Adaptively Secure Recipient Revocable Broadcast Encryption with Constant size Ciphertext

Kamalesh Acharya and Ratna Dutta
Department of Mathematics
Indian Institute of Technology Kharagpur
Kharagpur-721302, India
kamaleshiitkgp@gmail.com,ratna@maths.iitkgp.ernet.in

ABSTRACT

In this paper, we put forward the *first adaptively secure* recipient revocable broadcast encryption (RR-BE) scheme in the *standard model.* The scheme is adaptively secure against *chosen plaintext attack* (CPA) under the q-weaker Decisional Augmented Bilinear Diffie-Hellman Exponent (q-wDABDHE) assumption. Our scheme compares well with the only existing RR-BE scheme of Susilo et al. which is selectively secure in the random oracle model. More interestingly, achieving adaptive security in the standard model does not blow up the communication cost in our construction. To be more precise, the size of the ciphertext which is broadcasted by the broadcaster is constant.

Keywords

recipient revocable broadcast encryption, chosen plaintext attack, adaptive security.

1. INTRODUCTION

Broadcast encryption (BE) is a cryptographic primitive for delivering encrypted content to a group of users enabling only the subscribed users to recover the message from the encrypted content. Large number of works have been done [1, 3, 4, 5, 6, 7, 8, 10, 11, 13, 12] since its formal introduction by Fiat and Naor [9] in 1994. The versatility of BE makes them useful tool for many natural applications, spanning from protecting copyright content distributed as stored media to managing digital subscription of satellite TV. Recipient revocable broadcast encryption (RR-BE) is a recently introduced variant of BE by Susilo et al. [15], featuring a content provider to send encrypted content to the broadcaster who in tern is capable of revoking some user identities without decrypting the content. RR-BE is a variant of identity based broadcast encryption (IBBE). A private key generation centre generates the public parameter and user secret key. A content provider and a broadcaster agrees upon a common set of users (recipients). Instead of the broadcaster, the content provider provides the encrypted content. The broadcaster broadcasts a ciphertext by modifying the original encrypted content received from the content provider in such a way that enables the broadcaster to revoke intended subscribers. A subscribed user can decrypt this modified content using its secret key and recover the message.

RR-BE fits for several application scenarios. With the advent of Internet-based distribution and immediate access to content with low-cost delivery raise security threats and risk of abusing intellectual property and copyrights. RR-BE facilitates scalability in business model and allows to make several business strategies. Consider the following scenarios where RR-BE is useful:

- Suppose in an academic institute, the head wants to send an important message to the current students. He makes an encrypted message for all the enrolled students. Some students may leave the institute as they get jobs or for other reasons. Academic stuffs make a list of current students and want to revoke the students who are currently not present in the institute without having eligibility of recovering the message.

- To increase the business, let Internet service provider, such as CenturyLink, collaborates with movie content provider CinemaNow and provides free access of CinemaNow to the subscribers. CinemaNow permits CenturyLink to send the content upto a fixed number of user according to their contract amount. CenturyLink wants to distribute the content to as many users as possible to increase its profit. Therefore, CinemaNow cannot send the content in a plaintext form. It sends the content in encrypted form. From users' point of view, a user may want to get revoked if he has already seen the movies. Now the challenge for CenturyLink comes to revoke users using the encrypted content provided by CinemaNow.

In this work, we obtain the *first* adaptively chosen plaintext attack (CPA) secure recipient revocable broadcast encryption scheme in the standard model. The starting point of our construction is the identity based broadcast encryption scheme of Ren et al. [14]. The only existing RR-BE scheme [15] has extended the identity based encryption scheme of Delerablee [6] to achieve the recipient revocation property. The selective semantic security is under the $(\hat{f}, g, F)$- General Decisional Diffie-Hellman Exponent ($(\hat{f}, g, F)$-GDDHE) assumption in the random oracle model. Selective security [3] is a weaker model for broadcast encryption where the adversary commits a target recipient set

G of user indices before the setup phase. This is static security model and does not capture the powers of several types of attackers. Adaptive security introduced by Gentry et al. [10], on the other hand is known as full security of broadcast encryption. Here, the adversary can fix the target recipient set after seeing the public parameter and compromised private keys. It is the strongest security model. We achieve security in the standard model in contrast to [15] which uses random oracles for its security analysis. A proof in the random oracle model can only serve as a heuristic argument, as all parties in a random oracle model get black-box access to a truly random function. Achieving adaptive security in standard model is a challenging task in RR-BE framework. Our RR-BE scheme is secure under the q-weaker Decisional Augmented Bilinear Diffie-Hellman Exponent (q-wDABDHE) assumption which is a variant of General Decisional Diffie-Hellman Exponent Problem [2]. We achieve adaptive security in the standard model at the expense of increase in secret key size. We emphasizes that other parameter sizes, communication overhead and computation cost are comparable to those in [15]. More specifically, the ciphertext size broadcasted by the broadcaster is still constant.

Furthermore, new users can join any time without any updation of pre-existing public key and secret key, provided the number of subscribed users in the system does not exceed the maximum number of users allowed in the system. More interestingly, the broadcaster has the control to revoke any user of the group (for which original content was created by the content provider) without changing the existing setup. Besides, the scheme is non-interactive in the sense that the private key generation centre does not need to interact with the subscribed users after issuing users' private key.

Organization: The rest of the paper is organized as follows. Section 2 provides necessary definitions and background materials. We describe our main construction in Section 3 and its security in Section 4. Efficiency and comparison with the existing work is presented in Section 5. We finally conclude in Section 6.

2. PRELIMINARIES

Notation: Let $[m]$ denotes integers from 1 to m and $[a, b]$ denotes integers from a to b. We use the notation $x \in_R S$ to denote x is a random element of S and λ to represent bit size of prime integer p. Let $\epsilon : \mathbb{N} \to \mathbb{R}$ be a function, where $\mathbb{N}$ and $\mathbb{R}$ are the sets of natural and real number respectively. The function ϵ is said to be a *negligible function* if $\exists\ d \in \mathbb{N}$ such that $\epsilon(\lambda) \le \frac{1}{\lambda^d}$. Let $|G|$ denotes the number of elements of group G. For sets A, B, let $A + B$ denotes union of A, B and $A - B$ denotes set difference of A, B respectively.

2.1 Recipient Revocable Broadcast Encryption

The concept of recipient revocable broadcast encryption (RR-BE) was proposed by Susilo et al. [15] in 2016. Informally speaking, in a RR-BE, a private key generation centre (PKGC) generates public parameter and secret key. A content provider provides encrypted content to the broadcaster. The broadcaster will be able to revoke some users without having the ability to decrypt it.

Syntax of RR-BE: A recipient revocable broadcast encryption (RR-BE) scheme $\mathsf{RR\text{-}BE} = (\mathsf{RR\text{-}BE.Setup}, \mathsf{RR\text{-}BE.KeyGen}, \mathsf{RR\text{-}BE.Encrypt}, \mathsf{RR\text{-}BE.Revoke}, \mathsf{RR\text{-}BE.Decrypt})$ consists of three probabilistic polynomial time (PPT) algorithms - $\mathsf{RR\text{-}BE.Setup}$, $\mathsf{RR\text{-}BE.KeyGen}$, $\mathsf{RR\text{-}BE.Encrypt}$ and two deterministic polynomial time algorithms - $\mathsf{RR\text{-}BE.Revoke}$, $\mathsf{RR\text{-}BE.Decrypt}$. Formally, RR-BE is described as follows:

- $(\mathsf{PP}, \mathsf{MK}) \leftarrow \mathsf{RR\text{-}BE.Setup}(N, \lambda)$: Taking as input the total number of users N in the system and security parameter λ, the PKGC constructs the public parameter PP and a master key MK. It makes PP public and keeps MK secret to itself.
- $(sk_i) \leftarrow \mathsf{RR\text{-}BE.KeyGen}(\mathsf{PP}, \mathsf{MK}, i)$: The PKGC takes as input PP, MK and a subscribed user i and generates a secret key sk_i of user i and sends sk_i to user i through a secure communication channel between the PKGC and user i.
- $(\mathsf{CT}) \leftarrow \mathsf{RR\text{-}BE.Encrypt}(S, \mathsf{PP}, k, M)$: The content provider takes as input PP, user set S of n ($\le N$) users, message M, maximum revocation number k ($< n$) and produces a encrypted content CT (containing the set S) for the set S. It sends CT securely to the broadcaster.
  Note that broadcaster and content provider shares the information of set S. They can make the information of set S public.
- $(\mathsf{CT}') \leftarrow \mathsf{RR\text{-}BE.Revoke}(\mathsf{PP}, \mathsf{CT}, R)$: The broadcaster takes as input PP, encrypted content CT, revocation set R of l ($\le k$) users and produces a ciphertext CT' containing the set G where $G = S - R$. The broadcaster broadcast CT and makes G public.
- $(M) \leftarrow \mathsf{RR\text{-}BE.Decrypt}(\mathsf{PP}, sk_i, \mathsf{CT}')$: A subscribed user i with secret key sk_i outputs the message M using PP, CT'.

