Chinese Journal of Electronics
Vol.28, No.3, May 2019

An Efficient Broadcast Encryption Supporting Designation and Revocation Mechanisms*

ZHU Yan[1], YU Ruyun[1], CHEN E[1] and HUANG Dijiang[2]

(1. *School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China*)

(2. *School of Computing Informatics and Decision System Engineering, Arizona State University, Tempe, Arizona 85287, USA*)

Abstract — In this paper our objective is to explore approaches of secure group-oriented communication with designation and revocation mechanisms simultaneously. We present a new scheme of Revocation-based broadcast encryption (RBBE) which is designed on Dan Boneh *et al.*'s scheme with the designation mechanism proposed in 2005. We combine two above-mentioned schemes into a new cryptosystem, called Dual-mode broadcast encryption (DMBE). Based on these work, we reach the following conclusions. We use the DMBE scheme as an example to show that it is feasible to construct a broadcast encryption scheme that supports designation and revocation mechanisms simultaneously. The cryptosystem with dual modes is more efficient than that with single mode over computational costs, and the performance is improved to at most $O(\lceil N/2 \rceil)$, where N is the total number of users in the system. We prove completely that both the RBBE scheme and the DMBE scheme are semantically secure against chosen plaintext attack with full collusion under the decisional bilinear Diffie-Hellman exponent assumption.

Key words — Cryptography, Broadcast encryption, Provable security, Revocation, Designation, Dual modes.

I. Introduction

Secure group-oriented communication over insecure channels is an essential cryptographic mechanism that allows the sender to transmit the message for some designated receivers in a secure and efficient way. The existing group-oriented communication can be divided into two categories:

1)Designation mechanism: a small set of designated users in system can decrypt the ciphertext;

2)Revocation mechanism: all but a small set of revoked users in system can decrypt the ciphertext.

Broadcast encryption (BE) is such a technique to implement the secure group-oriented communication. The concept of broadcast encryption was firstly introduced by Fiat and Naor in Ref.[1]. In a BE system, a broadcaster firstly chooses a receiver set and encrypts messages, and then broadcasts the ciphertext to all the users in the system while only the users in the chosen set can decrypt the ciphertext.

There has already existed various researches for BE with respect to designation mechanism. The scheme proposed by Dan Boneh *et al.*[2] in 2005 has been noted as one of the most significant works because they first presented a new method for achieving fully collusion resistant by using groups with bilinear maps. Moreover, both ciphertexts and private keys are of constant size (*i.e.*, $O(1)$) for any subset of receivers, and the public key size is directly proportional to the total number of users in the system (*i.e.*, $O(N)$, where N is the total number of users). Due to its significant breakthrough on BE, many extensive researches have been done to explore more efficient and secure schemes. In 2007, Cécile Delerablée *et al.*[3] proposed the first Identity-based BE (IBBE) scheme with $O(1)$-size ciphertexts and private keys. Also, in contrast to Dan Boneh *et al.*'s BE scheme, the size of public key is improved to linear in the maximal size m of the set of receivers (*i.e.*, $O(m)$), which is smaller than the number of possible users (identities) in the system. After that, Craig Gentry *et al.*[4] improved Dan Boneh *et al.*'s BE scheme in the aspect of security and presented the first Adaptively Secure BE scheme

*Manuscript Received Nov. 10, 2017; Accepted Apr. 27, 2018. This work is supported by the National Natural Science Foundation of China (No.61472032), NSFC-Genertec Joint Fund for Basic Research (No.U1636104), and NSFC-Joint Research Fund for Overseas Chinese Scholars and Scholars in Hong Kong and Macao (No.61628201).

 DOI:10.1049/cje.2019.02.005

with sublinear ciphertexts (*i.e.*, $O(\sqrt{\lambda \cdot |S|})$, where λ is the security parameter and $|S|$ denotes the number of users in a designated set S). Recently, Duong-Hieu Phan *et al.*[5] also enhanced the selective Chosen-plaintext attacks (CPA) secure proposal by Dan Boneh *et al.* with a new CPA-to-CCA transform method. They proposed an adaptive Chosen-ciphertext attacks (CCA) secure scheme based on standard assumptions, which has ciphertexts that are shorter than those of the previous CCA secure schemes. Besides these above-mentioned schemes, there are some other researches about designation mechanism over BE on efficiency[6,7] and security[8,9].

Another important research direction about BE is to realize revocation mechanism, which is suitable for the setting that the number m of authorized users for decryption is close to that of all users in the system, *i.e.*, $N - m \ll N$. In 2000, Moni Naor *et al.*[10] presented a public-key revocation scheme based on t-threshold secret sharing, such that it can remove up to t parties and is secure against a coalition of the t revoked users. The advantage of this scheme is constant-size private key, but the computational overheads of a new key, encryption, and decryption are linear in t (*i.e.*, $O(t)$). Yevgeniy Dodis *et al.*[11] combined Subset difference (SD) with a Hierarchical IBE (HIBE) scheme[12] to construct an efficient revocation scheme with the ciphertext size of $O(r)$, the private key size of $O(\log^{2.5} N)$, and the public key size of $O(\log N)$ for r revoked users. Michael T. Goodrich *et al.*[13] addressed the problem of broadcasting messages to a collection of N devices which are organized in a tree structure while providing the ability to revoke an arbitrary subset of those devices. Their scheme uses $O(\log N)$ keys per device to achieve the broadcast cost of $O(r)$, where r is the number of revoked devices. In 2007, Cécile Delerablée *et al.*[14] put forward two public-key revocation schemes which can permanently revoke any subgroup of users. Their schemes are provably resist full collusions of users under the (t, n)-GDDHE (General decisional Diffie-Hellman exponent) assumption without any dependency on random Oracles. Recently, Jianchang Lai *et al.*[15] addressed the problem of removing target designated receivers from the ciphertext. They constructed an anonymous IBBE scheme with full anonymity, in which only the sender knows the receivers' identities and the revocation process does not reveal any information of the plaintext and receiver identity. However, their scheme is proved to be semantically secure in the random Oracle model. In addition, there are other research aspects of revocation mechanism to be explored, *e.g.*, traitor tracing[16–18].

Through the above scoping review of existing researches, it is not difficult to find that the construction supporting dual modes, designation and revocation mechanisms, is scarcely discussed. Moreover, there seems to be no evidence that such two mechanisms cannot coexist in a cryptosystem. Hence, it remains a fascinating problem to achieve dual mechanisms while keeping fewer construction discrepancy. Moreover, it is intuitively plausible that the advantage of BE construction with dual mechanisms is the decreasing of computational overheads on encryption and decryption. In addition, considering that these two mechanisms are opposite (or complementary) in terms of functionality, we must deal carefully with the security impact caused by integrating them into one cryptosystem.

Our Approach In order to design a dual-mode broadcast encryption supporting both designation and revocation mechanisms, we get inspiration from the most well-known scheme proposed by Dan Boneh *et al.*[2]. First of all, we observe that they aggregate the elements in a designated set S to obtain the aggregated value f_S of S, and then use it to achieve encryption on a designated set. In this process of aggregation, each element $e \in S$ is mapped into a random point in the algebraic system, then cumulative multiplication is applied on these points to produce f_S in the encryption phase. While in the decryption phase, all elements in S other than the specified element e (denoted as S_-) are shifted (related to the element e) and aggregated to f_{S_-}. Finally, the value f_{S_-} will be canceled with the shift of f_S, such that the hidden fixed secret would be recovered if $e \in S$.

Given a revoked set R, our revocation scheme intends to adopt an opposite method, in which we make an appropriate modification of the above-mentioned aggregation, *i.e.*, cumulative multiplication on the inverse of the point corresponding to the element e in R. By using this method, all elements in the revoked set R are aggregated to f_R in the encryption phase. However, in the decryption phase all elements in R and the specified element e (denoted as R_+) are shifted (related to the element e) and aggregated to f_{R_+}. Finally, the value f_{R_+} will be canceled with the shift of f_R, such that the hidden fixed secret would be recovered if $e \notin R$.

The above two opposite or complementary methods bring challenges to Dual-mode broadcast encryption scheme (DMBE), which are described as follows:

1) How to unify the different private keys in the above two schemes into one format such that each user only needs to hold one private key to work in dual modes;

2) How to separately implement the aggregation of either a specified set S or a revoked set R in the encryption phase so as to guarantee the ciphertext has a similar form;

3) How to unify the proofs of dual models into one complete proof in the security analysis of the DMBE scheme, which is a challenge related to Secure protocol composition (SPC) problem.

For comparison with the above-described methods,

it is clearly that they both combine aggregation, shift, and cancellation processes into one cryptosystem which achieves designation mechanism and revocation mechanism, respectively. However, these two methods implement opposite or complementary functionalities when dealing with two mechanisms. In the aspect of security, these two schemes also adopt the opposite or complementary defense approaches, which are described as follows:

1) In the BE scheme supporting designation mechanism, if the element e is in the designated set S, *i.e.*, $e \in S$, it is easy to remove e from S for acquiring $S_- = S/\{e\}$. Conversely, it is infeasible to remove e that does not exist in the set S.

2) In the BE scheme supporting revocation mechanism, if the element e is not in the revoked set R, *i.e.*, $e \notin R$, it is easy to add e into R for acquiring $R_+ = R \cup \{e\}$. Conversely, it is infeasible to add e that does exist in the set R.

