Recipient Revocable Identity-Based Broadcast Encryption

How to Revoke Some Recipients in IBBE without Knowledge of the Plaintext

Willy Susilo
University of Wollongong, Australia
wsusilo@uow.edu.au

Rongmao Chen
University of Wollongong, Australia
rc517@uowmail.edu.au

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

Guomin Yang
University of Wollongong, Australia
gyang@uow.edu.au

Yi Mu
University of Wollongong, Australia
ymu@uow.edu.au

Yang-Wai Chow
University of Wollongong, Australia
caseyc@uow.edu.au

ABSTRACT

In this paper, we present the notion of recipient-revocable identity-based broadcast encryption scheme. In this notion, a content provider will produce encrypted content and send them to a third party (which is a broadcaster). This third party will be able to revoke some identities from the ciphertext. We present a security model to capture these requirements, as well as a concrete construction. The ciphertext consists of $k + 3$ group elements, assuming that the maximum number of revocation identities is k. That is, the ciphertext size is linear in the maximal size of $\mathcal{R}$, where $\mathcal{R}$ is the revocation identity set. However, we say that the additional elements compared to that from an IBBE scheme are only for the revocation but not for decryption. Therefore, the ciphertext sent to the users for decryption will be of constant size (i.e.,3 group elements). Finally, we present the proof of security of our construction.

Categories and Subject Descriptors

E.3 [**Data Encryption**]: Public Key Cryptosystems

Keywords

Identity-based Broadcast Encryption, Recipients, Revocation, Constant Size

1. INTRODUCTION

In this paper, we develop a new cryptographic primitive called a recipient revocable identity-based broadcast encryption (RR-IBBE) scheme. This is an extension of the identity-based broadcast encryption scheme, in the case where a third party can remove some of the receivers from the set of receivers stated in the original ciphertext. The third party cannot decrypt the content of the ciphertext, but rather, this third party can only revoke some of the recipients of the original ciphertext. Consider the following example where this primitive is useful.

Motivating Story. Consider the case where a major telco provider, such as Verizon, collaborates with a big content provider such as Netflix. In order to win the competition in the market, Verizon offers its subscribers free access to Netflix's movies database. Nevertheless, obviously Netflix does not want to offer this service for an unlimited number of users due to the copyright issue, and hence, there is a need to know the total number of users that may receive the content. Additionally, Netflix cannot provide the content in clear to Verizon as by doing this way, Netflix will no longer have any control on the number of recipients. Due to the collaboration, it is evident that Netflix and Verizon must share the information about the subscribers. From Netflix's point of view, the total number of users is important and Netflix is not interested to know which user will eventually be able to retrieve the content, as this will be decided by Verizon. On the other hand, Verizon would like to send the content to as many subscribers as possible, since when the subscribers receive the content, then they will have to use Verizon's network, and hence, this will provide income to Verizon as Verizon can charge its users. When we consider the recipient's point of view, some recipient (or subscriber) may not like to receive the content (for example, a subscriber has seen a particular movie). As such, this particular recipient will tell Verizon to not send the movie to him/her. In this situation, then Verizon must have the ability to *revoke* this person's access so that he/she can no longer access the encrypted content provided by Netflix, and therefore, no charge to this user. The complication happens since Netflix will provide the encrypted content to Verizon, rather than its plaintext form. Hence, it is required that Verizon can only *revoke* the users who opt-out for this particular content, without the need to decrypt and re-encrypt the content. We need to highlight that Verizon cannot provide the information about which recipients would like to view the encrypted content a priori, since Verizon does not know whether any particular recipient will opt-out from viewing a particular movie. The situation is illustrated in Figure 1. We need to highlight that the ciphertext sent by Netflix to Verizon is via a secure channel, as this ciphertext is solely created for Verizon. On the other hand, Verizon can use a public channel to broadcast the "modified" ciphertext to its subscribers.

ASIA CCS'16, May 30-June 03, 2016, Xi'an, China

DOI: http://dx.doi.org/10.1145/2897845.2897848

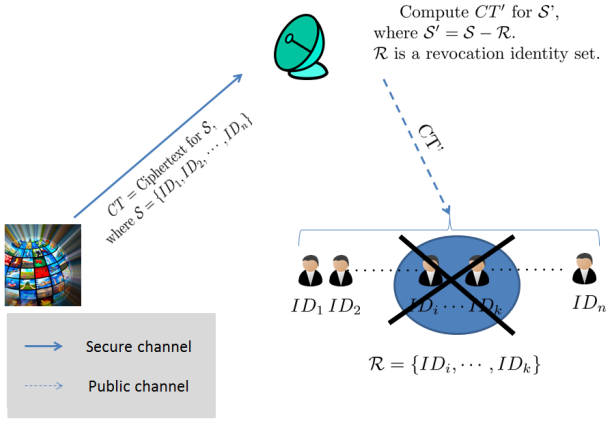

Figure 1: RR-IBBE

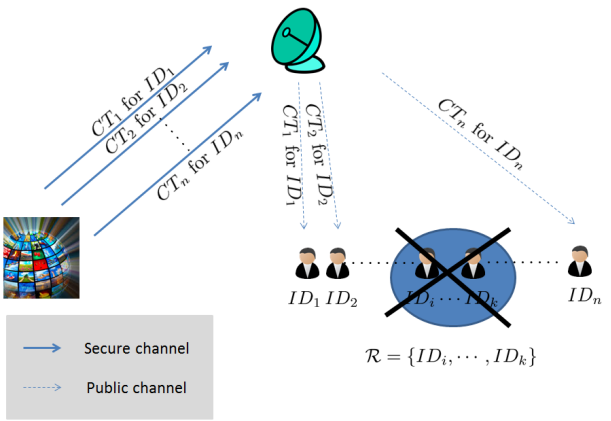

Figure 2: Trivial Solution

TRIVIAL SOLUTION. One may think that the above scenario can be solved trivially via an identity-based encryption scheme. The way it works is as follows. The content provider (i.e. Netflix) will encrypt the content for each of the individual identities, and then send these ciphertexts to the telco provider (i.e. Verizon). Then, the telco provider has the liberty whether to transmit the ciphertext to each individual subscriber one by one. This solution is depicted in Figure 2. We note that this solution is very impractical and therefore, unusable, since the number of ciphertexts is linear to the number of users. Hence, a clear requirement for this kind of situation is the need for a *constant size* ciphertext.

One may think that this scenario can be easily solved by incorporating a proxy re-encryption scheme. The idea is as follows. A proxy re-encryption scheme allows one to change the encryption for ID to ID'. Since our goal is to revoke ID, then we can use the re-encryption scheme to change the encryption to a random $\widetilde{ID}$, where nobody can in fact decrypt this. Nevertheless, this solution is less desirable as the third party applies and maintains a lot of keys. Furthermore, to date, there exists no identity-based broadcast encryption that supports re-encryption.

The last trivial solution is the adoption of double encryption. That is, the telco provider sets CT as a message and runs another broadcast encryption on the message CT for the new identity set $\mathcal{S}'$. This solution is trivial because the second encryption will increase the ciphertext size and the receivers know who have been revoked from two different identity sets $\mathcal{S}$ and $\mathcal{S}'$.

1.1 Related Work

The notion of broadcast encryption was put forth by Berkovits [2] to enable senders to efficiently broadcast ciphertexts to a large set of receivers such that only this chosen receivers can decrypt them. The formal analysis was later provided by Fiat and Naor in [12]. Since then, there have been many schemes that have been proposed in the literature (such as [1, 6, 16, 15, 14]) with various aims to offer improvements on private key size, ciphertext size, public key size, and computational costs for encryption and decryption. The idea of identity-based broadcast encryption (IBBE) was firstly proposed in [20] to avoid the necessity of a PKI setting. This allows the broadcaster to merely uses the identity of the recipients rather than their public keys. The construction with constant size ciphertext and private keys was proposed in [11].

Sahai and Waters extended this notion to construct a fuzzy identity-based encryption [19], which makes use of the similar identity to allow decryption, where the similarity is measured based on the hamming distance. This notion has been thoroughly studied under the banner of attribute-based encryption [13, 17, 22, 3], which is a very popular notion due to its fine-grain access control mechanism.

