Revocable Identity-Based Encryption Revisited: Security Model and Construction

Jae Hong Seo and Keita Emura

National Institute of Information and Communications Technology (NICT), 4-2-1, Nukui-kitamachi, Koganei, Tokyo, 184-8795, Japan
{jaehong,k-emura}@nict.go.jp

Abstract. In ACM CCS 2008, Boldyreva et al. proposed an elegant way of achieving an Identity-based Encryption (IBE) with *efficient* revocation, which we call revocable IBE (RIBE). One of the significant benefit of their construction is scalability, where the overhead of the trusted authority is logarithmically increased in the number of users, whereas that in the Boneh-Franklin naive revocation way is linearly increased. All subsequent RIBE schemes follow the Boldyreva et al. security model and syntax. In this paper, we first revisit the Boldyreva et al. security model, and aim at capturing the exact notion for the security of the naive but non-scalable Boneh-Franklin RIBE scheme. To this end, we consider a realistic threat, which we call *decryption key exposure*. We also show that all prior RIBE constructions except for the Boneh-Franklin one are vulnerable to decryption key exposure. As the second contribution, we revisit approaches to achieve (efficient and adaptively secure) scalable RIBE schemes, and propose a simple RIBE scheme, which is the first scalable RIBE scheme with decryption key exposure resistance, and is more efficient than previous (adaptively secure) scalable RIBE schemes. In particular, our construction has the shortest ciphertext size and the fastest decryption algorithm even compared with all scalable RIBE schemes without decryption key exposure resistance.

Keywords: Identity-based encryption with revocation, decryption key exposure.

1 Introduction

Identity-based Encryption (IBE) provides an important alternative way to avoid the need for a public key infrastructure (PKI). Revocation capability is very important for IBE setting as well as PKI setting. An efficient way to revoke users in the traditional PKI setting has been studied in numerous studies [2, 17, 18, 20, 30–33]. In contrast to PKI setting, there are only a few studies on IBE setting. First, Boneh and Franklin [11] consider one naive revocation way as follows. Let ID be a receiver's identity and T be a time to be decrypted. An encryptor uses (ID, T) as the public key, and a trusted authority, called key generation center (KGC), issues private keys $\mathsf{pvk}_{(ID,T)}$ for all non-revoked user

K. Kurosawa and G. Hanaoka (Eds.): PKC 2013, LNCS 7778, pp. 216–234, 2013.

IDs on each time period T via secure channels.[1] We call the Boneh-Franklin revocable IBE (RIBE) scheme BF-RIBE. However, the BF-RIBE does not scale well; that is, the overhead on KGC is linearly increased in the number of users. Recently, some studies [7, 13, 28] have aimed at offering scalability in the RIBE scheme while preserving the same security level as the BF-RIBE.

For the first time, Boldyreva et al. [7] formalized the security model of RIBE by capturing possible threats, and proposed the first *scalable* RIBE (BGK-RIBE) scheme by combining Fuzzy IBE [36] with a binary tree data structure, which was previously used in a revocation scheme [32]; Each user is given a long-term secret key sk_{ID} from KGC (via a secure channel as in IBE), and KGC broadcasts key update ku_T in each time period T (i.e., no secure channel is required in this phase). Only a non-revoked user can generate a short-term decryption key $\mathsf{dk}_{ID,T}$ from sk_{ID} and ku_T, which can be used to decrypt ciphertexts in time T. By using a binary tree data structure, the size of ku_T can be much smaller than the overhead of KGC in the BF-RIBE scheme.[2] Several scalable RIBE schemes have been proposed and those are provably secure in the Boldyreva et al. security model.

Our Contribution. Our contribution consists of two parts. First, we separate the Boldyreva et al. security model and the security level of the BF-RIBE by introducing a new realistic threat, which we call *decryption key exposure*, and also show that all previous RIBE schemes, except the BF-RIBE, are vulnerable to decryption key exposure.[3] That is, we show that the Boldyreva et al. security model does not fully capture the exact notion for security of the BF-RIBE scheme. Roughly speaking, the Boldyreva et al. security model allows an adversary to obtain any secret keys of a chosen identity. The only one restriction is that if the adversary obtains sk_{ID^*} of the challenge identity ID^*, then ID^* should be revoked before the challenge time T^*. This model is a natural extension of the security of the ordinary IBE scheme. However, *does this security model formalize all realistic threats?* For example, if the short-term decryption key $\mathsf{dk}_{ID,T}$ ($T \neq T^*$) is leaked, is the RIBE scheme still secure? The answer to this question may naturally appear to be 'yes' since the adversary can obtain secret keys of any chosen identity, and the decryption key can be generated from a secret key and (public) key update. But to show this thinking is wrong, we give an exceptional attack (decryption key exposure), wherein an adversary is allowed to obtain a decryption key $\mathsf{dk}_{ID^*,T}$ with the condition $T \neq T^*$. This setting is based on the similar attitude of key-insulated PKE [16], where it is desired that no information of the plaintext is revealed from a ciphertext even if

[1] Boldyreva et al. [7] provided an alternative way for this naive solution to avoid a secure channel, wherein the previous-time key is used to establish a public channel. However, this does not match the framework of RIBE, and thus we do not discuss it in this paper.

[2] In fact, the size of ku_T is $O(R\log(N/R))$ if $R \leq N/2$, and $O(N-R)$, otherwise, where N is the number of users and R is the number of revoked users.

[3] We do not contradict the security proofs given in previous schemes. Our attack is positioned in outside of their security models.

Table 1. (Pairing-based) Revocable IBE schemes

	CT size	Dec. cost	Mpk size	Model	Scalability	DKE resistance	Assumption
BF [11]	$1\tau_{\mathbb{G}} + 1\tau_H$	1p	$3\tau_{\mathbb{G}}$ +2hash ft.	RO, Adaptive		$\surd$	BDH
BGK [7]	$3\tau_{\mathbb{G}} + 1\tau_{\mathbb{G}_t}$	4p	$6\tau_{\mathbb{G}}$	Standard, Selective	$\surd$		DBDH
LV [28]	$3\tau_{\mathbb{G}} + 2\tau_{\mathbb{G}_t}$	3p	$(n+6)\tau_{\mathbb{G}}$	Standard, Adaptive	$\surd$		DBDH
Ours	$3\tau_{\mathbb{G}} + 1\tau_{\mathbb{G}_t}$	3p	$(n+6)\tau_{\mathbb{G}}$	Standard, Adaptive	$\surd$	$\surd$	DBDH

$\tau_{\mathbb{G}}$ and $\tau_{\mathbb{G}_t}$ are the sizes of groups $\mathbb{G}$ and $\mathbb{G}_t$, respectively, over which a bilinear pairing $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_t$ is defined. τ_H is the range-size of a hash function. p is the cost for performing a bilinear pairing e. n is the size of the identity space. RO (Standard, respectively) is a random oracle model (standard model, respectively). Selective (Adaptive, respectively) means a selective-security model (adaptive-security model, respectively). 'DKE' means decryption key exposure. (D)BDH is (Decisional) Bilinear Diffie-Hellman assumption.

all (short-term) decryption keys of a "different time period" are exposed. This kind of attack is not covered by the Boldyreva et al. security model; that is, the adversary may obtain not a secret key sk_{ID^*} but a decryption key $\mathsf{dk}_{ID^*,T}$, and ID^* can still be alive in the system in the challenge time period $T^* \neq T$. However, we can easily show that the BF-RIBE is still secure against decryption key exposure since every decryption key in the BF-RIBE is a private key with a distinct identity (ID, T) in the Boneh-Franklin IBE scheme.