Correctness: The correctness of the scheme RR-BE lies in the fact that the message M can be retrieved from the ciphertext CT' by any subscribed user in G. Suppose $(\mathsf{PP}, \mathsf{MK}) \leftarrow \mathsf{RR\text{-}BE.Setup}(N, \lambda)$, $(\mathsf{CT}) \leftarrow \mathsf{RR\text{-}BE.Encrypt}(S, \mathsf{PP}, k, M)$, $(\mathsf{CT}') \leftarrow \mathsf{RR\text{-}BE.Revoke}(\mathsf{PP}, \mathsf{CT}, R)$. Then for every subscribed user $i \in G$,

$$\mathsf{RR\text{-}BE.Decrypt}\Big(\mathsf{PP}, \mathsf{RR\text{-}BE.KeyGen}\big(\mathsf{PP}, \mathsf{MK}, i\big), \mathsf{CT}'\Big) = M.$$

2.2 Security Framework

Message indistinguishability of RR-BE under CPA: We describe the adaptive security of the scheme $\mathsf{RR\text{-}BE}$ as a message indistinguishability game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$, following Susilo et al. [15]. Let n ($\le N$) be maximum size of the set of users in S and t be the number of corrupted users. Both the challenger $\mathcal{C}$ and adversary $\mathcal{A}$ are given as input n and t.

Setup: The challenger $\mathcal{C}$ generates $(\mathsf{PP}, \mathsf{MK}) \leftarrow \mathsf{RR\text{-}BE.Setup}(n, \lambda)$. It keeps the master key MK secret to itself and sends public parameter PP to $\mathcal{A}$.

Phase 1: Receiving key generation queries for users $i_1, \ldots, i_m$, the adversary $\mathcal{A}$ generates $sk_i \leftarrow \mathsf{RR\text{-}BE.KeyGen}(\mathsf{PP}, \mathsf{MK}, i)$ for user $i \in \{i_1, \ldots, i_m\}$ and sends to $\mathcal{C}$.

Challenge: The adversary $\mathcal{A}$ sends a set G to $\mathcal{C}$ where indices of G has not been queried before. It also sends two equal length plaintext M_0, M_1, maximum revocation number k ($\le n$) and a revocation set R to the challenger $\mathcal{C}$ where no identity of R lies in G. Let

$S = G + R$. The challenger $\mathcal{C}$ picks a bit $b \in_R \{0, 1\}$ and generates CT, CT' as

$$(\mathsf{CT}) \leftarrow \mathsf{RR\text{-}BE.Encrypt}(S, \mathsf{PP}, k, M_b)$$

$$(\mathsf{CT}') \leftarrow \mathsf{RR\text{-}BE.Revoke}(\mathsf{PP}, \mathsf{CT}, R).$$

The adversary is given $\mathsf{CT}^* = \mathsf{CT}$ when $R = \phi$ else it is given $\mathsf{CT}^* = \mathsf{CT}'$.

Phase 2: This is identical to Phase 1 key generation queries with a restriction that queried user indices does not lie in G.

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

Adversary $\mathcal{A}$ is allowed to get reply up to t key generation queries. The adversary $\mathcal{A}$'s advantage in the above security game is defined as $Adv_{\mathcal{A}}^{\mathsf{RR-BE-IND}}(t, n) = |Pr(b' = b) - \frac{1}{2}|$. The probability is taken over random bits used by $\mathcal{C}$ and $\mathcal{A}$.

Definition 1. The broadcast encryption scheme RR-BE is said to be (t, n)-secure if $Adv^{\mathsf{RR-BE-IND}}(t, n) = \epsilon(\lambda)$, where $\epsilon(\lambda)$ is a negligible function in security parameter λ.

This security model considers two type of scenarios:

- If $R = \phi$, then no user revoke, adversary gets full encrypted content as challenge ciphertext. This model guarantees that adversary who does not have secret key cannot learn about plaintext. This is the property of indistinguishability against selective identity and chosen plaintext attack (IND-sID-CPA) of IBBE.
- If $R \neq \phi$, adversary gets decryption key assistance for users in R and challenge ciphertext for $G = S - R$. This model guarantees that users who are revoked unable to recover the plaintext.

2.3 Complexity Assumptions

Definition 2. **(Bilinear Map).** Let $\mathbb{G}$ and $\mathbb{G}_1$ be two multiplicative groups of prime order p. Let g be a generator of $\mathbb{G}$. A function $e : \mathbb{G} \times \mathbb{G} \longrightarrow \mathbb{G}_1$ is said to be bilinear mapping if it has the following properties:
1. $e(u^a, v^b) = e(u, v)^{ab}$, $\forall\ u, v \in \mathbb{G}$ and $\forall\ a, b \in \mathbb{Z}_p$.
2. The function is non-degenerate, i.e., $e(g, g)$ is a generator of $\mathbb{G}_1$.
3. e is efficiently computable.
The tuple $\mathbb{S} = (p, \mathbb{G}, \mathbb{G}_1, e)$ is called a prime order bilinear group system.

The l-wDABDHE Assumption [14]:
Input: $\langle Z = (\mathbb{S}, h, h^{\alpha^{l+2}}, \ldots, h^{\alpha^{2l}}, g, g^{\alpha}, \ldots, g^{\alpha^l}), K\rangle$, where $\mathbb{S} = (p, \mathbb{G}, \mathbb{G}_1, e)$ is a bilinear group system, g is a generator of $\mathbb{G}$, $h \in_R \mathbb{G}, \alpha \in_R \mathbb{Z}_p$, K is either $e(g, h)^{\alpha^{l+1}}$ or a random element $X \in \mathbb{G}_1$.
Output: 0 if $K = e(g, h)^{\alpha^{l+1}}$; 1 otherwise.

Figure 1: l-wDABDHE assumption.

Definition 3. The l-wDABDHE assumption holds with (T, ϵ) if for every PPT adversary $\mathcal{A}$ with running time at most T, the advantage of solving the above problem is at most ϵ, i.e.,

$$Adv_{\mathcal{A}}^{l-\mathsf{wDABDHE}}$$
$$= |Pr[\mathcal{A}(Z, K = e(g, h)^{\alpha^{l+1}}) = 0] - Pr[\mathcal{A}(Z, K = X) = 0]|$$
$$\leq \epsilon(\lambda),$$

where $\epsilon(\lambda)$ is a negligible function in security parameter λ.

Note that, cryptographic hardness of l-wDABDHE assumption follows from General Decisional Diffie-Hellman Exponent (GDDHE) problem of Boneh et al. [2].

