputs the session key K if the user ID_i is an intended receiver. Then the message M could be recovered by decrypting the broadcast body C_M with session key K. Otherwise, the algorithm produces $\perp$.

Correctness. For arbitrary $(params, MK) \leftarrow$ **Setup**(1^λ), $SK_i \leftarrow$ **KeyGen**$(params, MK, ID_i)$, $i \in [1, N]$, $S \subseteq \{ID_1, ID_2, ..., ID_N\}$, $CT \leftarrow$ **Encrypt**$(params, S, M)$, if $ID_i \in S$, then **Decrypt**$(params, CT, ID_i, SK_i) = M$. Otherwise, **Decrypt**$(params, CT, ID_i, SK_i) = \perp$.

2.4 Security Model

For the security model of anonymous IBBE against CCA2 adversaries (ANON-CCA2), it is defined by a game which is played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$. Both the challenger $\mathcal{C}$ and the adversary $\mathcal{A}$ are provided with the maximum size of target receiver set N as well as the security parameter λ.

Setup. For obtaining $params$ and MK, $\mathcal{C}$ runs the aforementioned **Setup**(1^λ) algorithm. Then $\mathcal{C}$ holds MK secretly and sends $params$ to $\mathcal{A}$.

Phase 1. $\mathcal{A}$ adaptively issues the following two types of queries during this phase.

(1) Key generation query for user ID_i. $\mathcal{C}$ executes **KeyGen** algorithm to obtain the user ID_i's private key, then returns the user private key to $\mathcal{A}$.

(2) Decryption query for tuple (CT, ID_i) where $ID_i \in S$ and $S \subset \{ID_1, ID_2, ..., ID_N\}$. The challenger $\mathcal{C}$ executes the algorithm **Decrypt** and then returns the result to the adversary $\mathcal{A}$.

Challenge. If $\mathcal{A}$ ascertains the above **Phase 1** is finished, the adversary $\mathcal{A}$ submits two equal-size receiver sets (S_0^*, S_1^*) ($S_0^*, S_1^* \subset \{ID_1, ID_2, ..., ID_N\}$, $|S_0^*| = |S_1^*|$), as well as two equal-length broadcast messages (M_0, M_1) for challenging. The restriction is that, in **Phase 1**, no user $ID_i \in S_0^* \Delta S_1^* = (S_0^* \setminus S_1^*) \cup (S_1^* \setminus S_0^*)$ had been queried the user secret key. $\mathcal{C}$ tosses a coin b on {0,1} randomly, and then encrypts M_b on S_b^*. Finally, the adversary $\mathcal{A}$ obtains the challenge ciphertext CT^*=**Encrypt**$(params, S_b^*, M_b)$ returned from $\mathcal{C}$.

Phase 2. As similar in **Phase 1**, $\mathcal{A}$ continues to adaptively launch the following two types of queries.

(1) Key generation query for user ID_i. As similar in **Phase 1**, $\mathcal{C}$ responds the query, but with the constraint that the user $ID_i \notin S_0^* \Delta S_1^*$.

(2) Decryption query for tuple (CT, ID_i) with $ID_i \in S$ and $S \subset \{ID_1, ID_2, ..., ID_N\}$. As

similar in **Phase 1**, $\mathcal{C}$ responds the query, but with the constraint that the ciphertext $CT \neq CT^*$ and the user $ID_i \notin S_0^* \Delta S_1^*$.

Guess. Finally, $\mathcal{A}$ produces a guess $b' \in \{0,1\}$. If $b' = b$, $\mathcal{A}$ wins the game.

As shown below, we define $\mathcal{A}$'s advantage for winning the above game:

$$\mathrm{Adv}_{\mathcal{A}}^{ANON-CCA2}(\lambda) = \left| \Pr[b' = b] - \frac{1}{2} \right|.$$

Definition 4. Suppose the amount of key generation queries is q_K, and the amount of decryption queries is q_D. An anonymous IBBE scheme achieves (q_K, q_D, ε)-ANON-CCA2 security, if for arbitrary PPT adversary $\mathcal{A}$, $\mathcal{A}$'s advantage is negligible, that is $\mathrm{Adv}_{\mathcal{A}}^{ANON-CCA2}(\lambda) < \varepsilon$.

If no decryption query is permitted in the above game, then the anonymous IBBE scheme only achieves the CPA security (ANON-CPA). Similarly, the ANON-CPA security for anonymous IBBE could be defined as below.

Definition 5. Suppose the amount of key generation queries is q_K. An anonymous IBBE scheme achieves (q_K, ε)-ANON-CPA security, if for arbitrary PPT adversary $\mathcal{A}$, $\mathcal{A}$'s advantage is negligible, that is $\mathrm{Adv}_{\mathcal{A}}^{ANON-CPA}(\lambda) < \varepsilon$.

It is extremely challenging to achieve CCA2 security directly in an anonymous IBBE scheme. Fortunately, Canetti et al. [46,47] proposed an approach to convert a scheme's security from CPA to CCA2. Therefore, the strategy we take is, we first construct an anonymous CPA-secure IBBE scheme, and then promote the scheme's secure level from CPA to CCA2 by using the conversion approach.

3. Proposed Scheme and Its Application

We describe our scheme combined with its application to the data access control mechanism in cloud storage service. As illustrated in **Fig. 1**, four entities are involved in the system framework, namely data owner (DO), data users (DUs), cloud storage server (CSS) and private key generator (PKG). The access control procedure includes the following three steps.

Step 1. The DO applies a symmetric encryption algorithm (e.g. Advanced Encryption Standard) to encrypt his/her data with a randomly generated session key and stores the encrypted data on the CSS. Let **SE** denote the symmetric encryption scheme which includes two algorithms, **SE.Enc** and **SE.Dec**. Let K denote the session key and F denote the data to be encrypted. The final encrypted data stored on the CSS is $F' = \mathbf{SE.Enc}(F, K)$.

Step 2. The DO adopts anonymous IBBE scheme to send the session key K to the authorized set of DUs. Given the maximum amount of intended receivers N and the security parameter λ, the four algorithms of our scheme are described as follows.

Setup. First, the PKG runs the algorithm $\mathcal{G}(1^\lambda)$ to produce composite order bilinear groups $(p, \mathbb{G}, \mathbb{G}_T, e)$. In specific, as mentioned previously, p is the product of three disparate large primes p_1, p_2 and p_3, i.e., $p = p_1 p_2 p_3$. $\mathbb{G}$ and $\mathbb{G}_T$ are two multiplicative cyclic groups with the same order p, while e is a bilinear map with the form $e: \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. Then the PKG randomly selects $g \in \mathbb{G}_{p_1}$ as the subgroup $\mathbb{G}_{p_1}$'s generator. Besides, the PKG randomly chooses $h \in \mathbb{G}_{p_1}$ and $\alpha \in \mathbb{Z}_p^*$. Next, the PKG computes $v = e(g,g)^\alpha$. Let $H_1 : \{0,1\}^* \to \mathbb{G}_{p_1}$

denote a collision-resistant cryptographic hash function. Finally, the system public parameters are defined as $params = \{p, \mathbb{G}, \mathbb{G}_T, e, g, h, v, H_1\}$ and the system master key $MK = \alpha$.

KeyGen. Suppose the target set of DUs is $S = \{ID_{s_1}, ID_{s_2}, ..., ID_{s_n}\}$, $n \le N$. The PKG computes $u_{s_i} = H_1(ID_{s_i})$ for all $i \in [1,n]$. For a target DU, $ID_{s_i} \in S$, $i \in [1,n]$, the PKG randomly selects $r_{s_i} \in \mathbb{Z}_p^*$, $R_{s_i 0}, R'_{s_i 0}, \{R_{s_i t_j}\} \in \mathbb{G}_{p_3}$ for $t_j = s_1, s_2, ..., s_{i-1}, s_{i+1}, ..., s_n$. Then the PKG computes secret key SK_{s_i} as follows:

$$SK_{s_i} = (SK_{s_i,0}, SK_{s_i,1}, SK_{s_i,2}) = (g^{\alpha}(hu_{s_i}^{ID_{s_i}})^{r_{s_i}} R_{s_i 0}, g^{r_{s_i}} R'_{s_i 0}, \prod_{j=1, t_j \neq s_i}^{n} (u_{t_j}^{ID_{t_j}})^{r_{s_i}} R_{s_i t_j}).$$

Encrypt. Given $params$, the intended set of DUs $S = \{ID_{s_1}, ID_{s_2}, ..., ID_{s_n}\}$ and session key K, the broadcaster computes $u_{s_i} = H_1(ID_{s_i})$ for all $i \in [1,n]$, randomly selects $t \in \mathbb{Z}_p^*$, $h_1, h_2 \in \mathbb{G}_{p_2}$. Then it computes the ciphertext as below:

$$CT = (C_0, C_1, C_2) = ((h\prod_{i=1}^{n} u_{s_i}^{ID_{s_i}})^t h_1, g^t h_2, v^t K).$$

The header $Hdr = (C_0, C_1)$ and $C_M = C_2$. Note that, v is in the system public parameters and $u_{s_i}^{ID_{s_i}}$ could be pre-computed.