Next, we revisit approaches to achieve (adaptively secure) scalable RIBE schemes, and propose a simple RIBE scheme by combining the (adaptively secure) Waters IBE scheme [38] and the (selectively secure) Boneh-Boyen IBE scheme [8]. This is the first scalable RIBE scheme with decryption key exposure resistance, and is more efficient than previous (adaptively secure) scalable RIBE schemes. Surprisingly, our construction does not require any additional efficiency cost for achieving decryption key exposure resistance. In particular, our construction has the shortest ciphertext size and a fastest decryption algorithm even compared with all scalable RIBE schemes without decryption key exposure resistance. Table 1 gives a detailed comparison with previous (efficient pairing-based) schemes. From our standard model RIBE construction, we can easily obtain more efficient RIBE construction in the random oracle model, by replacing both the Waters hash and the Boneh-Boyen hash into cryptographic hash functions that are modeled as random oracles.

Our construction is natural in the sense that its security can be reduced to the original (non-revocable) Waters IBE scheme. However, in [28], Libert and Vergnaud mentioned that this kind of simple construction using the original Waters IBE scheme will face with the difficulty in the security proof, and they

circumvented this by using a variant of the Waters IBE scheme [29] instead of the original.[4] We resolve this difficulty by carefully dealing with the means of assigning nodes of a binary tree to each user, which we call *random node assignment* technique. This allows us to circumvent the difficulty, and is explained in section 4. Surprisingly, such a simple construction is secure against decryption key exposure. The main difference between ours and previous constructions is the *re-randomizable* property of the decryption key, whereas decryption keys use the same randomness used in the secret key in all previous constructions.

Related Work. After the Boneh-Franklin RIBE scheme [11] and the Boldyreva et al. *scalable* (but *selectively secure*) RIBE scheme [7], there were some results. Libert and Vergnaud [28] proposed the first *adaptively secure* RIBE scheme (LV-RIBE) without assuming any stronger assumption compared with that of the Boldyreva et al.[5] Later an RIBE scheme from lattices [13] also have proposed. All these RIBE schemes are proven secure in the security model proposed by Boldyreva et al. [7].

Revocable IBE with mediators [5, 10, 14, 26] has been considered, where a special semi-trusted authority called a mediator who helps users to decrypt each ciphertext. However, this essentially requires communication between users and the mediator at each decryption and so is not totally satisfactory in some practical circumstances.

Recently, several functional encryption (FE) schemes, which are generalizations of the IBE scheme, have been proposed [23, 36], and the revocation capability in FE has also been studied [3, 4, 34]. The revocation method used in [4, 34] differs from RIBE contexts; the senders carry out the revocation, so it does not require any private key update procedures on the recipient's side. In [3] Attrapadung and Imai considered two different ways for revocation method; one is similar to that in [4, 34], and the other is similar to that in RIBE schemes. However, decryption key exposure is not considered in [3], so achieving revocation capabilities in FE with decryption key exposure resistance would be an interesting future area of study.

All revocable IBE schemes use a strategy in which only decryption keys of users who are not revoked in a time period T can be updated in time period T. This strategy is similar to those for cryptosystems against key exposure such as key-insulated PKE [6, 16, 27] and IBE [21, 22, 39, 40], forward secure encryption [12], and intrusion-resilient PKE [15]. However, these systems require a secure channel between a user and a key issuer or do not support scalability.

Outline. The next section gives preliminaries. In Section 3, we provide definitions for the RIBE scheme and explain the vulnerability of previous RIBE schemes against decryption key exposure. Section 4 gives our construction for a

[4] In a footnote of [28], there is a remark that a two-level hierarchical version of the Waters original IBE seems to work, however the details are not provided.

[5] Both schemes are secure under the Decisional Bilinear Diffie-Hellman (DBDH) assumption.

scalable RIBE scheme (with decryption key exposure resistance) and a high-level description of its security proof. We discuss about a room for extention of our RIBE scheme in Section 5. Finally, we summarize our result and leave several interesting open problems in Section 6.

2 Bilinear Groups and Waters IBE Scheme

Definition 1 (Bilinear Groups). *A bilinear group generator $\mathcal{G}(\cdot)$ is an algorithm that takes as input a security parameter λ and outputs a bilinear group $(p, \mathbb{G}, \mathbb{G}_t, e)$, where p is a prime of size 2λ, $\mathbb{G}$ and $\mathbb{G}_t$ are cyclic groups of order p, and e is an efficiently computable bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ with*

- *Bilinearity : for all $u, u', v, v' \in \mathbb{G}$, $e(uu', v) = e(u, v)e(u', v)$ and $e(u, vv') = e(u, v)e(u, v')$,*
- *Non-degeneracy : for a generator g of $\mathbb{G}$, $e(g, g) \neq 1_{\mathbb{G}_t}$, where $1_{\mathbb{G}_t}$ is the identity element in $\mathbb{G}_t$.*

In the security proof of our RIBE construction, we provide a reduction from our IND-RID-CPA secure RIBE scheme to the IND-ID-CPA secure Waters IBE scheme, which is secure under the DBDH assumption. We give the definition of the DBDH assumption, description of the Waters IBE scheme, and IND-ID-CPA security of ordinary IBE schemes.

Definition 2 (Decision Bilinear Diffie-Hellman (DBDH) Assumption). *Given a bilinear group $(p, \mathbb{G}, \mathbb{G}_t, e)$ generated by $\mathcal{G}(\lambda)$, define two distributions $\mathcal{D}_0(\lambda) = (g, g^a, g^b, g^c, e(g, g)^{abc}) \in \mathbb{G}^4 \times \mathbb{G}_T$ and $\mathcal{D}_1(\lambda) = (g, g^a, g^b, g^c, e(g, g)^z) \in \mathbb{G}^4 \times \mathbb{G}_T$, where $g \xleftarrow{\$} \mathbb{G}$ and $a, b, c, z \xleftarrow{\$} \mathbb{Z}_p$. The DBDH problem in the bilinear group $(p, \mathbb{G}, \mathbb{G}_t, e)$ is to decide a bit b from given $\mathcal{D}_b$, where $b \xleftarrow{\$} \{0, 1\}$. The advantage of $\mathcal{A}$ in solving the DBDH problem in the bilinear group $(p, \mathbb{G}, \mathbb{G}_t, e)$ is defined by*

$$Adv^{DBDH}_{\mathcal{G},\mathcal{A}}(\lambda) = \Big|\Pr[\mathcal{A}(\mathcal{D}_0(\lambda)) \to 1] - \Pr[\mathcal{A}(\mathcal{D}_1(\lambda)) \to 1]\Big|.$$

We say that the DBDH assumption holds in the bilinear group $(p, \mathbb{G}, \mathbb{G}_t, e)$ if no Probabilistic Polynomial Time (PPT) algorithm has a non-negligible advantage in solving the DBDH problem in the bilinear group $(p, \mathbb{G}, \mathbb{G}_t, e)$.