3. OUR RR-BE CONSTRUCTION

The communication model of our recipient-revocable broadcast encryption (RR-BE) construction involves a PKGC, a content provider, a broadcaster and several users. The PKGC runs $\mathsf{RR\text{-}BE.Setup}$ to generate PP and MK and runs $\mathsf{RR\text{-}BE.\ KeyGen}$ to generate sk_i of user i. A content provider and a broadcaster agree upon a common set of users. The content provider provides an encrypted content to the broadcaster. From this encrypted content the broadcaster revokes a subset of users which it wants to revoke. Legal users uses their secret keys to recover the content. Our scheme RR-BE = (RR-BE.Setup, RR-BE. KeyGen, RR-BE.Encrypt, RR-BE.Revoke, RR-BE.Decrypt) is described as follows:

- $(\mathsf{PP}, \mathsf{MK}) \leftarrow \mathsf{RR\text{-}BE.Setup}(N, \lambda)$: Given the security parameter λ and public identity $\mathsf{ID} = \{ID_1, ID_2, \ldots, ID_N\} \in (\mathbb{Z}_p)^N$ of a group of N users, the PKGC generates the public parameter PP and a master key MK as follows:
  1. Chooses a prime order bilinear group system $\mathbb{S} = (p, \mathbb{G}, \mathbb{G}_1, e)$, where $\mathbb{G}, \mathbb{G}_1$ are groups of prime order p and $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$ is a bilinear mapping.
  2. Selects $\alpha, \beta \in_R \mathbb{Z}_p$, and sets MK, PP as
     $\mathsf{MK} = (\alpha, \beta)$,
     $\mathsf{PP} = (\mathbb{S}, l_0, l_0^{\alpha}, \ldots, l_0^{\alpha^N}, g, g^{\alpha}, \ldots, g^{\alpha^N}, g^{\alpha\beta}, \ldots, g^{\alpha^{N+1}\beta}, e(g, g), e(g, l_0), \mathsf{ID})$,
     where g is generator of $\mathbb{G}$ and l_0 is random non-identity element of $\mathbb{G}$.
  3. Keeps MK secret to itself and makes PP public.

  Note that the public identity of the user i is $ID_i \in \mathbb{Z}_p$ for $i \in [N]$.
- $(sk_i) \leftarrow \mathsf{RR\text{-}BE.KeyGen}(\mathsf{PP}, \mathsf{MK}, i)$: For each user $i \in [N]$, the PKGC selects $h_i \in_R \mathbb{G}$, $r_i \in_R \mathbb{Z}_p$ and generates a secret key $sk_i = (d_{1,i}, d_{2,i}, d_{3,i}, \mathsf{label}_i)$, using $\mathsf{MK} = (\alpha, \beta), g, l_0$ and ID_i, by setting

  $$d_{1,i} = (h_i g^{r_i})^{\frac{1}{\alpha\beta(\alpha + ID_i)}}, d_{2,i} = r_i,$$

  $$d_{3,i} = (h_i l_0^{r_i})^{\frac{1}{\alpha\beta}}, \mathsf{label}_i = (h_i, h_i^{\alpha}, \ldots, h_i^{\alpha^N}).$$

  Here ID_i is extracted from ID given in PP. It sends sk_i to user i through a secure communication channel between them.
- $(\mathsf{CT}) \leftarrow \mathsf{RR\text{-}BE.Encrypt}(S, \mathsf{PP}, k, M)$: The content provider performs the following to produce an encrypted content for the user set $S \subseteq [N]$ of n users, using PP, maximum revocation number k $(< n)$ and message M:

1. Sets a polynomial $F(x) = \prod_{i_j \in S} (x + ID_{i_j}) = \sum_{i=0}^{n} F_i x^i$, where F_i's are function of ID_j for $j \in S$.

2. Picks $r \in_R \mathbb{Z}_p$ and generates the encrypted content $\mathsf{CT} = (S, c_1, c_2, \hat{c}_1, \ldots, \hat{c}_{k+1}, c_M)$ by setting

$$c_1 = \prod_{i=0}^{n} (g^{\alpha^{i+1}\beta})^{rF_i} = g^{\sum_{i=0}^{n} \beta\alpha^{i+1} rF_i} = g^{\alpha\beta F(\alpha) r},$$
$$c_2 = e(g,g)^{-r}, \hat{c}_1 = (g^{\alpha})^{-r} = g^{-r\alpha},$$
$$\hat{c}_i = \left(g^{\alpha^i}\right)^r = g^{\alpha^i r} \text{ for } 2 \leq i \leq k+1,$$
$$c_M = Me(g, l_0)^r.$$

Here $g^{\alpha}, \ldots, g^{\alpha^k}, g^{\alpha^{k+1}}, g^{\alpha\beta}, \ldots, g^{\alpha^n\beta}, g^{\alpha^{n+1}\beta}$, $e(g,g), e(g,l_0)$ are extracted from PP.

3. Sends CT to the broadcaster through a secure communication channel between the broadcaster and the content provider.

Note that, the broadcaster and the content provider shares the information of set S. They can make the information of set S public.

- $(\mathsf{CT}') \leftarrow \mathsf{RR\text{-}BE.Revoke}(\mathsf{PP}, \mathsf{CT}, R)$: Using PP, $\mathsf{CT} = (S, c_1, c_2, \hat{c}_1, \ldots, \hat{c}_{k+1}, c_M)$ for the user set S, revocation set $R = \{i_1, i_2, \ldots, i_l\} \subseteq S$, $(l \leq k)$ the broadcaster generates ciphertext for the set $G = S - R$ as:

  1. If $R = \phi$, sets $C_1 = c_1$, $C_2 = c_2, \widehat{C}_1 = \hat{c}_1, C_M = c_M$.

  2. If $R \neq \phi$, then

     (a) Computes $\frac{\prod_{j \in R} (x + ID_j)}{\prod_{j \in R} ID_j} = \sum_{i=0}^{l} f_i x^i$, where $f_i, 0 \leq i \leq l$ are function of ID_j for $j \in R$. Note that $f_0 = 1$.

     Also computes $X = \prod_{i=2}^{l} \hat{c}_i^{f_i} = g^{r \sum_{i=2}^{l} f_i \alpha^i}$.

     (b) Implicitly sets $s = r \sum_{i=0}^{l} f_i \alpha^i$ and generates $C_1, C_2, \widehat{C}_1, C_M$ as

$$C_1 = c_1^{\left\{\frac{1}{\prod_{j \in R} ID_j}\right\}}$$
$$= g^{r\alpha\beta\left\{\frac{\prod_{j \in R}(\alpha + ID_j) \prod_{j \in G}(\alpha + ID_j)}{\prod_{j \in R} ID_j}\right\}}$$
$$= g^{\alpha\beta\left\{s \prod_{j \in G}(\alpha + ID_j)\right\}},$$

$$C_2 = c_2 e(g, \hat{c}_1^{f_1} X^{-1})$$
$$= e(g,g)^{-r} e(g,g)^{-r(\alpha f_1 + \alpha^2 f_2 + \alpha^3 f_3 + \ldots + \alpha^l f_l)}$$
$$= e(g,g)^{-r(1 + \alpha f_1 + \alpha^2 f_2 + \alpha^3 f_3 + \ldots + \alpha^l f_l)}$$
$$= e(g,g)^{-s},$$
$$\widehat{C}_1 = \hat{c}_1 (\prod_{i=2}^{l+1} \hat{c}_i^{f_{i-1}})^{-1}$$
$$= (g^{-\alpha r})(g^{-\alpha^2 r})^{f_1}(g^{-\alpha^3 r})^{f_2} \ldots (g^{-\alpha^{l+1} r})^{f_l}$$
$$= g^{-\alpha r(1 + \alpha f_1 + \alpha^2 f_2 + \alpha^3 f_3 + \ldots + \alpha^l f_l)} = g^{-\alpha s},$$
$$C_M = c_M e(\hat{c}_1^{\{-f_1\}} X, l_0)$$
$$= Me(g, l_0)^r e(g, l_0)^{r(\alpha f_1 + \alpha^2 f_2 + \alpha^3 f_3 + \ldots + \alpha^l f_l)}$$
$$= Me(g, l_0)^{r(1 + \alpha f_1 + \alpha^2 f_2 + \alpha^3 f_3 + \ldots + \alpha^l f_l)}$$
$$= Me(g, l_0)^s.$$

     In this computation, $g, l_0, ID_j (j \in G)$ are extracted from PP and $f_i, 0 \leq i \leq l$ are computed as in step 2(a).

