INFORMATICA, 2012, Vol. 23, No. 3, 487–505

A Fully Secure Revocable ID-Based Encryption in the Standard Model

Tung-Tso TSAI[1], Yuh-Min TSENG[1], Tsu-Yang WU[2]
[1]*Department of Mathematics, National Changhua University of Education*
Jin-De Campus, Chang-Hua City 500, Taiwan
[2]*School of Computer Science and Technology*
Harbin Institute of Technology Shenzhen Graduate School
Shenzhen 518055, China
e-mail: ymtseng@cc.ncue.edu.tw

Received: December 2011; accepted: April 2012

Abstract. Revocation problem is a critical issue for key management of public key systems. Any certificate-based or identity (ID)-based public key systems must provide a revocation method to revoke misbehaving/compromised users from the public key systems. In the past, there was little work on studying the revocation problem of ID-based public key systems. Most recently, Tseng and Tsai presented a novel ID-based public key system with efficient revocation using a public channel, and proposed a practical revocable ID-based encryption (called RIBE). They proved that the proposed RIBE is semantically secure in the random oracle model. Although the ID-based encryption schemes based on the random oracle model can offer better performance, the resulting schemes could be insecure when random oracles are instantiated with concrete hash functions. In this paper, we employ Tseng and Tsai's revocable concept to propose a new RIBE without random oracles to provide full security. We demonstrate that the proposed RIBE is semantically secure against adaptive-ID attacks in the standard model.

Keywords: revocation, identity-based encryption, standard model, bilinear pairing.

1. Introduction

In the certificate-based public key systems, the certificates make publicly available the mapping between identities and public keys. In order to eliminate the required certificates in the certificate-based public key systems, Shamir (1984) presented a good idea that a user's identity such as social security number, e-mail address or telephone number may be viewed as the user's public key. Boneh and Franklin (2001) followed Shamir's idea to propose the first practical identity (ID)-based encryption (IBE), in which there are two roles: a trusted private key generator (PKG) and users. Users can authenticate themselves to the PKG and then the PKG generates the corresponding private keys to the users. Boneh and Franklin's IBE was built on the progress in elliptic curves with bilinear pairings such as Weil, Tate and Ate pairings. Subsequently, the study of ID-based cryptographic mechanisms using bilinear pairings has received a great attention from researchers. A large number of literatures have been presented such as Cha and Cheon

(2003), Choi *et al.* (2004), Bellare *et al.* (2004b), Waters (2005), Chen *et al.* (2007), Tseng *et al.* (2008), Boneh and Hamburg (2008), Choi *et al.* (2008), Tseng *et al.* (2009), Wu and Tseng (2010), Liu and Huang (2010), Ren *et al.* (2010), Wu *et al.* (2011), Chen *et al.* (2012).

In the public key systems, several situations require a revocation mechanism to remove a misbehaving/compromised user before its intended expiration date. For example, the user's company may request revocation if the user leaves the company and is no longer entitled to use the public key. In the certificate-based public key systems, certificate revocation list (CRL) (Housley *et al*., 2002) is generally used to revoke the users' public keys, and then users can know misbehaving/compromised users by querying the CRL. Using the CRL technique to remove misbehaving/compromised users is an efficient approach for the certificate-based public key systems. Actually, efficient revocation is a well-studied problem in the certificate-based public key systems (Aiello *et al*., 1998; Micali, 2002; Gentry, 2003; Elwailly *et al*., 2004; Goyal, 2007). However, the ID-based public key systems have eliminated the need of certificates, thus the CRL method and the related revocation solutions will not be well-suited for ID-based public key systems.

For the revocation problem in the ID-based public key systems, Boneh and Franklin (2001) suggested that the PKG generates all non-revoked users' new private keys for each time period and then the PKG uses a secure channel to transmit these periodic private keys to non-revoked users. As a result, the PKG and each non-revoked user must encrypt and decrypt these periodic private keys, respectively. And the total size of the periodic update keys grows linearly with the number of non-revoked users. For reducing the PKG and user's periodic workload, Boldyreva *et al.* (2008) used a binary tree structure to construct a revocable ID-based encryption that reduces the key update size to logarithmic in the number of users. However, each user must keep $3 \log n$ private keys while the PKG needs to maintain a binary tree data structure of n leaf nodes, where n denotes the total number of users. Boldyreva *et al.* (2008) proved that their RIBE is secure in the relaxed selective-ID model (Canetti *et al.*, 2003), in which adversaries must choose the target identity before the system begins to be operated. Later on, Libert and Vergnaud (2009) improved Boldyreva *et al*.'s scheme to present an adaptive-ID secure RIBE scheme. However, the mentioned three schemes above need a secure channel to transmit the users' new private keys for each time period. For the PKG and non-revoked users, it raised enormous computation workload of encryption and decryption procedures, respectively.

Quite recently, Tseng and Tsai (2012) presented a new ID-based public key setting and its associated revocation mechanism with a public channel. They partitioned a user's private (decryption) key into two components including an initial secret key and a time update key. The initial secret key is fixed and unchanged, while the time update key is changed along with time period. The PKG periodically generates new time update keys for non-revoked users, the PKG then sends them to users using a public channel. Non-revoked users may update their own decryption keys while the PKG stops to issue the new time update keys of the revoked users. It can eliminate the requirement for the secure channel established between the PKG and each user. In such a case, no encryption or decryption is required the PKG and each non-revoked user. In the meantime, Tseng

and Tsai also proposed a practical revocable ID-based encryption (called RIBE) with a public channel. They proved that their RIBE scheme is secure in an adaptive-ID model, but their RIBE scheme only provided the security in the random oracle model (Bellare and Rogaway, 1993).

Although the ID-based encryption schemes based on the random oracle model can offer better performance, the resulting schemes could be insecure when random oracles are instantiated with concrete hash functions (Canetti *et al*., 1998; Bellare *et al*., 2004a; Boneh and Boyen, 2004a). Canetti *et al*. (2003) presented an IBE scheme without random oracles, in which the security is proven in the relaxed selective-ID model. Subsequently, Boneh and Boyen (2004a) provided more practical IBE schemes in the selective-ID model without random oracles. Afterwards, Boneh and Boyen (2004b) presented a fully secure IBE scheme in the adaptive-ID model without random oracles. For improving the efficiency of Boneh and Boyen's IBE scheme, Waters (2005) also proposed a fairly efficient IBE scheme without random oracles. Furthermore, Gentry (2006) proposed a new fully secure IBE scheme to reduce the required public parameters in Waters's scheme, but it relies on a stronger complexity assumption called the augmented bilinear Diffie–Hellman exponent (ABDHE) assumption (Gentry, 2006).

In this paper, we will employ the revocable concept and the framework presented by Tseng and Tsai (2012) to propose a new revocable ID-based encryption (RIBE) in the standard model (without random oracles) to provide full security. For security analysis, as the adversary model presented in Tseng and Tsai's RIBE scheme, the attackers consists of two kinds: an inside adversary (or a revoked user) and an outside adversary. We will give formal security analysis of the proposed RIBE schemes for the inside and the outside adversaries, respectively. Under the bilinear decision Diffie–Hellman problem (Boneh and Franklin, 2001), we demonstrate that the proposed RIBE scheme is semantically secure against adaptive-ID attacks in the standard model. Meanwhile, we discuss the transformation technique from a chosen-plaintext secure (CPA) RIBE scheme to a chosen-ciphertext secure (CCA) RIBE scheme.

The remainder of the paper is organized as follows. Preliminaries are given in Section 2. In Section 3, we present the definitions and security notions of revocable ID-based encryption (RIBE) with a public channel. Section 4 gives the concrete RIBE scheme. In Section 5, we analyze the security of the proposed RIBE scheme. Discussions and comparisons are presented in Section 6. Conclusions are given in Section 7.