While identity-based cryptographic notion offers nice features, such as the unnecessity of public key certification, it has the drawback on having the difficulty to revoke the user's private key. The issue of efficient revocation mechanism has been studied in the seminal study by Boneh and Franklin in [8], where they represent an identity as $ID||T$, where ID is the real identity and T is a current time, but it is inefficient and not scalable because of the requirement of secure channels between the center and all users. Subsequently, a scalable revocable identity-based encryption was proposed in [4]. In the case of attribute-based encryption, the notion of dynamic credential and ciphertext delegation have been proposed in [18].

1.2 Our Contributions

We present the notion of recipient-revocable identity-based broadcast encryption, to answer the above aforementioned motivation. In our setting, the content provider (i.e. the encryptor) will produce encrypted content and send them to a third party, which is the broadcaster. Whilst this third party can broadcast the encrypted content to its subscribers, this third party will also be able to revoke some identities from the ciphertext, even without the ability of decrypting it. We present a security model to capture these requirements, together with a concrete construction. In our construction, the ciphertext consists of $k + 3$ group elements, assuming that the maximum number of revocation identities is k. That is, the ciphertext size is linear in the maximal size of $\mathcal{R}$, where $\mathcal{R}$ is the revocation identity set. However, we say that the additional elements compared to that from an IBBE scheme *are only* for the revocation *but not for decryption*. Therefore, the ciphertext sent to the user for decryption will be of *constant size* (i.e.,3 group elements). We also present the proof of security of our construction.

2. RECIPIENT-REVOCABLE IBBE

In this section, we define Recipient-Revocable Identity-Based Broadcast Encryption (RR-IBBE) and its security model.

2.1 Definition

Roughly speaking, an RR-IBBE scheme is based on the Identity-Based Broadcast Encryption (IBBE) with a new functionality, i.e., recipient revocation. Formally, an RR-IBBE scheme $\mathcal{RR}$-$\mathcal{IBBE}$ with security parameter 1^λ and maximum size N of the broadcast set, is composed of algorithms $\mathcal{RR}$-$\mathcal{IBBE}$ = (Setup, KeyGen, Encrypt, Revoke, Decrypt) defined as follows:

$\mathsf{Setup}(1^\lambda, N)$. Takes as input the security parameter 1^λ and an integer N the maximum size of the set of receivers for one encryption, and outputs a master public key mpk and a master secret key msk;

$\mathsf{KeyGen}(\mathsf{ID}, \mathsf{mpk}, \mathsf{msk})$. Takes as input a user identity ID and the master key pair (mpk, msk), and generates a user private key $\mathsf{sk}_{\mathsf{ID}}$;

$\mathsf{Encrypt}(\mathcal{S}, k, M, \mathsf{mpk})$. Takes as input a set of identities $\mathcal{S} = \{\mathsf{ID}_1, \mathsf{ID}_2, \cdots, \mathsf{ID}_n\}$ $(n \leq N)$, a maximum revocation number $k \leq n$, a message M and the master public key mpk, the algorithm encrypts M and outputs the ciphertext CT for the receivers $\mathcal{S}$;

$\mathsf{Revoke}(\mathcal{S}, CT, \mathcal{R}, \mathsf{mpk})$. Takes as input a ciphertext CT, a revocation identity set $\mathcal{R} = \{\mathsf{ID}_1, \mathsf{ID}_2, \cdots, \mathsf{ID}_l\} \subseteq \mathcal{S}$ $(l \leq k)$ and the master public key mpk, the revocation algorithm outputs a new ciphertext CT' for the receivers $\mathcal{S}' = \mathcal{S} - \mathcal{R}$;

$\mathsf{Decrypt}(\mathcal{S}', CT', \mathsf{mpk}, \mathsf{sk}_{\mathsf{ID}})$. Takes as input a ciphertext CT' for $\mathcal{S}'$, the master public key mpk and the private key $\mathsf{sk}_{\mathsf{ID}}$, and outputs M if $ID \in \mathcal{S}'$.

Correctness. It is required that for any message M, and $\mathsf{Encrypt}(\mathcal{S}, k, M, \mathsf{mpk}) = CT$, $\mathsf{Revoke}(\mathcal{S}, CT, \mathcal{R}, \mathsf{mpk}) = CT'$ we have

$$\mathsf{Decrypt}(\mathcal{S}, CT, \mathsf{mpk}, \mathsf{sk}_{\mathsf{ID}}) = M$$

$$\mathsf{Decrypt}(\mathcal{S}', CT', \mathsf{mpk}, \mathsf{sk}_{\mathsf{ID}}) = M$$

when $\mathsf{ID} \in \mathcal{S}$ and $\mathsf{ID} \in \mathcal{S}'$, where $\mathcal{S}' = \mathcal{S} - \mathcal{R}$.

In the definition of the encryption algorithm, we allow the encryptor to select the identity set $\mathcal{S}$ and the maximum revocation number k. The number k is smaller than n and its size is dependent on the real applications. If $k = 0$, it means the encryptor does not allow the third party to revoke any identity. If $k = n$, it means the third party can revoke all identities in the identity set.

2.2 Security Models

The security of an RR-IBBE scheme requires indistinguishability of encrypted message without a valid private key. Let CT be the original ciphertext for receiver $\mathcal{S}$ and CT' be the ciphertext after revocation for receiver $\mathcal{S}'$. The security requires that

- The message in the ciphertext CT cannot be distinguished without a private key associated with an identity $ID \in \mathcal{S}$.
- The message in the ciphertext CT' cannot be distinguished without a private key associated with an identity $ID \in \mathcal{S}'$. Mostly important, the adversary is allowed to have a private key associated with an identity in the revocation set $\mathcal{R}$.

We define the selective-ID semantic security (weaker than full security) for the RR-IBBE system. We use one security model to capture two different attacks. Our definition is similar to the notion of IND-sID-CPA for an IBBE scheme.

Init : The adversary $\mathcal{A}$ outputs a set $\mathcal{S}^* = \{ID_1^*, ..., ID_{s^*}^*\}$ $(s^* \leq n)$ of target identities.

Setup : The challenger runs $\mathsf{Setup}(1^\lambda, n)$ to obtain the master public key mpk and gives it to the adversary $\mathcal{A}$.

Extraction Query I : The adversary $\mathcal{A}$ adaptively issues key extraction query for any identity ID under the restriction that $ID \notin S^*$. The challenger runs KeyGen on ID and forwards the resulting private key to the adversary.

Challenge : Once $\mathcal{A}$ decides that extraction query I is over, it outputs two equal length plaintexts M_0, M_1 and a revocation identity set $\mathcal{R}^*$. The only constraint is that any identity in $\mathcal{R}^*$ cannot be the target identity in $\mathcal{S}^*$. Let $|\mathcal{R}^*| = k, \mathcal{S} = \mathcal{R}^* + \mathcal{S}^*$. The challenger picks a bit $b \in \{0, 1\}$ and generates the challenge ciphertext CT^* as follows:

$$CT = \mathsf{Encrypt}(\mathcal{S}, k, M_b, \mathsf{mpk})$$

$$CT' = \mathsf{Revoke}(\mathcal{S}, CT, \mathcal{R}^*, \mathsf{mpk}).$$

The adversary $\mathcal{A}$ is then given the challenge ciphertext $CT^* = CT'$ when $R^* \neq \emptyset$, otherwise it is given $CT^* = CT$ as the challenge ciphertext.

Extraction Query II : The adversary $\mathcal{A}$ continues to issue extraction query, as in Extraction Query I.

Guess : Finally, the adversary $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$ and wins the game if $b = b'$.

The total number of extraction queries issued by the adversary during the game is denoted by t. We then define the advantage of $\mathcal{A}$ in winning the above game as

$$\mathsf{Adv}^{\mathsf{sID\text{-}SS}}_{\mathcal{RR}\text{-}\mathcal{IBBE}}(t, n, \mathcal{A}) = \Pr[b = b'] - 1/2.$$

The probability is over the random coins of $\mathcal{A}$, the challenger and all probabilistic algorithms run by the challenger.

Definition 1. *A recipient-revocable identity-based broadcast encryption scheme $\mathcal{RR}$-$\mathcal{IBBE}$ is (t, n)-semantically secure if $\mathsf{Adv}^{\mathsf{SS}}_{\mathcal{RR}\text{-}\mathcal{IBBE}}(t, n) = \mathsf{negl}(\lambda)$ where $\mathsf{Adv}^{\mathsf{SS}}_{\mathcal{RR}\text{-}\mathcal{IBBE}}(t, n) = \max_{\mathcal{A}} \mathsf{Adv}^{\mathsf{SS}}_{\mathcal{RR}\text{-}\mathcal{IBBE}}(t, n, \mathcal{A})$ for all probabilistic polynomial time adversary $\mathcal{A}$.*

Remark. It is worth noting that our defined model considers two different types of attackers as follows.