  3. Finally, publishes $\mathsf{CT}' = (G, C_1, C_2, \widehat{C}_1, C_M)$ as ciphertext where $G = S - R$.

- $(M) \leftarrow \mathsf{RR\text{-}BE.Decrypt}(\mathsf{PP}, sk_i, \mathsf{CT}')$: A subscribed user i with the secret key $sk_i = \big(d_{1,i}, d_{2,i}, d_{3,i}, \mathsf{label}_i = (h_i, h_i^{\alpha}, \ldots, h_i^{\alpha^N})\big)$ uses PP, the ciphertext $\mathsf{CT}' = (G, C_1, C_2, \widehat{C}_1, C_M)$, and computes $e(g, h_i g^{r_i})^s, e(g, h_i)^s$, $e(g, h_i l_0^{r_i})^s, K = e(g, l_0)^s$ to recover the message M as follows:

$$e(g, h_i g^{r_i})^s =$$
$$\begin{cases} \Big[e(C_1, d_{1,i}) e\Big(\widehat{C}_1, (h_i g^{d_{2,i}})^{A_{i,G,\alpha}}\Big)\Big]^{\left\{\frac{1}{\prod_{j \in G, j \neq i} ID_j}\right\}} & \text{if } |G| > 1 \\ e(C_1, d_{1,i}) e(\widehat{C}_1, g)^{d_{2,i}} & \text{if } |G| = 1 \end{cases}$$
$$e(g, h_i)^s = e(g, h_i g^{r_i})^s C_2^{d_{2,i}}$$

$$e(g, h_i l_0^{r_i})^s = \Big[e(C_1, d_{3,i}) e\Big(\widehat{C}_1, (h_i l_0^{d_{2,i}})^{B_{G,\alpha}}\Big)\Big]^{\left\{\frac{1}{\prod_{j \in G} ID_j}\right\}},$$
$$K = \Big\{\frac{e(g, h_i l_0^{r_i})^s}{e(g, h_i)^s}\Big\}^{\frac{1}{d_{2,i}}} = e(g, l_0)^s, M = \frac{C_M}{K}.$$

where

$$A_{i,G,\alpha} = \frac{1}{\alpha}\Big\{\prod_{j \in G, j \neq i} (\alpha + ID_j) - \prod_{j \in G, j \neq i} ID_j\Big\},$$

$$B_{G,\alpha} = \frac{1}{\alpha}\Big\{\prod_{j \in G} (\alpha + ID_j) - \prod_{j \in G} ID_j\Big\}.$$

We explain below how a user $i \in G$ can compute $(h_i g^{d_{2,i}})^{A_{i,G,\alpha}}$, $(h_i l_0^{d_{2,i}})^{B_{G,\alpha}}$ without knowing α. Note that the polynomial $\frac{1}{x}\Big\{\prod_{j \in G, j \neq i} (x + ID_j) - \prod_{j \in G, j \neq i} (ID_j)\Big\} = \sum_{i=0}^{n-l-2} a^i x^i$ is of degree $(n - l - 2)$ in x where $|G| = n - l > 1$. With the knowledge of G, the user $i \in G$ can compute the co-efficients

a_i, $i \in [0, n-l-2]$ which are functions of ID_j where $j \in G, j \neq i$. Since g^{α^j} for $j \in [0, n-l-2]$ are available in public parameter PP and $h_i^{\alpha^j}$ for $j \in [0, n-l-2]$ are extractable from sk_i, user $i \in G$ can compute

$$\prod_{j=0}^{n-l-2} (h_i^{\alpha_j})^{a_j} \prod_{j=0}^{n-l-2} (g^{\alpha^j})^{d_{2,i} a_j}$$
$$= h_i^{\left\{\sum_{j=0}^{n-l-2} a_j \alpha^j\right\}} g^{d_{2,i}\left\{\sum_{j=0}^{n-l-2} a_j \alpha^j\right\}} = (h_i g^{d_{2,i}})^{A_{i,G,\alpha}}$$

without the knowledge of α.
Similarly, the polynomial $\frac{1}{x}\left\{\prod_{j\in G}(x+ID_j) - \prod_{j\in G}(ID_j)\right\} = \sum_{i=0}^{n-l-1} b^i x^i$ is of degree $(n-l-1)$ in x where $|G| = n-l$.
With the knowledge of G, the user $i \in G$ can compute the co-efficients b_i, $i \in [0, n-l-1]$ which are functions of ID_j where $j \in G$. Since $l_0^{\alpha^j}$ for $j \in [0, n-l-1]$ are available in public parameter PP and $h_i^{\alpha^j}$ for $j \in [0, n-l-1]$ are extractable from sk_i, user $i \in G$ can compute

$$\prod_{j=0}^{n-l-1} (h_i^{\alpha_j})^{b_j} \prod_{j=0}^{n-l-1} (l_0^{\alpha^j})^{d_{2,i} b_j}$$
$$= h_i^{\left\{\sum_{j=0}^{n-l-1} b_j \alpha^j\right\}} l_0^{d_{2,i}\left\{\sum_{j=0}^{n-l-1} b_j \alpha^j\right\}} = (h_i l_0^{d_{2,i}})^{B_{G,\alpha}}$$

without the knowledge of α.

Correctness: The correctness of decryption procedure is provided below:

if |G|>1,

$$\left[e(C_1, d_{1,i}) e\Big(\widehat{C}_1, (h_i g^{d_{2,i}})^{A_{i,G,\alpha}}\Big)\right]^{\left\{\frac{1}{\prod_{j\in G, j\neq i} ID_j}\right\}}$$
$$= \left[e(C_1, d_{1,i}) e(\widehat{C}_1, h_i g^{d_{2,i}})^{A_{i,G,\alpha}}\right]^{\left\{\frac{1}{\prod_{j\in G, j\neq i} ID_j}\right\}}$$
$$= \left[e\Big(g^{s\alpha\beta \prod_{j\in G}(\alpha+ID_j)}, (h_i g^{r_i})^{\frac{1}{\alpha\beta(\alpha+ID_i)}}\Big) \times \right.$$
$$\left. e(g^{-\alpha s}, h_i g^{r_i})^{\frac{1}{\alpha}\left\{\prod_{j\in G, j\neq i}(\alpha+ID_j) - \prod_{j\in G, j\neq i} ID_j\right\}}\right]^{\left\{\frac{1}{\prod_{j\in G, j\neq i} ID_j}\right\}}$$
$$= \left[e(g, h_i g^{r_i})^{s\left\{\prod_{j\in G, j\neq i}(\alpha+ID_j)\right\}} \times \right.$$
$$\left. e(g, h_i g^{r_i})^{-s\left\{\prod_{j\in G, j\neq i}(\alpha+ID_j) - \prod_{j\in G, j\neq i} ID_j\right\}}\right]^{\left\{\frac{1}{\prod_{j\in G, j\neq i} ID_j}\right\}}$$
$$= \left[e(g, h_i g^{r_i})^{s \prod_{j\in G, j\neq i} ID_j}\right]^{\left\{\frac{1}{\prod_{j\in G, j\neq i} ID_j}\right\}} = e(g, h_i g^{r_i})^s,$$

if $|G| = 1$, $e(C_1, d_{1,i}) = e\Big(g^{s\alpha\beta(\alpha+ID_i)}, (h_i g^{r_i})^{\frac{1}{\alpha\beta(\alpha+ID_i)}}\Big)$
$= e(g, h_i g^{r_i})^s$,

$$\Longrightarrow \quad e(g, h_i g^{r_i})^s C_2^{d_{2,i}} = e(g, h_i g^{r_i})^s e(g, g)^{-sr_i}$$
$$= e(g, h_i)^s,$$