2. Preliminaries

In this section, we briefly introduce the concept of bilinear pairings and the related mathematical assumptions. Bilinear pairings such as Weil, Tate and Ate pairings that have been used to establish efficient ID-based encryption (Boneh and Franklin, 2001; Baek and Zheng 2004; Sakai and Kasahara, 2003; Waters, 2005). For the details of the relationship between the security levels and speed of pairing computations, please refer to (Galbraith *et al*., 2008; Wu and Tseng, 2010) for full descriptions.

2.1. *Bilinear Pairings*

Let G_1 and G_2 be two multiplicative cyclic groups of large prime order p, and g be a generator of G_1. We say that the map $\hat{e}$: $G_1 \times G_1 \to G_2$ is an admissible bilinear map if it satisfies the following properties:

(1) Bilinearity: $\hat{e}(g^a, g^b) = \hat{e}(g, g)^{ab}$ for $g \in G_1$ and $a, b \in Z_p^*$.
(2) Non-degeneracy: There exist $g_1, g_2 \in G_1$ such that $\hat{e}(g_1, g_2) \neq 1$.
(3) Computability: For any $g_1, g_2 \in G_1$, there exists an efficient algorithm to compute $\hat{e}(g_1,\ g_2) \in G_2$.

It is obvious that since $\hat{e}(g^a,\ g^b) = \hat{e}(g, g)^{ab}$, it implies

$$\hat{e}\big(g^a g^b, g^c\big) = \hat{e}\big(g^{a+b}, g^c\big) = \hat{e}(g, g)^{(a+b)c} = \hat{e}(g, g)^{ac+bc} = \hat{e}\big(g^a, g^c\big)\hat{e}\big(g^b, g^c\big)$$

and

$$\hat{e}\big(g^a, g^b g^c\big) = \hat{e}\big(g^a, g^{b+c}\big) = \hat{e}(g, g)^{a(b+c)} = \hat{e}(g, g)^{ab+ac} = \hat{e}\big(g^a, g^b\big)\hat{e}\big(g^a, g^c\big).$$

Full descriptions of groups, maps and other parameters are discussed in Boneh and Franklin (2001), Waters (2005), Paterson and Schuldt (2006).

2.2. *Related Mathematical Assumptions*

Here, we present two mathematical problems and define a security assumption for bilinear pairings on which our scheme is based.

- Bilinear Diffie–Hellman (BDH) problem: Given $g, g^a, g^b, g^c \in G_1$ for unknown $a, b, c \in Z_p^*$, this problem is to compute $\hat{e}(g, g)^{abc} \in G_2$.
- Bilinear Decision Diffie–Hellman (BDDH) problem: Given $g, g^a, g^b, g^c \in G_1$ for some $a, b, c \in Z_p^*$ and $K \in G_2$, this problem is to decide whether $K = \hat{e}(g, g)^{abc}$.

DEFINITION 1 (BDDH assumption). Given $g, g^a, g^b, g^c \in G_1$ for some $a, b, c \in Z_p^*$ and $K \in G_2$, there exists no probabilistic polynomial-time adversary $\mathcal{A}$ with non-negligible probability who can decide whether $K = \hat{e}(g, g)^{abc}$. The successful probability (advantage) of the adversary $\mathcal{A}$ is presented as

$$\mathrm{Adv}_A = \Pr\big[\mathcal{A}\big(g, g^a, g^b, g^c, \hat{e}(g, g)^{abc}\big) = 1\big] - \Pr\big[\mathcal{A}\big(g, g^a, g^b, g^c, K\big) = 1\big],$$

where $K \in G_2$ is chosen uniformly at random and the probability is over the random choice consumed by the adversary $\mathcal{A}$.

2.3. *Notations*

We define the following notations that are used throughout this paper:

- $\hat{e}$: an admissible bilinear map, $\hat{e}$: $G_1 \times G_1 \to G_2$.

- g: a generator of the group G_1.
- *id*: the identity-related information of a user.
- d_{id}: the user's initial secret key.
- t: a time period, where $1 \leqslant t \leqslant z$ and z denotes the total number of time periods.
- $d_{id,t}$: a user *id*'s time update key for time period t.
- $D_{id,t}$: a user *id*'s entire decryption key for time period t. Note that the user's entire decryption key $D_{id,t}$ is obtained by the user's initial secret key d_{id} and time update key $d_{id,t}$.

3. Framework and Security Notions of RIBE

Tseng and Tsai (2012) have defined the framework and security notions of revocable ID-based encryption (RIBE) with a public channel. Under their framework of RIBE, a user's decryption key is divided into two components including a fixed initial secret key and a changed time update key along with time periods. As a result, the framework will add one *time key update algorithm* except for four algorithms defined in ID-based encryption (IBE) proposed by Boneh and Franklin (2001). We follow the revocable concept, the framework and security notions presented by Tseng and Tsai (2012). Here, we present the framework and security notions of revocable ID-based encryption (RIBE) with a public channel.

3.1. *Framework*

In this subsection, the framework of revocable ID-based encryption with a public channel is formally defined as follows.

DEFINITION 2. A revocable ID-based encryption (RIBE) with a public channel has 5-tuple of polynomial time algorithms $(\mathcal{G}, \mathcal{IKE}, \mathcal{TKU}, \mathcal{E}, \mathcal{D})$ as follows:

- *System setup algorithm* $\mathcal{G}$: Take a security parameter l and the total number z of all time periods as input, the algorithm returns the system secret key and the public parameters *Parms*. The public parameters *Parms* are made public and implicitly inputted to all the following algorithms.
- *Initial key extract algorithm* $\mathcal{IKE}$: Take the system secret key and a user's identity-related information *id* as input, the algorithm returns the user's initial secret key d_{id}.
- *Time key update algorithm* $\mathcal{TKU}$: For a time period t, take the system secret key and a user identity-related information id as input, the algorithm returns the user's time update key $d_{id,t}$. Note that the non-revoked user can use the initial secret key d_{id} and the time update key $d_{id,t}$ to obtain the entire decryption key $D_{id,t}$.
- *Encryption algorithm* $\mathcal{E}$: For a time period t, take an identity *id* and a message M as input, the algorithm generates a ciphertext C.
- *Decryption algorithm* $\mathcal{D}$: Take a ciphertext C and the user's entire decryption key $D_{id,t}$ as input, the algorithm returns a plaintext M.

3.2. *Security Model*

By the standard security model of ID-based encryption (IBE) in Boneh and Franklin (2001), Boneh and Boyen (2004a), Waters (2005), the indistinguishability (IND) of encryption is under selective/adaptive-ID and chosen-plaintext/chosen-ciphertext attacks. In which, the selective-ID model means that before the system begins to be operated, the adversary has to decide which identities it would like to attack. The selective-ID version proposed by Canetti *et al.* (2003) is a weaker security than the adaptive-ID version. Tseng and Tsai (2012) extended Boneh and Franklin's notions to define the security model of revocable ID-based encryption that includes the indistinguishability of encryption under adaptive-ID, chosen-plaintext attacks (IND-RID-CPA), as well as the indistinguishability of encryption under adaptive-ID, chosen-ciphertext attacks (IND-RID-CCA). Here, we first define a security game, and then present the definitions of both IND-RID-CPA and IND-RID-CCA attacks.