Definition 3 (Waters IBE). *The Waters IBE consists of four algorithms* $\mathsf{Setup}_{\mathsf{Wat}}$, $\mathsf{PKG}_{\mathsf{Wat}}$, $\mathsf{Enc}_{\mathsf{Wat}}$, *and* $\mathsf{Dec}_{\mathsf{Wat}}$.

- $\mathsf{Setup}_{\mathsf{Wat}}(\lambda)$: *Generate a bilinear group $(p, \mathbb{G}, \mathbb{G}_t, e) \leftarrow \mathcal{G}(\lambda)$. Choose g, g_2, u', $u_1, \ldots, u_n \xleftarrow{\$} \mathbb{G}$ and $\alpha \xleftarrow{\$} \mathbb{Z}_p$. Set $g_1 = g^\alpha$. Publish a master public key $\mathsf{mpk}_{\mathsf{Wat}} = \{g, g_1, g_2, u', u_1, \ldots, u_n\}$ and keep a master secret key $\mathsf{msk}_{\mathsf{Wat}} = \{g_2^\alpha\}$.*

– $\mathsf{PKG}_{\mathsf{Wat}}(\mathsf{mpk}_{\mathsf{Wat}}, \mathsf{msk}_{\mathsf{Wat}}, ID)$: *Parse* $ID = (b_1, \ldots, b_n) \in \{0,1\}^n$, *where for all* $i \in [1, n]$, $b_i \in \{0,1\}$. *Choose* $r \xleftarrow{\$} \mathbb{Z}_p$ *and return the private key*

$$\mathsf{pvk}_{ID} = (g_2^{\alpha}(u' \prod_{i=1}^{n} u_i^{b_i})^r,\ g^r).$$

– $\mathsf{Enc}_{\mathsf{Wat}}(\mathsf{mpk}_{\mathsf{Wat}}, ID, M)$: *Parse* $ID = (b_1, \ldots, b_n) \in \{0,1\}^n$. *Choose* $t \xleftarrow{\$} \mathbb{Z}_p$ *and return a ciphertext*

$$\mathsf{CT}_{\mathsf{Wat}} := (M \cdot e(g_1, g_2)^t,\ g^{-t},\ (u' \prod_{i=1}^{n} u_i^{b_i})^t).$$

– $\mathsf{Dec}_{\mathsf{Wat}}(\mathsf{mpk}_{\mathsf{Wat}}, \mathsf{pvk}_{ID}, \mathsf{CT}_{\mathsf{Wat}})$: *Parse* $\mathsf{CT}_{\mathsf{Wat}} = (C_0, C_1, C_2)$ *and* $\mathsf{pvk}_{ID} = (d_0, d_1)$ *and return*

$$C_0 \cdot e(C_1, d_0) \cdot e(C_2, d_1).$$

Definition 4 (IND-ID-CPA). *Let* $\mathcal{IBE} = (\mathsf{Setup}, \mathsf{PKG}, \mathsf{Enc}, \mathsf{Dec})$ *be an IBE scheme. For adversary* $\mathcal{A}$ *define the following experiment:*

$\mathbf{Exp}^{IND\text{-}ID\text{-}CPA}_{\mathcal{IBE},\mathcal{A}}(\lambda)$
$(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(\lambda)$;
$(M_0^*, M_1^*, ID^*, \mathsf{st}) \leftarrow \mathcal{A}^{\mathsf{PKG}(\cdot)}(\mathsf{mpk})$ *such that* $|M_0^*| = |M_1^*|$;
$b \xleftarrow{\$} \{0,1\}$;
$\mathsf{CT}^* \leftarrow \mathsf{Enc}(\mathsf{mpk}, ID^*, M_b^*)$;
$b' \leftarrow \mathcal{A}^{\mathsf{PKG}(\cdot)}(\mathsf{CT}^*, \mathsf{st})$;
If $b = b'$ *return* 1 *else return* 0.

In the above experiment, $\mathsf{PKG}(\cdot)$ *is an oracle, which returns a private key* pvk_{ID} *of given identity* ID, *and* $\mathcal{A}$ *is not allowed to send* ID^* *to* $\mathsf{PKG}(\cdot)$.

An IBE scheme is said to be IND-ID-CPA if for all PPT adversaries $\mathcal{A}$ *the following advantage is negligible in the security parameter* λ.

$$Adv^{IND\text{-}ID\text{-}CPA}_{\mathcal{IBE},\mathcal{A}}(\lambda) = \left| \Pr\left[\mathbf{Exp}^{IND\text{-}ID\text{-}CPA}_{\mathcal{IBE},\mathcal{A}}(\lambda) = 1\right] - \frac{1}{2} \right|.$$

Theorem 1 ([38]). *The Waters IBE scheme is IND-ID-CPA secure under DBDH assumption. More precisely, if there exists an adversary* $\mathcal{A}$ *breaking IND-ID-CPA security of the Waters IBE scheme with* ϵ *advantage, then by using* $\mathcal{A}$, *we can construct an algorithm* $\mathcal{B}$ *solving DBDH problem in the same bilinear group, over which the Waters IBE scheme is defined, with* $O(\frac{\epsilon}{nq})$ *advantage, where* q *is the maximum number of key extraction queries issued by* $\mathcal{A}$.

3 Definition of RIBE Scheme

In this subsection, we give the formal definition of the syntax and the security model of our RIBE construction. First, we give the syntax of RIBE scheme.

Our syntax of RIBE scheme is slightly different from previous one [7, 28][6] ; Our DKG algorithm is probabilistic, whereas the Boldyreva et al. one is deterministic.[7] A RIBE scheme $\mathcal{RIBE}$ consists of seven algorithms (Setup, PKG, KeyUp, DKG, Enc, Dec, Revoke). Let $\mathcal{M}$, $\mathcal{I}$, and $\mathcal{T}$ be a message space, an identity space, and a time space, respectively.

Definition 5 (Syntax of RIBE).