1. When $R^* = \emptyset$. In this case, no revocation is involved and the adversary is given the ciphertext CT, which is directly generated for the target identity set S^*. This model guarantees that an adversary who has no decryption key (i.e, any private key of the recipient identity) learns nothing about the plaintext given the corresponding ciphertext. It is exactly the property of IND-sID-CPA security for an IBBE scheme.

2. When $R^* \neq \emptyset$. In this case, the challenge first encrypts M_b for the identity set $S = R^* + S^*$ to get the original ciphertext CT and then revoke the identity set R^* in CT to output the final challenge ciphertext CT'. This model guarantees that a revoked recipient cannot learn any information about the plaintext given the revocation ciphertext even though he has the decryption key for the original ciphertext (the one before revoked).

One may consider a stronger security notion of chosen ciphertext security by allowing the adversary to access the decryption oracle. However, we emphasize that any RR-IBBE scheme cannot meet such a security requirement, where the adversary is allowed to launch decryption queries on any ciphertext different from the challenge ciphertext. Essentially, the functionality of an RR-IBBE scheme requires that the encryption should be rerandomizable. This property allows the adversary to rerandomize the challenge ciphertext and query it to the decryption oracle to reveal the chosen challenge plaintext M_b.

3. THE PROPOSED RR-IBBE SCHEME

In this section, we present our concrete construction of the RR-IBBE system.

3.1 Overview

Let $\mathbb{G}, \mathbb{G}_T$ be two groups of order p and $g \in \mathbb{G}$ be the generator of $\mathbb{G}$. Our RR-IBBE system makes use of a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ which satisfies the following properties:

- For all $u, v \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p$, we have
$$e(u^a, v^b) = e(u, v)^{ab}.$$
- $e(g, g) \neq 1$;

A bilinear group $\mathbb{BG} = (\mathbb{G}, \mathbb{G}_T, e, p)$ is composed of objects as described above. We impose all group operations as well as the bilinear map e to be efficiently computable.

The central idea of our construction is to utilize the tricky role of the randomness used in the encryption. Roughly speaking, we revoke an identity from the ciphertext by transferring its "identity" role in the ciphertext to be part of the "new" randomness. Let g be a group element, r be a random number from $\mathbb{Z}_p$, $\alpha \in \mathbb{Z}_p$ be the master secret key and ID_1, ID_2 from $\mathbb{Z}_p$ be the identities. Suppose the ciphertext comprises of the following group element
$$g^{r(\alpha+ID_1)(\alpha+ID_2)}.$$
This encryption can be seen as an encryption for ID_1, ID_2 because ID_1 and ID_2 play the same role in the ciphertext. Let $r^* = r(\alpha + ID_1)$. We have the above element changed to the element
$$g^{r^*(\alpha+ID_2)}.$$
The corresponding ciphertext then is encrypted for ID_2 only if given such a ciphertext after transformation, anyone cannot change it back to the original one. To make sure this transformation is one-way, the random number r will be computed in other group elements to stop the adversary from changing it back. Our scheme construction is modified from an IBBE scheme proposed in [11]. More precisely, in comparison with [11], we add group elements $C_2, C_3, \cdots, C_{k+1}$ in the ciphertext which are used for revoking users. All these elements will be removed after the revocation. The structure of the final ciphertext is the same as the original ciphertext before revocation, which is equal to the ciphertext in [11].

3.2 Construction

Our concrete construction is as follows.

$\mathsf{Setup}(1^\lambda, N)$ Given a security parameter 1^λ and an integer N, the algorithm generates a bilinear group $\mathbb{BG} = (\mathbb{G}, \mathbb{G}_T, e, p)$ with two random generators $g, h \in \mathbb{G}$. Then, it randomly chooses a group exponent $\alpha \in \mathbb{Z}_p$ and computes $g_i = g^{\alpha^i}$, $h_i = h^{\alpha^i}, v = e(g, h)$ for all $i = 1, 2, \cdots, N$. Let $H : \{0,1\}^* \to \mathbb{Z}_p$ be a cryptographic hash function. The master public key mpk is
$$mpk = \Big(\mathbb{BG}, g, g_1, g_2, \cdots, g_N, h_1, h_2, \cdots, h_N, v, H\Big)$$
and the master secret key is $msk = (h, \alpha)$.

$\mathsf{KeyGen}(ID, mpk, msk)$ Given an identity $ID \in \mathbb{Z}_p$ and the master key pair (mpk, msk), the key generation algorithm computes d_{ID} as
$$d_{ID} = h^{\frac{1}{\alpha + H(ID)}}.$$

$\mathsf{Encrypt}(\mathcal{S}, k, M, mpk)$ Given a set of identities $\mathcal{S} = \{ID_1, ID_2, \cdots, ID_n\}$ $(n \leq N)$, a maximum revocation number $k \leq n$, a message $M \in \mathbb{G}_T$ and the master public key mpk, the encryption algorithm randomly chooses a value $r \in \mathbb{Z}_p$ and creates the ciphertext as
$$\begin{aligned} & CT \\ = \; & (C_m, C_0, C_1, C_2, \cdots, C_{k+1}) \\ = \; & \Big(v^r \cdot M,\ g^{r(\alpha+H(ID_1))\cdots(\alpha+H(ID_n))},\ h_1^r, h_2^r, \cdots, h_{k+1}^r\Big) \end{aligned}$$

$\mathsf{Revoke}(\mathcal{S}, CT, \mathcal{R}, mpk)$ Given a ciphertext $CT = (C_m, C_0, C_1, C_2, \cdots, C_{k+1})$ for $\mathcal{S}$, a revocation identity set $\mathcal{R} = \{ID'_1, ID'_2, \cdots, ID'_l\} \subseteq \mathcal{S}$ $(l \leq k)$ and the master public key mpk, the revocation algorithm works as follows.

- Let $F(x)$ be the polynomial in x as
$$\begin{aligned} F(x) &= \frac{1}{\prod_{ID' \in R} H(ID')} \prod_{ID' \in R} (x + H(ID')) \\ &= f_l x^l + f_{l-1} x^{l-1} + \cdots + f_1 x + f_0. \end{aligned}$$
We have $f_0 = 1$.
- Compute C'_m as
$$C'_m = C_m \cdot e(g, \prod_{i=1}^{l} C_i^{f_i}).$$
- Compute $C'_0 = C_0^{\frac{1}{\prod_{ID' \in R} H(ID')}}$.
- Compute C'_1 as
$$C'_1 = \prod_{i=1}^{l+1} C_i^{f_{i-1}}.$$
- Return the new ciphertext $CT' = (C'_m, C'_0, C'_1)$ for $\mathcal{S}' = \mathcal{S} - \mathcal{R}$.

$\mathsf{Decrypt}(\mathcal{S}', CT', mpk, d_{ID})$ Given a ciphertext $CT' = (C'_m, C'_0, C'_1)$ for $\mathcal{S}'$, the master public key mpk and the private key d_{ID}, the decryption algorithm works as follows.