Decrypt. Given $params$ and $CT = (C_0, C_1, C_2)$, an intended data user ID_{s_i} decrypts with SK_{s_i} to obtain K as below:

$$K = C_2 \cdot \frac{e(SK_{s_i,1}, C_0)}{e(SK_{s_i,0} SK_{s_i,2}, C_1)}.$$

Step 3. The target DU access the encrypted data F' which is stored on the CSS, and then decrypt it with the session key K. Finally, the target DU get the original data $F = \mathbf{SE.Dec}(F', K)$.

Correctness. We primarily concern the correctness of our anonymous IBBE construction. For a target data user in the set S, all the random elements chosen in the subgroups $\mathbb{G}_{p_2}$ and $\mathbb{G}_{p_3}$ would be eliminated in the process of pairing operation according to the orthogonality property. As long as the ciphertext $CT = (C_0, C_1, C_2)$ is well-formed, the following equation must hold.

$$\begin{aligned}
&\frac{e(SK_{s_i,1}, C_0)}{e(SK_{s_i,0} SK_{s_i,2}, C_1)} \\
&= \frac{e(g^{r_{s_i}} R'_{s_i 0}, (h\prod_{i=1}^{n} u_{s_i}^{ID_{s_i}})^t h_1)}{e((g^{\alpha}(hu_{s_i}^{ID_{s_i}})^{r_{s_i}} R_{s_i 0})(\prod_{j=1, t_j \neq s_i}^{n} (u_{t_j}^{ID_{t_j}})^{r_{s_i}} R_{s_i t_j}), g^t h_2)} \\
&= \frac{e(g^{r_{s_i}} R'_{s_i 0}, (h\prod_{i=1}^{n} u_{s_i}^{ID_{s_i}})^t h_1)}{e((g^{\alpha}(hu_{s_i}^{ID_{s_i}})^{r_{s_i}} R_{s_i 0})(\prod_{j=1, t_j \neq s_i}^{n} (u_{t_j}^{ID_{t_j}})^{r_{s_i}})(\prod_{j=1, t_j \neq s_i}^{n} R_{s_i t_j}), g^t h_2)} \\
&= \frac{e(g^{r_{s_i}}, (h\prod_{i=1}^{n} u_{s_i}^{ID_{s_i}})^t h_1) e(R'_{s_i 0}, (h\prod_{i=1}^{n} u_{s_i}^{ID_{s_i}})^t h_1)}{e((g^{\alpha} R_{s_i 0})(h\prod_{j=1}^{n} u_{t_j}^{ID_{t_j}})^{r_{s_i}} (\prod_{j=1, t_j \neq s_i}^{n} R_{s_i t_j}), g^t h_2)}
\end{aligned}$$

$$= \frac{e(g^{r_{s_i}}, (h\prod_{i=1}^{n} u_{s_i}^{ID_{s_i}})^t) e(g^{r_{s_i}}, h_1) e(R'_{s_i 0}, (h\prod_{i=1}^{n} u_{s_i}^{ID_{s_i}})^t) e(R'_{s_i 0}, h_1)}{e(g^{\alpha}, g^t h_2) e(R_{s_i 0}, g^t h_2) e((h\prod_{j=1}^{n} u_{t_j}^{ID_{t_j}})^{r_{s_i}}, g^t h_2) e(\prod_{j=1, t_j \neq s_i}^{n} R_{s_i t_j}, g^t h_2)}$$

$$= \frac{e(g^{r_{s_i}}, (h\prod_{i=1}^{n} u_{s_i}^{ID_{s_i}})^t) e(g^{r_{s_i}}, h_1) e(R'_{s_i 0}, (h\prod_{i=1}^{n} u_{s_i}^{ID_{s_i}})^t) e(R'_{s_i 0}, h_1)}{e(g^{\alpha}, g^t) e(g^{\alpha}, h_2) e(R_{s_i 0}, g^t) e(R_{s_i 0}, h_2)} \cdot$$

$$\frac{1}{e((h\prod_{j=1}^{n} u_{t_j}^{ID_{t_j}})^{r_{s_i}}, g^t) e((h\prod_{j=1}^{n} u_{t_j}^{ID_{t_j}})^{r_{s_i}}, h_2) e(\prod_{j=1, t_j \neq s_i}^{n} R_{s_i t_j}, g^t) e(\prod_{j=1, t_j \neq s_i}^{n} R_{s_i t_j}, h_2)}$$

$$= \frac{1}{e(g^{\alpha}, g^t)}$$

$$= \frac{1}{v^t}$$

According to the orthogonality property, the following terms in the above expansion could be eliminated.

$$e(g^{r_{s_i}}, h_1) = 1,\ e(R'_{s_i 0}, (h\prod_{i=1}^{n} u_{s_i}^{ID_{s_i}})^t) = 1,\ e(R'_{s_i 0}, h_1) = 1$$

$$e(g^{\alpha}, h_2) = 1,\ e(R_{s_i 0}, g^t) = 1,\ e(R_{s_i 0}, h_2) = 1$$

$$e((h\prod_{j=1}^{n} u_{t_j}^{ID_{t_j}})^{r_{s_i}}, h_2) = 1,\ e(\prod_{j=1, t_j \neq s_i}^{n} R_{s_i t_j}, g^t) = 1,\ e(\prod_{j=1, t_j \neq s_i}^{n} R_{s_i t_j}, h_2) = 1$$

Then the session key K in the ciphertext could be decrypted as follows:

$$K = C_2 \cdot \frac{e(SK_{s_i,1}, C_0)}{e(SK_{s_i,0} SK_{s_i,2}, C_1)} = C_2 \cdot \frac{1}{v^t} = v^t K \cdot \frac{1}{v^t} = K.$$

Remark 1. The non-linkability (or unlinkability) is an important security property when discussing anonymity [49]. In anonymous IBBE, the non-linkability means that, for unauthorized users outside the target receiver set and the target DUs, 1) none of them could ascribe any broadcast ciphertext to a particular data user, and 2) none of them could link two different broadcast ciphertexts to the same data user. As for our scheme, the non-linkability can be assured with respect to both unauthorized users outside the target receiver set and the target DUs. Firstly, the identities of the target DUs are never transmitted in a plaintext form. Specifically, the identities of the target DUs are always embedded and combined with fresh nonce in the broadcast ciphertext. Hence, for an unauthorized user outside the target receiver set, he/she can neither associate a broadcast ciphertext with a particular data user, nor ascribe two broadcast ciphertexts to the same data user. Secondly, for a target data user, he/she can only decrypt the broadcast ciphertext successfully, thereby knowing himself/herself is in the intended receiver set. However, as mentioned previously, the identities of the target DUs are hidden in the broadcast ciphertext, a target data user cannot associate a broadcast ciphertext with another data user except himself/herself. Furthermore, the identities of the target DUs are always encrypted with fresh nonce and session key in each broadcast process, a target data user cannot ascribe two broadcast ciphertexts to the same data user except himself/herself.