Setup *: This is the (stateful) setup algorithm which takes as input the security parameter λ and the number of users N, and outputs the public parameter* mpk*, the master secret key* msk*, the initial revocation list $RL = \emptyset$, and a state* st*.*

PKG *: This is the (stateful) private key generation algorithm which takes as input* mpk*,* msk*, an identity $ID \in \mathcal{I}$, and outputs a secret key sk_{ID} associated with ID and an updated state* st*.*

KeyUp *: This is the key update generation algorithm which takes as input* mpk*,* msk*, the key update time $T \in \mathcal{T}$, the current revocation list RL, and* st*, and outputs the key update ku_T.*

DKG *: This is the probabilistic decryption key algorithm which takes as input* mpk*, sk_{ID}, and ku_T, and outputs a decryption key $\mathsf{dk}_{ID,T}$ or $\perp$ if ID has been revoked.*

Enc *: This is the probabilistic encryption algorithm which takes as input* mpk*, $ID \in \mathcal{I}$, $T \in \mathcal{T}$, and a message $M \in \mathcal{M}$, and outputs a ciphertext* CT*.*

Dec *: This is the deterministic decryption algorithm which takes as input* mpk*, $\mathsf{dk}_{ID,T}$, and* CT*, and outputs M or $\perp$ if* CT *is an invalid ciphertext.*

Revoke *: This is the stateful revocation algorithm which takes as input an identity to be revoked $ID \in \mathcal{I}$, a revocation time $T \in \mathcal{T}$, the current revocation list RL, and a state* st*, and outputs an updated RL.*

Every RIBE scheme should satisfy the following correctness condition: For any $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(\lambda)$, $M \in \mathcal{M}$, all possible state st, and a revocation list RL, if $ID \in \mathcal{I}$ is not revoked on a time $T \in \mathcal{T}$, then for $(\mathsf{sk}_{ID}, \mathsf{st}) \leftarrow \mathsf{PKG}(\mathsf{mpk}, \mathsf{msk}, ID, \mathsf{st})$, $\mathsf{ku}_T \leftarrow \mathsf{KeyUp}(\mathsf{mpk}, \mathsf{msk}, T, RL, \mathsf{st})$, and $\mathsf{dk}_{ID,T} \leftarrow \mathsf{DKG}(\mathsf{mpk}, \mathsf{sk}_{ID}, \mathsf{ku}_T)$,

$$\mathsf{Dec}(\mathsf{mpk}, \mathsf{dk}_{ID,T}, \mathsf{Enc}(\mathsf{mpk}, ID, T, M)) = M \quad \text{holds.}$$

Next, we provide a security definition of RIBE scheme that captures realistic threats including decryption key exposure.

Definition 6 (IND-RID-CPA). *Let $\mathcal{RIBE}$ =* (Setup, PKG, KeyUP, DKG, Enc, Dec, Revoke) *be a RIBE scheme. For an adversary $\mathcal{A}$ define the following experiment:*

[6] Boldyreva et al. [7] define the *selective* security, and Libert-Vergnaud [28] extends it to *adaptive* security.

[7] All DKG algorithms in the previous constructions are deterministic and invertible in the sense that a secret key can be recovered from a corresponding decryption key (and key update), and so previous schemes are vulnerable against decryption key exposure. To prevent such an attack by inversion, we define DKG to be probabilistic.

$\mathbf{Exp}^{IND\text{-}RID\text{-}CPA}_{\mathcal{RIBE},\mathcal{A}}(\lambda, N)$
$(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(\lambda, N)$;
$(M_0^*, M_1^*, ID^*, T^*, \mathsf{st}) \leftarrow \mathcal{A}^{\mathcal{O}}(\mathsf{mpk})$ *such that* $|M_0^*| = |M_1^*|$;
$b \xleftarrow{\$} \{0,1\}$;
$\mathsf{CT}^* \leftarrow \mathsf{Enc}(\mathsf{mpk}, ID^*, T^*, M_b^*)$;
$b' \leftarrow \mathcal{A}^{\mathcal{O}}(\mathsf{CT}^*, \mathsf{st})$;
If $b = b'$ *return* 1 *else return* 0.

In the above experiment, $\mathcal{O}$ *is a set of oracles* $\{\mathsf{PKG}(\cdot), \mathsf{KeyUp}(\cdot), \mathsf{Revoke}(\cdot,\cdot), \mathsf{DKG}(\cdot,\cdot)\}$ *defined as follows:*

$\mathsf{PKG}(\cdot)$ *: For* $ID \in \mathcal{I}$*, it returns* sk_{ID} *(by running* $\mathsf{PKG}(\mathsf{mpk}, \mathsf{msk}, ID, \mathsf{st}) \rightarrow \mathsf{sk}_{ID}$*).*

$\mathsf{KeyUp}(\cdot)$ *: For* $T \in \mathcal{T}$*, it returns* ku_T *(by running* $\mathsf{KeyUp}(\mathsf{mpk}, \mathsf{msk}, T, RL, \mathsf{st}) \rightarrow \mathsf{ku}_T$*).*

$\mathsf{Revoke}(\cdot,\cdot)$ *: For* $ID \in \mathcal{I}$ *and* $T \in \mathcal{T}$*, it returns the updated revocation list* RL *(by running* $\mathsf{Revoke}(\mathsf{mpk}, ID, T, RL, \mathsf{st}) \rightarrow RL$*).*

$\mathsf{DKG}(\cdot,\cdot)$ *: For* $ID \in \mathcal{I}$ *and* $T \in \mathcal{T}$*, it returns* $\mathsf{dk}_{ID,T}$ *(by running* $\mathsf{PKG}(\mathsf{mpk}, \mathsf{msk}, ID, \mathsf{st})) \rightarrow \mathsf{sk}_{ID}$ *and* $\mathsf{DKG}(\mathsf{mpk}, \mathsf{sk}_{ID}, \mathsf{ku}_T) \rightarrow \mathsf{dk}_{ID,T}$*).*

$\mathcal{A}$ *is allowed to issue the above oracles with the following restrictions:*[8]

1. $\mathsf{KeyUp}(\cdot)$ *and* $\mathsf{Revoke}(\cdot,\cdot)$ *can be queried on time which is greater than or equal to the time of all previous queries.*
2. $\mathsf{Revoke}(\cdot,\cdot)$ *cannot be queried on time* T *if* $\mathsf{KeyUp}(\cdot)$ *was queried on* T*.*
3. *If* $\mathsf{PKG}(ID^*)$ *was queried, then* $\mathsf{Revoke}(ID^*, T)$ *must be queried for* $T \leq T^*$*.*
4. $\mathsf{DKG}(\cdot,\cdot)$ *cannot be queried on time* T *before* $\mathsf{KeyUp}(\cdot)$ *was queried on* T*.*
5. $\mathsf{DKG}(ID^*, T^*)$ *cannot be queried.*

A RIBE scheme is said to be IND-RID-CPA if for all PPT adversaries $\mathcal{A}$ *and polynomials* N*, the following advantage is negligible in the security parameter* λ*.*

$$Adv^{IND\text{-}RID\text{-}CPA}_{\mathcal{RIBE},\mathcal{A}}(\lambda, N) = \left| \Pr\left[\mathbf{Exp}^{IND\text{-}RID\text{-}CPA}_{\mathcal{RIBE},\mathcal{A}}(\lambda, N) = 1\right] - \frac{1}{2} \right|.$$

3.1 Security Analysis of Previous RIBE Schemes

In this section, we analyze the security of previous RIBE schemes in our security model, which assumes a stronger adversary than Boldyreva et al. adversarial model: our adversary can access the decryption key oracle, which is not given in the Boldyreva et al. model. First, we show that the (simple but non-scalable) BF-RIBE scheme is secure in the new adversarial model. Next, we show that all previous RIBE schemes except for the BF-RIBE are vulnerable against

[8] The fourth and fifth restrictions are the difference between our definition and Boldyreva et al.'s one [7].

decryption key exposure. More precisely, we can construct polynomial time adversaries using decryption key oracles.[9] We briefly explain the BGK-RIBE scheme and the LV-RIBE scheme are vulnerable against decryption key exposure.