Similarly,

$$\left[e(C_1, d_{3,i}) e\Big(\widehat{C}_1, (h_i l_0^{d_{2,i}})^{B_{G,\alpha}}\Big)\right]^{\left\{\frac{1}{\prod_{j\in G} ID_j}\right\}}$$
$$= \left[e(C_1, d_{3,i}) e(\widehat{C}_1, h_i l_0^{d_{2,i}})^{B_{G,\alpha}}\right]^{\left\{\frac{1}{\prod_{j\in G} ID_j}\right\}}$$
$$= \left[e\Big(g^{s\alpha\beta \prod_{j\in G}(\alpha+ID_j)}, (h_i l_0^{r_i})^{\frac{1}{\alpha\beta}}\Big) \times \right.$$
$$\left. e(g^{-\alpha s}, h_i l_0^{r_i})^{\frac{1}{\alpha}\left\{\prod_{j\in G}(\alpha+ID_j) - \prod_{j\in G} ID_j\right\}}\right]^{\left\{\frac{1}{\prod_{j\in G} ID_j}\right\}}$$
$$= \left[e(g, h_i l_0^{r_i})^{s\left\{\prod_{j\in G}(\alpha+ID_j)\right\}} \times \right.$$
$$\left. e(g, h_i l_0^{r_i})^{-s\left\{\prod_{j\in G}(\alpha+ID_j) - \prod_{j\in G} ID_j\right\}}\right]^{\left\{\frac{1}{\prod_{j\in G} ID_j}\right\}}$$
$$= \left[e(g, h_i l_0^{r_i})^{s \prod_{j\in G} ID_j}\right]^{\left\{\frac{1}{\prod_{j\in G} ID_j}\right\}} = e(g, h_i l_0^{r_i})^s,$$

$$\text{Hence,} \quad K = \left\{\frac{e(g, h_i l_0^{r_i})^s}{e(g, h_i)^s}\right\}^{\frac{1}{d_{2,i}}} = \left\{\frac{e(g, h_i)^s e(g, l_0^{r_i})^s}{e(g, h_i)^s}\right\}^{\frac{1}{r_i}}$$
$$= e(g, l_0)^s,$$
$$M = \frac{C_M}{K}.$$

Remark 1. *We can remove the secure communication between the content provider and the broadcaster as follows: In key generation phase the PKGC takes a random number $r \in \mathbb{G}_1$ and sends securely to both the content provider and the broadcaster. The content provider makes the following encrypted content public*

$$\mathsf{CT} = (G, c_1, c_2, \hat{c}_1, \ldots, \hat{c}_{k+1}, E_r(c_M)).$$

Here $E_r(c_M)$ is symmetric key encryption of c_M using r. The broadcaster has the secret key r, he recovers c_M by decrypting $E_r(c_M)$. Now the broadcasted can run the revocation algorithm as previous. Note that except c_M other components don't involve the content M, thereby don't require encryption to make it public.

Remark 2. *If the content provider sends different encrypted content then the broadcaster will broadcast a ciphertext which is different from original ciphertext. As a result subscribed user will unable to recover actual content. Users will complain to the broadcaster that they are not getting desired content. The broadcaster informs to the content provider that information are wrongly provided. Now an attacker can also change the encrypted content. To prevent this we need to use an unforgeable signature scheme which will sign on ciphertext and will also make verification key public as in the chosen ciphertext attack secue construction of Boneh et. al. [3]. Each subscribed user will verify the signature, if the verification succeeds then it will decrypt the content. As we are discussing CPA security, we did not included signature and its verification in our RR-BE scheme.*

4. SECURITY

We prove semantic security of our scheme under q-$\mathsf{wDABDHE}$ ($q \geq 2n$) assumption. We achieve adaptive security in standard model, whereas the existing scheme achieves selective semantic security in random oracle model.

Theorem 1. *Our proposed scheme RR-BE described in Section 3 achieves adaptive semantic (indistinguishability against CPA) security as per the message indistinguishability security game of Section 2.2 under the q-$\mathsf{wDABDHE}$ ($q \geq 2n$) hardness assumption where n ($\leq N$) is the maximum size of the set of users in S.*

Proof. Assume that there is a PPT adversary $\mathcal{A}$ that breaks the adaptive semantic security of our proposed RR-BE scheme with a non-negligible advantage. We construct a PPT distinguisher $\mathcal{C}$ that attempts to solve the q-$\mathsf{wDABDHE}$ problem using $\mathcal{A}$ as a subroutine. Let $\mathcal{C}$ be given a q-$\mathsf{wDABDHE}$ ($q \geq 2n$) instance $\langle Z, X \rangle$ with

$$Z = (\mathbb{S}, \hat{g}, \hat{g}^{\alpha^{q+2}}, \ldots, \hat{g}^{\alpha^{2q}}, g, g^{\alpha}, \ldots, g^{\alpha^q}),$$

where $\mathbb{S} = (p, \mathbb{G}, \mathbb{G}_1, e)$ is a prime order bilinear group system, g is generator of group $\mathbb{G}$, $\hat{g} \in_R \mathbb{G}$, $\alpha \in_R \mathbb{Z}_p$, X is either $e(\hat{g}, g)^{\alpha^{q+1}}$ or a random element of $\mathbb{G}_1$. We describe below the interaction of $\mathcal{A}$ with the distinguisher $\mathcal{C}$ who attempts to output 0 if $X = e(\hat{g}, g)^{\alpha^{q+1}}$ and 1 otherwise.

Setup: The challenger $\mathcal{C}$ generates the public parameter PP and master key MK as follows:

- Chooses $b_{0,j} \in_R \mathbb{Z}_p, j \in [0, n-1]$ and sets the polynomials $P^0(x), Q^0(x)$ as
  $P^0(x) = \sum\limits_{j=0}^{n-1} b_{0,j} x^j, Q^0(x) = xP^0(x) + 1.$

- Using $g, g^{\alpha}, \ldots, g^{\alpha^q}$ ($q \geq 2n$) computes $l_0^{\alpha^i}, i \in [0, n]$ as
  $l_0^{\alpha^i} = g^{\alpha^i} \prod\limits_{j=0}^{n-1} (g^{\alpha^{j+i+1}})^{b_{0,j}} = g^{\alpha^i (1 + \alpha P^0(\alpha))}$
  $= g^{\alpha^i Q^0(\alpha)}$, for $i \in [0, n]$.

- Sets $\mathsf{PP} = (\mathbb{S}, l_0, l_0^{\alpha}, \ldots, l_0^{\alpha^n}, g, g^{\alpha}, \ldots, g^{\alpha^N}, g^{\alpha\beta}, \ldots, g^{\alpha^{N+1}\beta}, e(g, g), e(g, l_0), \mathsf{ID})$, where $\beta \in \mathbb{Z}_p$, $\mathsf{ID} = \{ID_1, ID_2, \ldots, ID_n\} \in (\mathbb{Z}_p)^n$ is the set of public identities of n users. Sets $\mathsf{MK} = (\alpha, \beta)$, where α is not known to $\mathcal{C}$ explicitly.

As $Q^0(x), \beta$ is random, the distribution of the public parameter PP is identical to that in the original scheme.