Remark 2. For the data access control mechanism in cloud storage service based on the proposed anonymous IBBE scheme, the anonymity mainly refers a target data user in cloud storage service is unable to obtain the identities of other target DUs who are accessing the same cloud storage service. Specifically, the anonymity is guaranteed in virtue of the orthogonality of the bilinear map for composite order bilinear groups in the phases of secret

key generation and encryption. Then in the decryption phase, any data user is only allowed to ascertain whether himself/herself is in the intended set of DUs by decrypting the ciphertext. If he/she can decrypt successfully and obtain the session key, then it means he/she is a target data user. Otherwise, it means he/she is not a target data user. However, he/she would never know the identities of the other target DUs whether he/she is in the target set of DUs or not. The collusion resistance is another important security property to be focused when designing anonymous IBBE schemes. For the proposed scheme, it also achieves collusion resistance. As mentioned previously, a data user is constrained to test whether himself/herself is a target receiver according to the decryption result, but he/she would never know the identities of the other target receivers. As a matter of fact, even a group of data users collude, who have confirmed they are all target receivers after the decryption phase, they still cannot ascertain whether they constitute the complete set of all target receivers. In other words, they cannot figure out the identities of the other data users involved in the complete target receiver set. Because the full identities of the complete set of all target receivers are hidden in the first part of ciphertext, i.e., C_0. Moreover, it is a computationally hard problem for a group of data users if they collude and try to extract the identities of the other target receivers hidden in C_0. Therefore, the anonymity of our scheme can also be guaranteed under the attack of collusion.

Remark 3. When there are DUs leaving the system, the revoked DUs should be excluded in the target set of DUs in the encryption phase, while the immediate updating of secret keys of current DUs is not necessary. Specifically, the process of updating can be postponed to the event of new data users' join. When there is a new data user joins, the PKG needs to regenerate the secret keys for all current DUs in the secret key generation phase. The PKG bears the main computation overhead involved in the process. It is worth mentioning that, for our scheme, the trusted PKG is assumed with powerful computing ability and sufficient storage space. Hence the computation cost of lightweight DUs, whose computation ability is usually limited, can be reduced significantly. However, in the extreme case, if the number of secret key updating operations is at the same level of the broadcasting operations, the PKG who is responsible for distributing secret keys to current DUs may become the bottleneck of the system. The reason is that, in our scheme, there exists a positive correlation between the computation cost for generating a data user's private key and the amount of current data users. Therefore, it is necessary but also challenging to improve the secret key generation algorithm and reduce the computation cost of the PKG in our future work. Concretely, the computation cost for generating a data user's secret key should be independent of the amount of current data users. Ideally, the computation cost for generating a data user's secret key should be constant. In terms of communication overhead, when a data user leaves the system, as mentioned previously, there is no need to update the secret keys of current DUs immediately. Hence there is no extra communication overhead when a data user leaves the system. For the scenario of new join, we assume that, the number of current DUs including the new data user is n. Then the communication overhead when a new data user joins consists of n unicasts, in which the length of each unicast message is equal to the length of secret key for a data user.

4. Security Analysis

We prove that our scheme achieves adaptive CPA security in the aspects of confidentiality as well as anonymity without random oracles. The confidentiality means the broadcast message (for our scheme, the broadcast message refers to the session key designated by the broadcaster) should be protected, more specifically, the corresponding ciphertext of broadcast message

cannot be decrypted by the unauthorized users outside the target receiver set. While the anonymity means the identities of target receivers should be protected, more specifically, the identities of target receivers cannot be revealed by the users in the same intended receiver set or by the users outside the set of intended receivers.

The security of our scheme is proved by utilizing the dual system encryption [50] methodology. Before presenting our security proof, we first provide the definitions for semi-functional secret key as well as ciphertext, which are merely used for security proof and would not exist in the real system. Let g_2 be the subgroup $\mathbb{G}_{p_2}$'s generator. Then, the semi-functional secret key and ciphertext are defined as below.

Semi-functional key. For the user $ID_{s_i} \in S$, $i \in [1,n]$, let $(SK_{s_i,0}, SK_{s_i,1}, SK_{s_i,2})$ be a normal secret key generated by executing **KeyGen** algorithm, we randomly choose some elements $\gamma_0, \gamma_0', \{\gamma_{t_j}\} \in \mathbb{Z}_p^*$ for $t_j = s_1, s_2, ..., s_{i-1}, s_{i+1}, ..., s_n$. Then we define the semi-functional private key $\widetilde{SK}_{s_i,0} = SK_{s_i,0} g_2^{\gamma_0}$, $\widetilde{SK}_{s_i,1} = SK_{s_i,1} g_2^{\gamma_0'}$, $\widetilde{SK}_{s_i,2} = SK_{s_i,2} \prod_{j=1, t_j \neq s_i}^{n} g_2^{\gamma_{t_j}}$, which is used in the proof.

Semi-functional ciphertext. Let (C_0, C_1, C_2) denote a normal ciphertext generated via executing **Encrypt** algorithm. Subsequently, we randomly choose two elements $\lambda_1, \lambda_2 \in \mathbb{Z}_p^*$. Then we define the semi-functional ciphertext used in the proof as below:

$$\tilde{C}_0 = C_0 g_2^{\lambda_1 \lambda_2}, \ \tilde{C}_1 = C_1 g_2^{\lambda_2}, \ \tilde{C}_2 = C_2.$$

Next, we will prove that, for the following security games, no PPT adversary could distinguish them with advantage which is non-negligible under GSD assumption.

$Game_{Real}^{ANON-IBBE}$. This game is a real one, and it follows the adaptive security model for anonymous IBBE. All of the private keys and the challenge ciphertext are normal.

$Game_k^{ANON-IBBE}$. Assume that in **Phase 1** as well as **Phase 2**, the adversary could launch at most q key generation queries. Then in $Game_k^{ANON-IBBE}$ ($0 \le k \le q$), the challenge ciphertext is semi-functional, while the first k secret keys and the remainder $(q-k)$ secret keys are semi-functional and normal, respectively.

Particularly, for $Game_0^{ANON-IBBE}$, only the ciphertext for challenging is semi-functional. As for $Game_q^{ANON-IBBE}$, all of the private keys and the challenge ciphertext are semi-functional.

$Game_{Final}^{ANON-IBBE}$. For this game, all of the private keys are semi-functional. Meanwhile, the challenge ciphertext is also semi-functional, but it is an encryption on a randomly chosen element in $\mathbb{G}_T$, not the message submitted by the adversary.

Denote $\mathrm{Adv}_{\mathcal{A}}^{Game}$ as the PPT adversary $\mathcal{A}$'s advantage in a certain game. Then, we will demonstrate that the above games are indistinguishable for any PPT adversaries with a series of lemmas.

Lemma 1. Assume there exists a PPT adversary $\mathcal{A}$ which achieves $\mathrm{Adv}_{\mathcal{A}}^{Game_{Real}^{ANON-IBBE}} - \mathrm{Adv}_{\mathcal{A}}^{Game_0^{ANON-IBBE}} = \varepsilon$. Then we can build a PPT algorithm $\mathcal{B}$ to break through Assumption 1 with advantage ε.

Proof. As mentioned before, $\mathbb{G}$ and $\mathbb{G}_T$ represent two multiplicative cyclic groups with the same order $p = p_1 p_2 p_3$, in which p_1, p_2 as well as p_3 are three disparate large primes, while $e: \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a bilinear map. In addition, $g \in \mathbb{G}_{p_1}$, $L_1, L_2 \in \mathbb{G}_{p_2}$, $X_3 \in \mathbb{G}_{p_3}$. The algorithm

$\mathcal{B}$ is provided with the instantiation tuple (g, L_1, L_2, X_3, T). The algorithm $\mathcal{B}$ will simulate $Game_{Real}^{ANON-IBBE}$ or $Game_0^{ANON-IBBE}$ with the adversary $\mathcal{A}$. Then, the interaction process between $\mathcal{B}$ and $\mathcal{A}$ is described as below.

Setup. $\mathcal{B}$ selects two arbitrary elements $a, b \in \mathbb{Z}_p^*$. Let $h = g^b$ and $v = e(g,g)^a$. The cryptographic hash function $H_2 : \{0,1\}^* \to \mathbb{Z}_p^*$ is collision-resistant. Then $\mathcal{B}$ publishes the public parameters $params = \{p, \mathbb{G}, \mathbb{G}_T, e, g, h, v, H_2\}$.

Phase 1. Suppose the receiver set is $S = \{ID_{s_1}, ID_{s_2}, ..., ID_{s_n}\}$. $\mathcal{A}$ launches a key generation query for user $ID_{s_i} \in S$. $\mathcal{B}$ first computes $u_{s_i} = g^{H_2(ID_{s_i})}$ for $i \in [1,n]$, and randomly chooses some elements $r, w_0, w_0', \{w_{t_j}\} \in \mathbb{Z}_p^*$ for $t_j = s_1, s_2, ..., s_{i-1}, s_{i+1}, ..., s_n$. Then the algorithm $\mathcal{B}$ answers the adversary $\mathcal{A}$ with the following secret key:

$$SK_{s_i} = (SK_{s_i,0}, SK_{s_i,1}, SK_{s_i,2}) = (g^a (hu_{s_i}^{ID_{s_i}})^r X_3^{w_0}, g^r X_3^{w_0'}, \prod_{j=1, t_j \neq s_i}^{n} u_{t_j}^{rID_{t_j}} X_3^{w_{t_j}}).$$

The above well-formed secret key looks like a normal secret key generated by **KeyGen** algorithm. Therefore, it is a proper simulation for the secret key.