Boneh-Franklin RIBE Scheme: To fit the BF-RIBE scheme into our syntax of the RIBE scheme, BF-RIBE can be instantiated with the $IND\text{-}CPA$ secure symmetric encryption scheme. Let $\mathsf{Enc}_{\mathsf{BF}}(\mathsf{mpk}_{\mathsf{BF}}, ID, M)$ and $\mathsf{PKG}_{\mathsf{BF}}(\mathsf{msk}_{\mathsf{BF}}, ID)$ be an encryption algorithm and private key generation algorithm for the BF-IBE scheme, respectively, where $(\mathsf{mpk}_{\mathsf{BF}}, \mathsf{msk}_{\mathsf{BF}})$ is a pair of a master public key and master secret key, ID is a receiver's identity, and M is a message. Let $\mathsf{SE} = (\mathsf{SEnc}, \mathsf{SDec})$ be a symmetric encryption scheme. For each user ID, KGC randomly chooses a secret key of SE and gives it to the user ID as sk_{ID}. The encryption algorithm of the (modified) BF-RIBE scheme is defined as $\mathsf{Enc}(\mathsf{mpk}_{\mathsf{BF}}, ID, T, M) := \mathsf{Enc}_{\mathsf{BF}}(\mathsf{mpk}_{\mathsf{BF}}, (ID, T), M)$. In each time period T, KGC runs $\mathsf{PKG}_{\mathsf{BF}}(\mathsf{msk}_{\mathsf{BF}}, (ID, T)) \rightarrow \mathsf{pvk}_{(ID,T)}$, where $\mathsf{pvk}_{(ID,T)}$ will be a decryption key for ID on time T, that is, $\mathsf{pvk}_{(ID,T)} = \mathsf{dk}_{ID,T}$. Then KGC posts $\mathsf{ku}_T = \{\mathsf{SEnc}_{\mathsf{sk}_{ID}}(\mathsf{dk}_{ID,T}) | ID \text{ is a non-revoked user in time period } T\}$. Then, only non-revoked users can recover $\mathsf{dk}_{ID,T}$. If the BF-IBE scheme is IND-ID-CPA secure and the SE is IND-CPA secure, then the (modified) BF-RIBE scheme is IND-RID-CPA secure, which can easily be proven by using the standard hybrid argument.

Boldyreva-Goyal-Kumar RIBE Scheme: Boldyreva et al. [7] proposed the first scalable but selectively secure RIBE scheme by using Fuzzy IBE [36]. Due to the collusion resistance of the Fuzzy IBE scheme, no revoked user can compute its decryption key. The user's decryption keys are associated with two attributes: identity ID and time period T. The decryption key is split into two components corresponding to ID and T. A secret key sk_{ID} is associated with ID and key update ku_T is associated with T. The DKG algorithm is only to put parts of sk_{ID} and ku_T together.[10] More concretely, the PKG algorithm returns $\{(x, D_x, d_x)\}_{x \in \mathsf{I}}$ which is a private key of a user who is assigned to a leaf node η, and the KeyUp algorithm returns $\{(y, E_y, e_y)\}_{y \in \mathsf{J}}$. If a user is not revoked on T, then there exist x where $x \in \mathsf{I} \cap \mathsf{J}$. The DKG algorithm finds such a x, and returns (D_x, E_x, d_x, e_x) which is a decryption key $\mathsf{dk}_{ID,T}$ of this user on time T. Therefore, an adversary that has $\mathsf{dk}_{ID^*,T}$ and ku_T can always recover a part (D_{x^*}, d_{x^*}) of sk_{ID^*} for some x^* if ID^* is not revoked in time T, and can always compute $\mathsf{dk}_{ID^*,T^*} = (D_{x^*}, E_{x^*}, d_{x^*}, e_{x^*})$ from the parts (D_{x^*}, d_{x^*}) of sk_{ID^*} and (E_{x^*}, e_{x^*}) of ku_{T^*} if ID^* is still not revoked in the challenge time T^*.

[9] As we mentioned in the introduction, a goal of this subsection is to not contradict the security proofs of previous RIBE schemes. Our attack is positioned outside of their security models.

[10] Chen et al. [13] proposed an RIBE scheme based on lattices by applying the Agrawal et al. lattice-based IBE [1]. They used the same methodology as that of BGK-RIBE, where a private key itself is contained in a corresponding decryption key. Therefore, the same attack works.

Libert-Vergnaud RIBE Scheme: Libert and Vergnaud [28] proposed the first adaptively secure RIBE scheme without random oracles. In the LV-RIBE scheme, the process of $\mathsf{DKG}(\mathsf{mpk}, \mathsf{sk}_{ID}, \mathsf{ku}_T)$ is component-wise multiplications or additions between sk_{ID} and ku_T. Since ku_T is public information, if an adversary obtains a decryption key $\mathsf{dk}_{ID^*,T}$, where $T \neq T^*$, it can then recover sk_{ID} in polynomial-time by performing the inverse process of DKG, that is, divisions or subtractions. More concretely, the PKG algorithm returns $\mathsf{sk}_{ID} = \{(i, d_{ID,i})\}_{i \in \mathsf{I}}$, where $d_{ID,i} := (d_{1,i}, d_{2,i}, r_{1,i})$, and the KeyUp algorithm returns $\mathsf{ku}_T = \{\mathsf{ku}_{T,j}\}_{j \in \mathsf{J}}$, where $\mathsf{ku}_{T,j} := (\mathsf{ku}_{1,j}, \mathsf{ku}_{2,j}, r_{2,j})$. The DKG algorithm parses $\mathsf{sk}_{ID} = \{(i, d_{ID,i})\}_{i \in \mathtt{I}}$ and $\mathsf{ku}_T = \{(j, \mathsf{ku}_{T,j}\}_{j \in \mathtt{J}}$. If there is no pair $(i, j) \in \mathtt{I} \times \mathtt{J}$ such that $i = j$, then return $\perp$. Otherwise, choose such pair $i = j$. Return $\mathsf{dk}_{ID,T} = (d_{T,1}, d_{T,2}, d_{T,3}, d_{T,4}) = (d_{1,i} \cdot \mathsf{ku}_{1,i}, d_{2,i}, \mathsf{ku}_{2,i}, r_{1,i} + r_{2,i})$. Therefore, anyone can easily compute $(d_{1,i}, d_{2,i}, r_{1,i}) \in \mathsf{sk}_{ID}$ from "both" $\mathsf{dk}_{ID,T}$ and $\mathsf{ku}_{T,i}$ such that $d_{1,i} = d_{T,1}/\mathsf{ku}_{1,i}$ and $r_{1,i} = d_{T,4} - r_{2,i}$. Moreover, $d_{2,i}$ is directly contained in $\mathsf{dk}_{ID,T}$.