Security game. The semantic security under adaptive-ID attacks for revocable ID-based encryption is defined using the following game between a challenger and an adversary:

- *Phase* 1. The challenger $\mathcal{B}$ runs the *system setup algorithm* $\mathcal{G}$ of RIBE to generate a system secret key and produce the public parameters *Parms*. Then the challenger $\mathcal{B}$ gives the adversary $\mathcal{A}$ the *Parms* and keeps the system secret key to itself.
- *Phase* 2. The adversary $\mathcal{A}$ may issue a number of different queries to $\mathcal{B}$ as follows:
  - *Initial key extract query* (*id*). Upon receiving this query with identity-related information *id*, the challenger $\mathcal{B}$ runs the *initial key extract algorithm* $\mathcal{IKE}$ to return the user's initial secret key d_{id} to $\mathcal{A}$.
  - *Time key update query* (id, t). Upon receiving this query with (id, t), the challenger $\mathcal{B}$ runs the *time key update algorithm* $\mathcal{TKU}$ to return the user's time update key $d_{id,t}$ to $\mathcal{A}$.
  - *Decryption query* (id, t, C). Upon receiving the query, the challenger $\mathcal{B}$ accesses the entire decryption key $D_{id,t}$. The entire decryption key $D_{id,t}$ is implicitly obtained by issuing the *initial key extract query* (*id*) and the *time key update query* (id, t). The challenger $\mathcal{B}$ runs the *decryption algorithm D* to decrypt the ciphertext C. Then it returns $D(D_{id,t}, C)$ to $\mathcal{A}$.
- *Phase* 3. The adversary $\mathcal{A}$ gives a target identity *id**, a plaintext pair (M_0^*, M_1^*) and a time period t^* to B. $\mathcal{B}$ chooses a random $\gamma \in \{0, 1\}$ and computes C^* by running the *encryption algorithm E*(*Parms*, *id**, t^*, M_γ^*). Then B sends C^* to $\mathcal{A}$.
- *Phase* 4. The adversary $\mathcal{A}$ may issue more queries as in *Phase* 2. A restriction here is that either *id** or (*id**, t^*) is disallowed to be queried in the *initial key extract query* or the *time key update query*, respectively. The other restriction is that (*id*, $t, C) \neq (id^*, t^*, C^*)$.
- *Phase* 5. The adversary $\mathcal{A}$ outputs $\gamma' \in \{0, 1\}$ and wins this game if $\gamma' = \gamma$.
  We define the adversary $\mathcal{A}$'s advantage in attacking a RIBE scheme in the security game as

$$\mathrm{Adv}_{\mathcal{A}}(l) = \left|\Pr[\gamma = \gamma'] - 1/2\right|.$$

DEFINITION 3 (IND-RID-CCA). We say that a RIBE scheme is $(\tau, q_E, q_U, q_D, \varepsilon)$-IND-RID-CCA secure against adaptive-ID, chosen ciphertext attacks if no probabilistic polynomial-time adversary $\mathcal{A}$ that has a non-negligible ε against the RIBE scheme within a running time τ and making at most q_E initial key extract queries, q_U time key update queries, and q_D decryption queries.

For the security of adaptive-ID, chosen plaintext attacks (IND-RID-CPA), the adversary $\mathcal{A}$ cannot issue the *decryption queries* of Phases 2 and 4 in the security game above.

DEFINITION 4 (IND-RID-CPA). We say that a RIBE scheme is $(\tau, q_E, q_U, \varepsilon)$-IND-RID-CPA secure against adaptive-ID, chosen plaintext attacks if no probabilistic polynomial-time adversary $\mathcal{A}$ that has a non-negligible ε against the RIBE scheme within a running time τ and making at most q_E initial key extract queries and q_U time key update queries.

4. The Proposed RIBE Scheme

The RIBE scheme without random oracles consists of five algorithms: the *system setup*, the *initial key extract*, the *time key update*, the *encryption* and the *decryption* algorithms.

- *System setup*: As in Waters (2005), Paterson and Schuldt (2006), a trusted private key generation (PKG) takes a security parameter l and the total number z of all time periods as input. Two groups G_1, G_2 of prime order $p > 2^l$, an admissible bilinear map $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$ and a generator g of G_1 are generated by the PKG. The PKG sets two collision-resistant hash functions H_n: $\{0,1\}^* \rightarrow \{0,1\}^n$ and H_m: $\{0,1\}^* \rightarrow \{0,1\}^m$, where n and m are fixed lengths. Then the PKG randomly chooses two secret values $\alpha,\ \beta \in Z_p^*$ and computes $g_1 = g^{\alpha+\beta} \in G_1$. In addition, the PKG also chooses a random value $g_2 \in G_1$, two random values $u',\ t' \in G_1$, as well as two vectors $U = (u_i)$ of length n and $T = (t_j)$ of length m, where $u_i,\ t_j \in G_1$ for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, m$. Finally, the PKG returns the system secret key = $(g_2^{\alpha}, g_2^{\beta})$ and the public parameters *Parms* $= (G_1, G_2, \hat{e}, g, g_1, g_2, H_m, H_n, u', U, t', T)$.
- *Initial key extract*: Given a user's identity-related information *id*$\in \{0,1\}^*$, the PKG computes $v = H_n(id)$. Here, v is a bit string of length n representing an identity *id*, and v_i denotes the ith bit of v. Let U $\subset \{1, 2, \ldots, n\}$ be the set of index i such that $v_i = 1$, for $i = 1, 2, \ldots, n$. The PKG chooses a random $r_v \in Z_p^*$ and uses u_i to compute the initial key $d_{id} = (d_{id1}, d_{id2}) = (g_2^{\alpha}(u' \prod_{i \in U} u_i)^{r_v}, g^{r_v})$ or $(g_2^{\alpha}(u' \prod u_i^{v_i})^{r_v}, g^{r_v})$ for $i = 1, 2, \ldots, n$. Finally, the PKG transmits d_{id} to the user via a secure channel.
- *Time key update*: Let *vt* = $H_m(id, t)$ be a bit string of length m representing the identity-related information *id* and the time period t, and vt_j denotes the jth bit of *vt*. Let T $\subset \{1, 2, \ldots, m\}$ be the set of index j such that $vt_j = 1$, for $j = 1, 2, \ldots, m$. The PKG chooses a random $r_t \in Z_p^*$ and uses t_j to compute the time update key $d_{id,t} = (d_{id,t1}, d_{id,t2}) = (g_2^{\beta}(t' \prod_{j \in T} t_j)^{r_t}, g^{r_t})$ or

$(g_2^{\beta}(t' \prod t_j^{vt_j})^{r_t}, g^{r_t})$ for $j = 1, 2, \ldots, m$. The PKG sends $d_{id,t}$ to the user via a public channel. Thus, the non-revoked user can use d_{id} and $d_{id,t}$ to compute his/her entire decryption key for the time period t as

$$\begin{aligned} D_{id,t} &= (D_1, D_2, D_3) \\ &= (d_{id1} \cdot d_{id,t1}, d_{id2}, d_{id,t2}) \\ &= \left(g_2^{\alpha+\beta} \cdot \left(u' \prod_{i \in U} u_i \right)^{r_v} \cdot \left(t' \prod_{j \in T} t_j \right)^{r_t}, g^{r_v}, g^{r_t} \right). \end{aligned}$$

- *Encryption*: For a time period t, given a message M and a receiver *id*, a sender also computes two bit strings $v = H_n(id)$ and *vt* = $H_m(id, t)$ to obtain two sets U and T . Thus, the sender computes $u' \prod_{i \in U} u_i$and $t' \prod_{j \in T} t_j$. Then the sender chooses a random number $r \in Z_p^*$ and computes the ciphertext as

$$\begin{aligned} C &= (C_1, C_2, C_3, C_4) \\ &= \left(\hat{e}(g_1, g_2)^r \cdot M, g^r, \left(u' \prod_{i \in U} u_i \right)^r, \left(t' \prod_{j \in T} t_j \right)^r \right). \end{aligned}$$