Challenge. $\mathcal{A}$ presents two messages (M_0, M_1) with equal length, together with two equal-size receiver sets $S_0^* = \{ID_{s_{01}}^*, ID_{s_{02}}^*, ..., ID_{s_{0n}}^*\}$ and $S_1^* = \{ID_{s_{11}}^*, ID_{s_{12}}^*, ..., ID_{s_{1n}}^*\}$ to the algorithm $\mathcal{B}$ for challenging. The restriction is that, in **Phase 1**, no user $ID_{s_i} \in S_0^* \Delta S_1^* = (S_0^* \setminus S_1^*) \cup (S_1^* \setminus S_0^*)$ had been queried its secret key. The algorithm $\mathcal{B}$ chooses $\sigma \in \{0,1\}$, then computes $a_{s_{\sigma i}} = H_2(ID_{s_{\sigma i}}^*)$ for $i \in [1,n]$, and sets up challenging ciphertext $CT = (C_0, C_1, C_2) = (T^{b + \sum_{i=1}^{n} a_{s_{\sigma i}} ID_{s_{\sigma i}}^*} L_1, TL_2, e(g,T)^a M_\sigma)$.

Phase 2. Be similar to **Phase 1**, $\mathcal{A}$ goes on issuing key generation query for any user ID_{s_i}, but with the constraint that the user $ID_{s_i} \notin S_0^* \Delta S_1^*$.

Guess. $\mathcal{A}$ finally submits a guess b' from $\{0,1\}$. If $b' = b$, $\mathcal{A}$ wins the game.

Observe the structure of CT, it is easy to see that, if $T \in \mathbb{G}_{p_1}$, CT is a normal ciphertext, which means $\mathcal{B}$ simulates $Game_{Real}^{ANON-IBBE}$ properly. If $T \in \mathbb{G}_{p_1 p_2}$, on the other hand, CT is a semi-functional ciphertext, which means $\mathcal{B}$ simulates $Game_0^{ANON-IBBE}$ properly. Therefore, $\mathcal{B}$ can utilize the guess of $\mathcal{A}$ to break through Assumption 1 while $\mathcal{B}$'s advantage is ε. □

Lemma 2. Assume there exists a PPT adversary $\mathcal{A}$ which launches at most q key generation queries and achieves $\mathrm{Adv}_{\mathcal{A}}^{Game_{k-1}^{ANON-IBBE}} - \mathrm{Adv}_{\mathcal{A}}^{Game_k^{ANON-IBBE}} = \varepsilon$, $k \in [1,q]$. Then we can build a PPT algorithm $\mathcal{B}$ to break through Assumption 2 with advantage ε.

Proof. As mentioned before, $\mathbb{G}$ and $\mathbb{G}_T$ represent two multiplicative cyclic groups with the same order $p = p_1 p_2 p_3$, in which p_1, p_2 as well as p_3 are three disparate large primes, while $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a bilinear map. In addition, $g, X_1 \in \mathbb{G}_{p_1}$, $X_2, Y_2, L_1, L_2 \in \mathbb{G}_{p_2}$, $X_3, Y_3 \in \mathbb{G}_{p_3}$. The algorithm $\mathcal{B}$ is provided with the instantiation tuple $(g, X_1 X_2, X_3, Y_2 Y_3, L_1, L_2, T)$. The algorithm $\mathcal{B}$ will simulate $Game_{k-1}^{ANON-IBBE}$ or $Game_k^{ANON-IBBE}$ with the adversary $\mathcal{A}$. Then, the interaction process between the algorithm $\mathcal{B}$ and the adversary $\mathcal{A}$ is described as below.

Setup. The algorithm $\mathcal{B}$ selects two arbitrary elements $a,b\in\mathbb{Z}_p^*$. Let $h=g^b$ and $v=e(g,g)^a$. The cryptographic hash function $H_2:\{0,1\}^*\to\mathbb{Z}_p^*$ is collision-resistant. Then $\mathcal{B}$ publishes the public parameters $params=\{p,\mathbb{G},\mathbb{G}_T,e,g,h,v,H_2\}$.

Phase 1. Suppose the receiver set is $S=\{ID_{s_1},ID_{s_2},...,ID_{s_n}\}$. The adversary $\mathcal{A}$ launches a key generation query for user $ID_{s_i}\in S$. According to the relationship between s_i and k, the algorithm $\mathcal{B}$ answers the adversary $\mathcal{A}$ with one of the three cases as follows.

Case 1: $s_i<k$. The algorithm $\mathcal{B}$ first computes $u_{s_i}=g^{H_2(ID_{s_i})}$ for $i\in[1,n]$, and randomly selects some elements $r,w_0,w_0',\{w_{t_j}\}\in\mathbb{Z}_p^*$ for $t_j=s_1,s_2,...,s_{i-1},s_{i+1},...,s_n$. Then it sets user ID_{s_i}'s secret key $SK_{s_i}=(SK_{s_i,0},SK_{s_i,1},SK_{s_i,2})=(g^a(hu_{s_i}^{ID_{s_i}})^r(Y_2Y_3)^{w_0},g^r(Y_2Y_3)^{w_0'},\prod_{j=1,t_j\neq s_i}^{n}u_{t_j}^{rID_{t_j}}(Y_2Y_3)^{w_{t_j}})$.

The above well-formed secret key looks like a normal secret key generated by **KeyGen** algorithm. Therefore, it is a proper simulation for the secret key.

Case 2: $s_i=k$. The algorithm $\mathcal{B}$ first randomly selects some elements $w_0,\{w_{t_j}\}\in\mathbb{Z}_p^*$ for $t_j=s_1,s_2,...,s_{i-1},s_{i+1},...,s_n$. The algorithm $\mathcal{B}$ computes $a_k=H_2(ID_k)$ and $a_{t_j}=H_2(ID_{t_j})$ for $t_j=s_1,s_2,...,s_{i-1},s_{i+1},...,s_n$. Then it sets user ID_{s_i}'s secret key as follows:

$$SK_{s_i}=(SK_{s_i,0},SK_{s_i,1},SK_{s_i,2})=(g^aT^{b+a_kID_k}X_3^{w_0},T,\prod_{j=1,t_j\neq s_i}^{n}T^{a_{t_j}ID_{t_j}}X_3^{w_{t_j}}).$$

Observe the structure of SK_{s_i}, it is easy to see that, if $T\in\mathbb{G}_{p_1p_3}$, SK_{s_i} is a normal private key for the user ID_{s_i}. If $T\in\mathbb{G}$, SK_{s_i} is a semi-functional private key for the user ID_{s_i}.

Case 3: $s_i>k$. The algorithm $\mathcal{B}$ runs the algorithm **KeyGen** to generate the normal private key for the user ID_{s_i}.

Challenge. $\mathcal{A}$ presents two messages (M_0,M_1) with equal length, together with two equal-size receiver sets $S_0^*=\{ID_{s_{01}}^*,ID_{s_{02}}^*,...,ID_{s_{0n}}^*\}$ and $S_1^*=\{ID_{s_{11}}^*,ID_{s_{12}}^*,...,ID_{s_{1n}}^*\}$ to the algorithm $\mathcal{B}$ for challenging. The restriction is that, in **Phase 1**, no user $ID_{s_i}\in S_0^*\Delta S_1^*=(S_0^*\setminus S_1^*)\cup(S_1^*\setminus S_0^*)$ had been queried its secret key. The algorithm $\mathcal{B}$ chooses $\sigma\in\{0,1\}$, then computes $a_{s_{\sigma i}}=H_2(ID_{s_{\sigma i}}^*)$ for $i\in[1,n]$, and sets up the challenging ciphertext $CT=(C_0,C_1,C_2)=((X_1X_2)^{b+\sum_{i=1}^{n}a_{s_{\sigma i}}ID_{s_{\sigma i}}^*}L_1,X_1X_2L_2,e(g,X_1X_2)^aM_\sigma)$.