- Let $G(x)$ be the polynomial in x as

$$G(x) = \frac{\prod_{ID' \in \mathcal{S}'}(x + H(ID'))}{x + H(ID)} = \prod_{i=0}^{n'-1} G_i x^i,$$

where G_i are coefficients. Compute

$$e_0 = e(C_1', g^{G_1} \prod_{i=1}^{n'-1} g_i^{G_{i+1}})$$

- Decrypt the message by

$$M = C_m' \cdot \left(\frac{e_0}{e(C_0', d_{ID})} \right)^{\frac{1}{G_0}}.$$

3.3 Correctness

Below we show that our construction meets the correctness requirement. When everything is computed as above, we can see that after revoking the identity set $\mathcal{R}$ from a ciphertext CT,

$$\begin{aligned}
C_m' &= C_m \cdot e(g, \prod_{i=1}^{l} C_i^{f_i}) \\
&= M \cdot e(g,h)^r \cdot \prod_{i=1}^{l} e(g,h)^{r f_i \alpha^i} \\
&= M \cdot e(g,h)^{r \cdot \frac{1}{\prod_{ID' \in R} H(ID')} \prod_{ID' \in R}(x + H(ID'))}, \\
C_0' &= C_0^{\frac{1}{\prod_{ID' \in R} H(ID')}} \\
&= g^{r \cdot \frac{1}{\prod_{ID' \in R} H(ID')} (\alpha + H(ID_1)) \cdots (\alpha + H(ID_n))} \\
&= g^{r \cdot \frac{1}{\prod_{ID' \in R} H(ID')} \prod_{ID' \in R}(x + H(ID')) \cdot \prod_{ID' \in \mathcal{S}'}(\alpha + H(ID'))}, \\
C_1' &= \prod_{i=1}^{l+1} C_i^{f_{i-1}} \\
&= \prod_{i=1}^{l+1} h^{r \alpha^i f_{i-1}} \\
&= h^{\alpha r (f_0 + f_1 \alpha + \cdots + f_l \alpha^l)} \\
&= h^{\alpha r \frac{1}{\prod_{ID' \in R} H(ID')} \prod_{ID' \in R}(x + H(ID'))}.
\end{aligned}$$

Let r' be a number defined as

$$r' = r \cdot \frac{1}{\prod_{ID' \in R} H(ID')} \prod_{ID' \in R} (x + H(ID')).$$

Then, we have

$$\begin{aligned}
C_m' &= M \cdot e(g,h)^{r \cdot \frac{1}{\prod_{ID' \in R} H(ID')} \prod_{ID' \in R}(x + H(ID'))} \\
&= M \cdot e(g,h)^{r'}, \\
C_0' &= g^{r \cdot \frac{1}{\prod_{ID' \in R} H(ID')} \prod_{ID' \in R}(x + H(ID')) \cdot \prod_{ID' \in \mathcal{S}'}(\alpha + H(ID'))} \\
&= g^{r' \prod_{ID' \in \mathcal{S}'}(\alpha + ID')}, \\
C_1' &= h^{\alpha r \frac{1}{\prod_{ID' \in R} H(ID')} \prod_{ID' \in R}(x + H(ID'))} \\
&= h^{\alpha r'} \\
&= h_1^{r'}.
\end{aligned}$$

This ciphertext can be seen as a ciphertext generated from the encryptor where $k = 0$.

As for the decryption algorithm $\mathsf{Decrypt}(\mathcal{S}', CT', mpk, d_{ID})$, we have that,

$$\begin{aligned}
e_0 &= e(C_1', g^{G_1} \prod_{i=1}^{n'-1} g_i^{G_{i+1}}) \\
&= e(h^{r'\alpha},\ g^{G_1 + \sum_{i=2}^{n'-1} G_{i+1} \alpha^i}) \\
&= e(h,g)^{r' \cdot \sum_{i=0}^{n'} G_i \alpha_i - r' G_0} \\
&= e(h,g)^{r' G(\alpha) - r' G_0} \\
e(C_0', d_{ID}) &= e\Big(g^{r' \prod_{ID' \in \mathcal{S}'}(x + H(ID'))}, h^{\frac{1}{\alpha + H(ID)}}\Big) \\
&= e(g,h)^{r' G(\alpha)}
\end{aligned}$$

Therefore, we have

$$\begin{aligned}
& C_m' \cdot \left(\frac{e_0}{e(C_0', d_{ID})} \right)^{\frac{1}{G_0}} \\
&= M \cdot e(g,h)^{r'} \cdot \left(e(g,h)^{-r' G_0} \right)^{\frac{1}{G_0}} \\
&= M.
\end{aligned}$$

That is, applying decryption on the ciphertext using a valid private key produces the original message m.

3.4 Ciphertext Size

One can note that the ciphertext from the original encryptor consists of $k + 3$ group elements, assuming that the maximum number of revocation identities is k. That is, the ciphertext size is linear in the maximal size of $\mathcal{R}$. However, we say that the additional elements compared to that from an IBBE scheme are only for the revocation but not for decryption. Therefore, the ciphertext sent to the user for decryption will be of constant size (i.e.,3 group elements), which is the same as that in an IBBE scheme.

4. COMPLEX ASSUMPTION

In this section, we first review the general Diffie-Hellman exponent assumption [6] and define a new assumption for our security analysis.

4.1 General Diffie-Hellman Exponent Assumption

In [6], Boneh, Boyen and Goh generalized a number of Diffie-Hellman-type complexity assumptions in generic group model[21], which includes Bilinear DH assumption (BDH) [9], the DH Inversion assumption (DHI)[5], the linear DH assumption [7], and the BDHE assumption [10], and others.

Here we give an overview of the generalization of the Diffie-Hellman Exponent assumptions in the symmetric case in [6]. Let $\mathbb{BG} = (\mathbb{G}, \mathbb{G}_T, e, p)$ be a bilinear map with $g_0 \in \mathbb{G}$ the generator of $\mathbb{G}$ and $g_T = e(g_0, g_0) \in \mathbb{G}_T$. Let s, n be positive integers and $P, Q \in \mathbb{F}_p[X_1, \cdots, X_{\widehat{n}}]^s$ be two s-tuples of $\widehat{n}$-variate polynomials over $\mathbb{F}_p$. Therefore, P and Q are just two ordered sets containing s multi-variate polynomials each. We write $P = (p_1, p_2, \cdots, p_s)$ and $Q = (q_1, q_2, \cdots, q_s)$ and require that $p_1 = q_1 = 1$. For a set Ω, a function $\widehat{h} : \mathbb{F}_p \to \Omega$ and a vector $(x_1, x_2, \cdots, x_{\widehat{n}}) \in \mathbb{F}_p^n$, we write

$$\widehat{h}(P(x_1, \cdots, x_{\widehat{n}})) = (\widehat{h}(p_1(x_1, \cdots, x_{\widehat{n}}), \cdots, \widehat{h}(p_s(x_1, \cdots, x_{\widehat{n}})).$$

We use a similar notation for the s-tuple Q.

We say that a polynomial $F \in \mathbb{F}_p[X_1, \cdots, X_{\widehat{n}}]$ is *dependent* on (P, Q) (denoted by $F \in < P, Q >$) if there exist $s^2 + s$ constants $\{a_{i,j}\}_{i,j=1}^{s}, \{b_i\}_{i=1}^{s}$ such that

$$F = \sum_{i,j=1}^{s} a_{i,j} p_i p_j + \sum_{i=1}^{s} b_i q_i.$$

We say that F is *independent* on (P, Q) (denoted by $F \notin < P, Q >$) if F is not dependent on $< P, Q >$.

The (P, Q, F)-*General Decision Diffie-Hellman Exponent* ((P, Q, F)-GDDHE) problem is defined as follows.

DEFINITION 2. ((P, Q, F)-GDDHE). *Given the tuple*

$$\widehat{H}(x_1, \cdots, x_{\widehat{n}}) = (g_0^{P(x_1, \cdots, x_{\widehat{n}})}, g_T^{Q(x_1, \cdots, x_{\widehat{n}})}) \in \mathbb{G}^s \times \mathbb{G}_T^s,$$

and $T \in \mathbb{G}_T$, decide whether $T = g_T^{F(x_1, \cdots, x_{\widehat{n}})} \in \mathbb{G}_T$.

We say that an algorithm $\mathcal{D}$ that outputs $b \in \{0, 1\}$ has advantage $\mathsf{Adv}^{\mathsf{gddhe}}(P, Q, F, \mathcal{D})$ in solving the (P, Q, F)-GDDHE problem if

$$|\Pr[\mathcal{D}(\widehat{H}(x_1, \cdots, x_{\widehat{n}}), g_T^{F(x_1, \cdots, x_{\widehat{n}})}) = 0] - \Pr[\mathcal{D}(\widehat{H}(x_1, \cdots, x_{\widehat{n}}), T) = 0]| \geq \mathsf{Adv}^{\mathsf{gddhe}}(P, Q, F, \mathcal{D})$$

where the probability is over the random choice of generator g_0 in $\mathbb{G}$, the random choice of $x_1, \cdots, x_n$, the random choice of $T \in \mathbb{G}_T$.

Below we show a result on the (P, Q, F)-GDDHE problem from [6].