One may expect that we can impede this attack by adding a randomization process in DKG, but it does not seem easy to prove the security of such a modification of the LV-RIBE scheme. LV-RIBE scheme is based on a variant of the Waters IBE (LV-IBE) scheme proposed in [29]. The security strategy of the LV-IBE is somewhat similar to the Gentry IBE [19] such that the simulator can compute a private key for any identity, even the challenge identity, in the proof. The simulator can generate a private key using "fixed" randomness and this fixed randomness is also used in making the challenge ciphertext.[11] Therefore, in the adversarial view, the challenge ciphertext is uniformly generated since it cannot obtain the corresponding private key of the challenge ciphertext. Since the LV-RIBE is based on the LV-IBE, the LV-RIBE does not support full re-randomization of the decryption key. Therefore, decryption key exposure reveals randomness used in the secret key. Since ku_{T^*} is public, if dk_{ID^*,T^*} is leaked, the randomness of sk_{ID^*} will be also leaked. (Not all parts of the randomness, but fixed randomness, which is essentially used in the security proof, will be leaked.) As mentioned, the simulation of this type of IBE scheme, such as the LV-IBE and the Gentry IBE scheme, succeeds only when the fixed randomness of the private key is hidden from the adversary's view. Therefore, we cannot construct a simulator for the LV-RIBE scheme when we directly follow the same strategy used in the LV-IBE scheme.

4 Our Construction

In this section, we propose an RIBE scheme. For the revocation process, we basically follow previous RIBE schemes' strategy using a binary tree structure; that is, to reduce the key update costs, we apply a binary tree structure and

[11] The term "fixed" means that the simulator can generate only one private key using fixed randomness per each identity after publishing mpk. A decryption key may have other flexible randomness, but at least a part of the randomness should be fixed according to the identity.

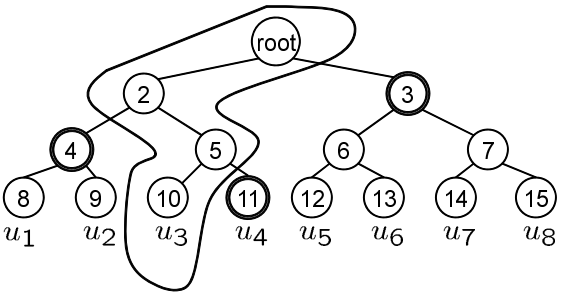

Fig. 1. Example of KUNode

define the KUNode algorithm. In the actual schemes, this algorithm is used in a black-box manner.

4.1 KUNode Algorithm

We introduce the KUNode algorithm and Boldyreva et al.'s idea for efficient revocation.

Definition 7 (KUNode **Algorithm [7]).** *This algorithm takes as input a binary tree* BT*, revocation list* RL*, and time* T*, and outputs a set of nodes. A formal description of this algorithm is as follows: If* η *is a non-leaf node, then* η_{left} *and* η_{right} *denote the left and right child of* η*, respectively. Each user is assigned to a leaf node. If a user (assigned to* η*) is revoked on time* T*, then* $(\eta, T) \in RL$*.* Path(η) *denotes the set of nodes on the path from* η *to* root*. The description of* KUNode *is given below.*

KUNode(BT, RL, T) :
  X, Y $\leftarrow \emptyset$;
  $\forall(\eta_i, T_i) \in RL$
    If $T_i \leq T$ *then add* Path(η_i) *to* X
  $\forall x \in$ X
    If $x_{left} \notin$ X *then add* x_{left} *to* Y
    If $x_{right} \notin$ X *then add* x_{right} *to* Y
  If Y $= \emptyset$ *then add* root *to* Y
  Return Y

Figure 1 gives a simple example to help the readers easily understand KUNode(BT, RL, T). In the example, let a user u_3 (assigned to x_{10}) be revoked.

Then, $X = \mathsf{Path}(x_{10}) = \{x_{10}, x_5, x_2, \mathsf{root} = x_1\}$, and $Y = \{x_3, x_4, x_{11}\}$. Intuitively, all users, except u_3, have a node $x \in Y$ that is contained in the set of nodes on the path from their assigned node to `root`: e.g., x_4 for u_1 and u_2, x_{11} for u_4, and x_3 for u_5, u_6, u_7, and u_8, whereas $Y \cap \mathsf{Path}(x_{10}) = \emptyset$.

When a user joins the system, KGC assigns it to the leaf node η of a complete binary tree, and issues a set of keys, wherein each key is associated with each node on $\mathsf{Path}(\eta)$. At time period T, KGC publishes key updates for a set $\mathsf{KUNode}(\mathtt{BT}, RL, T)$. Then, only non-revoked users have at least one key corresponding to a node in $\mathsf{KUNode}(\mathtt{BT}, RL, T)$ and are able to generate decryption keys on time T.

4.2 Our Construction

For a simple description of our RIBE scheme, we use notation F_{Wat} and F_{BB} to denote the respective hash functions used in the Waters IBE scheme and Boneh-Boyen IBE scheme. More precisely, for an identity space $\mathcal{I}$ and time space $\mathcal{T}$, define $F_{\mathsf{Wat}} : \mathcal{I} \to \mathbb{G}$ and $F_{\mathsf{BB}} : \mathcal{T} \to \mathbb{G}$ by

$$F_{\mathsf{Wat}}(ID) = u' \prod_{i=1}^{n} u_i^{b_i} \text{ and } F_{\mathsf{BB}}(T) = v' v^T, \text{ respectively,}$$

where $ID = (b_1, b_2, \ldots, b_n) \in \{0,1\}^n$.

Before describing our construction, we will explain the intuition behind it. As mentioned, we need a different approach to achieve an (adaptively secure) RIBE scheme with decryption key exposure. To this end, we begin with a simple two-level HIBE scheme (without delegating property). More precisely, the first level is assigned for identity and the second level is assigned for the time period. Since we consider only polynomially bounded time (as all previous RIBE schemes), we combine the adaptively secure Waters IBE scheme (for the first level) and the selectively secure Boneh-Boyen IBE scheme (for the second level). The decryption key of our RIBE scheme is exact second level secret key of the HIBE scheme, that is,

$$\mathsf{dk}_{ID,T} = (g_2^{\alpha} F_{\mathsf{Wat}}(ID)^r F_{\mathsf{BB}}(T)^s,\ g^r,\ g^s).$$

The above decryption key allows user to re-randomize r and s in the exponent without knowing master key g_2^{α}.[12] Decryption key exposure will then not be helpful for the adversary in obtaining information about the challenge ciphertext since this combined two-level hierarchical extension can be considered as a secure HIBE scheme (for exponentially many identities and polynomially many time periods) in the sense that it has resistance against collusion attacks. To generate secret keys and key updates, we use a technique similar to that used in [28].

[12] As mentioned in section 3.1, the LV-RIBE does not support such re-randomization process in decryption keys, and this is the essential difference between ours and previous schemes.