Contributions In this paper our objective is to explore approaches of secure group-oriented communication with designation and revocation mechanisms simultaneously. We present a new scheme of Revocation-based broadcast encryption (RBBE) which is designed on Dan Boneh *et al.*'s scheme over the designation mechanism. Moreover, we combine two above-mentioned schemes into a new cryptosystem, called Dual-mode broadcast encryption. These work confirm the following results:

1) We use the DMBE scheme as an example to show that it is feasible to construct a broadcast encryption scheme that supports designation and revocation mechanisms simultaneously;

2) We prove completely that both the RBBE scheme and the DMBE scheme are semantically secure against chosen plaintext attack with full collusion under the Decisional bilinear Diffie-Hellman exponent (DBDHE) assumption;

3) The cryptosystem with dual modes is more efficient than that with single mode over computational costs, *e.g.*, the performance of our scheme is improved to $O(\min\{|S|, |R|\}) \leq O(\lceil \frac{N}{2} \rceil)$ for any designated set S or any revoked set R, where N is the total number of users and $|S| + |R| = N$.

In contrast to a single-mode BE scheme, in which the encryption and decryption should be performed with computational complexity of $O(|S|)$ or $O(|R|)$, the DMBE scheme has a considerable computational advantage. This means that one can determine an encryption mode with small overheads according to the relationship between the number of the authorized users and the total number of users in the system, namely, the designation mechanism (called Select-mode) is efficient if $|S| < N/2$; otherwise ($|R| \leq N/2$), the revocation mechanism (called Cut-mode) is better.

Organization The remainder of our paper is organized as follows. In Sections II and III, we provide some definitions basic notions and our RBBE Scheme. The construction of RBBE is presented in Section IV, as well as its performance evaluation and security analysis. We then describe the dual-mode broadcast encryption cryptosystem and its security proof in Section V. Finally, we conclude in Section VI.

II. Preliminaries and Definitions

In this section, we firstly give the preliminaries which are used to build our construction and security proof. And then we present the Dan Boneh *et al.*'s BE scheme[2].

1. Bilinear maps

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two cyclic groups of prime order p. A map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is said to be bilinear[19] if the following conditions hold:

• Bilinear. $e(P^a, Q^b) = e(P, Q)^{ab}$ for all $P, Q \in \mathbb{G}$ and all $a, b \in \mathbb{Z}_p^*$.

• Non-Degenerate. There exists some $P, Q \in \mathbb{G}$, such that $e(P, Q) \neq 1$, where 1 is the identity of $\mathbb{G}_T$.

• Computable. For any $P, Q \in \mathbb{G}$, there exists an efficient algorithm to compute $e(P, Q)$.

In the following sections, we will frequently use the bilinear map group system $\mathbb{S}$ which is denoted as $\mathbb{S} = (p, \mathbb{G}, \mathbb{G}_T, e(\cdot, \cdot))$. All the items in $\mathbb{S}$ are the same as these in the definition above.

2. Complexity assumptions

Before describing the complexity assumptions, we firstly give the definition of negligible function as follows:

Definition 1 (Negligible function[20]) The function ϵ is negligible if for every $c \in \mathbb{N}$ there exists an integer N such that $\epsilon(k) \leq \frac{1}{k^c}$ for all $k \geq N$.

Note that $\mathbb{N}$ denotes the nature number set. In this paper, we use ϵ to denote a negligible function. In order to simplify the symbol, we use both $\in_R$ and $\xleftarrow{R}$ to denote randomly choose an element from the group after the symbol[21]. The security of our scheme is based on a complexity assumption called Bilinear Diffie-Hellman exponent (BDHE) assumption[22]. With the bilinear map group system $\mathbb{S}$, and a randomly chosen generator g of $\mathbb{G}$, the Computational bilinear Diffie-Hellman exponent (CBDHE) problem in $\mathbb{S}$ is defined as follows:

Definition 2 (CBDHE problem) Given a $(2n+1)$-tuple $(g, g^t, \{g^{\mu^i}\}_{i=1, i\neq n}^{2n}) \in \mathbb{G}^{2n+1}$, output $e(g^{\mu^n}, g)^t \in \mathbb{G}_T$, where $\mu, t \in_R \mathbb{Z}_p^*$ and $n \in \mathbb{N}$.

We define the advantage of an algorithm $\mathcal{A}$ in solving the CBDHE problem as Eq.(1).

$$Adv_{\mathrm{CBDHE}}^{\mathrm{IND}}(\mathcal{A}) \stackrel{\mathrm{def}}{=} Pr[\mathcal{A}(\mathcal{R}) = e(g^{\mu^n}, g)^t] \qquad (1)$$

where $\mathcal{R} = (g, g^t, \{g^{\mu^i}\}_{i=1,i\neq n}^{2n})$ and the probability is over the random choice of generator $g \in \mathbb{G}$ and the random choice of exponents $t, \mu \in \mathbb{Z}_p^*$ by $\mathcal{A}$. We say that an algorithm $\mathcal{A}$ solves the (ϵ, n)-CBDHE problem if $\mathcal{A}$ runs in probabilistic polynomial-time and $Adv_{\mathrm{CBDHE}}^{\mathrm{IND}}(\mathcal{A})$ is at least ϵ, *i.e.*, $Adv_{\mathrm{CBDHE}}^{\mathrm{IND}}(\mathcal{A}) \geq \epsilon$.

Definition 3 ((ϵ, n)-CBDHE assumption) We say that the CBDHE assumption is (ϵ, n)-secure in $\mathbb{S}$, if for all probabilistic polynomial-time algorithms $\mathcal{A}$ the advantage of solving the CBDHE problem is at most ϵ, *i.e.*, $Adv_{\mathrm{CBDHE}}^{\mathrm{IND}}(\mathcal{A}) < \epsilon$.

Next, we define the Decisional bilinear Diffie-Hellman exponent problem (DBDHE) in $\mathbb{S}$ as follows:

Definition 4 (DBDHE problem) Given a $(2n+1)$-tuple $(g, g^t, \{g^{\mu^i}\}_{i=1,i\neq n}^{2n}) \in \mathbb{G}^{2n+1}$ and a random element $W \overset{R}{\leftarrow} \mathbb{G}_T$ as input, output 1 if $W = e(g^{\mu^n}, g)^t$ and 0 otherwise.

We define the advantage of an algorithm $\mathcal{B}$ in solving the DBDHE problem as follows:

$$Adv_{\mathrm{DBDHE}}^{\mathrm{IND}}(\mathcal{B}) \overset{\mathrm{def}}{=} \left| \begin{array}{l} Pr[\mathcal{B}(\mathcal{R}, e(g^{\mu^n}, g)^t) = 1 : g \overset{R}{\leftarrow} \mathbb{G}, \mu, t \overset{R}{\leftarrow} \mathbb{Z}_p^*] - \\ Pr[\mathcal{B}(\mathcal{R}, W) = 1 : g \overset{R}{\leftarrow} \mathbb{G}, \mu, t \overset{R}{\leftarrow} \mathbb{Z}_p^*, W \overset{R}{\leftarrow} \mathbb{G}_T] \end{array} \right|$$

where $\mathcal{R} = (g, g^t, \{g^{\mu^i}\}_{i=1,i\neq n}^{2n})$. The probability is over the uniform random choice of the parameters to $\mathcal{B}$ and over the coin tosses of $\mathcal{B}$. We say that an algorithm $\mathcal{B}$ solves the (ϵ, n)-DBDHE problem if $\mathcal{B}$ runs in probabilistic polynomial-time and $Adv_{\mathrm{DBDHE}}^{\mathrm{IND}}(\mathcal{B})$ is at least ϵ, *i.e.*, $Adv_{\mathrm{DBDHE}}^{\mathrm{IND}}(\mathcal{B}) \geq \epsilon$.

Definition 5 ((ϵ, n)-DBDHE assumption) We say that the DBDHE assumption is (ϵ, n)-secure in $\mathbb{S}$, if for all probabilistic polynomial-time algorithms $\mathcal{B}$, the advantage of solving the DBDHE problem is at most ϵ, *i.e.*, $Adv_{\mathrm{DBDHE}}^{\mathrm{IND}}(\mathcal{B}) < \epsilon$.

3. Dan Boneh *et al.*'s BE scheme

In Ref.[2], Dan Boneh *et al.* proposed a fully collusion resistant broadcast encryption scheme. There are n users in their scheme and the user group is denoted as $U = \{1, 2, \ldots, n\}$, where $n \in \mathbb{N}$. Their scheme designates a user set such that only the users in the designated set can decrypt the ciphertext. The scheme is built in $\mathbb{S}$ and is a collection of three polynomial-time algorithms: *Setup*, *Encrypt* and *Decrypt*. Next, we illustrate their scheme in detail.

• $Setup(n)$: Let $\mathbb{G}$ be a bilinear group of prime order p. This algorithm firstly picks a random generator $g \in \mathbb{G}$ and a random $\alpha \in \mathbb{Z}_p$. It computes $g_i = g^{(\alpha^i)} \in \mathbb{G}$ for $i = 1, 2, \ldots, n, n+2, \ldots, 2n$. Next, it picks a random $\gamma \in \mathbb{Z}_p$ and sets $v = g^\gamma \in \mathbb{G}$. The public key is:

$$PK = (g, g_1, \ldots, g_n, g_{n+2}, \ldots, g_{2n}, v) \in \mathbb{G}^{2n+1}$$

The private key for user $i \in \{1, \ldots, n\}$ is set as: $d_i = g_i^\gamma \in \mathbb{G}$. Note that $d_i = v^{\alpha^i}$. The algorithm outputs the public key PK and the n private keys $d_1, \ldots, d_n$.

• $Encrypt(PK, S)$: Given a set of user identities $S \subseteq U$, this algorithm picks a random $t \in \mathbb{Z}_p$ and sets $K = e(g_{n+1}, g)^t \in \mathbb{G}_T$. The value $e(g_{n+1}, g)$ can be computed as $e(g_n, g_1)$. Next, set

$$Hdr = (g^t, (v \cdot \prod_{j \in S} g_{n+1-j})^t) \in \mathbb{G}^2 \tag{2}$$

and output the pair (Hdr, K).