THEOREM 1. *[6] Let $P, Q \in \mathbb{F}_p[X_1, \cdots, X_{\widehat{n}}]^s$ be two s-tuples of $\widehat{n}$-variate polynomials over $\mathbb{F}_p$ and let $F \in \mathbb{F}_p[X_1, \cdots, X_{\widehat{n}}]$. Let d_P (resp, d_Q, d_F) denote the maximal degree of elements of P (resp. of Q, F) and $d = \max(2d_P, d_Q, d_F)$. If $F \notin < P, Q >$ then for any generic-model distinguisher $\mathcal{D}$ that makes a total of at most q queries to the oracles computing the group operation in $\mathbb{G}, \mathbb{G}_T$ and the bilinear pairing $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, we have*

$$\mathsf{Adv}^{\mathsf{gddhe}}(P, Q, F, \mathcal{D}) \leq \frac{(q + 2s + 2)^2 \cdot d}{2p}.$$

4.2 A New Complexity Assumption

We first recall a concrete Diffie-Hellman exponent problem defined in [11], namely (f, g, F)-GDDHE. The details are as follows.

DEFINITION 3. ((f, g, F)-GDDHE)*[11]. Let $\mathbb{BG} = (\mathbb{G}, \mathbb{G}_T, e, p)$ be a bilinear map group system and let f and g be two coprime polynomials with pairwise distinct roots, of respective orders t and n. Let g_0, h_0 be two generators of $\mathbb{G}$. Then the* (f, g, F)-GDDHE) *problem consists, given*

$$\begin{array}{llll} g_0, & g_0^{\alpha}, & \cdots, g_0^{\alpha^{2n}}, & g_0^{r \cdot g(\alpha)}, \\ h_0, & h_0^{\alpha}, & \cdots, h_0^{\alpha^{t-1}}, h_0^{\alpha \cdot f(\alpha)}, & h_0^{r \cdot \alpha \cdot f(\alpha)}, \end{array}$$

and $T \in \mathbb{G}_T$, in deciding whether T is equal to $e(g_0, h_0)^{r \cdot f(\alpha)}$, or to some random element of $\mathbb{G}_T$.

One can note that if we reformulate the above problem as the generic (P, Q, F)-GDDHE problem, then we have (assuming $h_0 = g_0^{\beta}$),

$$\begin{aligned} P &= \Big(1, \alpha, \cdots, \alpha^{2n}, r \cdot g(\alpha), \\ &\quad \beta, \beta \cdot \alpha, \cdots, \beta \cdot \alpha^{t-1}, \beta \cdot \alpha \cdot f(\alpha), \beta \cdot r \cdot \alpha \cdot f(\alpha)\Big), \\ Q &= 1, \\ F &= r \cdot \beta \cdot f(\alpha). \end{aligned}$$

It is shown in [11] that $F \notin < P, Q >$ and hence we have the following conclusion according to THEOREM 1.

Corollary 1 (Generic security of (f, g, F)-GDDHE). *For any probabilistic algorithm $\mathcal{D}$ that totalizes of at most q queries to the oracles performing the group operations in $\mathbb{G}, \mathbb{G}_T$ and the bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$,*

$$\mathsf{Adv}^{\mathsf{gddhe}}(f, g, F, \mathcal{D}) \leq \frac{(q + 2(2n + t + 4) + 2)^2 \cdot d}{2p},$$

where $d = 2 \cdot \max(2n, t + 1)$.

In this paper, we introduce a new Diffie-Hellman exponent problem, denoted as $(\widehat{f}, g, F)$-GDDHE, by slightly revising the above (f, g, F)-GDDHE problem. Roughly speaking, we enrich the input of the problem while still preserve its hardness. Details are as follows.

DEFINITION 4. ($(\widehat{f}, g, F)$-GDDHE). *Let $\mathbb{BG} = (\mathbb{G}, \mathbb{G}_T, e, p)$ be a bilinear map group system and let f and g be two coprime polynomials with pairwise distinct roots, of respective orders t and n. Let g_0, h_0 be two generators of $\mathbb{G}$. Then the* (f, g, F)-GDDHE) *problem consists, given*

$$\begin{array}{llll} g_0, & g_0^{\alpha}, & \cdots, g_0^{\alpha^{2n}}, & g_0^{r \cdot g(\alpha)}, \\ h_0, & h_0^{\alpha}, & \cdots, h_0^{\alpha^{t-1}}, & \\ h_0^{\alpha \cdot f(\alpha)}, & h_0^{\alpha^2 \cdot f(\alpha)}, & \cdots, h_0^{\alpha^n \cdot f(\alpha)}, & \\ h_0^{r \cdot \alpha \cdot f(\alpha)}, & h_0^{r \cdot \alpha^2 \cdot f(\alpha)}, & \cdots, h_0^{r \cdot \alpha^n \cdot f(\alpha)}, & \end{array}$$

and $T \in \mathbb{G}_T$, in deciding whether T is equal to $e(g_0, h_0)^{r \cdot f(\alpha)}$, or to some random element of $\mathbb{G}_T$.

As for the security of our new $(\widehat{f}, g, F)$-GDDHE problem, we have the following conclusion.

Corollary 2 (Generic security of $(\widehat{f}, g, F)$-GDDHE). *For any probabilistic algorithm $\mathcal{D}$ that totalizes of at most q queries to the oracles performing the group operations in $\mathbb{G}, \mathbb{G}_T$ and the bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$,*

$$\mathsf{Adv}^{\mathsf{gddhe}}(\widehat{f}, g, F, \mathcal{D}) \leq \frac{(q + 2(4n + t + 2) + 2)^2 \cdot d}{2p}$$

where $d = 2 \cdot \max(2n, t + 1)$.

PROOF. Below we prove that the $(\widehat{f}, g, F)$-GDDHE problem lies in the scope of THEOREM 1.

Let $h_0 = g_0^{\beta}$ and we reformulate the above problem as (P, Q, F)-GDDHE problem where

$$\begin{aligned} P &= \Big(1, \alpha, \cdots, \alpha^{2n}, r \cdot g(\alpha), \\ &\quad \beta, \beta \cdot \alpha, \cdots, \beta \cdot \alpha^{t-1}, \\ &\quad \beta \cdot \alpha \cdot f(\alpha), \beta \cdot \alpha^2 \cdot f(\alpha), \cdots, \beta \cdot \alpha^n \cdot f(\alpha), \\ &\quad \beta \cdot r \cdot \alpha \cdot f(\alpha), \beta \cdot r \cdot \alpha^2 \cdot f(\alpha), \cdots, \beta \cdot r \cdot \alpha^n \cdot f(\alpha)\Big), \\ Q &= 1, \\ F &= r \cdot \beta \cdot f(\alpha). \end{aligned}$$

One can see that in the above reformulated problem, $\widehat{n} = 3, s = 2n + t + 4$. Now we prove that F is independent of $< P, Q >$. We illustrate this statement by giving a contradiction as follows.

Assume that F is dependent of $< P, Q >$ (i.e, $F \in < P, Q >$), then there should exist coefficients $\{a_{i,j}\}_{i,j=1}^{s}, b_1$ such that

$$F = \sum_{i,j=1}^{s} a_{i,j} p_i p_j + b_1 q_1,$$

where $p_i \in P$ and $q_1 = 1 \in Q$. Noting that $F = r \cdot \beta \cdot f(\alpha)$, we have that, for all $i, j \in [1, s]$, $a_{i,j} p_i p_j$ should be multiples of $r \cdot \beta$. Below we list all the possible products of two polynomials from P that satisfy the above property.

$$\begin{aligned} R_1 &= r \cdot \beta \cdot g(\alpha), r \cdot \beta \cdot \alpha \cdot g(\alpha), \cdots, r \cdot \beta \cdot \alpha^{t-1} \cdot g(\alpha), \\ R_2 &= r \cdot \beta \cdot \alpha \cdot g(\alpha) f(\alpha), \cdots, r \cdot \beta \cdot \alpha^{n} \cdot g(\alpha) f(\alpha), \\ R_3 &= r \cdot \beta \cdot \alpha \cdot f(\alpha), \cdots, r \cdot \beta \cdot \alpha^{3n} \cdot f(\alpha). \end{aligned}$$