The master secret key is randomly divided into two parts, which are respectively contained in the secret key and key updates, that is,

$$(g_\theta^\alpha F_{\mathsf{Wat}}(ID)^{r_\theta},\ g^{r_\theta}) \in \mathsf{sk}_{ID} \text{ and } (\tilde{g}_\theta^\alpha F_{\mathsf{BB}}(T)^{s_\theta},\ g^{s_\theta}) \in \mathsf{ku}_T,$$

where $g_\theta \cdot \tilde{g}_\theta = g_2$. Therefore, if the adversary cannot obtain both the secret key and key updates, which will contribute to computing the target decryption key dk_{ID^*,T^*}, then in the security proof we can simulate either the secret key or key update. (We can assume that the part not given to the adversary contains information about the master key and the other part is a random element.)

Even if the above intuition explains the decryption key exposure resistance of a combination of the Waters IBE and the Boneh-Boyen IBE, we need an additional technique to circumvent the difficulty pointed out in [28]. The difficulty occurs when the adversary issues a secret key query for the target identity ID^*. For each node θ in the binary tree, a random value g_θ is assigned. Whenever PKG is run, the identity ID is assigned in the leaf node and the value g_θ on the path to the root node is used in the secret key sk_{ID}. In the security proof, whenever a secret key query or key update query regarding ID is issued, the simulator should decide which of two shares g_θ^α and $\tilde{g}_\theta^\alpha$ will contain the master secret key, where θ is on the path to the root of tree; that is, one share is $g_2^\alpha S_\theta$ and the other is S_θ^{-1} for random group element S_θ. However, when the target identity ID^* is unknown and has yet to be assigned a leaf, the other path regarding the different identity ID may or may not have connection with the path regarding ID^* (except the root node). To address this issue, Libert and Vergnaud used a variant of the Waters IBE wherein the simulator can generate at least one valid decryption key for each identity and can answer queries regardless of whether nodes are on the path from ID^* to the root node. However, our construction does not support a simulation strategy such as is used in [28, 29] since the original Waters IBE scheme uses a different proof strategy, called *partitioning*, in the security proof. Instead, we carefully deal with the method to assign identity into the tree. In our RIBE scheme, whenever a new identity joins the system, KGC assigns a random leaf node among the undefined nodes.[13] In the security proof, this simple random node assignment technique allows the simulator to pre-assign a random leaf node for the target identity (therefore nodes on the path to the root node are also pre-determined) and to simulate for a secret key, decryption key, and key update queries before receiving queries regarding ID^*. When the first query regarding ID^* is issued, the simulator can use the pre-assigned leaf node for ID^*. We can show that this simulation for node assignment is identically distributed to that in the real protocol.

We describe the proposed RIBE scheme below.

$\mathsf{Setup}(\lambda, N)$: Randomly choose $g, g_2, u', u_1, \ldots, u_n, v', v \xleftarrow{\$} \mathbb{G}$ and $\alpha \xleftarrow{\$} \mathbb{Z}_p$. Set $\mathsf{mpk} = \{g, g_1 = g^\alpha, g_2, u', u_1, \ldots, u_n, v', v\}$, $\mathsf{msk} = \{g_2^\alpha\}$, $RL = \emptyset$, and $\mathsf{st} = \mathsf{BT}$, where BT is a binary tree with N leaves.

[13] KGC can use a pseudorandom generator for this process.

$\mathsf{PKG}(\mathsf{mpk}, \mathsf{msk}, ID, \mathsf{st})$: Randomly choose an unassigned leaf η from $\mathtt{BT}$, and store ID in the node η. For each node $\theta \in \mathsf{Path}(\eta)$,

1. Recall g_θ if it was defined. Otherwise, $g_\theta \xleftarrow{\$} \mathbb{G}$ and store $(g_\theta, \tilde{g}_\theta = g_2/g_\theta)$ in the node θ.[14]
2. Choose $r_\theta \xleftarrow{\$} \mathbb{Z}_p$.
3. Compute $(D_{\theta,0}, D_{\theta,1}) := (g_\theta^\alpha F_{\mathsf{Wat}}(ID)^{r_\theta}, g^{r_\theta})$.

Return $\mathsf{sk}_{ID} = \{(\theta, D_{\theta,0}, D_{\theta,1})\}_{\theta \in \mathsf{Path}(\eta)}$.

$\mathsf{KeyUp}(\mathsf{mpk}, \mathsf{msk}, T, RL, \mathsf{st})$: Parse $\mathsf{st} = \mathtt{BT}$. For each node $\theta \in \mathsf{KUNode}(\mathtt{BT}, RL, T)$,

1. Retrieve $\tilde{g}_\theta$ (note that $\tilde{g}_\theta$ is always pre-defined in the PKG algorithm).
2. Choose $s_\theta \xleftarrow{\$} \mathbb{Z}_p$.
3. Compute $(\tilde{D}_{\theta,0}, \tilde{D}_{\theta,1}) := (\tilde{g}_\theta^\alpha F_{\mathsf{BB}}(T)^{s_\theta}, g^{s_\theta})$.

Return $\mathsf{ku}_T = \{(\theta, \tilde{D}_{\theta,0}, \tilde{D}_{\theta,1})\}_{\theta \in \mathsf{KUNode}(\mathtt{BT}, RL, T)}$.

$\mathsf{DKG}(\mathsf{mpk}, \mathsf{sk}_{ID}, \mathsf{ku}_T)$: Parse $\mathsf{sk}_{ID} = \{(\theta, D_{\theta,0}, D_{\theta,1})\}_{\theta \in \mathtt{I}}$ and $\mathsf{ku}_T = \{(\theta, \tilde{D}_{\theta,0}, \tilde{D}_{\theta,1})\}_{\theta \in \mathtt{J}}$. If $\mathtt{I} \cap \mathtt{J} = \emptyset$, then return $\perp$. Otherwise, choose $\theta \in \mathtt{I} \cap \mathtt{J}$ and $r, s \xleftarrow{\$} \mathbb{Z}_p$ and return

$$\mathsf{dk}_{ID,T} = (D_{\theta,0} \cdot \tilde{D}_{\theta,0} \cdot F_{\mathsf{Wat}}(ID)^r \cdot F_{\mathsf{BB}}(T)^s, \quad D_{\theta,1} \cdot g^r, \quad \tilde{D}_{\theta,1} \cdot g^s).$$

$\mathsf{Enc}(\mathsf{mpk}, ID, T, M)$: Choose a random integer $t \xleftarrow{\$} \mathbb{Z}_p$ and return

$$\mathsf{CT} = (M \cdot e(g_1, g_2)^t, \quad g^{-t}, \quad F_{\mathsf{Wat}}(ID)^t, \quad F_{\mathsf{BB}}(T)^t).$$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{dk}_{ID,T}, \mathsf{CT})$: Parse $\mathsf{CT} = (C_0, C_1, C_2, C_3)$ and $\mathsf{dk}_{ID,T} = (D_1, D_2, D_3)$ and return

$$C_0 \prod_{i=1}^{3} e(C_i, D_i).$$

$\mathsf{Revoke}(\mathsf{mpk}, ID, T, RL, \mathsf{st})$: Let η be the leaf node associated with ID. Update the revocation list by $RL \leftarrow RL \cup \{(\eta, T)\}$ and return the updated revocation list.