• $Decrypt(PK, S, Hdr, i, d_i)$: Let $Hdr = (C_0, C_1)$ and recall that $d_i \in \mathbb{G}$, the value K is retrieved as Eq.(3).

$$K = e(g_i, C_1)/e(d_i \cdot \prod_{j \in S, j \neq i} g_{n+1-j+i}, C_0) \tag{3}$$

Their scheme is secure against the collusion over all invalid receivers. In their construction both ciphertexts and private keys are of constant size (at most two group elements), for any designated set of users. However, as we can see in the Eq.(2), the computational overhead of *Encrypt* is linear with the number of users in the designated set S, which is denoted as $|S|$. When n is large and the number of users in S is much closer to n, the computation is inefficient. Based on this requirement, we extend their scheme and proposed a new scheme, called Revocation-based broadcast encryption, which will be described in the following sections.

III. Definition of Revocation-Based Broadcast Encryption

In this section we propose a formal definition of the revocation-based broadcast encryption scheme. And then we give its security definition.

1. The definition of RBBE scheme

In our scheme, all the valid users outside the revoked set can decrypt the ciphertext. We set the user group $U = \{1, 2, \ldots, n-1\}$, where $n \in \mathbb{N}$ and R is a subset of U, *i.e.*, $R \subseteq U$. Similar to most definitions of broadcast encryption, our scheme is a collection of four algorithms: *Setup*, *KeyGen*, *Encrypt* and *Decrypt*, which are described as follows:

• $Setup(1^\kappa, U)$: This algorithm takes as input the security parameter κ and the user group U. It outputs the public key PK and the master key MK.

• $KeyGen(PK, MK, i)$: This algorithm takes as input the public key PK, the master key MK and the user identity $i \in U$. It outputs the user's private key sk_i.

• $Encrypt(PK, R)$: This algorithm takes as input the public key PK and a revoked set $R \subseteq U$. It outputs the ciphertext C_R and the session key ek.

• $Decrypt(PK, R, C_R, i, sk_i)$: This algorithm takes

as input the public key PK, the revoked set R and the ciphertext C_R, such that each user $i \notin R$ can use his private key sk_i to recover ek.

2. Security definition

Firstly, we require the proposed RBBE scheme is correct, so it must meet the following requirement:

Definition 6 (Correctness) We say that a RBBE scheme is correct, for each revoked set $R \subseteq U$, if $(PK, MK) \leftarrow Setup(1^\kappa, U)$, $sk_i \leftarrow KeyGen(PK, MK, i)$ for all $i \in U$ and $(C_R, ek) \leftarrow Encrypt(PK, R)$, then $Decrypt(PK, R, C_R, i, sk_i) = ek$ for all $i \notin R$. That is,

$$Pr\left[\begin{array}{l} Decrypt(PK, R, C_R, i, sk_i) = ek : \\ (PK, MK) \leftarrow Setup(1^\kappa, U); \\ sk_i \leftarrow KeyGen(PK, MK, i), \forall\ i \in U; \\ (C_R, ek) \leftarrow Encrypt(PK, R), \forall\ R \subseteq U; \\ \text{s.t. } \forall\ i \notin R; \end{array}\right] \geq 1-\epsilon(\kappa)$$

where $\epsilon(\kappa)$ is a negligible function of κ.

Secondly, we define the semantic security against Chosen plaintext attack with full collusion (IND-CPA-FC) by using the following game between an adversary $\mathcal{A}$ and a simulator $\mathcal{B}$, which follows the left-or-right encryption oracle[23].

• Initialization. The adversary $\mathcal{A}$ declares the revoked user set $R^* \subseteq U$ he wants to attack.

• Setup. The simulator simulates $Setup$ to obtain the public key PK, and then he sends PK to $\mathcal{A}$.

• Learning. The adversary $\mathcal{A}$ makes secret key queries to the $KeyGen$ Oracle for any user $i \in R^*$.

• Challenge. The adversary $\mathcal{A}$ picks two messages m_0 and m_1, and then sends them to the simulator. The simulator randomly picks $\sigma \in \{0, 1\}$, and runs $Encrypt(PK, R^*)$ to acquire the ciphertext C_{R^*} and session key ek. At last, the simulator sends the challenge $(C_{R^*}, m_\sigma \oplus ek)$ to the adversary.

• Response. The adversary $\mathcal{A}$ outputs $\sigma^* \in \{0, 1\}$ as the guess. The adversary wins the game if and only if $\sigma^* = \sigma$.

In this game, the adversary can designate a revoked user set $R^* \subseteq U$ and learn all their secret keys. Here, the set R^* is also called an unauthorized set, and we say that it is Full collusion (FC) if the adversary is able to corrupt all the users in R^*. Moreover, the scheme is said to be secure against full collusion attack if the adversary cannot launch a successful attack even with all secret keys of the users in R^*.

The above-mentioned game would be used to define the security of our RBBE construction. Our goal is to ensure the unpredictability of ek which is the output of $Decrypt$ algorithm. According to the equivalence of pseudorandomness and unpredictability[24], the unpredictability of ek can be guaranteed by the indistinguishability of the ciphtertext $m_\sigma \oplus ek$ which is the encryption of m_σ by on one-time pad. Hence, we set $Adv^{\mathrm{IND}}_{\mathrm{RBBE}}(\mathcal{A})$ denote the advantage that $\mathcal{A}$ wins the above game as Eq.(4).

$$Adv^{\mathrm{IND}}_{\mathrm{RBBE}}(\mathcal{A}) = |Pr[\sigma^* = \sigma] - 1/2| \tag{4}$$

Definition 7 (IND-CPA-FC security) We say that an RBBE scheme is secure against the IND-CPA-FC game if for all probabilistic polynomial-time algorithms $\mathcal{A}$, we have $Adv^{\mathrm{IND}}_{\mathrm{RBBE}}(\mathcal{A}) < \epsilon$, where ϵ is a negligible function.

IV. Construction of Revocation-Based Broadcast Encryption

Based on the above-mentioned definition, we give a specific construction of RBBE. The RBBE scheme is an extendation of Dan Boneh *et al.*'s scheme in Ref.[2] (see Section II.3), but our objective is to achieve the revocation mechanism. In fact, our scheme is particularly efficient for the case that most users in the group U can decrypt the ciphertext.

1. The construction of RBBE

Our construction is built on the bilinear map group system $\mathbb{S}$. In our construction the user group is defined as $U = \{1, 2, \ldots, n-1\}$, where $n \in \mathbb{N}$. We present the construction by describing four algorithms: $Setup$, $KeyGen$, $Encrypt$ and $Decrypt$, which are described as below:

• $Setup(1^\kappa, U)$: Given the security parameter κ and the user group U, this algorithm firstly generates the bilinear map group system $\mathbb{S} = (p, \mathbb{G}, \mathbb{G}_T, e(\cdot, \cdot))$. Secondly, it randomly chooses two elements μ, r in $\mathbb{Z}_p^*$, picks a generator g of $\mathbb{G}$, and chooses $h \in_R \mathbb{G}$. Thirdly, it computes $w = g^r \cdot h$. Finally, it computes $g_i = g^{\mu^i}$ for $i = 1, 2, \ldots, n-1, n+1, \ldots, 2n$. The master key is outputted as $MK = (\mu, r, h)$ and the public key is $PK = (g, w, \{g_i\}_{i=1, i\neq n}^{2n})$.

• $KeyGen(PK, MK, i)$: For each user $i \in U$, this algorithm computes his secret key as $sk_i = g_i^r \cdot \dfrac{h^{\mu^i}}{g_n}$.

• $Encrypt(PK, R)$: Given the public key PK and the revoked set R, this algorithm randomly chooses $t \in \mathbb{Z}_p^*$. The ciphertext $C_R = (C_0, C_1)$ can be computed as Eq.(5).

$$\begin{cases} C_0 = g^t \\ C_1 = (w/\prod\limits_{j\in R} g_{n-j})^t \end{cases} \tag{5}$$

And then, this algorithm sets the session key $ek = e(g_n, g)^t$. Note that ek can be computed by $ek = e(g_n, g)^t = e(g_{n-1}, g_1)^t$.