Phase 2. As similar in in **Phase 1**, $\mathcal{A}$ goes on launching key generation query for any user ID_{s_i}, but with the constraint that the user $ID_{s_i}\notin S_0^*\Delta S_1^*$.

Guess. $\mathcal{A}$ finally submits a guess b' from $\{0,1\}$. If $b'=b$, $\mathcal{A}$ wins the game.

We can easily see that, if $T\in\mathbb{G}_{p_1p_3}$, which means $\mathcal{B}$ simulates $Game_{k-1}^{ANON-IBBE}$ properly. If $T\in\mathbb{G}$, on the other hand, which means $\mathcal{B}$ simulates $Game_k^{ANON-IBBE}$ properly. Therefore, $\mathcal{B}$ can utilize the guess of $\mathcal{A}$ to break through Assumption 2 while $\mathcal{B}$'s advantage is ε. □

Lemma 3. Assume there exists a PPT adversary $\mathcal{A}$ which achieves $\mathrm{Adv}_{\mathcal{A}}^{Game_q^{ANON-IBBE}}-\mathrm{Adv}_{\mathcal{A}}^{Game_{Final}^{ANON-IBBE}}=\varepsilon$. Then a PPT algorithm $\mathcal{B}$ can be built, which can break through Assumption 3 with advantage ε.

Proof. As mentioned before, $\mathbb{G}$ and $\mathbb{G}_T$ represent two multiplicative cyclic groups with the same order $p = p_1 p_2 p_3$, in which p_1, p_2 as well as p_3 are three disparate large primes, while $e: \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a bilinear map. In addition, $g \in \mathbb{G}_{p_1}$, $X_2, Y_2, Z_2, L_1, L_2 \in \mathbb{G}_{p_2}$, $X_3 \in \mathbb{G}_{p_3}$, $a, s \in \mathbb{Z}_p^*$. The algorithm $\mathcal{B}$ is given the instantiation tuple $(g, g^a X_2, X_3, g^s Y_2, Z_2, L_1, L_2, T)$. The algorithm $\mathcal{B}$ will simulate $Game_q^{ANON-IBBE}$ or $Game_{Final}^{ANON-IBBE}$ with the adversary $\mathcal{A}$. Then, the interaction process between the algorithm $\mathcal{B}$ and the adversary $\mathcal{A}$ is as below.

Setup. The algorithm $\mathcal{B}$ selects a random element $b \in \mathbb{Z}_p^*$. Let $h = g^b$ and $v = e(g^a X_2, g)$. The cryptographic hash function $H_2 : \{0,1\}^* \to \mathbb{Z}_p^*$ is collision-resistant. Then $\mathcal{B}$ publishes the public parameters $params = \{p, \mathbb{G}, \mathbb{G}_T, e, g, h, v, H_2\}$.

Phase 1. Suppose the receiver set is $S = \{ID_{s_1}, ID_{s_2}, ..., ID_{s_n}\}$. The adversary $\mathcal{A}$ issues a key generation query for user $ID_{s_i} \in S$. The algorithm $\mathcal{B}$ first computes $u_{s_i} = g^{H_2(ID_{s_i})}$ for $i \in [1, n]$, and randomly chooses some elements $r, w_0, w_0', \{w_{t_j}\}, y_0, y_0', \{y_{t_j}\} \in \mathbb{Z}_p^*$ for $t_j = s_1, s_2, ..., s_{i-1}, s_{i+1}, ..., s_n$. Then the algorithm $\mathcal{B}$ answers the adversary $\mathcal{A}$ with the secret key

$$SK_{s_i} = (SK_{s_i,0}, SK_{s_i,1}, SK_{s_i,2}) = (g^a X_2 Z_2^{y_0} (h u_{s_i}^{ID_{s_i}})^r X_3^{w_0}, g^r Z_2^{y_0'} X_3^{w_0'}, \prod_{j=1, t_j \neq s_i}^{n} u_{t_j}^{rID_{t_j}} Z_2^{y_{t_j}} X_3^{w_{t_j}}).$$

The above well-formed secret key looks like a normal secret key generated by **KeyGen** algorithm. Therefore, it is a proper simulation for the secret key.

Challenge. $\mathcal{A}$ presents two messages (M_0, M_1) with equal length, together with two equal-size receiver sets $S_0^* = \{ID_{s_{01}}^*, ID_{s_{02}}^*, ..., ID_{s_{0n}}^*\}$ and $S_1^* = \{ID_{s_{11}}^*, ID_{s_{12}}^*, ..., ID_{s_{1n}}^*\}$ to $\mathcal{B}$ for challenging. The restriction is that, in **Phase 1**, no user $ID_{s_i} \in S_0^* \Delta S_1^* = (S_0^* \setminus S_1^*) \cup (S_1^* \setminus S_0^*)$ had been queried its secret key. The algorithm $\mathcal{B}$ chooses $\sigma \in \{0,1\}$, then computes $a_{s_{\sigma i}} = H_2(ID_{s_{\sigma i}}^*)$ for $i \in [1, n]$, and further sets up the final ciphertext for challenging as below:

$$CT = (C_0, C_1, C_2) = ((g^s Y_2)^{b + \sum_{i=1}^{n} a_{s_{\sigma i}} ID_{s_{\sigma i}}^*} L_1, g^s Y_2 L_2, TM_\sigma).$$

Phase 2. Be similar to **Phase 1**, $\mathcal{A}$ goes on launching key generation query for any user ID_{s_i}, but with the constraint that the user $ID_{s_i} \notin S_0^* \Delta S_1^*$.

Guess. $\mathcal{A}$ finally submits a guess b' from $\{0,1\}$. If $b' = b$, $\mathcal{A}$ wins the game.

Observe the structure of CT, it is easy to see that, if $T = e(g,g)^{as}$, CT is a proper semi-functional ciphertext, which means the algorithm $\mathcal{B}$ simulates $Game_q^{ANON-IBBE}$ properly. But if T is a randomly chosen element in $\mathbb{G}_T$, then CT is a proper semi-functional ciphertext for a randomly chosen element, which means $\mathcal{B}$ simulates $Game_{Final}^{ANON-IBBE}$ properly. Therefore, $\mathcal{B}$ can utilize $\mathcal{A}$'s guess to break through Assumption 3 with the advantage ε.

Theorem 1. Denote $\mathbb{G}$ as a group with composite order p. There exists an efficient bilinear map on $\mathbb{G}$. If Assumption 1, Assumption 2 as well as Assumption 3 are all valid in $\mathbb{G}$, the proposed anonymous IBBE scheme is ANON-CPA secure.

Proof. If Assumption 1, Assumption 2 as well as Assumption 3 are all valid in $\mathbb{G}$, an adversary's advantage in the real game is negligible according to Lemma 1, Lemma 2 and Lemma 3. Therefore, the proposed anonymous IBBE scheme is ANON-CPA secure.

Remark 4. It's worth noting that, on the basis of the security model for anonymous IBBE presented in Section 2.4, the security requirement of confidentiality and anonymity is combined in one game by submitting two equal-size receiver sets and two equal-length broadcast messages for challenging at the same time. Therefore, the above security analysis proved both the confidentiality and the anonymity of our scheme simultaneously.

5. Conversion from CPA to CCA2

In this section, we promote our scheme's security from CPA to CCA2 by using the conversion approach in [46,47]. For simplicity, we only give the construction sketch for the new scheme. The algorithms of **Setup**, **KeyGen**, **Encrypt** as well as **Decrypt** have been described previously (cf. Section 2.3).

Let **Sig** = (**Gen**, **Sign**, **Verify**) denote a one-time signature scheme with strong unforgeability, which means it is impossible for an adversary to fabricate a new and valid signature on the message which is signed previously. The construction process is as below.

Step 1. The PKG runs **Setup**(1^{λ}) algorithm to produce the system master key MK as well as the public parameters $params$.

Step 2. The PKG runs the algorithm **KeyGen**$(params, MK, ID_i)$ to produce the user private key SK_i for the user ID_i.

Step 3. Given the message M and the receiver set S, firstly, the broadcaster executes **Gen**(1^{λ}) algorithm to get vk and sk, which are two keys used for verification and signing, respectively. vk is regarded as a dummy receiver in S. Let $S' = S \cup \{vk\}$. Then the broadcaster runs the algorithm **Encrypt**$(params, S', M)$ to get ciphertext CT', and executes **Sign**$_{sk}(CT')$ algorithm to get signature φ. The final outputted ciphertext is $CT = (vk, CT', \varphi)$.