Phase 1: The adversary $\mathcal{A}$ issues m key generation queries on $\{ID_{i_j}\}_{j=1}^{m}$. The challenger $\mathcal{C}$ generates the private key sk_i for users $i \in \{i_1, \ldots, i_m\} \subseteq [n]$ as follows:

- Chooses $b_{i,j}, b_i \in_R \mathbb{Z}_p, j \in [0, n-2]$ and sets
  $P^i(x) = \sum\limits_{j=0}^{n-2} b_{i,j} x^j,$
  $Q^i(x) = x(x + ID_i)P^i(x) + b_i.$

- Computes

$$d_{1,i} = \Big(\prod_{j=0}^{n-2} (g^{\alpha^j})^{b_{i,j}} \Big)^{\frac{1}{\beta}}$$

$$= \Big(g^{\sum_{j=0}^{n-2} b_{i,j}\alpha^j} \Big)^{\frac{1}{\beta}} = g^{\frac{P^i(\alpha)}{\beta}},$$

$$d_{2,i} = -Q^i(-ID_i)$$

$$= ID_i(-ID_i + ID_i)P^i(-ID_i) - b_i$$

$$= -b_i,$$

$$d_{3,i} =$$

$$\Big(\prod_{j=0}^{n-1} (g^{\alpha^j})^{-b_i b_{0,j}} \prod_{j=0}^{n-2} \{ (g^{\alpha^{j+1}})^{b_{i,j}} (g^{\alpha^j})^{b_{i,j} ID_i} \} \Big)^{\frac{1}{\beta}}$$

$$= \Big(\prod_{j=0}^{n-1} g^{-b_i b_{0,j} \alpha^j} \prod_{j=0}^{n-2} g^{\{ b_{i,j}(\alpha + ID_i)\alpha^j \}} \Big)^{\frac{1}{\beta}}$$

$$= \Big(g^{-b_i \sum_{j=0}^{n-1} b_{0,j}\alpha^j} g^{\{ (\alpha + ID_i) \sum_{j=0}^{n-2} b_{i,j}\alpha^j \}} \Big)^{\frac{1}{\beta}}$$

$$= \Big(g^{-b_i P^0(\alpha) + (\alpha + ID_i)P^i(\alpha)} \Big)^{\frac{1}{\beta}},$$

$$h_i^{\alpha^k} = (g^{\alpha^k})^{b_i} \prod_{j=0}^{n-2} \{ (g^{\alpha^{k+j+2}})^{b_{i,j}} (g^{\alpha^{k+j+1}})^{b_{i,j} ID_i} \}$$

$$= g^{\alpha^k \Big(\alpha(\alpha + ID_i)P^i(\alpha) + b_i \Big)} = g^{\alpha^k Q^i(\alpha)}.$$

- Sets $\mathsf{label}_i = (h_i^{\alpha^k}, k \in [0, n])$ and sends $sk_i = (d_{1,i}, d_{2,i}, d_{3,i}, \mathsf{label}_i)$ to the adversary $\mathcal{A}$.

As $b_i, Q^i(x)$ are random, $d_{2,i}, \mathsf{label}_i$ have identical distribution to those in the original scheme. It is left to show that $d_{1,i}, d_{3,i}$ follow the original distribution.

$$d_{1,i} = g^{\frac{P^i(\alpha)}{\beta}} = g^{\frac{Q^i(\alpha\beta) - b_i}{\alpha(\alpha + ID_i)}} = g^{\frac{Q^i(\alpha\beta) + d_{2,i}}{\alpha(\alpha + ID_i)}}$$

$$= (h_i g^{d_{2,i}})^{\frac{1}{\alpha\beta(\alpha + ID_i)}},$$

$$\text{Now, } -b_i P^0(\alpha) + (\alpha + ID_i)P^i(\alpha)$$

$$= \frac{1}{\alpha} \Big\{ -b_i \alpha P^0(\alpha) + Q^i(\alpha) - b_i \Big\}$$

$$= \frac{1}{\alpha} \Big\{ -b_i(Q^0(\alpha) - 1) + Q^i(\alpha) - b_i \Big\}$$

$$= \frac{1}{\alpha} \Big\{ -b_i Q^0(\alpha) + Q^i(\alpha) \Big\}$$

$$\Rightarrow d_{3,i} = \Big(g^{-b_i P^0(\alpha) + (\alpha + ID_i)P^i(\alpha)} \Big)^{\frac{1}{\beta}}$$

$$= g^{\frac{1}{\alpha\beta} \Big\{ -b_i Q^0(\alpha) + Q^i(\alpha) \Big\}}$$

$$= \Big(g^{Q^i(\alpha)} g^{-b_i Q^0(\alpha)} \Big)^{\frac{1}{\alpha\beta}} = (h_i l_0^{d_{2,i}})^{\frac{1}{\alpha\beta}}.$$

Thus $d_{1,i}, d_{3,i}$ are identical to original scheme.

Challenge: The adversary $\mathcal{A}$ sends a set of user indices G to $\mathcal{C}$, where identities of users of G has not been queried before. It also sends two equal length messages M_0, M_1, maximum revocation number k ($< n$) and a revocation set R to the challenger $\mathcal{C}$ where no identity in the set R lies in G. Let $S = G + R$. The challenger $\mathcal{C}$ does the following:

- Computes $\prod_{i=0}^{n-1} (g^{\alpha^i})^{b_{0,i}} = g^{\sum_{i=0}^{n-1} b_{0,i}\alpha^i} = g^{P^0(\alpha)}$ by extracting g^{α^i} values from the given instance $\langle Z, X\rangle$.

- Selects $M_b, b \in_R \{0,1\}$ and sets C_{M_b} as, $C_{M_b} = M_b X e(\hat{g}^{\alpha^{q+2}}, g^{P^0(\alpha)})$, where X is extracted from $\langle Z, X\rangle$. Here X is either $e(\hat{g}, g)^{\alpha^{q+1}}$ or a random element of $\mathbb{G}_1$. If $X = e(\hat{g}, g)^{\alpha^{q+1}}$ then the simulated $C_{M_b} (= c_{M_b})$ has the same distribution as in the original scheme as

$$\begin{aligned} C_{M_b} &= M_b X e(\hat{g}^{\alpha^{q+2}}, g^{P^0(\alpha)}) \\ &= M_b e(\hat{g}, g)^{\alpha^{q+1}} e(\hat{g}^{\alpha^{q+2}}, g^{P^0(\alpha)}) \\ &= M_b e(\hat{g}^{\alpha^{q+1}}, g) e(\hat{g}^{\alpha^{q+1}}, g^{\alpha P^0(\alpha)}) \\ &= M_b e(\hat{g}^{\alpha^{q+1}}, g^{\alpha P^0(\alpha)+1}) \\ &= M_b e(\hat{g}^{\alpha^{q+1}}, g^{Q^0(\alpha)}) \\ &= M_b e(g^s, l_0) = M_b e(g, l_0)^s \end{aligned}$$

where s is implicitly set as $s = \alpha^{q+1} \log_g \hat{g}$.

- Sets $\lambda(x) = \prod_{j\in G} (x + ID_j) = \sum_{i=0}^{|G|} \lambda_i x^i$, where λ_i are function of ID_j for $j \in G$.

- Computes $\prod_{i=0}^{|G|} (\hat{g}^{\alpha^{q+2+i}\beta})^{\lambda_i} = (\hat{g}^{\alpha^{q+2}\beta})^{\sum_{i=0}^{|G|} \lambda_i \alpha^i} = (\hat{g}^{\alpha^{q+2}\beta})^{\prod_{i\in G}(\alpha+ID_i)}$.
 Note that $\hat{g}^{\alpha^i}, i \in [q+2, 2q], q \geq 2n$ are available to $\mathcal{C}$ through the given instance $\langle Z, X\rangle$.

- If $R \neq \phi$, sets the challenge ciphertext CT^* as, $\mathsf{CT}^* = \Big(G, (\hat{g}^{\alpha^{q+2}\beta})^{\prod_{i\in G}(\alpha+ID_i)}, X^{-1}, \hat{g}^{-\alpha^{q+2}}, C_{M_b}\Big)$ $= (G, C_1, C_2, \widehat{C}_1, C_{M_b})$.
 else if $R = \phi$ (i.e. $G = S$), sets CT^* as

$$\begin{aligned} \mathsf{CT}^* = \Big(&G, (\hat{g}^{\alpha^{q+2}\beta})^{\prod_{i\in G}(\alpha+ID_i)}, X^{-1}, \hat{g}^{-\alpha^{q+2}}, \\ &\hat{g}^{\alpha^{q+3}}, \ldots, \hat{g}^{\alpha^{q+k+1}}, C_{M_b}\Big) \\ = (&G, c_1, c_2, \hat{c}_1, \hat{c}_2, \ldots, \hat{c}_{k+1}, c_{M_b}). \end{aligned}$$