Here R_1 is the products of $r \cdot g(\alpha)$ and $\beta \cdot \alpha^i$ for all $i \in [0, t-1]$, R_2 is the products of $r \cdot g(\alpha)$ and $\beta \cdot \alpha^i \cdot f(\alpha)$ for all $i \in [1, n]$ and R_3 is the products of α^i and $\beta \cdot r \cdot \alpha^j \cdot f(\alpha)$ for all $i \in [0, 2n], j \in [1, n]$. Note that for any $i \in [1, n]$, $r \cdot \beta \cdot \alpha^i \cdot g(\alpha) f(\alpha)$ can be written as a linear combination of polynomials in R_3. That is, any linear combination of polynomials in R_2 can be also represented with the ones in R_3. Therefore, F should be the linear combination of polynomials in R_1, R_3 if $F \in < P, Q >$. Formally, we have

$$F = r \cdot \beta \cdot f(\alpha) = r \cdot \beta \cdot A(\alpha) \cdot g(\alpha) + r \cdot \beta \cdot \alpha \cdot B(\alpha) \cdot f(\alpha)$$

where $A(\alpha), B(\alpha)$ are polynomials such that $d_A \leq t-1, d_B \leq 3n - 1$. We then simplify the above equation as follows,

$$f(\alpha) = A(\alpha) \cdot g(\alpha) + \alpha \cdot B(\alpha) \cdot f(\alpha),$$

which can be further simplified as,

$$f(\alpha) \cdot (1 - \alpha \cdot B(\alpha)) = A(\alpha) \cdot g(\alpha).$$

Noting that $f(\alpha)$ and $g(\alpha)$ are coprime in α, we then have that $f(\alpha) | A(\alpha)$, which implies $A(\alpha) = 0$ since $d_f = t$ and $d_A \leq t - 1$. Therefore, we have that $\alpha \cdot B(\alpha) = 1$ for any α, which, however, cannot hold when $\alpha = 0$.

Therefore, the assumption that F is dependent of $< P, Q >$ cannot hold and hence $F \notin < P, Q >$. According to the THEOREM 1, we then have

$$\mathsf{Adv}^{\mathsf{gddhe}}(\widehat{f}, g, F, \mathcal{D}) \leq \frac{(q + 2(4n + t + 2) + 2)^2 \cdot d}{2p},$$

where $d = 2 \cdot \max(2n, t + 1)$. This completes the proof. □

5. SECURITY ANALYSIS

We prove the security of our RR-IBBE scheme under the $(\widehat{f}, g, F)$-GDDHE assumption with the random oracle.

THEOREM 2. *For any n, t, we have* $\mathsf{Adv}^{\mathsf{SS}}_{\mathcal{RR}\text{-}\mathcal{IBBE}}(t, n) \leq \mathsf{Adv}^{\mathsf{gddhe}}(f, g, F)$.

PROOF. Suppose there is an adversary $\mathcal{A}$ that has advantage $\mathsf{Adv}^{\mathsf{SS}}_{\mathcal{RR}\text{-}\mathcal{IBBE}}(t, n)$ in attacking our RR-IBBE scheme. We build an algorithm $\mathcal{B}$ that solves the $(\widehat{f}, g, F)$-GDDHE problem in $\mathbb{G}_T$. More precisely, $\mathcal{B}$ plays as the challenger in the security game against the adversary $\mathcal{A}$.

Assume the adversary (i.e, $\mathcal{A}$) and the challenger (i.e, $\mathcal{B}$) take as input n, which is the maximum size of a set of included users $\mathcal{S}$, and t the total number of extraction queries and random oracle queries that can be issued by the adversary.

Algorithm $\mathcal{B}$ is given as input a bilinear group $\mathbb{BG} = (\mathbb{G}, \mathbb{G}_T, e, p)$ with g_0, h_0 the two generators of $\mathbb{G}$. $\mathcal{B}$ is then given a $(\widehat{f}, g, F)$-GDDHE instance in $\mathbb{BG}$ as:

$$\begin{aligned} & g_0, \quad g_0^{\alpha}, \quad \cdots, g_0^{\alpha^{2n}}, \quad g_0^{r \cdot g(\alpha)}, \\ & h_0, \quad h_0^{\alpha}, \quad \cdots, h_0^{\alpha^{t-1}}, \\ & h_0^{\alpha \cdot f(\alpha)}, \quad h_0^{\alpha^2 \cdot f(\alpha)}, \quad \cdots, h_0^{\alpha^n \cdot f(\alpha)}, \\ & h_0^{r \cdot \alpha \cdot f(\alpha)}, \quad h_0^{r \cdot \alpha^2 \cdot f(\alpha)}, \quad \cdots, h_0^{r \cdot \alpha^n \cdot f(\alpha)}, \end{aligned}$$

as well as $T \in \mathbb{G}_T$ which is either equal to $e(g_0, h_0)^{r \cdot f(\alpha)}$ or to some random element of $\mathbb{G}_T$. Among them $f(\alpha)$ and $g(\alpha)$ are two coprime polynomials in α and we define the following notations used in our proof.

- $f(X) = \prod_{i=1}^{t}(X + x_i), g(X) = \prod_{i=t+1}^{t+n}(X + x_i)$;
- $f_i(X) = \frac{f(X)}{X + x_i}$ for $i \in [1, t]$;
- $g_i(X) = \frac{g(X)}{X + x_i}$ for $i \in [t + 1, t + n]$.

Algorithm $\mathcal{B}$'s goal is to output 1 if $T = e(g_0, h_0)^{r \cdot f(\alpha)}$ and 0 otherwise.

$\mathcal{B}$ works by interacting with $\mathcal{A}$ in the following game:

Init : The adversary $\mathcal{A}$ outputs a set $\mathcal{S}^* = \{\mathsf{ID}_1^*, ..., \mathsf{ID}_{s^*}^*\} (s^* \leq n)$ of target identities.

Setup : To generate the system parameters, $\mathcal{B}$ implicitly sets $h = h_0^{f(\alpha)}$ and other parameters as follows,

$$\begin{aligned} h_i &= h_0^{\alpha^i f(\alpha)} = h^{\alpha^i}, \forall i \in [1, n] \\ g &= g_0^{\prod_{i=t+s^*+1}^{t+n}(\alpha + x_i)} \\ v &= e(g_0, h_0)^{f(\alpha) \cdot \prod_{i=t+s^*+1}^{t+n}(\alpha + x_i)} = e(g, h) \end{aligned}$$

$\mathcal{B}$ defines the public key as $\mathsf{PK} = \{g, g^{\alpha}, ..., g^{\alpha^n}, h_1, ..., h_n, v\}$. $\mathcal{B}$ then runs $\mathcal{A}$ on the system parameters $\mathbb{BG}, \mathsf{PK}$ and $\mathcal{H}$, which is a random oracle controlled by $\mathcal{B}$ described below.

Hash Queries : At any time $\mathcal{A}$ can query the random oracle on any identity ID_i (at most t-q_E) times, with q_E the number of extraction queries. To respond to these queries, $\mathcal{B}$ maintains a list $\mathcal{L}_H$ of tuples ID_i, x_i that contains at the beginning:

$$\{(*, x_i)\}_{i=1}^{t}, \qquad \{(\mathsf{ID}_i^*, x_i)\}_{i=t+1}^{t+s^*}$$

Here " $*$ " denotes an empty entry in $\mathcal{L}_H$. When the adversary issues a hash query on identity ID_i, $\mathcal{B}$ responds as follows:

- If ID_i already appears in the list $\mathcal{L}_H$, $\mathcal{B}$ responds with the corresponding x_i;
- Otherwise, $\mathcal{B}$ sets $H(\mathsf{ID}_i) = x_i$, and completes the list with (ID_i, x_i)

Extraction Query I : The adversary A adaptively issues extraction queries on any $\mathsf{ID}_i \notin \mathcal{S}^*$ for all $i \in [1, q_E]$. $\mathcal{B}$ generate the private key of each queried identity as follows.

- If $\mathcal{A}$ has already issued a hash query on ID_i, then $\mathcal{B}$ generates the corresponding private key as

$$\mathsf{sk}_{\mathsf{ID}_i} = h^{\frac{1}{\alpha+H(\mathsf{ID}_i)}} = h_0^{f_i(\alpha)},$$

which is computable from the given instance.

- Otherwise, $\mathcal{B}$ sets $H(\mathsf{ID}_i) = x_i$, computes the corresponding private key $\mathsf{sk}_{\mathsf{ID}_i}$ as above.