• $Decrypt(PK, R, C_R, i, sk_i)$: On receiving the ciphertext C_R, with the knowledge of PK and the revoked set R, each user $i \notin R$ can use his secret key sk_i to recover

the session key as Eq.(6).

$$ek = \frac{e(C_1, g_i)}{e(sk_i / \prod_{j \in R} g_{n-j+i}, C_0)} \tag{6}$$

Correctness We firstly verify the correctness of our construction, that is, the *Decrypt* algorithm works correctly. Suppose $i \notin R$, then the user i can recover the session key as Eq.(7).

$$\begin{aligned} ek' =& \frac{e(C_1, g_i)}{e(sk_i / \prod_{j \in R} g_{n-j+i}, C_0)} \\ =& \frac{e((w / \prod_{j \in R} g_{n-j})^t, g_i)}{e(g_i^r \cdot h^{\mu^i} / (g_n \cdot \prod_{j \in R} g_{n-j+i}), g^t)} \\ =& \frac{e(g^r \cdot h / \prod_{j \in R} g_{n-j}, g_i)^t}{e([g^r \cdot h / (g_{n-i} \cdot \prod_{j \in R} g_{n-j})]^{\mu^i}, g)^t} \\ =& \frac{e(g^r \cdot h / \prod_{j \in R} g_{n-j}, g_i)^t}{[e(g^r \cdot h / \prod_{j \in R} g_{n-j}, g_i)^t / e(g_{n-i}, g_i)^t]} \\ =& e(g_{n-i}, g_i)^t = e(g_n, g)^t = ek \end{aligned} \tag{7}$$

2. Performance evaluation of RBBE

In this subsection, we will analyze the performance of our RBBE scheme. For simplification, we give several notations to denote the time for various operations in our scheme. Let $E(\mathbb{G})$ and $E(\mathbb{G}_T)$ denote the exponentiation operation in $\mathbb{G}$ and $\mathbb{G}_T$, respectively. $M(\mathbb{G})$ and $M(\mathbb{G}_T)$ denote the multiplication in $\mathbb{G}$ and $\mathbb{G}_T$, respectively. $D(\mathbb{G})$ and $D(\mathbb{G}_T)$ denote the division in $\mathbb{G}$ and $\mathbb{G}_T$, respectively. B denotes the bilinear pairing $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. Also, we define that $n-1$ is the number of users in set U, *i.e.*, $|U| = n-1$, and $|R|$ denotes the number of users in set R. The performance evaluation of our RBBE scheme is presented in Table 1, where $l_{\mathbb{Z}_p^*}$, $l_{\mathbb{G}}$ and $l_{\mathbb{G}_T}$ denote the length of elements in $\mathbb{Z}_p^*$, $\mathbb{G}$ and $\mathbb{G}_T$, respectively. We neglect the operations in $\mathbb{Z}_p^*$, since they are much more efficient than exponentiation operation and pairing operations.

From Table 1, we can see that the computational overheads of *Setup* and *KeyGen* are directly proportional to the number of users in U, *i.e.*, $|U|$. However, the storage overheads of each user's secret key and ciphertext are constant, just one group element and two group elements, respectively. The computational costs of *Encrypt* and *Decrypt* are directly proportional to the number of users in revoked set R, such that the smaller the size of the set R, the better the performance. Hence, our scheme is more efficient for the case that almost all users in group are authorized to decrypt the ciphertext.

Table 1. Performance evaluation of the RBBE scheme

	Computational complexity	Communication/Storage complexity
Setup	$(2n) \cdot E(\mathbb{G}) + 1 \cdot M(\mathbb{G})$	$(2n+1) \cdot l_{\mathbb{G}}(PK)$, $2 \cdot l_{\mathbb{Z}_p^*} + 1 \cdot l_{\mathbb{G}}(MK)$
KeyGen	$\lvert U\rvert \cdot (3 \cdot E(\mathbb{G}) + 1 \cdot M(\mathbb{G}) + 1 \cdot D(\mathbb{G}))$ (for $\lvert U\rvert$ users)	$\lvert U\rvert \cdot l_{\mathbb{G}}$ (sk_i, for $\lvert U\rvert$ users)
Encrypt	$2 \cdot E(\mathbb{G}) + 1 \cdot E(\mathbb{G}_T) + (\lvert R\rvert - 1) \cdot M(\mathbb{G}) + 1 \cdot D(\mathbb{G}) + 1 \cdot B$	$2 \cdot l_{\mathbb{G}}$ (C_R)
Decrypt	$(\lvert R\rvert - 1) \cdot M(\mathbb{G}) + 1 \cdot D(\mathbb{G}) + 2 \cdot B + 1 \cdot D(\mathbb{G}_T)$	$1 \cdot l_{\mathbb{G}_T}$ (ek)

3. Security analysis of RBBE

In this subsection, we provide the security analysis of our RBBE scheme. We now prove that our RBBE scheme is semantically secure against chosen plaintext attack with full collusion.

Theorem 2 (Semantic security) Our RBBE scheme for group with $n-1$ users is (ϵ, n) semantically secure against chosen plaintext attack with full collusion under the (ϵ, n)-DBDHE assumption in $\mathbb{S}$, and the advantage of the adversary $\mathcal{A}$ is $Adv^{\mathrm{IND}}_{\mathrm{RBBE}}(\mathcal{A}) < \epsilon$.

Proof Suppose there exists an adversary $\mathcal{A}$ can break our RBBE scheme with the advantage ϵ, that is, $Adv^{\mathrm{IND}}_{\mathrm{RBBE}}(\mathcal{A}) \geq \epsilon$. Given the user group $U = \{1, 2, \ldots, n-1\}$, our objective is to build a simulator $\mathcal{B}$ to solve the DBDHE problem: given elements $(G, G^t, \{G^{\mu^i}\}_{i=1, i \neq n}^{2n}) \in \mathbb{G}^{2n+1}$ and $W \xleftarrow{R} \mathbb{G}_T$ to output 1 if $W = e(G^{\mu^n}, G)^t$, otherwise output 0. We utilize the following game to depict the construction of $\mathcal{B}$.

• Initialization. The adversary $\mathcal{A}$ declares the set $R^* \subseteq U$ he wants to attack.

• Setup. The simulator $\mathcal{B}$ simulates *Setup* to obtain the public key PK. And then he sends PK to the adversary $\mathcal{A}$. This process is divided into the following 4 steps:

1) Set $g = G$, where G is a generator of $\mathbb{G}$;

2) Set $G_i = G^{\mu^i}$ for $i = 1, 2, \ldots, n-1, n+1, \ldots, 2n$, so we have $g_i = g^{\mu^i} = G^{\mu^i} = G_i$, where $\mu \in \mathbb{Z}_p^*$ and μ is unknown;

3) Randomly select λ in $\mathbb{Z}_p^*$, set $r = \lambda + \sum_{j \in R^*} \mu^{n-j}$ and r is unknown;

4) Randomly select δ in $\mathbb{Z}_p^*$, set $h = G^{\delta}$, so we can compute $w = g^r \cdot h = G^{\lambda+\delta} \cdot \prod_{j \in R^*} G_{n-j}$.

Finally, $\mathcal{B}$ sends $PK := (g = G, w = g^r \cdot h =$

$G^{\lambda+\delta} \cdot \prod_{j\in R^*} G_{n-j}, \{G^{\mu^i}\}_{i=1,i\neq n}^{2n})$ to $\mathcal{A}$.

Note that λ and δ are chosen uniformly at random, this public key has an identical distribution to that in the actual construction.

• Learning. The adversary $\mathcal{A}$ makes secret key queries to the *KeyGen* Oracle for any user $i \in R^*$. Due to $G_n \in \bigcup_{j\in R^*} \{G_{n-j+i}\}$, the secret key sk_i can be computed as Eq.(8).

$$\begin{aligned} sk_i =& g_i^r \cdot \frac{h^{\mu^i}}{g_n} = G_i^r \cdot \frac{G_i^\delta}{G_n} \\ =& G_i^{\lambda+\delta} \cdot \frac{\prod_{j\in R^*} G_{n-j+i}}{G_n} \\ =& G_i^{\lambda+\delta} \cdot \prod_{j\in R^*, j\neq i} G_{n-j+i} \end{aligned} \tag{8}$$

Remark: Note that it is infeasible for the simulator to generate the secret key corresponding to the user that not in the revoked set R^*. The reason is that if the user $i \notin R^*$, $\mathcal{B}$ cannot compute $G_i^{\lambda+\delta} \cdot \frac{\prod_{j\in R^*} G_{n-j+i}}{G_n}$ because G_n is unknown and $G_n \notin \bigcup_{j\in R^*} \{G_{n-j+i}\}$.

• Challenge. The adversary $\mathcal{A}$ picks two messages m_0 and m_1, and then sends them to the simulator. The simulator $\mathcal{B}$ randomly picks $\sigma \in \{0,1\}$, and simulates the *Encrypt* algorithm to acquire C_{R^*} and the ciphertext of m_σ as follows: with the known G^t, the ciphertext $C_{R^*} = (C_0, C_1)$ can be computed as Eq.(9).

$$\begin{cases} C_0 = g^t = G^t, \\ C_1 = (w/\prod_{j\in R^*} g_{n-j})^t = (G^t)^{\lambda+\delta} \end{cases} \tag{9}$$

$\mathcal{B}$ sets $ek = e(g_n, g)^t = e(G_n, G^t) = e(G_n, G)^t = W$, such that the ciphertext of m_σ is $m_\sigma \oplus W$. Finally, the simulator $\mathcal{B}$ sends the challenge $(C_{R^*}, m_\sigma \oplus W)$ to the adversary.

• Response. The adversary $\mathcal{A}$ outputs $\sigma^* \in \{0,1\}$ as the guess. If $\sigma^* = \sigma$, $\mathcal{B}$ outputs 1; otherwise outputs 0.

Availability of secret keys At first, we illustrate the availability of the queried secret key sk_i. Here we choose a set $R' \subseteq \overline{R^*} = U \setminus R^*$ to see whether the secret key sk_i is valid. In this setting, the user i is not a member in R', *i.e,* $i \notin R'$. We choose t' in $\mathbb{Z}_p^*$ randomly, the session key is $ek = e(G_n, G)^{t'}$ and the ciphertext $C_{R'} = (C_0', C_1')$ can be computed as follows:

$$\begin{cases} C_0' &= g^{t'} = G^{t'} \\ C_1' &= (w/\prod_{j\in R'} g_{n-j})^{t'} \\ &= [G^{\lambda+\delta} \cdot (\prod_{j\in R^*} G_{n-j})/(\prod_{j\in R'} G_{n-j})]^{t'} \end{cases}$$

And then, the user i can run the *Decrypt* algorithm to recover ek as Eq.(10).

$$\begin{aligned} ek' =& e(C_1', g_i)/e(sk_i/\prod_{j\in R'} g_{n-j+i}, C_0') \\ =& \frac{e(G^{\lambda+\delta} \cdot (\prod_{j\in R^*} G_{n-j})/(\prod_{j\in R'} G_{n-j}), G_i)^{t'}}{e(G_i^{\lambda+\delta} \cdot \prod_{j\in R^*, j\neq i} G_{n-j+i}/\prod_{j\in R'} G_{n-j+i}, G^{t'})} \\ =& \frac{e(G^{\lambda+\delta} \cdot (\prod_{j\in R^*} G_{n-j})/(\prod_{j\in R'} G_{n-j}), G)^{\mu^i t'}}{e(G^{\lambda+\delta} \cdot \prod_{j\in R^*, j\neq i} G_{n-j}/\prod_{j\in R'} G_{n-j}, G)^{\mu^i t'}} \\ =& e(G_{n-i}, G)^{\mu^i t'} = e(G_{n-i}, G_i)^{t'} \\ =& e(G_n, G)^{t'} = ek \end{aligned} \tag{10}$$

So we end the description on the availability of the secret key sk_i constructed by the simulator.