- *Decryption*: Given a ciphertext $C = (C_1, C_2, C_3, C_4)$, the receiver can use his/her entire decryption key $D_{id,t} = (D_1, D_2, D_3)$ to decrypt C as follows:

$$\begin{aligned} & C_1 \cdot \frac{\hat{e}(D_2, C_3) \cdot \hat{e}(D_3, C_4)}{\hat{e}(D_1, C_2)} \\ &= \left(\hat{e}(g_1, g_2)^r \cdot M \right) \cdot \frac{\hat{e}(g^{r_v}, (u' \prod_{i \in U} u_i)^r) \cdot \hat{e}(g^{r_t}, (t' \prod_{j \in T} t_j)^r)}{\hat{e}(g_2^{\alpha+\beta} (u' \prod_{i \in U} u_i)^{r_v} \cdot (t' \prod_{j \in T} t_j)^{r_t}, g^r)} \\ &= \left(\hat{e}(g_1, g_2)^r \cdot M \right) \\ &\quad \times \frac{\hat{e}(g^r, (u' \prod_{i \in U} u_i)^{r_v} \cdot (t' \prod_{j \in T} t_j)^{r_t})}{\hat{e}(g_2^{\alpha+\beta}, g^r) \cdot \hat{e}((u' \prod_{i \in U} u_i)^{r_v} \cdot (t' \prod_{j \in T} t_j)^{r_t}, g^r)} \\ &= M. \end{aligned}$$

5. Security Analysis

In the proposed RIBE scheme, the entire decryption key is divided into two parts, the initial secret key and the time update key. As the mentioned IND-RID-CPA attack in Definition 4, the adversary is allowed to obtain either the initial secret key or the time update key in the security game. Hence, we consider two types of adversaries to simplify the security proof. One is the outside adversary and the other is the inside adversary (or a revoked user). The outside adversary is allowed to issue all queries in the security game except for the *initial key extract query* on *id**. The inside adversary is allowed to issue all queries in the security game except for the *time key update query* on (*id**, t^*). In the

following theorems, we use the similar technique in Waters (2005), Paterson and Schuldt (2006) to prove that the proposed RIBE scheme is semantically secure for the outside and the inside adversaries, respectively.

Theorem 1. *In the standard model, the proposed RIBE scheme is a semantically outsider-secure RIBE scheme (IND-O-RID-CPA) under the BDDH assumption. Concretely, assume that there is an outside adversary A that has an advantage ε against the proposed RIBE scheme within a running time τ and A can make at most $q_E > 0$ initial key extract queries and $q_U > 0$ time key update queries. Then the proposed RIBE scheme is $(\tau, q_E, q_U, \varepsilon)$-IND-O-RID-CPA secure assuming that the BDDH problem is (τ', ε')-intractable, where $\tau' = \tau + O((n \cdot q_E + m \cdot q_U) \cdot \tau_1 + (q_E + q_U) \cdot \tau_2)$ and $\varepsilon' = \frac{\varepsilon}{4q_E(n+1)}$, in which τ_1 and τ_2 denote the executing time of a multiplication in G_1 and an exponentiation in G_1, respectively.*

Proof. Assume that an adversary $\mathcal{A}$ can break the proposed RIBE scheme. Using the adversary A, we can construct a challenger $\mathcal{B}$ in the security game to solve the BDDH problem. We assume that the challenger $\mathcal{B}$ is given $\langle G_1, G_2, \hat{e}, g, g^a, g^b, g^c, K\rangle$ as an instance of the BDDH problem, where $a, b, c \in Z_p^*$ and $K \in G_2$. $\mathcal{B}$ would like to decide whether $K = \hat{e}(g, g)^{abc}$. $\mathcal{B}$ simulates the challenger in the security game for A as follows.

- *Phase* 1: The challenger $\mathcal{B}$ sets $l_v = 2q_E$, and randomly chooses an integer k_v with $0 \leqslant k_v \leqslant n$. We assume that $l_v(n+1) < p$ for the given values of q_E and n. The challenger $\mathcal{B}$ randomly chooses an integer $x' \in Z_{l_v}$ and a vector $X = (x_i)$ of length n, where $x_i \in Z_{l_v}$ for $i = 1, 2, \ldots, n$. The challenger $\mathcal{B}$ randomly chooses an integer $y' \in Z_p$ and a vector $Y = (y_i)$ of length n, where $y_i \in Z_p$ for $i = 1, 2, \ldots, n$. Finally, the challenger $\mathcal{B}$ randomly chooses an integer $z' \in Z_p$ and a vector $Z = (z_j)$ of length m, where $z_j \in Z_p$ for $j = 1, 2, \ldots, m$. We define three functions for $v = H_n(id)$ and *vt* = $H_m(id, t)$ as follows:

$$F(v) = x' + \sum_{i \in U} x_i - l_v k_v,$$
$$J(v) = y' + \sum_{i \in U} y_i,$$
$$L(vt) = z' + \sum_{j \in T} z_j.$$

  The challenger $\mathcal{B}$ chooses a value $\beta \in Z_p$ as the secret value of the time update key, then assigns $g_1 = g^a g^\beta$, $g_2 = g^b$, $u' = g_2^{-l_v k_v + x'} g^{y'}$, $u_i = g_2^{x_i} g^{y_i}$, $t' = g^{z'}$, and $t_j = g^{z_j}$, for $1 \leqslant i \leqslant n$ and $1 \leqslant j \leqslant m$.
- *Phase* 2: $\mathcal{B}$ respectively responds the *initial key extract query* with identity *id* and the *time key update query* with (*id*, t) as follows.
  - *Initial key extract query* (*id*): Upon receiving this query with identity *id*, the challenger $\mathcal{B}$ computes $v = H_n(id)$ and then computes $F(v)$ and $J(v)$. If

$F(v) = 0 \bmod p$, the challenger $\mathcal{B}$ reports failure and terminates. If $F(v) \neq 0 \bmod p$, the challenger $\mathcal{B}$ chooses a random $r_v \in Z_p$ and computes the initial secret key d_{id} as follows.

$$\begin{aligned} d_{id} &= (d_{id1}, d_{id2}) \\ &= \left(\left(\frac{g_1}{g^\beta} \right)^{-J(v)/F(v)} \cdot \left(u' \prod_{i \in U} u_i \right)^{r_v}, \left(\frac{g_1}{g^\beta} \right)^{-1/F(v)} g^{r_v} \right). \end{aligned}$$

Now, we show that $d_{id} = (d_{id1}, d_{id2})$ is a valid initial secret key as follows.

$$\begin{aligned} d_{id1} &= \left(\frac{g_1}{g^\beta} \right)^{-J(v)/F(v)} \cdot \left(u' \prod_{i \in U} u_i \right)^{r_v} \\ &= \left(\frac{g_1}{g^\beta} \right)^{-J(v/F(v)} \cdot \left(g_2^{-l_v k_v + x'} g^{y'} \cdot \prod_{i \in U} g_2^{x_i} g^{y_i} \right)^{r_v} \\ &= \left(\frac{g_1}{g^\beta} \right)^{-J(v)/F(v)} \cdot \left(g_2^{-l_v k_v + x'} g^{y'} \cdot g_2^{\sum_{i \in U} x_i} g^{\sum_{i \in U} y_i} \right)^{r_v} \\ &= \left(\frac{g_1}{g^\beta} \right)^{-J(v)/F(v)} \cdot \left(g_2^{F(v)} g^{J(v)} \right)^{r_v} \\ &= g_2^a \left(g_2^{F(v)} g^{J(v)} \right)^{-a/F(v)} \cdot \left(g_2^{F(v)} g^{J(v)} \right)^{r_v} \\ &= g_2^a \left(g_2^{F(v)} g^{J(v)} \right)^{r_v - a/F(v)} \\ &= g_2^a \left(u' \prod_{i \in U} u_i \right)^{r'_v} \end{aligned}$$

and

$$\begin{aligned} d_{id2} &= \left(\frac{g_1}{g^\beta} \right)^{-1/F(v)} g^{r_v} \\ &= g^{r_v - a/F(v)} \\ &= g^{r'_v}, \end{aligned}$$

where $r'_v = r_v - a/F(v)$.