Step 4. For decrypting CT, the user ID_i first tests whether **Verify**$_{vk}(CT', \varphi) \stackrel{?}{=} 1$ holds. If it does not hold, the user outputs $\perp$ directly. Otherwise, the user ID_i executes the algorithm **Decrypt**$(params, CT', ID_i, SK_i)$ to recover the message M.

The reader may refer the proof of correctness and effectiveness for the above conversion in [46]. With the conversion, the security level of our scheme is enhanced from CPA to CCA2.

6. Performance Analysis

Table 1 and **Table 2** show the efficiency comparison of our scheme with the existing representative (anonymous) PKBE/IBBE schemes. As defined above, N represents the maximum size of set for intended receivers, while n represents the size of current set for intended receivers, $n \le N$. The PKBE/IBBE schemes in [26,28-30,35] adopted prime order bilinear groups. For prime order bilinear groups, P_1 denotes bilinear pairing operation, E_1 and M_1 respectively denote exponentiation and multiplication operation in $\mathbb{G}$, while E_2 and M_2 respectively denote exponentiation and multiplication operation in $\mathbb{G}_T$. Similarly, for composite order bilinear groups, P_2 denotes bilinear pairing operation, E_3 and M_3 respectively denote exponentiation and multiplication operation in $\mathbb{G}$, while E_4 and M_4 respectively denote exponentiation and multiplication operation in $\mathbb{G}_T$. Note that, for ease of description, in composite order bilinear groups, we do not distinguish between the operations in the group $\mathbb{G}$

and in the subgroups $\mathbb{G}_{p_1}$, $\mathbb{G}_{p_2}$ and $\mathbb{G}_{p_3}$. Namely, the operations in $\mathbb{G}$ are substituted for the operations in $\mathbb{G}_{p_1}$, $\mathbb{G}_{p_2}$ and $\mathbb{G}_{p_3}$. Prime+Bilinear and Composite+Bilinear respectively represent the prime order and composite order bilinear map.

Table 1. Efficiency comparison between our and other (anonymous) PKBE/IBBE schemes (I)

Scheme	Public parameters size	Private key size	Private key amount	Ciphertext size	Encryption cost	Decryption cost
[26]	$O(N)$	$O(1)$	N	$O(1)$	$2E_1+E_2$	$2P_1+2E_2+M_2$
[28] I	$O(N)$	$O(N)$	N	$O(1)$	$P_1+2E_1+E_2+nM_1$	$2P_1+nM_1$
[28] II	$O(N)$	$O(N)$	N	$O(1)$	$P_1+3E_1+2E_2$	$2P_1+3E_1+E_2+2M_1$
[29]	$O(N)$	$O(N)$	n	$O(1)$	$3P_1+(n+3)E_1+3E_2+(n+1)M_1$	$2P_1+(n+2)E_1$
[30]	$O(1)$	$O(1)$	n	$O(1)$	$2P_1+2E_1+2E_2$	$P_1+E_1+E_2+M_1$
[31]	$O(N)$	$O(N)$	N	$O(1)$	$5E_3+E_4+M_3+M_4$	$4P_2+nE_3$
[35]	$O(1)$	$O(1)$	n	$O(n)$	$(n+1)P_1+(2n+2)E_1+E_2$	$nP_1+n/2E_1+n/2M_1$
[36]	$O(N)$	$O(N)$	n	$O(1)$	$(n+1)E_3+E_4+2M_3$	$2P_2+(n-1)E_3$
[39]	$O(\log_2 N)$	$O(1)$	n	$O(n)$	$(n+1)E_3+E_4+(3n+1)M_3$	$2P_2+(n-1)M_3$
Our scheme	$O(1)$	$O(1)$	n	$O(1)$	$2E_3+E_4+3M_3+M_4$	$2P_2+M_3$

Table 2. Efficiency comparison between our and other (anonymous) PKBE/IBBE schemes (II)

Scheme	Decryption attempt times	Arbitrary broadcaster	Dynamic membership	Identity-based	Map type
[26]	1	Yes	Yes	Yes	Prime+Bilinear
[28] I	1	Yes	No	No	Prime+Bilinear
[28] II	1	Yes	Yes	Yes	Prime+Bilinear
[29]	1	Yes	No	Yes	Prime+Bilinear
[30]	1	No	Yes	Yes	Prime+Bilinear
[31]	1	Yes	No	Yes	Composite+Bilinear
[35]	$n/2$	Yes	Yes	Yes	Prime+Bilinear
[36]	1	Yes	No	Yes	Composite+Bilinear
[39]	1	Yes	Yes	No	Composite+Bilinear
Our scheme	1	Yes	Yes	Yes	Composite+Bilinear

Table 1 shows that, the sizes of public parameters, user secret key as well as ciphertext in our scheme and the scheme in [30] are all constant. However, the scheme in [30] did not consider the anonymity of target receivers. **Table 2** shows that, the scheme in [26], the second scheme in [28] and our scheme all need only one decryption attempt, support arbitrary broadcaster as well as dynamic membership, and are identity-based. However, neither the scheme in [26] nor the second scheme in [28] achieved anonymity.

Furthermore, we implement our scheme and other three existing anonymous PKBE/IBBE schemes [35,36,39] utilizing the well-known PBC (Pairing-Based Cryptography) Library[1] (version 0.5.14). For simplicity, the operations for exponentiation, multiplication as well as bilinear pairing in the phased of encryption and decryption are emphasized. We choose type-A and type-A1 as the elliptic curve parameter for prime order and composite order bilinear groups, respectively. The orders of groups are all 160-bit. As for the experiment environment

[1] The PBC Library can be downloaded from https://crypto.stanford.edu/pbc/.

the host configuration of includes 2.3 GHz Intel i7 CPU, 8 GB RAM and 64-bit Windows 10, while the configuration of virtual machine (VMware 10.0.1) includes single CPU, 4 GB RAM and Ubuntukylin-15.10-desktop-i386.

Fig. 2 and **Fig. 3** illustrate the efficiency comparison between our scheme and other three anonymous PKBE/IBBE schemes. It is easy to see that, for our scheme, both the encryption and decryption time are the lowest. As a matter of fact, though added the security of anonymity, our scheme still has advantages over encryption and decryption costs, compared with those general PKBE/IBBE schemes, e.g., the scheme in [31] which was also constructed from composite order bilinear groups (cf. **Table 1**). Therefore, the proposed scheme is feasible for constructing data access control mechanism in cloud storage service. The security of our scheme and existing (anonymous) PKBE/IBBE schemes are compared in **Table 3**. The related hardness assumptions are explained as follows.

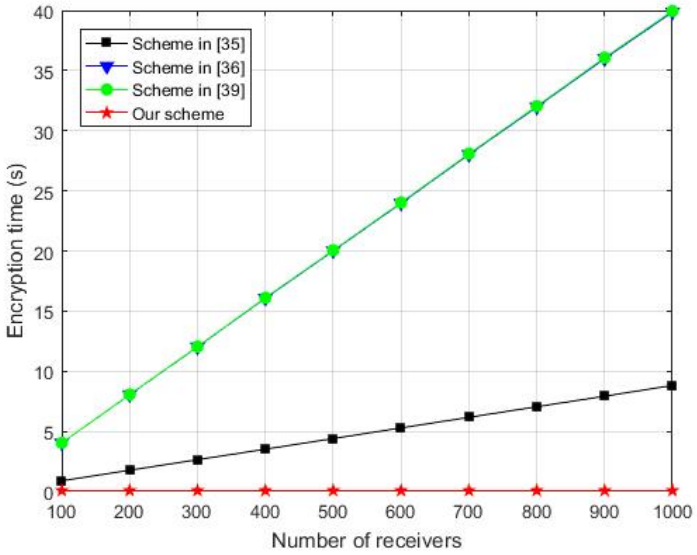

Fig. 2. Encryption time comparison between our and other three anonymous PKBE/IBBE schemes