Advantage evaluation Next, we analyze the advantage of the adversary $\mathcal{A}$ in attacking our RBBE scheme.

According to the definition of $Adv_{\mathrm{RBBE}}^{\mathrm{IND}}(\mathcal{A})$, we have the following equation as Eq.(11):

$$\begin{aligned} Adv_{\mathrm{RBBE}}^{\mathrm{IND}}(\mathcal{A}) &= |Pr[\sigma^* = \sigma] - 1/2| \\ &= 1/2|Pr[\sigma^* = \sigma] - Pr[\sigma^* \neq \sigma]| \\ &= 1/2 \left| \begin{matrix} Pr[\sigma^* = 1|\sigma = 1] - \\ Pr[\sigma^* = 1|\sigma = 0] \end{matrix} \right| \end{aligned} \tag{11}$$

Note that the probability $Pr[\sigma^* = \sigma]$ in the above equation is under the precondition of $W = e(G_n, G)^t$. With the help of the advantage of $\mathcal{A}$ in attacking our RBBE scheme, the simulator $\mathcal{B}$ can solve the DBDHE problem with nonnegligible probability. Next we will compute $Adv_{\mathrm{DBDHE}}^{\mathrm{IND}}(\mathcal{B})$. Remember that when W is ineffective, that is, $W \xleftarrow{R} \mathbb{G}_T$, the output of $\mathcal{A}$ is depended on the random guess with 1/2 possibility, so we have $Pr[\sigma^* = \sigma | W \xleftarrow{R} \mathbb{G}_T] = Pr[\sigma^* \neq \sigma | W \xleftarrow{R} \mathbb{G}_T] = 1/2$. We use $W \leftarrow_D \mathbb{G}_T$ to denote that W is effective, *i.e.*, $W = e(G_n, G)^t$. Set $\mathcal{L} = (G, G^t, \{G^{\mu^i}\}_{i=1,i\neq n}^{2n}, e(G_n, G)^t)$. The computation process is as Eq.(12).

$$\begin{aligned} & Adv_{\mathrm{DBDHE}}^{\mathrm{IND}}(\mathcal{B}) \\ &= \left| \begin{matrix} Pr[\mathcal{B}(\mathcal{L}, e(G_n, G)^t) = 1 : G \xleftarrow{R} \mathbb{G}, \mu, t \xleftarrow{R} \mathbb{Z}_p^*] \\ -Pr[\mathcal{B}(\mathcal{L}, W) = 1 : G \xleftarrow{R} \mathbb{G}, W \xleftarrow{R} \mathbb{G}_T, \mu, t \xleftarrow{R} \mathbb{Z}_p^*] \end{matrix} \right| \\ &= |Pr[\sigma^* = \sigma | W \leftarrow_D \mathbb{G}_T)] - Pr[\sigma^* = \sigma | W \xleftarrow{R} \mathbb{G}_T]| \\ &= \left| \begin{matrix} Pr[\sigma^* = 1 | \sigma = 1 \wedge W \leftarrow_D \mathbb{G}_T] \cdot 1/2 \\ +Pr[\sigma^* = 0 | \sigma = 0 \wedge W \leftarrow_D \mathbb{G}_T] \cdot 1/2 - 1/2 \end{matrix} \right| \\ &= 1/2 \left| \begin{matrix} Pr[\sigma^* = 1 | \sigma = 1 \wedge W = e(G_n, G)^t] \\ -Pr[\sigma^* = 1 | \sigma = 0 \wedge W = e(G_n, G)^t] \end{matrix} \right| \end{aligned} \tag{12}$$

Based on the above two equations, we get $Adv^{\mathrm{IND}}_{\mathrm{DBDHE}}(\mathcal{B}) = Adv^{\mathrm{IND}}_{\mathrm{RBBE}}(\mathcal{A})$. According to the hypothesis that $Adv^{\mathrm{IND}}_{\mathrm{RBBE}}(\mathcal{A}) \geq \epsilon$, we have $Adv^{\mathrm{IND}}_{\mathrm{DBDHE}}(\mathcal{B}) \geq \epsilon$. This is opposite to the definition of DBDHE assumption. So the hypothesis is wrong, *i.e.*, $Adv^{\mathrm{IND}}_{\mathrm{RBBE}}(\mathcal{A}) < \epsilon$. Consequently, our RBBE scheme is (ϵ, n) semantically secure against chosen plaintext attack with full collusion under the (ϵ, n)-DBDHE assumption in $\mathbb{S}$, and the advantage of the adversary $\mathcal{A}$ is $Adv^{\mathrm{IND}}_{\mathrm{RBBE}}(\mathcal{A}) = Adv^{\mathrm{IND}}_{\mathrm{DBDHE}}(\mathcal{B}) < \epsilon$.

V. Dual-Mode Broadcast Encryption

In this section, we present a new scheme, called Dual-mode broadcast encryption (DMBE), which is a mixture of Dan Boneh *et al.*'s scheme and our RBBE scheme. With the help of such a mixture, the DMBE system supports dual modes: *Select–mode* and *Cut–mode*, where we utilize Dan Boneh *et al.*'s scheme to achieve *Select–mode* while the *Cut–mode* is realized by our RBBE scheme.

1. The construction of DMBE

The user group in our DMBE scheme is also $U = \{1, 2, \ldots, n-1\}$, *i.e.*, $|U| = n-1$. We can easily see that $U = S \cup R$. Exactly, the *Select–mode* is used to achieve that a minority of users can decrypt the ciphertext, that is, $|S| < \frac{|U|}{2}$, while the *Cut–mode* is used to achieve that a majority of users can decrypt the ciphertext, that is, $R = U \setminus S$ and $|R| \leq \frac{|U|}{2}$. The dual modes are extremely essential for secure group-oriented communication because the computational overhead is optimized to $O(\min\{|S|, |R|\})$. The construction of DMBE is described as follows:

• $Setup(1^\kappa, U)$: Given the security parameter κ and the user group U, this algorithm firstly generates the bilinear map group system $\mathbb{S} = (p, \mathbb{G}, \mathbb{G}_T, e(\cdot,\cdot))$. Secondly, it randomly chooses two elements μ, r in $\mathbb{Z}_p^*$, picks a generator g of $\mathbb{G}$ and chooses $h \in_R \mathbb{G}$. Thirdly, it computes $v = g^r$ and $w = g^r \cdot h$. Finally, it computes $g_i = g^{\mu^i}$ for $i = 1, 2, \ldots, n-1, n+1, \ldots, 2n$ and $h_i = h^{\mu^i}/g_n$ for $i = 1, 2, \ldots, n-1$. The master key is outputted as $MK = (\mu, r)$ and the public key is $PK = (g, v = g^r, w = g^r \cdot h, \{h_i\}_{i=1}^{n-1}, \{g_i\}_{i=1, i\neq n}^{2n})$.

• $KeyGen(PK, MK, i)$: For each user $i \in U$, this algorithm computes his secret key $sk_i = g_i^r$.

• $Encrypt(PK, S/R, mode)$: Given the public key PK, the set S or R corresponding to different $mode \in \{Select, Cut\}$, this algorithm chooses $t \in \mathbb{Z}_p^*$ randomly. The ciphertext C is composed of (C_0, C_1), where $C_0 = g^t$ and C_1 is defined as follows:

$$C_1 = \begin{cases} (v \cdot \prod_{j\in S} g_{n-j})^t & \text{for } Select\text{–}mode \\ (w/\prod_{j\in R} g_{n-j})^t & \text{for } Cut\text{–}mode \end{cases}$$

Finally, this algorithm sets the session key $ek = e(g_n, g)^t = e(g_{n-1}, g_1)^t$ and outputs (C, ek).

• $Decrypt(PK, S/R, mode, C, i, sk_i)$: On receiving the ciphertext C, with the knowledge of PK, the set S or R, the ciphertext C and the chosen $mode$, either the user $i \in S$ for *Select–mode* or the user $i \notin R$ for *Cut–mode* can use sk_i to recover the session key as follows:

$$ek = \begin{cases} \dfrac{e(C_1, g_i)}{e(sk_i \cdot \prod\limits_{j\in S, j\neq i} g_{n-j+i}, C_0)} & \text{for } Select\text{–}mode \\ \dfrac{e(C_1, g_i)}{e(sk_i \cdot h_i/\prod\limits_{j\in R} g_{n-j+i}, C_0)} & \text{for } Cut\text{–}mode \end{cases}$$

It is easy to see that the secret key $sk_i = g_i^r$ is different from $sk_i = g_i^r \cdot \frac{h^{\mu^i}}{g_n}$ in our RBBE scheme. The reason is to keep consistent with Dan Boneh *et al.*'s scheme. For such a difference, we insert $n-1$ elements, $h_i = \frac{h^{\mu^i}}{g_n}$ for $i = 1, 2, \ldots, n-1$, into the public key PK to guarantee the successful decryption. Moreover, in the encryption phase, we can find out an interesting fact that two different elements, v and w, are used to produce the ciphertext under different modes, *i.e.*, v is used for *Select–mode* and w is used for *Cut–mode*, respectively. All others besides that in DMBE are the same as the previous schemes, *i.e.*, the Dan Boneh *et al.*'s scheme and our RBBE scheme.