– *Time key update query* (*id*, t): Upon receiving the time key update query with (*id*, t), the challenger $\mathcal{B}$ chooses a random $r_t \in Z_p$ and uses the secret value $\beta \in Z_p$ to compute the time update key as follows.

$$d_{id,t} = (d_{id,t1}, d_{id,t2}) = \left(g_2^\beta \cdot \left(t' \prod_{j \in T} t_j \right)^{r_t}, g^{r_t} \right).$$

- *Phase* 3: The adversary $\mathcal{A}$ gives a target identity *id**, a plaintext pair (M_0^*, M_1^*) and a time period t^* to B. The challenger $\mathcal{B}$ first chooses a random $\gamma \in \{0, 1\}$.

Then the challenger $\mathcal{B}$ computes $v^* = H_n(id^*)$ and $vt^* = H_m(id^*, t^*)$. The challenger $\mathcal{B}$ uses v^* and vt^* to compute $F(v^*), J(v^*)$ and $L(vt^*)$. If $F(v^*) \neq 0 \bmod p$, the challenger $\mathcal{B}$ reports failure and terminates. If $F(v^*) = 0 \bmod p$, the challenger $\mathcal{B}$ constructs a ciphertext C^* as follows.

$$C^* = \big(K \cdot \hat{e}\big(g^c, g^b\big)^{\beta} \cdot M_\gamma^*, g^c, g^{cJ(v^*)}, g^{cL(vt^*)}\big).$$

Now, we show that verify C^* is a valid ciphertext as follows.

$$\begin{aligned} C^* &= \big(K \cdot \hat{e}\big(g^c, g^b\big)^{\beta} \cdot M_\gamma^*, g^c, g^{cJ(v^*)}, g^{cL(vt^*)}\big) \\ &= \big(\hat{e}(g,g)^{abc} \cdot \hat{e}\big(g^\beta, g^b\big)^c \cdot M_\gamma^*, g^c, g^{cJ(v^*)}, g^{cL(vt^*)}\big) \\ &= \big(\hat{e}(g^a, g^b)^c \cdot \hat{e}\big(g^\beta, g^b\big)^c \cdot M_\gamma^*, g^c, g^{cJ(v^*)}, g^{cL(vt^*)}\big) \\ &= \left(\hat{e}(g_1, g_2)^c \cdot M_\gamma^*, g^c, \left(u' \prod_{i \in U} u_i\right)^c, \left(t' \prod_{j \in T} t_j\right)^c\right). \end{aligned}$$

- *Phase* 4: The challenger $\mathcal{B}$ responds to the *initial key extract query* or the *time key update query* as in *Phase* 2. A restriction here is that id^* is disallowed to be queried in the *initial key extract query*.
- *Phase* 5: The adversary $\mathcal{A}$ outputs its guess $\gamma' \in \{0, 1\}$, and wins this game if $\gamma' = \gamma$.

In *Phases* 2 and 3, it is obvious that the challenger $\mathcal{B}$ perfectly simulates the initial secret key extraction, the time key update queries and the ciphertext C^*. We analyze the probability of the challenger $\mathcal{B}$ not aborting. In *Phase* 2, if $F(v) = 0 \bmod p$, the challenger $\mathcal{B}$ reports failure and terminates. To make the analysis of the simulation easier, we force the challenger $\mathcal{B}$ to abort whenever $F(v) = 0 \bmod l_v$. By the mentioned assumption $l_v(n+1) < p$, we can imply $0 \leqslant l_v k_v \leqslant p$ and $0 \leqslant x' + \sum_{i \in U} x_i \leqslant p$. It is easy to see that $F(v) = 0 \bmod p$ implies $F(v) = 0 \bmod l_v$. On the other hand, in *Phase* 3, if $F(v^*) \neq 0 \bmod p$, the challenger $\mathcal{B}$ reports failure and terminates.

Let q_E and q_U be the total queries in the initial key extract query and the time key update query, respectively. To simplify the analysis, we define the events A_i: $F(v_i) \neq 0 \bmod l_v$ and A^*: $F(v^*) = 0 \bmod p$. From the above analysis, the probability of the challenger $\mathcal{B}$ not aborting is

$$\Pr[\neg\text{abort}] \geqslant \Pr\Big[\bigwedge_{i=1}^{q_E} A_i \wedge A^*\Big] = \Pr\big[A^*\big] \cdot \Pr[\Big[\bigwedge_{i=1}^{q_E} A_i | A^*\Big].$$

By the assumption $l_v(n+1) < p$, it leads to that $F(v) = 0 \bmod p$ implies $F(v) = 0 \bmod l_v$. Furthermore, this assumption gives that if $F(v) = 0 \bmod l_v$, there will be an unique choice of k_v with $0 \leqslant k_v \leqslant n$ such that $F(v) = 0 \bmod p$. Since k_v, x' and X are chosen randomly, we have the probability of the event A^* as follows.

$$\begin{aligned} &\Pr\big[A^*\big] = \Pr\big[F\big(v^*\big) = 0 \bmod p \wedge F\big(v^*\big) = 0 \bmod l_v\big], \\ &\Pr\big[A^*\big] = \Pr\big[F\big(v^*\big) = 0 \bmod l_v\big] \cdot \Pr\big[F\big(v^*\big) = 0 \bmod p \mid F\big(v^*\big) = 0 \bmod l_v\big], \end{aligned}$$

$$\Pr\left[A^*\right] = \frac{1}{l_v} \cdot \frac{1}{n+1}.$$

We also have that

$$\Pr\left[\bigwedge_{i=1}^{q_E} A_i \mid A^*\right] = 1 - \Pr\left[\bigvee_{i=1}^{q_E} \neg A_i \mid A^*\right] \geqslant 1 - \sum_{i=1}^{q_E} \Pr\left[\neg A_i | A^*\right] = 1 - \frac{q_E}{l_v}.$$

Hence, we can obtain that

$$\Pr\left[\bigwedge_{i=1}^{q_E} A_i \wedge A^*\right] = \Pr\left[A^*\right] \cdot \Pr\left[\bigwedge_{i=1}^{q_E} A_i \mid A^*\right] \geqslant \left(\frac{1}{l_v}\frac{1}{n+1}\right) \cdot \left(1 - \frac{q_E}{l_v}\right).$$

We set $l_v = 2q_E$, then get the resulting probability of the challenger $\mathcal{B}$ not aborting is

$$\Pr[\neg \text{abort}] \geqslant \Pr\left[\bigwedge_{i=1}^{q_E} A_i \wedge A^*\right] \geqslant \frac{1}{4q_E} \cdot \frac{1}{n+1}.$$

According to the above descriptions for the challenger $\mathcal{B}$, it is obvious that it requires $O(n)$ multiplications and $O(1)$ exponentiations in the *initial key extract query*. It is also obvious that it requires $O(m)$ multiplications and $O(1)$ exponentiations in the *time key update query*. So we have $\tau' = \tau + O(q_E \cdot n \cdot \tau_1 + q_U \cdot m \cdot \tau_1 + (q_E + q_U) \cdot \tau_2)$, where τ_1 and τ_2 denote the executing time of a multiplication in G_1 and an exponentiation in G_1, respectively. □

Theorem 2. *In the standard model, the proposed RIBE scheme is a semantically insider-secure RIBE scheme (IND-I-RID-CPA) under the BDDH assumption. Concretely, assume that there is an inside adversary A that has an advantage ε against the proposed RIBE scheme within a running time τ and A can make at most $q_E > 0$ initial key extract queries and $q_U > 0$ time key update queries. Then the proposed RIBE scheme is $(\tau, q_E, q_U, \varepsilon)$-IND-I-RID-CPA secure assuming that the BDDH problem is (τ', ε')-intractable, where $\tau' = \tau + O((n \cdot q_E + m \cdot q_U) \cdot \tau_1 + (q_E + q_U) \cdot \tau_2)$ and $\varepsilon' = \frac{\varepsilon}{4q_U(m+1)}$, in which τ_1 and τ_2 denote the executing time of a multiplication in G_1 and an exponentiation in G_1, respectively.*

Proof. Assume that an adversary $\mathcal{A}$ can break the proposed RIBE scheme. Using the adversary A, we can construct a challenger $\mathcal{B}$ to solve the BDDH problem. We assume that the challenger $\mathcal{B}$ is given $\langle G_1, G_2, \hat{e}, g, g^a, g^b, g^c, K\rangle$ as an instance of the BDDH problem, where $a, b, c \in Z_p^*$ and $K \in G_2$. $\mathcal{B}$ would like to decide whether $K = \hat{e}(g,g)^{abc}$. $\mathcal{B}$ simulates the challenger in the security game for $\mathcal{A}$ as follows.