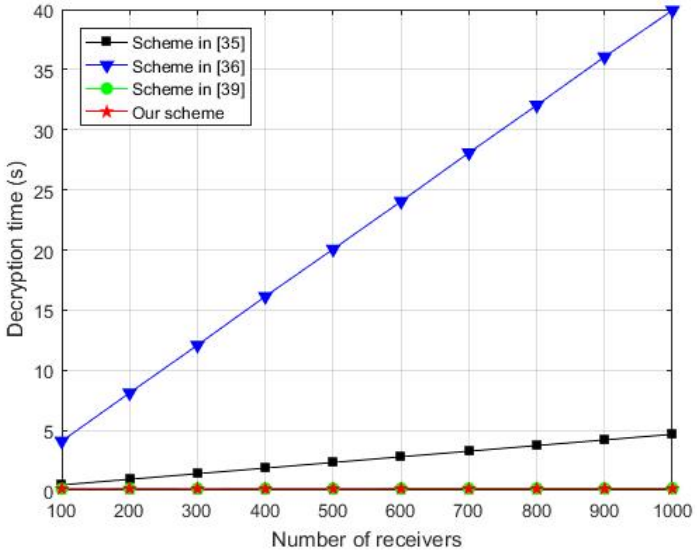

Fig. 3. Decryption time comparison between our and other three anonymous PKBE/IBBE schemes

GDDHE: general decisional Diffie-Hellman exponent. *q*-BDHE: decision *q*-bilinear Diffie-Hellman exponent. *q*-TBDHE: decisional truncated *q*-bilinear Diffie-Hellman exponent. *q*-ABDHE: truncated decisional *q*-augmented bilinear Diffie-Hellman exponent. GSD: general subgroup decision. BDH: bilinear Diffie-Hellman. SDA: subgroup decisional assumption. Composite DBDH: composite decisional bilinear Diffie-Hellman.

Table 3. Security comparison between our and other (anonymous) PKBE/IBBE schemes

Scheme	Anonymity	Security type	Adversary type	Standard model	Hardness assumption
[26]	No	Static	CPA	No	GDDHE
[28] I	No	Semi-static	CPA	Yes	*q*-BDHE
[28] II	No	Adaptive	CPA	Yes	*q*-BDHE
[29]	No	Adaptive	CCA2	Yes	*q*-TBDHE
[30]	No	Adaptive	CCA2	Yes	*q*-ABDHE
[31]	No	Adaptive	CPA	Yes	GSD
[35]	Yes	Static	CPA	No	BDH
[36]	Yes	Adaptive	CPA	Yes	GSD
[39]	Yes	Adaptive	CCA1[2]	Yes	SDA, Composite DBDH
Our scheme	Yes	Adaptive	CCA2	Yes	GSD

As shown in **Table 3**, only our scheme achieves CCA2 security as well as anonymity in the standard model simultaneously. Furthermore, the security of our scheme is built on GSD assumption, which is static and simple.

7. Conclusion

We bring forward an efficient anonymous IBBE scheme with CCA2 security. Compared with the previous anonymous PKBE/IBBE schemes, our scheme is more feasible for constructing data access control mechanism in cloud storage service, as the lengths of public parameters, user private key and ciphertext are all constant. In terms of computation cost, our scheme also has advantage. Furthermore, based on general subgroup decision assumption, the security of our scheme is proved in the standard model.

Generally, compared with the more commonly used prime order bilinear groups, the computation efficiency of composite order bilinear groups is not satisfactory. Besides, the CCA2 security in our scheme is not obtained directly. Therefore, it is challenging for us in the future to design more efficient anonymous IBBE schemes in virtue of prime order bilinear groups, which can achieve CCA2 security directly. Besides, the construction of anonymous IBBE schemes with leakage resilience [51,52] is another interesting issue.

References

[1] B. Hayes, "Cloud computing," *Communications of the ACM*, vol. 51, no. 7, pp. 9-11, 2008. Article (CrossRef Link).

[2] J. Li, H. Yan and Y. Zhang, "Certificateless public integrity checking of group shared data on cloud storage," *IEEE Transactions on Services Computing*, 2018, Article (CrossRef Link).

[2] CCA1 security means that, in the second query phase, the adversary is forbidden to issue decryption queries.

[3] H. Yan, J. Li, J. Han and Y. Zhang, "A novel efficient remote data possession checking protocol in cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 78-88, 2017. Article (CrossRef Link).
[4] J. Li, X. Lin, Y. Zhang and J. Han, "KSF-OABE: outsourced attribute-based encryption with keyword search function for cloud storage," *IEEE Transactions on Services Computing*, vol. 10, no. 5, pp. 715-725, 2017. Article (CrossRef Link).
[5] J. Li, W. Yao, Y. Zhang, H. Qian and J. Han, "Flexible and fine-grained attribute-based data storage in cloud computing," *IEEE Transactions on Services Computing*, vol. 10, no. 5, pp. 785-796, 2017. Article (CrossRef Link).
[6] Y. Lu and J. Li, "A pairing-free certificate-based proxy re-encryption scheme for secure data sharing in public clouds," *Future Generation Computer Systems*, vol. 62, pp. 140-147, 2016. Article (CrossRef Link).
[7] J. Li, W. Yao, J. Han, Y. Zhang and J. Shen, "User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage," *IEEE Systems Journal*, vol. 12, no. 2, pp. 1767-1777, 2018. Article (CrossRef Link).
[8] C. Zuo, J. Shao, J.K. Liu, G. Wei and Y. Ling, "Fine-grained two-factor protection mechanism for data sharing in cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 1, pp. 186-196, 2018. Article (CrossRef Link).
[9] C. Zuo, J. Shao, G. Wei, M. Xie and M. Ji, "CCA-secure ABE with outsourced decryption for fog computing," *Future Generation Computer Systems*, vol. 78, pp. 730-738, 2018. Article (CrossRef Link).
[10] J. Li, Y. Wang, Y. Zhang and J. Han, "Full verifiability for outsourced decryption in attribute based encryption," *IEEE Transactions on Services Computing*, 2018, DOI: 10.1109/TSC.2017.2710190. Article (CrossRef Link).
[11] H. Qian, J. Li, Y. Zhang and J. Han, "Privacy preserving personal health record using multi-authority attribute-based encryption with revocation," *International Journal of Information Security*, vol. 14, no. 6, pp. 487-497, 2015. Article (CrossRef Link).
[12] J. Li, Y. Shi and Y. Zhang, "Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage," *International Journal of Communication Systems*, vol. 30, no. 1, pp. e2942, 2017. Article (CrossRef Link).
[13] J. Ning, X. Dong, Z. Cao, L. Wei and X. Lin, "White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1274-1288, 2015. Article (CrossRef Link).
[14] J. Ning, Z. Cao, X. Dong, H. Ma, L. Wei and K. Liang, "Auditable σ-times outsourced attribute-based encryption for access control in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 1, pp. 94-105, 2018. Article (CrossRef Link).
[15] J. Li, Q. Yu and Y. Zhang, "Hierarchical attribute based encryption with continuous leakage-resilience," *Information Sciences*, vol. 484, pp. 113–134, 2019. Article (CrossRef Link).
[16] J. Li, Q. Yu and Y. Zhang, "Key-policy attribute-based encryption against continual auxiliary input leakage," *Information Sciences*, vol. 470, pp. 175–188, 2019. Article (CrossRef Link).
[17] H. Li, Q. Chen, H. Zhu, D. Ma, H. Wen and X. (Sherman) Shen, "Privacy leakage via de-anonymization and aggregation in heterogeneous social networks," *IEEE Transactions on Dependable and Secure Computing*, 2017. Article (CrossRef Link).
[18] H. Li, H. Zhu, S. Du, X. Liang and X. (Sherman) Shen, "Privacy leakage of location sharing in mobile social networks: attacks and defense," *IEEE Transactions on Dependable and Secure Computing*, 2016, DOI: 10.1109/TDSC.2016.2604383. Article (CrossRef Link).
[19] A. Fiat and M. Naor, "Broadcast encryption," in *CRYPTO 1993*, LNCS 773, pp. 480-491, 1994. Article (CrossRef Link).
[20] D. Naor, M. Naor and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in *CRYPTO 2001*, LNCS 2139, pp. 41-62, 2001. Article (CrossRef Link).
[21] Y. Dodis and N. Fazio, "Public key broadcast encryption for stateless receivers," in *DRM 2002*, LNCS 2696, pp. 61-80, 2002. Article (CrossRef Link).