Table 2. Performance evaluation of the DMBE scheme

	Computational complexity	Communication/Storage complexity
Setup	$(3n)\cdot E(\mathbb{G}) + 1\cdot M(\mathbb{G}) + (n-1)\cdot D(\mathbb{G})$	$(3n+1)\cdot l_{\mathbb{G}}(PK)$, $2\cdot l_{\mathbb{Z}_p^*}(MK)$
KeyGen	$\lvert U\rvert \cdot E(\mathbb{G})$ (for $\lvert U\rvert$ users)	$\lvert U\rvert \cdot l_{\mathbb{G}}$ (sk_i, for $\lvert U\rvert$ users)
Encrypt	$2\cdot E(\mathbb{G}) + 1\cdot E(\mathbb{G}_T) + \lvert S\rvert \cdot M(\mathbb{G}) + 1\cdot B$ (*Select-mode*) $2\cdot E(\mathbb{G}) + 1\cdot E(\mathbb{G}_T) + (\lvert R\rvert - 1)\cdot M(\mathbb{G}) + 1\cdot D(\mathbb{G}) + 1\cdot B$ (*Cut-mode*)	$2\cdot l_{\mathbb{G}}$ (C_S) (*Select-mode*) $2\cdot l_{\mathbb{G}}$ (C_R) (*Cut-mode*)
Decrypt	$(\lvert S\rvert - 1)\cdot M(\mathbb{G}) + 2\cdot B + 1\cdot D(\mathbb{G}_T)$ (*Select-mode*) $\lvert R\rvert \cdot M(\mathbb{G}) + 1\cdot D(\mathbb{G}) + 2\cdot B + 1\cdot D(\mathbb{G}_T)$ (*Cut-mode*)	$1\cdot l_{\mathbb{G}_T}$ (ek) (*Select-mode*) $1\cdot l_{\mathbb{G}_T}$ (ek) (*Cut-mode*)

Next we consider the validity of this scheme. According to these two modes described above, we have two cases. For case $mode = Select$, each user $i \in S$ can recover the session key as Eq.(13). For case $mode = Cut$, each user $i \notin R$ can recover the session key as Eq.(14).

$$\begin{aligned} ek' =& \frac{e(C_1, g_i)}{e(sk_i \cdot \prod_{j\in S, j\neq i} g_{n-j+i}, C_0)} \\ =& \frac{e(v \cdot \prod_{j\in S} g_{n-j}, g_i)^t}{e(g_i^r \cdot \prod_{j\in S, j\neq i} g_{n-j+i}, g)^t} \\ =& \frac{e(g^r \cdot \prod_{j\in S} g_{n-j}, g_i)^t}{e((g^r \cdot \prod_{j\in S, j\neq i} g_{n-j})^{\mu^i}, g)^t} \\ =& e(g_{n-i}, g_i)^t = e(g_n, g)^t = ek \end{aligned} \tag{13}$$

$$\begin{aligned} ek' =& \frac{e(C_1, g_i)}{e(sk_i \cdot h_i / \prod_{j\in R} g_{n-j+i}, C_0)} \\ =& \frac{e(w / \prod_{j\in R} g_{n-j}, g_i)^t}{e(g_i^r \cdot h^{\mu^i} / (g_n \cdot \prod_{j\in R} g_{n-j+i}), g)^t} \\ =& \frac{e(g^r \cdot h / \prod_{j\in R} g_{n-j}, g_i)^t}{e((g^r \cdot h / (g_{n-i} \cdot \prod_{j\in R} g_{n-j}))^{\mu^i}, g)^t} \\ =& e(g_{n-i}, g_i)^t = e(g_n, g)^t = ek \end{aligned} \tag{14}$$

2. Performance evaluation of DMBE

The performance evaluation of the DMBE scheme is described in Table 2. We define that $|S|$ and $|R|$ are the number of users in the authorized and unauthorized set, respectively. And, we have $|S| + |R| = |U| = n - 1$. For sake of clarity, the notations used are the same as defined in Section IV.2. In Table 2, the private key of each user is just a group element, which has fixed $l_{\mathbb{G}}$ length and $E(\mathbb{G})$ computational cost. Moreover, the total overheads of $KeyGen$ in system are $|U| \cdot E(\mathbb{G})$ for computational complexity and $|U| \cdot l_{\mathbb{G}}$ for storage complexity, respectively. The algorithm $Encrypt$ and $Decrypt$ can be performed with computational complexity of either $O(|S|)$ or $O(|R|)$ for each mode. In addition, both the session key and the ciphertext are constant size for each mode.

From Table 2, it is easy to see that the discrepancies in computational overheads on $Encrypt$ are $|S| \cdot M(\mathbb{G})$ for Select-mode and $(|R| - 1) \cdot M(\mathbb{G}) + 1 \cdot D(\mathbb{G})$ for Cut-mode, respectively. Assume that multiplication consumes nearly the same computational time as division in $\mathbb{G}$, *i.e.*, $M(\mathbb{G}) \approx D(\mathbb{G})$. The above overheads are further simplified as $|S| \cdot M(\mathbb{G})$ for Select-mode and $|R| \cdot M(\mathbb{G})$ for Cut-mode, respectively. Similarly, the differences on $Decrypt$ are $(|S| - 1) \cdot M(\mathbb{G})$ for Select-mode and $(|R| + 1) \cdot M(\mathbb{G})$ for Cut-mode, respectively. By using them, the performance can be optimized with respect to the following two aspects:

• When Select-mode is chosen, we require that the equations, $|S| \leq |R|$ for $Encrypt$ and $|S| - 1 \leq |R| + 1$ for $Decrypt$, should be satisfied simultaneously. According to $|S| + |R| = |U|$, we easily acquire the condition $|S| \leq \lfloor \frac{n-1}{2} \rfloor$, under which the overheads for Select-mode are smaller than those for Cut-mode.

• When Cut-mode is chosen, the equations, both $|S| \geq |R|$ for $Encrypt$ and $|S| - 1 \geq |R| + 1$ for $Decrypt$, should be satisfied. We also reach a conclusion that when the condition $|S| \geq \lceil \frac{n+1}{2} \rceil$ holds, the Cut-mode is more efficient than the Select-mode to encrypt and decrypt the message.

To summarize, the choice of encryption mode will be uniquely determined by the relationship between the number of the authorized users and the total number of users in the system. Namely, the Select-mode should be chosen if $|S| < |U|/2$; otherwise ($|R| \leq |U|/2$)**, the Cut-mode is chosen. Under this case, the computational complexity of our scheme can be optimized to $O(\min\{|S|, |R|\}) \leq O(\lceil \frac{|U|}{2} \rceil)$. This means that the performance of the DMBE scheme with dual modes is more efficient than that of the previous schemes supporting single mode.

By integrating such two modes, our DMBE scheme can help to improve the performance of secure group-oriented communication. Take the Email system as an example, there are usually two kinds of messages: one is the regular-mail messages that are sent only to a few friends; another is the notified messages (such as official document, bulletin, meeting announcement, *etc.*) which are usually used to broadcast messages. Our DMBE scheme is directly applicable to such a practical scenario: Select-mode for the former, and Cut-mode for the latter.

3. Security analysis of DMBE

In the DMBE scheme, we insert $n - 1$ elements $(h_1, \ldots, h_{n-1})$ into PK, which have no influence on the security of the new scheme due to the unknown μ and g_n. Next, we give the proof on the semantic security of the proposed DMBE scheme.

Theorem 2 The DMBE scheme is (ϵ, n) semantically secure against chosen plaintext attack with full

** When n is even, there exists the similar computational overheads on $|S| = n/2$ ($|R| = n/2 - 1$) for both modes.

collusion under the (ϵ, n)-DBDHE assumption in $\mathbb{S}$, and the advantage of the adversary $\mathcal{A}$ is $Adv^{\mathrm{IND}}_{\mathrm{DMBE}}(\mathcal{A}) < \epsilon$.

Proof Suppose there exists an adversary $\mathcal{A}$ who can break our DMBE scheme with the advantage ϵ, that is, $Adv^{\mathrm{IND}}_{\mathrm{DMBE}}(\mathcal{A}) \geq \epsilon$. Given the user group $U = \{1, 2, \ldots, n-1\}$, our objective is to build a simulator $\mathcal{B}$ to solve the DBDHE problem: given elements $(G, G^t, \{G^{\mu^i}\}_{i=1, i\neq n}^{2n}) \in \mathbb{G}^{2n+1}$ and $W \xleftarrow{R} \mathbb{G}_T$ to output 1 if $W = e(G^{\mu^n}, G)^t$, otherwise output 0. We utilize the following game to depict the construction of $\mathcal{B}$.

• Initialization. The adversary $\mathcal{A}$ declares the set $S^* \subseteq U$ which he wants to attack, so the revocation set is $R^* = U \setminus S^*$.