- *Phase* 1: The challenger $\mathcal{B}$ sets $l_{vt} = 2q_U$, and randomly chooses an integer k_{vt} with $0 \leqslant k_{vt} \leqslant m$. We assume that $l_{vt}(m+1) < p$ for the given values of q_U and m. The challenger $\mathcal{B}$ randomly chooses an integer $x' \in Z_{l_{vt}}$ and a vector $X = (x_i)$ of length m, where $x_i \in Z_{l_{vt}}$for $i = 1, 2, \ldots, m$. The challenger $\mathcal{B}$ also chooses

an integer $y' \in Z_p$ randomly and a vector $Y = (y_i)$ of length m, where $y_i \in Z_p$ for $i = 1, 2, \ldots, m$. Finally, the challenger $\mathcal{B}$ randomly chooses an integer $z' \in Z_p$ and a vector $Z = (z_j)$ of length n, where $z_j \in Z_p$ for $j = 1, 2, \ldots, n$. We define three functions for $v = H_n(id)$ and $vt = H_m(id, t)$ as follows.

$$F(vt) = x' + \sum_{i \in U} x_i - l_{vt} k_{vt},$$
$$J(vt) = y' + \sum_{i \in U} y_i,$$
$$L(v) = z' + \sum_{j \in T} z_j.$$

The challenger $\mathcal{B}$ chooses a value $\alpha \in Z_p$ as the secret value of the initial secret key, then assigns $g_1 = g^{\alpha} g^{a}$, $g_2 = g^{b}$, $u' = g_2^{-l_{vt} k_{vt} + x'} g^{y'}$, $u_i = g_2^{x_i} g^{y_i}$, $t' = g^{z'}$, and $t_j = g^{z_j}$ for $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$.

- *Phase* 2: Upon receiving the *initial key extract query* with identity *id* and the *time key update query* with (*id*, t), $\mathcal{B}$ respectively responds to the following queries.
  - *Initial key extract query* (*id*): Upon receiving the initial key extract query with identity *id*, the challenger $\mathcal{B}$ chooses random $r_v \in Z_p$ and uses the secret value α to compute the initial secret key as follows.

$$d_{id} = (d_{id1}, d_{id2}) = \left(g_2^{\alpha} \cdot \left(t' \prod_{j \in T} t_j \right)^{r_v}, g^{r_v} \right).$$

  - *Time key update query* (*id*, t): Upon receiving the time key update query with (*id*, t), the challenger $\mathcal{B}$ computes $vt = H_m(id, t)$ and then computes $F(vt)$ and $J(vt)$. If $F(vt) = 0 \bmod p$, the challenger $\mathcal{B}$ reports failure and terminates. If $F(vt) \neq 0 \bmod p$, the challenger $\mathcal{B}$ constructs a time update key $d_{id,t}$. It chooses a random $r_t \in Z_p$ and computes the initial secret key as follows.

$$\begin{aligned} d_{id,t} &= (d_{id,t1}, d_{id,t2}) \\ &= \left(\left(\frac{g_1}{g^{\alpha}} \right)^{-J(vt)/F(vt)} \cdot \left(u' \prod_{i \in U} u_i \right)^{r_t}, \left(\frac{g_1}{g^{\alpha}} \right)^{-1/F(vt)} g^{r_t} \right). \end{aligned}$$

    Now, we show that $d_{id,t} = (d_{id,t1}, d_{id,t2})$ is a valid initial secret key as follows.

$$\begin{aligned} d_{id,t1} &= \left(\frac{g_1}{g^{\alpha}} \right)^{-J(vt)/F(vt)} \cdot \left(u' \prod_{i \in U} u_i \right)^{r_t} \\ &= \left(\frac{g_1}{g^{\alpha}} \right)^{-J(vt)/F(vt)} \cdot \left(g_2^{-l_{vt} k_{vt} + x'} g^{y'} \cdot \prod_{i \in U} g_2^{x_i} g^{y_i} \right)^{r_t} \end{aligned}$$

$$
\begin{aligned}
&= \left(\frac{g_1}{g^\alpha}\right)^{-J(vt)/F(vt)} \cdot \left(g_2^{-l_{vt}k_{vt}+x'} g^{y'} \cdot g_2^{\sum_{i\in U} x_i} g^{\sum_{i\in U} y_i}\right)^{r_t} \\
&= \left(\frac{g_1}{g^\alpha}\right)^{-J(vt)/F(vt)} \cdot \left(g_2^{F(vt)} g^{J(vt)}\right)^{r_t} \\
&= g_2^a \left(g_2^{F(vt)} g^{J(vt)}\right)^{-a/F(vt)} \cdot \left(g_2^{F(vt)} g^{J(vt)}\right)^{r_t} \\
&= g_2^a \left(g_2^{F(vt)} g^{J(vt)}\right)^{r_t - a/F(vt)} \\
&= g_2^a \left(u' \prod_{i\in U} u_i\right)^{r'_t}
\end{aligned}
$$

and

$$
\begin{aligned}
d_{id,t2} &= \left(\frac{g_1}{g^\alpha}\right)^{-1/F(vt)} g^{r_t} \\
&= g^{r_t - a/F(vt)} \\
&= g^{r'_t},
\end{aligned}
$$

where $r'_t = r_t - a/F(vt)$.

- *Phase* 3: The adversary $\mathcal{A}$ gives a target identity *id**, a plaintext pair (M_0^*, M_1^*) and a time period t^* to $\mathcal{B}$. The challenger $\mathcal{B}$ first chooses a random $\gamma \in \{0,1\}$. Then the challenger $\mathcal{B}$ computes $v^* = H_n(id^*)$ and *vt*$^* = H_m(id^*,\ t^*)$. The challenger uses v^* and *vt** to compute $F(vt^*), J(vt^*)$ and $L(v^*)$. If $F(vt^*) \neq 0 \bmod p$, the challenger B reports failure and terminates. If $F(vt^*) = 0 \bmod p$, the challenger $\mathcal{B}$ constructs a ciphertext C^* as follows.

$$
C^* = \left(K \cdot \hat{e}\left(g^c, g^b\right)^\alpha \cdot M_\gamma^*, g^c, g^{cJ(vt^*)}, g^{cL(v^*)}\right).
$$

Now, we show that C^* is a valid ciphertext as follows.

$$
\begin{aligned}
C^* &= \left(K \cdot \hat{e}\left(g^c, g^b\right)^\alpha \cdot M_\gamma^*, g^c, g^{cJ(vt^*)}, g^{cL(v^*)}\right) \\
&= \left(\hat{e}(g,g)^{abc} \cdot \hat{e}\left(g^\alpha, g^b\right)^c \cdot M_\gamma^*, g^c, g^{cJ(vt^*)}, g^{cL(v^*)}\right) \\
&= \left(\hat{e}\left(g^a, g^b\right)^c \cdot \hat{e}\left(g^\alpha, g^b\right)^c \cdot M_\gamma^*, g^c, g^{cJ(vt^*)}, g^{cL(v^*)}\right) \\
&= \left(\hat{e}(g_1, g_2)^c \cdot M_\gamma^*, g^c, \left(u' \prod_{i\in U} u_i\right)^c, \left(t' \prod_{j\in T} t_j\right)^c\right).
\end{aligned}
$$

- *Phase* 4: The challenger $\mathcal{B}$ responds to the *initial key extract query* or the *time key update query* as in *Phase* 2. A restriction here is that (*id**, t^*) is disallowed to be queried in the *time key update query*.
- *Phase* 5: The adversary $\mathcal{A}$ outputs its guess $\gamma' \in \{0,1\}$, and wins this game if $\gamma' = \gamma$.