[22] A. Shamir, "Identity-based cryptosystems and signature schemes," in *CRYPTO 1984*, LNCS 196, pp. 47-53, 1985. Article (CrossRef Link).
[23] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *CRYPTO 2001*, LNCS 2139, pp. 213-229, 2001. Article (CrossRef Link).
[24] J. Li, M. Teng, Y. Zhang and Q. Yu, "A leakage-resilient CCA-secure identity-based encryption scheme," *The Computer Journal*, vol. 59, no. 7, pp. 1066-1075, 2016. Article (CrossRef Link).
[25] J. Li, Y. Guo, Q. Yu, Y. Lu and Y. Zhang, "Provably secure identity-based encryption resilient to post-challenge continuous auxiliary input leakage," *Security and Communication Networks*, vol. 9, no. 10, pp. 1016-1024, 2015. Article (CrossRef Link).
[26] C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys," in *ASIACRYPT 2007*, LNCS 4833, pp. 200-215, 2007. Article (CrossRef Link).
[27] D. Boneh, C. Gentry and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in *CRYPTO 2005*, LNCS 3621, pp. 258-275, 2005. Article (CrossRef Link).
[28] C. Gentry and B. Waters, "Adaptive security in broadcast encryption systems (with short ciphertexts)," in *EUROCRYPT 2009*, LNCS 5479, pp. 171-188, 2009. Article (CrossRef Link).
[29] X. Zhao and F. Zhang, "Fully CCA2 secure identity-based broadcast encryption with black-box accountable authority," *The Journal of Systems and Software*, vol. 85, no. 3, pp. 708-716, 2012. Article (CrossRef Link).
[30] Y. Yang, "Broadcast encryption based non-interactive key distribution in MANETs," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 533-545, 2014. Article (CrossRef Link).
[31] J. Kim, M. H. Au and J. Seberry, "Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 679-693, 2015. Article (CrossRef Link).
[32] A. Barth, D. Boneh and B. Waters, "Privacy in encrypted content distribution using private broadcast encryption," in *FC 2006*, LNCS 4107, pp. 52-64, 2006. Article (CrossRef Link).
[33] N. Fazio and I. M. Perera, "Outsider-anonymous broadcast encryption with sublinear ciphertexts," in *PKC 2012*, LNCS 7293, pp. 225-242, 2012. Article (CrossRef Link).
[34] B. Libert, K. G. Paterson and E. A. Quaglia, "Anonymous broadcast encryption: adaptive security and efficient constructions in the standard model," in *PKC 2012*, LNCS 7293, pp. 206-224, 2012. Article (CrossRef Link).
[35] J. Hur, C. Park and S. O. Hwang, "Privacy-preserving identity-based broadcast encryption," *Information Fusion*, vol. 13, no. 4, pp. 296-303, 2012. Article (CrossRef Link).
[36] L. Zhang, Q. Wu and Y. Mu, "Anonymous identity-based broadcast encryption with adaptive security," in *CSS 2013*, LNCS 8300, pp. 258-271, 2013. Article (CrossRef Link).
[37] Y. Ren, Z. Niu and X. Zhang, "Fully anonymous identity-based broadcast encryption without random oracles," *International Journal of Network Security*, vol. 16, no. 4, pp. 256-264, 2014. Article (CrossRef Link).
[38] L. Xie and Y. Ren, "Efficient anonymous identity- based broadcast encryption without random oracles," *International Journal of Digital Crime and Forensics*, vol. 6, no. 2, pp. 40-51, 2014. Article (CrossRef Link).
[39] F. Zhou, M. Lin, Y. Zhou and Y. Li, "Efficient anonymous broadcast encryption with adaptive security," *KSII Transactions on Internet and Information Systems*, vol. 9, no. 11, pp. 4680-4700, 2015. Article (CrossRef Link).
[40] K. He, J. Weng, J.-N. Liu, J. K. Liu, W. Liu and R. H. Deng, "Anonymous identity-based broadcast encryption with chosen-ciphertext security," in *Proc. of the 11th ACM Asia Conference on Computer and Communications Security (Asia CCS 2016)*, pp. 247-255, 2016. Article (CrossRef Link).
[41] K. He, J. Weng, M. H. Au, Y. Mao and R. H. Deng, "Generic anonymous identity-based broadcast encryption with chosen-ciphertext security," in *ACISP 2016*, LNCS 9723, pp. 207-222, 2016. Article (CrossRef Link).

[42] P. Xu, J. Li, W. Wang and H. Jin, "Anonymous identity-based broadcast encryption with constant decryption complexity and strong security," in *Proc. of the 11th ACM Asia Conference on Computer and Communications Security (Asia CCS 2016)*, pp. 223-233, 2016. Article (CrossRef Link).
[43] J. Lai, Y. Mu, F. Guo, W. Susilo and R. Chen, "Anonymous identity-based broadcast encryption with revocation for file sharing," in *ACISP 2016*, LNCS 9723, pp. 223-239, 2016. Article (CrossRef Link).
[44] J. Li, L. Chen, Y. Lu and Y. Zhang, "Anonymous certificate-based broadcast encryption with constant decryption cost," *Information Sciences*, vol. 454-455, pp. 110-127, 2018. Article (CrossRef Link).
[45] D. Boneh, E.-J. Goh and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in *TCC 2005*, LNCS 3378, pp. 325-341, 2005. Article (CrossRef Link).
[46] R. Canetti, S. Halevi and J. Katz, "Chosen-ciphertext security from identity-based encryption," in *EUROCRYPT 2004*, LNCS 3027, pp. 207-222, 2004. Article (CrossRef Link).
[47] R. Canetti, S. Halevi and J. Katz, "A forward-secure public-key encryption scheme," *Journal of Cryptology*, vol. 20, no. 3, pp. 265-294, 2007. Article (CrossRef Link).
[48] A. Lewko and B. Waters, "New techniques for dual system encryption and fully secure HIBE with short ciphertexts," in *TCC 2010*, LNCS 5978, pp. 455-479, 2010. Article (CrossRef Link).
[49] S. Xu and M. Yung, "k-anonymous secret handshakes with reusable credentials," in *Proc. of the 11th ACM Conference on Computer and Communications Security (CCS 2004)*, pp. 158-167, 2004. Article (CrossRef Link).
[50] B. Waters, "Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions," in *CRYPTO 2009*, LNCS 5677, pp. 619-636, 2009. Article (CrossRef Link).
[51] J. Li, Q. Yu and Y. Zhang, "Identity-based broadcast encryption with continuous leakage resilience," *Information Sciences*, vol. 429, pp. 177-193, 2018. Article (CrossRef Link).
[52] Y. Guo, J. Li, Y. Lu, Y. Zhang and F. Zhang, "Provably secure certificate-based encryption with leakage resilience," *Theoretical Computer Science*, vol. 711, pp. 1-10, 2018. Article (CrossRef Link).

Liqing Chen received B.S. degree in computer science and technology and M.S. degree in computer application technology from Nanjing Normal University, Nanjing, China in 2004 and 2007. He is currently lecturer in the Faculty of Computer and Software Engineering, Huaiyin Institute of Technology, Huai'an, Jiangsu, China. He is also currently PhD student in the College of Computer and Information Engineering, Hohai University, Nanjing, China. His research interests include cryptography and information security, network security. He has published more than 20 referred research papers at international conferences and journals.

Jiguo Li received his B.S. degree in mathematics from Heilongjiang University, Harbin, China in 1996, M.S. degree in mathematics and Ph.D. degree in computer science from Harbin Institute of Technology, Harbin, China in 2000 and 2003, respectively. During 2006.9-2007.3, he was a visiting scholar at Centre for Computer and Information Security Research, School of Computer Science & Software Engineering, University of Wollongong, Australia. During 2013.2-2014.1, he was a visiting scholar in Institute for Cyber Security in the University of Texas at San Antonio. He is currently a professor with the College of Mathematics and Informatics, Fujian Normal University, Fuzhou, China and College of Computer and Information, Hohai University, Nanjing, China. His research interests include cryptography and information security, cloud computing security, wireless security and trusted computing etc. He has published over 150 research papers in refereed international conferences and journals. His work has been cited more than 3000 times at Google Scholar. He has served as program committee member in over 30 international conferences and served as the reviewers in over 90 international journals and conferences.

Yichen Zhang received the Ph.D. degree in the College of Computer and Information, Hohai University, Nanjing, China in 2015. She is currently an associate professor with the College of Mathematics and Informatics, Fujian Normal University, Fuzhou, China. Her research interests include cryptography, network security. She has published over 30 research papers in refereed international conferences and journals.