Challenge : Once $\mathcal{A}$ decides that extraction query I is over, it outputs two equal length plaintexts M_0, M_1 and a revocation identity set $\mathcal{R}^* = \{\mathsf{ID}_{\mathcal{R}_1}, ..., \mathsf{ID}_{\mathcal{R}_k}\}$. $\mathcal{B}$ picks a random bit $b \leftarrow \{0,1\}$ and computes

$$C_m^* = T^{\prod_{i=t+s^*+1}^{t+n} x_i} \cdot e(g_0^{\overline{F}(\alpha)}, h_0^{r\alpha\cdot f(\alpha)}) \cdot M_b,$$

where $\overline{F}(\alpha)$ is defined as

$$\overline{F}(\alpha) = \frac{1}{\alpha}\Big(\prod_{i=t+s^*+1}^{t+n}(\alpha + x_i) - \prod_{i=t+s^*+1}^{t+n} x_i\Big).$$

It then sets

$$C_0^* = g_0^{r\cdot g(\alpha)}, C_1^* = h_0^{r\cdot\alpha\cdot f(\alpha)}.$$

$\mathcal{B}$ then responds to the adversary as follows.

Case 1 : When $\mathcal{R}^* = \emptyset$. In this case, $\mathcal{B}$ will generate a normal IBBE ciphertext. More precisely, $\mathcal{B}$ outputs the challenger ciphertext as

$$CT^* = (C_m^*, C_0^*, C_1^*, C_2^*, \cdots, C_{k+1}^*),$$

where

$$C_2^* = h_0^{r\cdot\alpha^2\cdot f(\alpha)}, \cdots, C_{k+1}^* = h_0^{r\cdot\alpha^{k+1}\cdot f(\alpha)},$$

are directly from the given instance.

Case 2 : When $\mathcal{R}^* \neq \emptyset$. In this case, $\mathcal{B}$ outputs the challenger ciphertext as

$$CT^* = (C_m^*, C_0^*, C_1^*).$$

Extraction Query II : The adversary A continues to issue extraction queries and $\mathcal{B}$ responds as in Phase Extraction Query I.

Guess : Finally, the adversary A outputs a guess $b' \in \{0,1\}$ and $\mathcal{B}$ outputs 1 if $b = b'$, otherwise outputs 0.

One can easily see that the responses to hash queries in the above simulation are as in the real attack since each response is uniformly from the view of $\mathcal{A}$. All responses to private key extraction queries are also valid. Below we mainly analyse the simulation of Challenge stage by $\mathcal{B}$ in Case 1 and Case 2 respectively.

Case 1 (i.e.,$\mathcal{R}^* = \emptyset$). One can verify that in this case,

$$\begin{aligned} C_0^* &= g_0^{r\cdot g(\alpha)} \\ &= g_0^{r\cdot\prod_{i=t+s^*+1}^{t+n}(\alpha+x_i)\cdot\prod_{i=t+1}^{t+s^*}(\alpha+x_i)} \\ &= g^{r\cdot\prod_{i=t+1}^{t+s^*}(\alpha+x_i))} \\ &= g^{r\cdot(\alpha+H(\mathsf{ID}_1^*))\cdots(\alpha+H(\mathsf{ID}_{s^*}^*))} \end{aligned}$$

and

$$C_i^* = h_0^{r\cdot\alpha^i\cdot f(\alpha)} = h_i^r,$$

for any $i \in [1, k+1]$. As for the C_m^*, we also note that if $T = e(g_0, h_0)^{r\cdot f(\alpha)}$, then

$$\begin{aligned} & C_m^* \\ = \; & T^{\prod_{i=t+s^*+1}^{t+n} x_i} \cdot e(g_0^{\overline{F}(\alpha)}, h_0^{r\alpha\cdot f(\alpha)}) \cdot M_b \\ = \; & e(g_0, h_0)^{r\cdot f(\alpha)\prod_{i=t+s^*+1}^{t+n} x_i} \cdot e(g_0^{\overline{F}(\alpha)}, h_0^{r\alpha\cdot f(\alpha)}) \cdot M_b \\ = \; & e(g_0^{\prod_{i=t+s^*+1}^{t+n}(\alpha+x_i)}, h_0^{f(\alpha)})^r \cdot M_b \\ = \; & e(g, h)^r \cdot M_b \\ = \; & v^r \cdot M_b. \end{aligned}$$

Therefore, the simulation of $\mathcal{B}$ is perfect when T is true and hence we have,

$$\mathsf{Adv}^{\mathsf{sID\text{-}SS}}_{\mathcal{RR}\text{-}\mathcal{IBBE}}(t,n) \geq \Pr[b = b' | T = e(g_0, h_0)^{r\cdot f(\alpha)}] - 1/2.$$

On the other hand, when T is a random element of $\mathbb{G}_T$, $T^{\prod_{i=t+s^*+1}^{t+n} x_i} \cdot e(g_0^{\overline{F}(\alpha)}, h_0^{r\alpha\cdot f(\alpha)})$ is random and independent from the view of $\mathcal{A}$ and the challenge ciphertext is a one-time pad. Therefore, we have

$$\Pr[b = b' | T \text{ is random}] = 1/2.$$

Therefore, the advantage of $\mathcal{B}$ in solving the (f, g, F)-GDDHE problem in Case 1 is,

$$\begin{aligned} & \mathsf{Adv}^{\mathsf{gddhe}}(f, g, F) \\ = \; & |\Pr[b = b' | T = e(g_0, h_0)^{r\cdot f(\alpha)}] - \Pr[b = b' | T \text{ is random}]| \\ \geq \; & \mathsf{Adv}^{\mathsf{sID\text{-}SS}}_{\mathcal{RR}\text{-}\mathcal{IBBE}}(t,n). \end{aligned}$$

Case 2 (i.e.,$\mathcal{R}^* \neq \emptyset$). In this case, we first show that what a real challenger (denoted as $\mathcal{B}^*$) should output as the challenge ciphertext of M_b to adversary $\mathcal{A}$. Formally, the correct procedures are as follows.

Let $\mathcal{S} = \mathcal{R}^* + \mathcal{S}^*$. $\mathcal{B}^*$ would first run $\mathsf{Encrypt}(\mathcal{S}, k, M_b, \mathsf{PK})$ to get CT. More precisely, it picks a randomness $r^* \leftarrow \mathbb{Z}_p$ and computes,

$$\begin{aligned} CT &= (C_m, C_0, C_1, C_2, \cdots, C_{k+1}) \\ &= \Big(v^{r^*} \cdot M_b,\ g^{r^*\cdot\prod_{\mathsf{ID}\in\mathcal{S}}(\alpha+H(\mathsf{ID}))},\ h_1^{r^*}, h_2^{r^*}, \cdots, h_{k+1}^{r^*}\Big). \end{aligned}$$

The challenger $\mathcal{B}^*$ then runs the revocation algorithm $\mathsf{Revoke}\ (\mathcal{S}, CT_{M_b}, \mathcal{R}^*, \mathsf{PK})$ to revoke the identity set $\mathcal{R}^*$ from the ciphertext CT. Precisely, $\mathcal{B}^*$ computes

$$\begin{aligned} C_m' &= M_b \cdot v^{r^*\cdot\frac{\prod_{i=1}^k(\alpha+H(\mathsf{ID}_{\mathcal{R}_i}))}{\prod_{i=1}^k H(\mathsf{ID}_{\mathcal{R}_i})}}, \\ C_0' &= C_0^{\frac{1}{\prod_{i=1}^k H(\mathsf{ID}_{\mathcal{R}_i})}} \\ &= g^{r^*\cdot\frac{\prod_{i=1}^k(\alpha+H(\mathsf{ID}_{\mathcal{R}_i}))}{\prod_{i=1}^k H(\mathsf{ID}_{\mathcal{R}_i})}\cdot\prod_{\mathsf{ID}\in\mathcal{S}^*}(\alpha+H(\mathsf{ID}))}, \\ C_1' &= C_1^{\frac{\prod_{i=1}^k(\alpha+H(\mathsf{ID}_{\mathcal{R}_i}))}{\prod_{i=1}^k H(\mathsf{ID}_{\mathcal{R}_i})}} \\ &= h_1^{r^*\cdot\frac{\prod_{i=1}^k(\alpha+H(\mathsf{ID}_{\mathcal{R}_i}))}{\prod_{i=1}^k H(\mathsf{ID}_{\mathcal{R}_i})}}. \end{aligned}$$

Finally, $\mathcal{B}^*$ would given $CT' = (C_m', C_0', C_1')$ to $\mathcal{A}$ as the challenge ciphertext.