• Setup. The simulator $\mathcal{B}$ simulates *Setup* to obtain the public key PK. And then he sends PK to the adversary $\mathcal{A}$. This process is divided into the following 5 steps:

1) Set $g = G$, where G is a generator of $\mathbb{G}$;

2) Set $G_i = G^{\mu^i}$ for $i = 1, 2, \ldots, n-1, n+1, \ldots, 2n$, so we have $g_i = g^{\mu^i} = G^{\mu^i} = G_i$, where $\mu \in \mathbb{Z}_p^*$ and μ is unknown;

3) Randomly select λ in $\mathbb{Z}_p^*$, set $r = \lambda + \sum_{j\in S^*} \mu^{n-j}$ and r is unknown;

4) Randomly select δ in $\mathbb{Z}_p^*$, set $h = G^\delta \cdot \prod_{k\in U} G_{n-k}$, so we can compute $v = g^r = G^\lambda \cdot \prod_{j\in S^*} G_{n-j}$ and $w = g^r \cdot h = G^{\lambda+\delta} \cdot \prod_{j\in S^*} G_{n-j} \cdot \prod_{k\in U} G_{n-k}$;

5) Compute

$$\begin{aligned} h_i &= \frac{h^{\mu^i}}{g_n} = \frac{G_i^\delta \cdot \prod_{k\in U} G_{n-k+i}}{G_n} \\ &= G_i^\delta \cdot \prod_{k\in U, k\neq i} G_{n-k+i} \end{aligned}$$

Finally, $\mathcal{B}$ sends $PK := (g, v, w, \{h_i\}_{i=1}^{n-1}, \{g_i\}_{i=1, i\neq n}^{2n})$ to $\mathcal{A}$. Note that λ and δ are chosen uniformly at random, this public key has an identical distribution to that in the actual construction.

• Learning. The adversary $\mathcal{A}$ makes secret key queries to the *KeyGen* Oracle for any user $i \in R^*$. The secret key sk_i can be computed as Eq.(15).

$$sk_i = g_i^r = G_i^r = G_i^\lambda \cdot \prod\nolimits_{j\in S^*} G_{n-j+i} \tag{15}$$

Remark. Note that it is infeasible for the simulator to generate the secret key corresponding to the user that in the designated set S^*. The reason is that if the user $i \in S^*$, $\mathcal{B}$ cannot compute $\prod_{j\in S^*} G_{n-j+i}$ because G_n is unknown.

• Challenge. The adversary $\mathcal{A}$ picks two messages m_0 and m_1, selects $mode \in \{Select, Cut\}$, and then sends them to the simulator. The simulator $\mathcal{B}$ randomly picks $\sigma \in \{0, 1\}$, and simulates the *Encrypt* algorithm to acquire $C = (C_0, C_1)$. With the known G^t, the ciphertext C can be computed according to the specified *mode*, where $C_0 = G^t$ and C_1 can be computed as follows:

$$C_1 = \begin{cases} (v \cdot \prod\limits_{j\in S^*} g_{n-j})^t & \text{for } Select\text{–}mode \\ (w/\prod\limits_{j\in R^*} g_{n-j})^t & \text{for } Cut\text{–}mode \end{cases}$$

where

$$\begin{aligned} (v \cdot \prod_{j\in S^*} g_{n-j})^t &= (G^\lambda \cdot \prod_{j\in S^*} G_{n-j} \cdot \prod_{j\in S^*} G_{n-j})^t \\ (w/\prod_{j\in R^*} g_{n-j})^t &= (G^{\lambda+\delta} \cdot \prod_{j\in S^*} G_{n-j} \cdot \prod_{j\in S^*} G_{n-j})^t \end{aligned}$$

$\mathcal{B}$ sets $ek = e(g_n, g)^t = e(G_n, G^t) = W$, such that the chosen message m_σ is encrypted by $m_\sigma \oplus W$. Finally, the simulator $\mathcal{B}$ sends the challenge $(C, mode, m_\sigma \oplus W)$ to the adversary.

• Response. The adversary $\mathcal{A}$ outputs $\sigma^* \in \{0, 1\}$ as the guess. If $\sigma^* = \sigma$, $\mathcal{B}$ outputs 1; otherwise outputs 0.

Availability of secret keys At first, we illustrate the availability of the queried secret key sk_i. Here we choose a set S' and $S' \cap R^* \neq \emptyset$ such that $R' = U \setminus S'$, our goal is to check the secret key sk_i $(i \in S' \cap R^*)$ constructed above is valid. In this setting, the user i is not a member in R', *i.e.*, $i \notin R'$. We choose t' in $\mathbb{Z}_p^*$ randomly, set the session key $ek = e(G_n, G)^{t'}$, and the ciphertext $C_{R'} = (C_0', C_1')$ where $C_0' = g^{t'} = G^{t'}$ and C_1' is computed as follows:

$$C_1' = \begin{cases} (v \cdot \prod\limits_{j\in S'} g_{n-j})^{t'} & \text{for } Select\text{–}mode \\ (w/\prod\limits_{j\in R'} g_{n-j})^{t'} & \text{for } Cut\text{–}mode \end{cases}$$

where

$$\begin{aligned} (v \cdot \prod_{j\in S'} g_{n-j})^{t'} &= (G^\lambda \cdot \prod_{j\in S^*} G_{n-j} \cdot \prod_{j\in S'} G_{n-j})^{t'} \\ (w/\prod_{j\in R'} g_{n-j})^{t'} &= (G^{\lambda+\delta} \cdot \prod_{j\in S^*} G_{n-j} \cdot \prod_{j\in S'} G_{n-j})^{t'} \end{aligned}$$

And then, the user i can run the *Decrypt* algorithm to recover ek' in terms of the *mode*.

If $mode = Select$, the user $i \in S'$ can recover the session key as follows:

$$ek' = e(C_1', g_i)/e(sk_i \cdot \prod_{j\in S', j\neq i} g_{n-j+i}, C_0')$$

$$
\begin{aligned}
&= \frac{e(G^{\lambda} \cdot \prod_{j \in S^*} G_{n-j} \cdot \prod_{j \in S'} G_{n-j}, G_i)^{t'}}{e(G_i^{\lambda} \cdot \prod_{j \in S^*} G_{n-j+i} \cdot \prod_{j \in S', j \neq i} G_{n-j+i}, G^{t'})} \\
&= \frac{e(G^{\lambda} \cdot \prod_{j \in S^*} G_{n-j} \cdot \prod_{j \in S'} G_{n-j}, G^{\mu^i})^{t'}}{e((G^{\lambda} \cdot \prod_{j \in S^*} G_{n-j} \cdot \prod_{j \in S', j \neq i} G_{n-j})^{\mu^i}, G)^{t'}} \\
&= \frac{e(G^{\lambda} \cdot \prod_{j \in S^*} G_{n-j} \cdot \prod_{j \in S'} G_{n-j}, G)^{\mu^i t'}}{e(G^{\lambda} \cdot \prod_{j \in S^*} G_{n-j} \cdot \prod_{j \in S', j \neq i} G_{n-j}, G)^{\mu^i t'}} \\
&= e(G_{n-i}, G)^{\mu^i t'} = e(G_{n-i}, G_i)^{t'} \\
&= e(G_n, G)^{t'} = ek
\end{aligned}
$$

If $mode = Cut$, the user $i \notin R'$ can also recover the session key as follows:

$$
\begin{aligned}
ek' &= e\left(C_1', g_i\right) / e(sk_i \cdot h_i / \prod_{j \in R'} g_{n-j+i}, C_0') \\
&= \frac{e(G^{\lambda+\delta} \cdot \prod_{j \in S^*} G_{n-j} \cdot \prod_{j \in S^*} G_{n-j}, G_i)^{t'}}{e\left(\frac{G_i^{\lambda+\delta} \cdot \prod_{j \in S^*} G_{n-j+i} \cdot \prod_{k \in U, k \neq i} G_{n-k+i}}{\prod_{j \in R'} G_{n-j+i}}, G^{t'}\right)} \\
&= \frac{e(G^{\lambda+\delta} \cdot \prod_{j \in S^*} G_{n-j} \cdot \prod_{j \in S'} G_{n-j}, G^{\mu^i})^{t'}}{e\left(\left(\frac{G^{\lambda+\delta} \cdot \prod_{j \in S^*} G_{n-j} \cdot \prod_{k \in U, k \neq i} G_{n-k}}{\prod_{j \in R'} G_{n-j}}\right)^{\mu^i}, G\right)^{t'}} \\
&= \frac{e(G^{\lambda+\delta} \cdot \prod_{j \in S^*} G_{n-j} \cdot \prod_{j \in S'} G_{n-j}, G)^{\mu^i t'}}{e(G^{\lambda+\delta} \cdot \prod_{j \in S^*} G_{n-j} \cdot \prod_{j \in S', j \neq i} G_{n-k}, G)^{\mu^i t'}} \\
&= e\left(G_{n-i}, G\right)^{\mu^i t'} = e\left(G_{n-i}, G_i\right)^{t'} \\
&= e\left(G_n, G\right)^{t'} = ek
\end{aligned}
$$

So we end the description on the availability of the secret key sk_i constructed by the simulator.