The analysis is similar to Theorem 1. The probability of the challenger $\mathcal{B}$ not aborting is $\Pr[\neg \text{abort}] \geqslant \frac{1}{4q_U} \cdot \frac{1}{m+1}$. Then the successful probability (advantage) of the challenger $\mathcal{B}$ who can solve the BDDH problem is at least $\frac{\varepsilon}{4q_U(m+1)}$. The executing time is $\tau + O(q_E \cdot n \cdot \tau_1 + q_U \cdot m \cdot \tau_1 + (q_E + q_U) \cdot \tau_2)$, where τ_1 and τ_2 denote the executing time of a multiplication in G_1 and an exponentiation in G_1, respectively. □

6. CCA Transformation and Comparisons

Here, we discuss the transformation technique from the proposed CPA-secure RIBE scheme to a CCA-secure RIBE scheme. We also make the comparisons between our proposed RIBE scheme and several IBE or RIBE schemes (Waters, 2005; Gentry, 2006; Tseng and Tsai, 2012).

Canetti *et al*. (2004) showed a generic conversion from a 2-level CPA-secure hierarchical ID-based encryption (HIBE) (Horwitz and Lynn, 2002; Gentry and Silverberg, 2002) to a CCA-secure IBE scheme by appending a one-time signature to the ciphertext, which is encrypted to an identity equal to the verification key. Boneh and Katz (2005) also improved the efficiency of Canetti *et al*.'s construction by using the MAC code instead of the one-time signature. Afterwards, Boyen *et al*.'s (2005) proposed a direct conversion approach avoiding the MAC codes and one-time signatures. In 2005, Waters adopted Canetti *et al*.'s generic conversion to obtain to a CCA-secure IBE scheme from a 2-level CPA-secure hierarchical ID-based encryption (HIBE). Following the idea in Waters (2005), we use our proposed scheme at the first level and employ the Boneh and Boyen's (2004a) CPA-secure IBE scheme at the second level to build a hybrid 2-level hierarchical revocable ID-based encryption (HRIBE) scheme. By the conversion techniques in (Canetti *et al*., 2004; Boneh and Katz, 2005), we can obtain an adaptive-ID, CCA-secure RIBE without random oracles. For the conversion approach in the random oracle model, Fujisaki and Okamoto (1999) presented a simple conversion from a weak public-key encryption scheme (IND-CPA) to a strong public-key encryption scheme (IND-CCA) in the random oracle model. Kitagawa *et al.* (2006) proposed an improvement on Fujisaki and Okamoto's (1999) conversion for ID-based encryption schemes. They can transform a weak ID-based encryption scheme (IND-ID-CPA) to a strong ID-based encryption scheme (IND-ID-CCA). Tseng and Tsai (2012) employed Kitagawa *et al*.'s conversion technique (2006) to obtain a CCA-secure RIBE scheme from their CPA-secure RIBE scheme in the random oracle model.

Table 1 lists the comparisons between our proposed RIBE scheme and some famous IBE or RIBE schemes (Waters, 2005; Gentry, 2006; Tseng and Tsai, 2012) in terms of underlying security assumption, security model, revocable functionality and computational cost. Note that we only compare the CPA-secure IBE or CPA-secure RIBE schemes in Table 1. Gentry's IBE scheme used a stronger security assumption called the augmented bilinear Diffie–Hellman exponent (ABDHE) assumption than the BDDH or BDH security assumptions which are used by the other three proposed schemes. Although Tseng and Tsai's RIBE scheme has the best performance, it could be insecure when random

Table 1
Comparisons between our proposed RIBE scheme and the previously proposed schemes

	Waters's IBE (2005)	Gentry's IBE (2006)	Tseng and Tsai's RIBE (2012)	Our proposed RIBE
Security assumption	BDDH	ABDHE	BDH	BDDH
Security model	Standard model	Standard model	Random oracle model	Standard model
Revocable property	No	No	Yes	Yes
Pairing operation for encryption	1	2	1	1
Pairing operation for decryption	2	1	1	3

oracles are instantiated with concrete hash functions (Canetti *et al*., 1998; Bellare *et al*., 2004a; Boneh and Boyen, 2004a). Our proposed RIBE scheme increase pairing operations as compared to Waters's and Gentry's IBE schemes for decryption, but the point is that our proposed RIBE scheme provides a flexible revocation mechanism with a public channel.

7. Conclusions

In this paper, we have proposed a fully secure RIBE scheme in the standard model (without random oracles) to provide robust security. We employed the revocable concept presented by Tseng and Tsai to provide an efficient and flexible revocation mechanism. For security analysis, we have demonstrated that the proposed RIBE scheme is semantically secure against adaptive-ID attacks in the standard model under the bilinear decision Diffie–Hellman assumption. For enhancing the practicality of ID-based public key systems, an efficient revocation mechanism must be involved in the design of various ID-based cryptographic schemes and protocols in the future.

Acknowledgements. The authors would like to thank the anonymous referees for their valuable comments and constructive suggestions. This research was partially supported by National Science Council, Taiwan, R.O.C., under contract No. NSC100-2221-E-018-027.

References

Aiello, W., Lodha, S., Ostrovsky, R. (1998). Fast digital identity revocation. In: *Proceedings of Crypto'98*, LNCS, Vol. 1462, pp. 137–152.

Baek, J., Zheng, Y. (2004). Identity-based threshold decryption. In: *Proceedings of PKC'04*, LNCS, Vol. 2947, pp. 262–276.

Bellare, M., Boldyreva, A., Palacio, A. (2004a). An uninstantiable random oracle model scheme for a hybrid encryption problem. In: *Proceedings of Cachin and Camenisch'04*, p.p. 171–188.

Bellare, M., Namprempre, C., Neven, G. (2004b). Security proofs for identity-based identification and signature schemes. *Journal of Cryptology*, 22(1), 1–61.

Bellare, M., Rogaway, P. (1993). Random oracles are practical: a paradigm for designing efficient protocols. In: *Proceedings of ACM CCS'93*, pp.62–73.

Boldyreva, A., Goyal, V., Kumar, V. (2008). Identity-based encryption with efficient revocation. In: *Proceedings of ACM CCS'08*, pp. 417–426.

Boneh, D., Boyen, X. (2004a). Efficient selective-ID identity based encryption without random oracles. In: *Proceedings of Eucrypt'04*, LNCS, Vol. 3027, pp. 223–238.

Boneh, D., Boyen, X. (2004b). Secure identity based encryption without random oracles. In: *Proceedings of Crypto'04*, LNCS, Vol. 3152, pp. 443–459.

Boneh, D., Franklin, M. (2001). Identity-based encryption from the Weil pairing. In: *Proceedings of Crypto'01*, LNCS, Vol. 2139, pp. 213–229.

Boneh, D., Hamburg, M. (2008). Generalized identity based and broadcast encryption schemes. In: *Proceedings of Asiacrypt'08*, LNCS, Vol. 5350, pp. 455–470.

Boneh, D., Katz, J. (2005). Improved efficiency for CCA-secure cryptosystems built using identity-based encryption. In: *Proceedings of CT-RSA'05*, LNCS, Vol. 3376, pp. 87–103.

Boyen, X., Mei, Q., Waters, B. (2005). Direct chosen ciphertext security from identity based techniques. In: *Proceedings of ACM CCS'05*, pp. 320–329.

Canetti, R., Goldreich, O., Halevi, S. (1998). The random oracle methodology, revisited (preliminary version). In: *Proceedings of STOC'98*, pp. 209–218.