We further assume that the randomness r^* used by $\mathcal{B}^*$ is as follows,

$$r^* = r \cdot \frac{\prod_{i=1}^k H(\mathsf{ID}_{\mathcal{R}_i})}{\prod_{i=1}^k(\alpha + H(\mathsf{ID}_{\mathcal{R}_i}))}.$$

Then for the challenge ciphertext $CT' = (C'_m, C'_0, C'_1)$, we have

$$\begin{aligned} C'_m &= M_b \cdot v^{r^* \cdot \frac{\prod_{i=1}^{k}(\alpha + H(\mathsf{ID}_{\mathcal{R}_i}))}{\prod_{i=1}^{k} H(\mathsf{ID}_{\mathcal{R}_i})}} \\ &= M_b \cdot v^r \\ C'_0 &= g^{r^* \cdot \frac{\prod_{i=1}^{k}(\alpha + H(\mathsf{ID}_{\mathcal{R}_i}))}{\prod_{i=1}^{k} H(\mathsf{ID}_{\mathcal{R}_i})} \cdot \prod_{\mathsf{ID} \in \mathcal{S}^*}(\alpha + H(\mathsf{ID}))} \\ &= g^{r \cdot \prod_{\mathsf{ID} \in \mathcal{S}^*}(\alpha + H(\mathsf{ID}))} \\ C'_1 &= h_1^{r^* \cdot \frac{\prod_{i=1}^{k}(\alpha + H(\mathsf{ID}_{\mathcal{R}_i}))}{\prod_{i=1}^{k} H(\mathsf{ID}_{\mathcal{R}_i})}} \\ &= h_1^r. \end{aligned}$$

We can see that these are actually the simulated challenge ciphertext (i.e.,$(C'_m, C'_0, C'_1) = (C^*_m, C^*_0, C^*_1)$) returned by $\mathcal{B}$ in Case 2 when $T = e(g_0, h_0)^{r \cdot f(\alpha)}$!

One should note that the above setting of r^* is indistinguishable from a real random value from the view of $\mathcal{A}$ since r is random to $\mathcal{A}$. Therefore, from the view of $\mathcal{A}$, the behaviours of $\mathcal{B}$ is indistinguishable from the real challenger $\mathcal{B}^*$ and hence we have,

$$\mathsf{Adv}^{\mathsf{sID\text{-}SS}}_{\mathcal{RR}\text{-}\mathcal{IBBE}}(t, n) \geq \Pr[b = b' | T = e(g_0, h_0)^{r \cdot f(\alpha)}] - 1/2.$$

Also, when T is a random element from $\mathbb{G}_T$, C^*_m is random and independent from the view of $\mathcal{A}$ and thus,

$$\Pr[b = b' | T \text{ is random}] = 1/2.$$

Therefore, the advantage of $\mathcal{B}$ in solving the (f, g, F)-GDDHE problem in Case 2 is,

$$\mathsf{Adv}^{\mathsf{gddhe}}(f, g, F) \geq \mathsf{Adv}^{\mathsf{sID\text{-}SS}}_{\mathcal{RR}\text{-}\mathcal{IBBE}}(t, n).$$

This completes the proof. □

6. CONCLUSION

We presented a new cryptographic notion called a recipient-revocable identity-based broadcast encryption (RR-IBBE) scheme. This notion allows a content provider to produce an encrypted content to be multicasted to a set of recipients, via a third party, which is a broadcaster. The broadcaster has the ability to revoke some of the users specified in the ciphertext, even without the ability of decrypting it. Hence, this broadcaster can sanitize (or censor) the ciphertext, so that it will not be readable by some of the designated recipients. We presented a scenario where this kind of primitives is required. We proposed a scheme to capture this requirement, where the ciphertext size is independent of the number of recipients. In our scheme, the ciphertext generated by the content provider for the broadcaster is linear to the maximum number of revoked users. The final ciphertext that is sent to the recipients is constant size, and hence, it is independent of the number of recipients. It is an interesting further research to construct a scheme where the ciphertexts for both cases are constant.

7. REFERENCES

[1] J. Anzai, N. Matsuzaki, and T. Matsumoto. A quick group key distribution scheme with "entity revocation". In K. Lam, E. Okamoto, and C. Xing, editors, *Advances in Cryptology - ASIACRYPT '99, International Conference on the Theory and Applications of Cryptology and Information Security, Singapore, November 14-18, 1999, Proceedings*, volume 1716 of *Lecture Notes in Computer Science*, pages 333–347. Springer, 1999.

[2] S. Berkovits. How to broadcast A secret. In D. W. Davies, editor, *Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings*, volume 547 of *Lecture Notes in Computer Science*, pages 535–541. Springer, 1991.

[3] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *2007 IEEE Symposium on Security and Privacy (S&P 2007), 20-23 May 2007, Oakland, California, USA*, pages 321–334. IEEE Computer Society, 2007.

[4] A. Boldyreva, V. Goyal, and V. Kumar. Identity-based encryption with efficient revocation. In P. Ning, P. F. Syverson, and S. Jha, editors, *Proceedings of the 2008 ACM Conference on Computer and Communications Security, CCS 2008, Alexandria, Virginia, USA, October 27-31, 2008*, pages 417–426. ACM, 2008.

[5] D. Boneh and X. Boyen. Efficient selective-id secure identity-based encryption without random oracles. In *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*, pages 223–238, 2004.

[6] D. Boneh, X. Boyen, and E. Goh. Hierarchical identity based encryption with constant size ciphertext. In *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, pages 440–456, 2005.

[7] D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, pages 41–55, 2004.

[8] D. Boneh and M. K. Franklin. Identity-based encryption from the weil pairing. In J. Kilian, editor, *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, 2001.

[9] D. Boneh and M. K. Franklin. Identity-based encryption from the weil pairing. In *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, pages 213–229, 2001.

[10] D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, pages 258–275, 2005.

[11] C. Delerablée. Identity-based broadcast encryption

with constant size ciphertexts and private keys. In *Advances in Cryptology - ASIACRYPT 2007, 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, December 2-6, 2007, Proceedings*, pages 200–215, 2007.

[12] A. Fiat and M. Naor. Broadcast encryption. In D. R. Stinson, editor, *Advances in Cryptology - CRYPTO '93, 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22-26, 1993, Proceedings*, volume 773 of *Lecture Notes in Computer Science*, pages 480–491. Springer, 1993.

[13] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In A. Juels, R. N. Wright, and S. D. C. di Vimercati, editors, *Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, Ioctober 30 - November 3, 2006*, pages 89–98. ACM, 2006.

[14] D. Halevy and A. Shamir. The LSD broadcast encryption scheme. In M. Yung, editor, *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*, volume 2442 of *Lecture Notes in Computer Science*, pages 47–60. Springer, 2002.

[15] D. Naor, M. Naor, and J. Lotspiech. Revocation and tracing schemes for stateless receivers. *Electronic Colloquium on Computational Complexity (ECCC)*, (043), 2002.

[16] M. Naor and B. Pinkas. Efficient trace and revoke schemes. *Int. J. Inf. Sec.*, 9(6):411–424, 2010.

[17] R. Ostrovsky, A. Sahai, and B. Waters. Attribute-based encryption with non-monotonic access structures. In P. Ning, S. D. C. di Vimercati, and P. F. Syverson, editors, *Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA, October 28-31, 2007*, pages 195–203. ACM, 2007.

[18] A. Sahai, H. Seyalioglu, and B. Waters. Dynamic credentials and ciphertext delegation for attribute-based encryption. In R. Safavi-Naini and R. Canetti, editors, *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, volume 7417 of *Lecture Notes in Computer Science*, pages 199–217. Springer, 2012.

[19] A. Sahai and B. Waters. Fuzzy identity-based encryption. In R. Cramer, editor, *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, volume 3494 of *Lecture Notes in Computer Science*, pages 457–473. Springer, 2005.

[20] R. Sakai and J. Furukawa. Identity-based broadcast encryption. *IACR Cryptology ePrint Archive*, 2007:217, 2007.

[21] V. Shoup. Lower bounds for discrete logarithms and related problems. In *Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding*, pages 256–266, 1997.

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