Advantage evaluation The computation of $Adv_{\mathrm{DMBE}}^{\mathrm{IND}}(\mathcal{A})$ and $Adv_{\mathrm{DBDHE}}^{\mathrm{IND}}(\mathcal{B})$ is similar to that in the proof of Theorem 1. Based on Eqs. (11) and (12), $Adv_{\mathrm{DMBE}}^{\mathrm{IND}}(\mathcal{A})$ and $Adv_{\mathrm{DBDHE}}^{\mathrm{IND}}(\mathcal{B})$ can be computed as follows:

$$
\begin{aligned}
Adv_{\mathrm{DMBE}}^{\mathrm{IND}}(\mathcal{A}) &= |Pr[\sigma^* = \sigma] - 1/2| \\
&= 1/2 \left| \begin{array}{l} Pr[\sigma^* = 1 | \sigma = 1] \\ -Pr[\sigma^* = 1 | \sigma = 0] \end{array} \right|
\end{aligned}
$$

$$
\begin{aligned}
&Adv_{\mathrm{DBDHE}}^{\mathrm{IND}}(\mathcal{B}) \\
&= \left| \begin{array}{l} Pr[\mathcal{B}(\mathcal{L}, e(G_n, G)^t) = 1 : G \overset{R}{\leftarrow} \mathbb{G}, \mu, t \overset{R}{\leftarrow} \mathbb{Z}_p^*] \\ -Pr[\mathcal{B}(\mathcal{L}, W) = 1 : G \overset{R}{\leftarrow} \mathbb{G}, W \overset{R}{\leftarrow} \mathbb{G}_T, \mu, t \overset{R}{\leftarrow} \mathbb{Z}_p^*] \end{array} \right| \\
&= 1/2 \left| \begin{array}{l} Pr[\sigma^* = 1 | \sigma = 1 \wedge W = e(G_n, G)^t] \\ -Pr[\sigma^* = 1 | \sigma = 0 \wedge W = e(G_n, G)^t] \end{array} \right|
\end{aligned}
$$

Based on the advantage evaluation, we get $Adv_{\mathrm{DBDHE}}^{\mathrm{IND}}(\mathcal{B}) = Adv_{\mathrm{DMBE}}^{\mathrm{IND}}(\mathcal{A})$. According to the hypothesis that $Adv_{\mathrm{DMBE}}^{\mathrm{IND}}(\mathcal{A}) \geq \epsilon$, we have $Adv_{\mathrm{DBDHE}}^{\mathrm{IND}}(\mathcal{B}) \geq \epsilon$. This is opposite to the definition of DBDHE assumption. So the hypothesis is wrong, *i.e.*, $Adv_{\mathrm{DMBE}}^{\mathrm{IND}}(\mathcal{A}) < \epsilon$. Consequently, our DMBE scheme is (ϵ, n) semantically secure against chosen plaintext attack with full collusion under the (ϵ, n)-DBDHE assumption in $\mathbb{S}$, and the advantage of the adversary $\mathcal{A}$ is $Adv_{\mathrm{DMBE}}^{\mathrm{IND}}(\mathcal{A}) < \epsilon$.

VI. Conclusions

In this paper we explore approaches to achieve secure group-oriented communication with designation and revocation mechanisms simultaneously. Based on this requirement, we present a new provable secure scheme of RBBE which is designed on Dan Boneh *et al.*'s scheme over the designation mechanism. Finally, we combine two above-mentioned schemes into a new cryptosystem, called Dual-mode broadcast encryption.

From the above work we can see that it is feasible to construct a BE cryptosystem which supports designation and revocation mechanisms, simultaneously. Our approach is to integrate such two opposite or complementary functionalities into one cryptosystem by designing the similar aggregation, shift, and cancellation methods. Moreover, we find that the computational costs of cryptosystem with dual modes is more efficient than that with single mode.

References

[1] A. Fiat and M. Naor, "Broadcast encryption", *Proc. of Annual International Cryptology Conference, LNCS,* Vol.773, pp.480–491, 1993.

[2] D. Boneh, C. Gentry and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys", *Proc. of Annual International Cryptology Conference, LNCS,* Vol.3621, pp.258–272, 2005.

[3] C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys", *Proc. of International Conference on the Theory and Application of Cryptology and Information Security*, Kuching, Malaysia, *LNCS*, Vol.4833, pp.200–215, 2007.

[4] C. Gentry and B. Waters, "Adaptive security in broadcast encryption systems (with short ciphertexts)", *Proc. of International Conference on the Theory and Applications of Cryptographic Techniques*, Cologne, Germany, *LNCS*, Vol.5479, pp.171–188, 2009.

[5] D.H. Phan, D. Pointcheval, S.F. Shahandashti, *et al.*, "Adaptive CCA broadcast encryption with constant-size

secret keys and ciphertexts", *International Journal of Information Security*, Vol.12, No.4, pp.251–265, 2013.

[6] B. Wesolowski and P. Junod, "Ciphertext-policy attribute-based broadcast encryption with small keys", *Proc. of International Conference on Information Security and Cryptology, LNCS*, Seoul, South Korea, Vol.9558, pp.53–68, 2015.

[7] M. Li, X. Xu, R. Zhuang, *et al.*, "Identity-based broadcast encryption schemes for open networks", *Proc. of International Conference on Frontier of Computer Science and Technology*, Dalian, China, IEEE, pp.104–109, 2015.

[8] B. Libert, K.G. Paterson, and E.A. Quaglia, "Anonymous broadcast encryption: Adaptive security and efficient constructions in the standard model", *Proc. of International Workshop on Public Key Cryptography, LNCS*, Darmstadt, Germany, Vol.7293, pp.206–224, 2012.

[9] W. Liu, J. Liu, Q. Wu, *et al.*, "Practical chosen-ciphertext secure hierarchical identity-based broadcast encryption", *International Journal of Information Security*, Vol.15, No.1, pp.35–50, 2016.

[10] M. Naor and B. Pinkas, "Efficient trace and revoke schemes", *Proc. of International Conference on Financial Cryptography, LNCS*, Anguilla, British West Indies, Vol.1962, pp.1–20, 2000.

[11] Y. Dodis and N. Fazio, "Public key broadcast encryption for stateless receivers", *Proc. of ACM Workshop on Digital Rights Management, LNCS*, Washington, DC, USA, Vol.2696, pp.61–80, 2002.

[12] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing", *Proc. of Annual International Cryptology Conference, LNCS*, Vol.2139, pp.213–229, 2001.

[13] M.T. Goodrich, J.Z. Sun and R. Tamassia, "Efficient tree-based revocation in groups of low-state devices", *Proc. of Annual International Cryptology Conference, LNCS*, Vol.3152, pp.511–527, 2004.

[14] C. Delerablée, P. Paillier, and D. Pointcheval, "Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys", *Proc. of International Conference on Pairing-Based Cryptography, LNCS,* Tokyo, Japan, Vol.4575, pp.39–59, 2007.

[15] J. Lai, Y. Mu, and F. Guo, *et al.*, "Anonymous identity-based broadcast encryption with revocation for file sharing", *Proc. of Australasian Conference on Information Security and Privacy, LNCS*, Melbourne, VIC, Australia, Vol.9723, pp.223–239, 2016.

[16] Q. Huang, Z. Ma, and Y. Yang, *et al.*, "Eabds: attribute-based secure data sharing with efficient revocation in cloud computing", *Chinese Journal of Electronics*, Vol.24, No.4, pp.862–868, 2015.

[17] Y. Zhu, D. Li, and L. Yang, "Traitor tracing based on partially-ordered hierarchical encryption", *Proc. of International Conference on Trusted Systems, LNCS*, Beijing, China, Vol.9473, pp.278–293, 2014.

[18] M.S. Lee, J. Lee, and J.D. Hong, "An efficient public trace and revoke scheme using augmented broadcast encryption scheme", *Journal of the Korea Institute of Information Security and Cryptology*, Vol.26, No.1, pp.17–30, 2016.

[19] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps", *Proc. of Annual International Cryptology Conference, LNCS*, Vol.3152, pp.56–72, 2004.

[20] M. Bellare, "A note on negligible functions", *Journal of Cryptology*, Vol.15, No.4, pp.271–284, 2002.

[21] D. Su and K. Lü, "Paillier' s trapdoor function hides θ (n) bits", *Science China Information Sciences*, Vol.54, No.9, pp.1827–1836, 2011.

[22] D. Boneh, X. Boyen, and E.J. Goh"Hierarchical identity based encryption with constant size ciphertext", *Proc. of International Conference on the Theory and Applications of Cryptographic Techniques, LNCS*, Aarhus, Denmark, Vol.3494, pp.440–456, 2005.

[23] M. Bellare, A. Desai, E. Jokipii, *et al.*, "A concrete security treatment of symmetric encryption", *Proc. of IEEE Annual Symposium on Foundations of Computer Science*, Miami Beach, FL, USA, pp.394–403, 1997.

[24] O. Goldreich, *Foundations of Cryptography: Vol.1, Basic Tools*, Cambridge University Press, Cambridge, UK, pp.119–123, 2001.

ZHU Yan received the Ph.D. degree in computer science from Harbin Engineering University, China, in 2005. He is currently a professor at the University of Science and Technology Beijing (USTB), China. He was an associate professor at Peking University, China, from 2007 to 2012. He was a visiting associate professor at the Arizona State University, from 2008 to 2009, and a visiting research investigator of the University of Michigan-Dearborn in 2012. His research interests include cryptography, secure computation, and network security. (Email: zhuyan@ustb.edu.cn)

YU Ruyun received the M.S. degree from the School of Computer and Communication Engineering, USTB, China, in 2015. She is currently working toward the Ph.D. degree at University of Science and Technology, Beijing, China. Her research interests include group-oriented encryption and fine-grained access control. (Email: yuruyun@xs.ustb.edu.cn)

CHEN E received the B.S. degree from the School of Mathematics and Physics, USTB. She is a Ph.D. candidate at USTB. Her research interests include attribute based system and lattice based cryptography. (Email: chene@xs.ustb.edu.cn)

HUANG Dijiang received the B.S. degree from the Beijing University of Posts and Telecommunications, China, in 1995, and the M.S. and Ph.D. degrees from the University of Missouri-Kansas City, in 2001 and 2004, respectively. He is an associate professor at the School of Computing Informatics and Decision System Engineering, Arizona State University. His current research interests include computer networking, security, and privacy. (Email: dijiang@asu.edu)