 If $X = e(\hat{g}, g)^{\alpha^{q+1}}$, then as s is implicitly set to be $s = \alpha^{q+1} \log_g \hat{g}$, we have

$$\begin{aligned} C_1 = c_1 &= (\hat{g}^{\alpha^{q+2}\beta})^{\prod_{i\in G}(\alpha+ID_i)} \\ &= (g^{\beta \log_g \hat{g}\alpha^{q+2}})^{\prod_{i\in G}(\alpha+ID_i)} \\ &= (g^{\beta\alpha\alpha^{q+1}\log_g \hat{g}})^{\prod_{i\in G}(\alpha+ID_i)} \\ &= (g^{\alpha\beta})^{s\prod_{i\in G}(\alpha+ID_i)}, \\ C_2 = c_2 &= X^{-1} = e(\hat{g}, g)^{-\alpha^{q+1}} \\ &= e(g^{\log_g \hat{g}}, g)^{-\alpha^{q+1}} \\ &= e(g,g)^{-\alpha^{q+1}\log_g \hat{g}} = e(g,g)^{-s}, \\ \widehat{C}_1 = \hat{c}_1 &= \hat{g}^{-\alpha^{q+2}} = g^{-(\log_g \hat{g})\alpha^{q+2}} \\ &= g^{-\alpha\alpha^{q+1}\log_g \hat{g}} = g^{-\alpha s}, \\ \hat{c}_i &= \hat{g}^{\alpha^{q+1+i}} = g^{\alpha^i\alpha^{q+1}\log_g \hat{g}} = g^{\alpha^i s}, 2 \leq i \leq k. \end{aligned}$$

 Consequently, distribution of CT^* is similar to our real construction from $\mathcal{A}$'s point of view.

- Returns CT^* to $\mathcal{A}$.

Note that in our RR-BE (see Section 3), components $c_1, c_2, \hat{c}_1, c_M$ generated for message M in RR-BE.Encrypt are identical to $C_1, C_2, \widehat{C}_1, C_M$ of RR-BE.Revoke respectively except from randomness. Therefore in this **Challenge** phase, from adversary $\mathcal{A}$'s point of view there is no difference between $(c_1, c_2, \hat{c}_1, c_{M_b})$ and $(C_1, C_2, \widehat{C}_1, C_{M_b})$. Consequently we can take $C_1 = c_1, C_2 = c_2, \widehat{C}_1 = \hat{c}_1, C_{M_b} = c_{M_b}$ as challenge ciphertext in $R \neq \phi$ case.

Phase 2: This is similar to Phase 1 key generation queries. The adversary $\mathcal{A}$ sends key generation queries for $\{i_{m+1}, \ldots, i_t\} \subseteq [n]$ with a restriction that $i_j \notin G$ and receives back secret keys $\{sk_{i_j}\}_{j=m+1}^{t}$ simulated in the same manner by $\mathcal{C}$ as in Phase 1.

Guess: Finally, $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$ of b to $\mathcal{C}$ and wins if $b' = b$. If $b' = b$, $\mathcal{C}$ outputs 0, indicating that $X = e(\hat{g}, g)^{\alpha^{q+1}}$; otherwise, it outputs 1, indicating that X is a random element of $\mathbb{G}_1$.

The simulation of $\mathcal{C}$ is perfect when $X = e(\hat{g}, g)^{\alpha^{q+1}}$. Therefore, we have

$$Pr[\mathcal{C}(Z, X = e(\hat{g}, g)^{\alpha^{q+1}}) = 0] = \frac{1}{2} + Adv_{\mathcal{A}}^{\mathsf{RR-BE-IND}},$$

where $Adv_{\mathcal{A}}^{\mathsf{RR-BE-IND}}$ is the advantage of the adversary $\mathcal{A}$ in the above indistinguishability game. On the other hand, M_b is completely hidden from the adversary $\mathcal{A}$ when $X = R$ is random, thereby

$$Pr[\mathcal{C}(Z, X = R) = 0] = \frac{1}{2}.$$

Hence, the advantage of the challenger $\mathcal{C}$ in solving q-$\mathsf{wDABDHE}$ is

$$\begin{aligned} &Adv_{\mathcal{C}}^{q-\mathsf{wDABDHE}}(t, n) \\ &= |Pr[\mathcal{C}(Z, X = e(\hat{g}, g)^{\alpha^{q+1}}) = 0] - Pr[\mathcal{C}(Z, X = R) = 0]| \\ &= \frac{1}{2} + Adv_{\mathcal{A}}^{\mathsf{RR-BE-IND}} - \frac{1}{2} = Adv_{\mathcal{A}}^{\mathsf{RR-BE-IND}}. \end{aligned}$$

Table 1: Comparative summaries of storage, communication bandwith and security of RR-BE schemes.

Scheme	$\lvert\mathsf{PP}\rvert$	$\lvert\mathsf{SK}\rvert$	$\lvert\mathsf{CT}\rvert$	$\lvert\mathsf{CT}'\rvert$	SM	Random Oracle	SA
[15]	$(2N{+}1)\lvert\mathbb{G}\rvert{+}1\lvert\mathbb{G}_1\rvert$	$(1)\lvert\mathbb{G}\rvert$	$(k+2)\lvert\mathbb{G}\rvert{+}1\lvert\mathbb{G}_1\rvert$	$2\lvert\mathbb{G}\rvert{+}1\lvert\mathbb{G}_1\rvert$	Selective	Yes	$(\hat{f}, g, F)$-GDDHE
Our RR-BE	$(3N{+}3)\lvert\mathbb{G}\rvert{+}2\lvert\mathbb{G}_1\rvert$	$(N{+}3)\lvert\mathbb{G}\rvert{+}1\lvert\mathbb{Z}_p\rvert$	$(k+2)\lvert\mathbb{G}\rvert{+}2\lvert\mathbb{G}_1\rvert$	$2\lvert\mathbb{G}\rvert{+}2\lvert\mathbb{G}_1\rvert$	Adaptive	No	q-wDABDHE

$|\mathsf{PP}|$ = public parameter size, $|\mathsf{SK}|$ = secret key size, $|\mathsf{CT}|$ = encrypted content size, $|\mathsf{CT}'|$ = ciphertext size, N = total number of users, $|\mathbb{G}|$ = bit size of an element of $\mathbb{G}$, $|\mathbb{G}_1|$ = bit size of an element of $\mathbb{G}_1$, $|\mathbb{Z}_p|$ = bit size of an element of $\mathbb{Z}_p$, SM = security model, SA = security assumption, $(\hat{f}, g, F)$-GDDHE = $(\hat{f}, g, F)$- general decisional diffie-hellman exponent, q-wDABDHE = q-weaker decisional augmented bilinear diffie-hellman exponent, $q \geq 2n$, n = number of users used in RR-BE.Encrypt phase.

Table 2: Comparative summary of computation cost of parameter generation, encryption and decryption algorithm for RR-BE schemes.

Scheme	PP		SK	Enc		Revoke			Dec		
	#exp	#pr	#exp	#exp	# inv	#exp	#pr	# inv	#exp	#pr	# inv
[15]	$2N$ in $\mathbb{G}$	1	1 in $\mathbb{G}$	$n+k{+}2$ in $\mathbb{G}$, 1 in $\mathbb{G}_1$	0	$2l{+}1$ in $\mathbb{G}$	1	0	n' in $\mathbb{G}$, 1 in $\mathbb{G}_1$	2	1 in $\mathbb{G}_1$
Our RR-BE	$3N{+}1$ in $\mathbb{G}$	2	$N+4$ in $\mathbb{G}$	$n+k{+}2$ in $\mathbb{G}$, 2 in $\mathbb{G}_1$	1 in $\mathbb{G}$, 1 in $\mathbb{G}_1$	$2l{+}1$ in $\mathbb{G}$	2	3 in $\mathbb{G}$	$4n'$-2 in $\mathbb{G}$, 4 in $\mathbb{G}_1$	4	1 in $\mathbb{G}_1$

PP = public parameter, SK = secret key, Enc = encryption, Revoke = revocation, Dec = decryption, N = total number of users, k = maximum number of revoked users, l = actual number of revoked users, n = number of users used in RR-BE.Encrypt phase, $n' = n - l$, #exp = number of exponentiations in $\mathbb{G}$ and $\mathbb{G}_1$,#pr = number of pairings, #inv = number of inversions in $\mathbb{G}$ and $\mathbb{G}_1$.