Canetti, R., Halevi, S., Katz, J. (2003). A forward-secure public-key encryption scheme. In: *Proceedings of Eurocrypt'03*, LNCS, Vol. 2656, pp. 255–271.

Canetti, R., Halevi, S., Katz, J. (2004). Chosen-ciphertext security from identity based encryption. In: *Proceedings of Eurocrypt'04*, LNCS, Vol. 3027, pp. 207–222.

Cha, J.C., Cheon, J.H. (2003). An identity-based signature from gap Diffie–Hellman groups. In: *Proceedings of PKC'03*, LNCS, Vol. 2567, pp. 18–30.

Chen, L., Cheng, Z., Smart, N.P. (2007). Identity-based key agreement protocols from pairings. *International Journal of Information Security*, 6(4), 213–241.

Chen, J., Chen, K., Wang, Y., Li, X., Long, Y., Wan, Z. (2012). Identity-based key-insulated signcryption. *Informatica*, 23(1), 27–45.

Choi, K.Y., Hwang, J.Y., Lee, D.H. (2004). Efficient ID-based group key agreement with bilinear maps. In: *Proceedings of PKC'04*, LNCS, Vol. 2947, pp. 130–144.

Choi, K.Y., Hwang, J.Y., Lee, D.H. (2008). ID-based authenticated group key agreement secure against insider attacks. *IEICE Transactions on Fundamentals*, E91-A(7), 1828–1830.

Elwailly, F.F., Gentry, C., Ramzan, Z. (2004). QuasiModo: Efficient certificate validation and revocation. In: *Proceedings of PKC'04*, LNCS, Vol. 2947, pp. 375–388.

Fujisaki, E., Okamoto, T. (1999). How to enhance the security of public-key encryption at minimum cost. In: *Proceedings of PKC'99*, LNCS, Vol. 1560, pp. 53–68.

Galbraith, S., Paterson, K., Smart, N.P. (2008). Pairings for cryptographers. *Discrete Applied Mathematics*, 156(16), 3113–3121.

Gentry, C. (2003). Certificate-based encryption and the certificate revocation problem. In: *Proceedings of Eurocrypt'03*, LNCS, Vol. 2656, pp. 272–293.

Gentry, C. (2006). Practical identity-based encryption without random oracles. In: *Proceedings of Eurocrypt'06*, LNCS, Vol. 4004, pp. 445–464.

Gentry, C., Silverberg, A. (2002). Hierarchical id-based cryptography. In: *Proceedings of Asiacrypt' 02*, LNCS, Vol. 2501, pp. 548–566.

Goyal, V. (2007). Certificate revocation using fine grained certificate space partitioning. In: *Proceedings of FC'07*, LNCS, Vol. 4886, pp. 247–259.

Horwitz, J., Lynn, B. (2002). Towards hierarchical identity-based encryption. In: *Proceedings of Eurocrypt'02*, LNCS, Vol. 2332, pp. 466–481.

Housley, R., Polk, W., Ford, W., Solo, D. (2002). Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile. RFC 3280, IETF.

Kitagawa, T., Yang, P., Hanaoka, G., Zhang, R., Matsuura, K., Imai, H. (2006). Generic transforms to acquire CCA-security for identity based encryption: the cases of FOPKC and REACT. In: *Proceedings of ACISP 2006*, LNCS, Vol. 4058, pp. 348–359.

Libert, B., Vergnaud, D. (2009). Adaptive-ID secure revocable identity-based encryption. In: *Proceedings of CT-RSA'09*, LNCS, Vol. 5473, pp. 1–15.

Liu, J., Huang, S. (2010). Identity-based threshold proxy signature from bilinear pairings. *Informatica*, 21(1), 41–56.

Micali, S. (2002). Novomodo: Scalable certificate validation and simplified PKI management. In: *Proceedings of 1st Annual PKI Research Workshop*, pp. 15–25.

Paterson, K.G., Schuldt, J.C.N. (2006). Efficient identity-based signatures secure in the standard model. In: *Proceedings of ACISP'06*, LNCS, Vol. 4058, pp. 207–222.

Ren, Y., Gu, D., Wang, S., Zhang, X. (2010). New fuzzy identity-based encryption in the standard model. *Informatica*, 21(3), 393–408.

Sakai, R., Kasahara, M. (2003). ID-based cryptosystems with pairing on elliptic curve. *Cryptology ePrint Archive*, Report 2003/054.

Shamir, A. (1984). Identity-based cryptosystems and signature schemes. In: *Proceedings of Crypto'84*, LNCS, Vol. 196, pp. 47–53.

Tseng, Y.M., Tsai, T.T. (2012). Efficient revocable ID-based encryption with a public channel. *The Computer Journal*, 55(4), 475–486.

Tseng, Y.M., Wu, T.Y., Wu, J.D. (2008). A pairing-based user authentication scheme for wireless clients with smart cards. *Informatica*, 19(2), 285–302.

Tseng, Y.M., Wu, T.Y., Wu, J.D. (2009). An efficient and provably secure ID-based signature scheme with batch verifications. *International Journal of Innovative Computing*, *Information and Control*, 5(11), 3911–3922.

Waters, B. (2005). Efficient identity-based encryption without random oracles. In: *Proceedings of Eurocrypt'05*, Vol. 3494, pp. 1–33.

Wu, T.Y., Tseng, Y.M. (2010). An ID-based mutual authentication and key exchange protocol for low-power mobile devices. *The Computer Journal*, 53(7), 1062–1070.

Wu, T.Y., Tseng, Y.M., Yu, C.W. (2011). A secure ID-based authenticated group key exchange protocol resistant to insider attacks. *Journal of Information Science and Engineering*, 27(3), 915–932.

T.-T. Tsai received the BS degree in Department of Applied Mathematics, Chinese Culture University, Taiwan, in 2006. He received the MS degree at Department of Applied Mathematics, National Hsinchu University of Education, Taiwan, in 2009. He is currently a PhD candidate in Department of Mathematics, National Changhua University of Education, Taiwan. His research interests include applied cryptography, pairing-based cryptography and network security.

Y.-M. Tseng is currently a professor in Department of Mathematics, National Changhua University of Education, Taiwan. He also serves as an editor of several international journals including *Computer Standards & Interfaces*, *International Journal of Advancements in Computing Technology*, *International Journal of Security and Its Applications, Wireless Engineering and Technology*, as well as *ISRN Communications and Networking*. He has published over a hundred scientific journal and conference papers on cryptography and information security topics. In 2006, his paper obtained the *Wilkes Award* from *The British Computer Society*. His research interests include cryptography, information security, network security, computer network and mobile communications.

T.-Y. Wu received the BS and the MS degrees in Department of Applied Mathematics, Tatung University, Taiwan, in 2003 and 2005, respectively. He received the PhD degree in Department of Mathematics, National Changhua University of Education, Taiwan, in 2010. He is currently an assistant professor in School of Computer Science and Technology, Harbin Institute of Technology Shenzhen Graduate School, China. His research interests include applied cryptography, pairing-based cryptography and information security.

Visiškai saugus susikompromitavusio vartotojo pašalinimas identifikatoriais grįstame standartiniame šifravimo modelyje

Bet kuri sertifikatais arba identifikatoriais grįsta viešojo rakto šifravimo sistema privalo turėti galimybę pašalinti susikompromitavusius viešojo rato sistemos vartotojus. Neseniai Tseng ir Tsai pasiūlė naują identifikatoriais grįstą viešojo rakto sistemą (RIBE), kuri, naudodama neapsaugotą ryšio kanalą, efektyviai pašalina susikompromitavusius vartotojus. Straipsnyje pasiūlytas modifikuotas Tseng ir Tsai metodas, kuris užtikrina visišką sistemos saugumą ir nenaudoja atsitiktinio juodosios dėžės modelio.