Therefore, if $\mathcal{A}$ has non-negligible advantage in correctly guessing b', then $\mathcal{C}$ predicts $X = e(\hat{g}, g)^{\alpha^{q+1}}$ or random element of $\mathbb{G}_1$ (i.e., solves q-wDABDHE ($q \geq 2n$) instance given to $\mathcal{C}$) with non-negligible advantage. Hence the theorem follows. □

5. EFFICIENCY

We have compared our RR-BE construction with the only known recipient revocable broadcast encryption scheme of Susilo et al. [15] in Table 1 and Table 2. We emphasize the following facts:

- Our scheme achieves adaptive security in the standard security model, while [15] is selectively secure in the random oracle model.

- Both the schemes are semantically secure under similar type of assumptions. Note that security of both $(\hat{f}, g, F)$-GDDHE, q-wDABDHE ($q \geq 2n$) follow from the General Decisional Diffie-Hellman Exponent (GDDHE) problem of Boneh et al. [2].

- Parameter sizes and computation costs asymptotically matches with those in [15] except from the secret key which is linear to the number of users (i.e. O(N)) in our scheme in contrast to constant size (i.e. O(1)) secret key in [15]. This trade-off is due to achieve the adaptively secure RR-BE scheme in the standard model.

6. CONCLUSION

We have proposed the first adaptively secure RR-BE scheme which is secure in standard model under q-wDABDHE ($q \geq 2n$) assumption. The proposed scheme compares favourably with the existing similar work [15] which is selectively secure in random oracle model.

7. REFERENCES

[1] A. Barth, D. Boneh, and B. Waters. Privacy in encrypted content distribution using private broadcast encryption. In *Proceedings of the 10th International Conference on Financial Cryptography and Data Security*, FC'06, pages 52–64, Berlin, Heidelberg, 2006. Springer-Verlag.

[2] D. Boneh, X. Boyen, and E.-J. Goh. Hierarchical identity based encryption with constant size ciphertext. In *Advances in Cryptology—EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 440–456. Berlin: Springer-Verlag, 2005. Available at `http://www.cs.stanford.edu/~xb/eurocrypt05a/`.

[3] D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In *Proceedings of the 25th Annual International Conference on Advances in Cryptology*, CRYPTO'05, pages 258–275, Berlin, Heidelberg, 2005. Springer-Verlag.

[4] D. Boneh, B. Waters, and M. Zhandry. Low overhead broadcast encryption from multilinear maps. In J. Garay and R. Gennaro, editors, *Advances in Cryptology - CRYPTO 2014*, volume 8616 of *Lecture Notes in Computer Science*, pages 206–223. Springer Berlin Heidelberg, 2014.

[5] B. Chor, A. Fiat, and M. Naor. Tracing traitors. In *Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '94, pages 257–270, London, UK, 1994. Springer-Verlag.

[6] C. Delerablée. Identity-based broadcast encryption with constant size ciphertexts and private keys. In *Proceedings of the Advances in Crypotology 13th International Conference on Theory and Application of Cryptology and Information Security*, ASIACRYPT'07, pages 200–215, Berlin, Heidelberg, 2007. Springer-Verlag.

[7] C. Delerablée, P. Paillier, and D. Pointcheval. Fully

collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys. In T. Takagi, T. Okamoto, E. Okamoto, and T. Okamoto, editors, *Pairing*, volume 4575 of *Lecture Notes in Computer Science*, pages 39–59. Springer, 2007.

[8] Y. Dodis and N. Fazio. Public key broadcast encryption for stateless receivers. In J. Feigenbaum, editor, *Digital Rights Management*, volume 2696 of *Lecture Notes in Computer Science*, pages 61–80. Springer Berlin Heidelberg, 2003.

[9] A. Fiat and M. Naor. Broadcast encryption. In *Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '93, pages 480–491, New York, NY, USA, 1994. Springer-Verlag New York, Inc.

[10] C. Gentry. Practical identity-based encryption without random oracles. In *Proceedings of the 24th Annual International Conference on The Theory and Applications of Cryptographic Techniques*, EUROCRYPT'06, pages 445–464, Berlin, Heidelberg, 2006. Springer-Verlag.

[11] A. Lewko, A. Sahai, and B. Waters. Revocation systems with very small private keys. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 273–285, May 2010.

[12] D. Naor, M. Naor, and J. Lotspiech. Revocation and tracing schemes for stateless receivers. In J. Kilian, editor, *Advances in Cryptology - CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 41–62. Springer Berlin Heidelberg, 2001.

[13] D. H. Phan, D. Pointcheval, S. Shahandashti, and M. Strefler. Adaptive cca broadcast encryption with constant-size secret keys and ciphertexts. *International Journal of Information Security*, 12(4):251–265, 2013.

[14] Y. Ren, S. Wang, and X. Zhang. Non-interactive dynamic identity-based broadcast encryption without random oracles. In *Proceedings of the 14th International Conference on Information and Communications Security*, ICICS'12, pages 479–487, Berlin, Heidelberg, 2012. Springer-Verlag.

[15] W. Susilo, R. Chen, F. Guo, G. Yang, Y. Mu, and Y.-W. Chow. Recipient revocable identity-based broadcast encryption: How to revoke some recipients in ibbe without knowledge of the plaintext. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '16, pages 201–210, New York, NY, USA, 2016. ACM.

APPENDIX

A. GENERAL DECISIONAL DIFFIE-HELLMAN EXPONENT PROBLEM [2]

We give an overview of General Decisional Diffie-Hellman Exponent problem in symmetric case. Let $\mathbb{S} = (p, \mathbb{G}, \mathbb{G}_1, e)$ is a bilinear group system. Let g be generator of group $\mathbb{G}$ and set $g_1 = e(g, g)$. Let $P, Q \in \mathbb{F}_p[X_1, \dots, X_n]^s$ be two s tuple of n variate polynomials over $\mathbb{F}_p$. We write $P = (p_1, \dots, p_s), Q = (q_1, \dots, q_s)$ and impose that $p_1 = 1, q_1 = 1$. For a set Ω, a function $h : \mathbb{F}_p \to \Omega$ and a vector $(x_1, \dots, x_n) \in {\mathbb{F}_p}^n$ we write,
$h(P(x_1, \dots, x_n)) =$
$\Big(h(p_1(x_1, \dots, x_n)), \dots, h(p_s(x_1, \dots, x_n))\Big) \in \Omega^s$.
We use similar notation for the s-tuple Q. A polynomial $f \in \mathbb{F}_p[X_1, \dots, X_n]$ depends on P, Q if there exists $a_{i,j}, b_i \in \mathbb{Z}_p$ such that

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

Otherwise, f is independent of P, Q. The (P, Q, f)-General Decisional Diffie-Hellman Exponent ((P, Q, f)-GDDHE) problem is defined as follows:

Definition 4. ((P, Q, f)-GDDHE:) Given $H(x_1, \dots, x_n) = (g^{P(x_1,\dots,x_n)}, g_1^{Q(x_1,\dots,x_n)})$ and $T \in \mathbb{G}_1$, decide whether $T = g_1^{f(x_1,\dots,x_n)}$.

Boneh et al. [2] have proved that (P, Q, f)-GDDHE is intractable, if f does not depend on P, Q.
Hardness of l-wDABDHE assumption: Let us consider $h = g^{\beta}$. If we formulate l-wDABDHE problem of Section 2.3 as the (P, Q, f)-GDDHE problem then

$$P = (1, \alpha, \alpha^2, \dots, \alpha^l, \beta, \beta\alpha^{l+2}, \dots, \beta\alpha^{2l})$$

$$Q = (1)$$

$$f = (\beta\alpha^{l+1})$$

Following the technique of [6], it is easy to show that f does not depend on P, Q. So, cryptographic hardness of l-wDABDHE assumption follows.