We should check the correctness of our scheme: Assume that mpk, msk, $\mathcal{M}$, $\mathcal{I}$, $\mathcal{T}$, st, and RL are normally generated and fixed. Moreover, assume that $\mathsf{sk}_{ID} = \{(\theta, D_{\theta,0}, D_{\theta,1})\}_{\theta \in \mathsf{Path}(\eta)}$ is a secret key of a non-revoked user ID on time T and $\mathsf{ku}_T = \{(\theta, \tilde{D}_{\theta,0}, \tilde{D}_{\theta,1})\}_{\theta \in \mathsf{KUNode}(\mathtt{BT}, RL, T)}$. Then, for some $\theta \in \mathsf{Path}(\eta) \cap \mathsf{KUNode}(\mathtt{BT}, RL, T)$, DKG should output

$$\begin{aligned}\mathsf{dk}_{ID,T} &= (D_{\theta,0} \cdot \tilde{D}_{\theta,0} \cdot F_{\mathsf{Wat}}(ID)^r \cdot F_{\mathsf{BB}}(T)^s, \quad D_{\theta,1} \cdot g^r, \quad \tilde{D}_{\theta,1} \cdot g^s) \\ &= (g_2^\alpha F_{\mathsf{Wat}}(ID)^{r_\theta + r} F_{\mathsf{BB}}(T)^{s_\theta + s}, \quad g^{r_\theta + r}, \quad g^{s_\theta + s}).\end{aligned}$$

For an encryption of M, $\mathsf{CT} = (M \cdot e(g_1, g_2)^t, \quad g^{-t}, \quad F_{\mathsf{Wat}}(ID)^t, \quad F_{\mathsf{BB}}(T)^t)$,

$$\begin{aligned}&\mathsf{Dec}(\mathsf{mpk}, \mathsf{dk}_{ID,T}, \mathsf{CT}) \\ &= M \cdot e(g_1, g_2)^t e(g^{-t}, g_2^\alpha F_{\mathsf{Wat}}(ID)^{r_\theta + r} F_{\mathsf{BB}}(T)^{s_\theta + s}) e(F_{\mathsf{Wat}}(ID)^t, g^{r_\theta + r}) \\ &\quad \cdot e(F_{\mathsf{BB}}(T)^t, g^{s_\theta + s}) \\ &= M.\end{aligned}$$

[14] As in the Libert-Vergnaud scheme, KGC can use a pseudorandom generator instead of storing g_θ.

We provide a (polynomial-time) reduction to the Waters IBE scheme, which is a non-revocable IBE secure under the DBDH assumption. Therefore, our scheme is secure under the DBDH assumption.

Theorem 2. *If there exists an adversary $\mathcal{A}$ attacking IND-RID-CPA security of the proposed RIBE scheme, then there exists another adversary $\mathcal{B}$ breaking IND-ID-CPA security of the Waters IBE scheme.*

Because of space constraints, we relegate the proof of Theorem 2 in the full version. Note that the reduction loss in our security proof is $2q|\mathcal{T}|$. Since the security proof to show that the Waters IBE scheme is secure under DBDH assumption losses $O(nq)$ [38], our RIBE scheme is secure under DBDH assumption with $O(nq^2|\mathcal{T}|)$ reduction loss. Although our proof is loose, we note that the previous adaptively secure LV-RIBE scheme lose the same factor $O(nq^2|\mathcal{T}|)$ in the security proof.

5 Discussion

In this section, we discuss several issues related to RIBE schemes.

Short Public Parameters: In high level explanation, our technique is to add the revocation capability to the IBE scheme without sacrificing efficiency, and we show that the underlying IBE scheme supporting key re-randomization can be provably secure against decryption key exposure. In fact, we essentially used the Water IBE as the underlying IBE scheme of our RIBE construction. Therefore, we may construct an RIBE scheme from other IBE schemes. We expect that a scalable RIBE scheme with decryption key exposure resilience can be constructed from the Lewko-Waters IBE [25], which supports key re-randomization. Then, we can reduce the size of public parameter, though we need to use composite-order bilinear groups and other complexity assumptions. Note that Lewko have shown a Lewko-Waters IBE scheme under the prime-order group setting [24], however, this scheme does not support key-rerandomization. It would be interesting to construct a RIBE scheme with decryption key exposure resilience and short public parameters in the prime-order group setting.

Better Efficiency from Random Oracle Heuristic: In our construction, we used two level hierarchical construction by combining the Water IBE and the Boneh-Boyen IBE, where both schemes are secure in the standard model. Both schemes use hash functions F_{Wat} and F_{BB}, respectively. The role of both hash functions is to apply *partitioning* technique; that is, in the security proof, the simulator divides the domain of hash functions into two subsets, one for the challenge query and the other for key extraction queries. By changing these two hash functions into cryptographic hash functions that are modeled as random oracles, we can achieve better efficiency since the random oracles allow such a partitioning technique but require low computational cost. Furthermore, by using one more hash function and standard techniques for random oracle model schemes, we can reduce the security of the random oracle model RIBE scheme to the BDH problem.

Revocable Identity-Based Signature (RIBS): We basically used two level hierarchical construction and it is not difficult to extend our construction to three level hierarchical construction (but revocation capability is allowed only for the first level). Therefore, we can apply the well-known Naor transformation from an IBE scheme to a signature scheme. More precisely, from the three level hierarchical construction, we can obtain a scalable identity-based signature scheme, where the first level is for identity, the second level is for time period, and the third level is for message. For better efficiency, we can apply the same transformation used in the previous paragraph to here, and then obtain an efficent RIBS scheme in the random oracle model.

Chosen Ciphertext Security: Due to the property of the underlying Waters IBE scheme, we can extend our RIBE scheme to a HIBE scheme with efficient revocation only for the first level users. There is a well-known transformation from a two-level HIBE scheme to a CCA-secure IBE scheme [9]. Therefore, we can obtain CCA-secure RIBE scheme by applying this transformation.

6 Conclusion

We revisited both the security model and construction methodology for RIBE schemes. First, we pointed out a gap between the Boldyreva et al. security model and the trivial but non-scalable BF-RIBE construction. We introduced a new security model for RIBE scheme by capturing realistic threat, called decryption key exposure, and proposed the first scalable RIBE construction in the new security model.

There are several interesting remaining problems. From a theoretical point of view, one natural question is how to construct a generic transformation from IBE to RIBE. In the practice, revocation is a necessary functionality in the public key encryption schemes. Therefore, finding efficient revocation methods in other encryption schemes such as (hierarchical) inner-product encryption [35] and attribute-based encryption [36] are also important. In this paper, we only focused on the pairing-based schemes, but it is interesting to construct schemes based on other mathematical structure such as lattice that are secure in our security model. Recently, a revocable hierarchical IBE (RHIBE) scheme is proposed, but its security is proven only in the weaker security notion, selective security [37]. Achieving full security in RHIBE construction is a direct open problem. To the best of our knowledge, all scalable RIBE use the *Complete Subtree* [32] method for revocation capability. Therefore, it is interesting to combine IBE with different revocation methods such as the *Subset Difference* [32].

Acknowledgements. We thank anonymous reviewers of PKC 2013 and members of Shin-Akarui-Angou-Benkyou-Kai for their helpful comments.

References

1. Agrawal, S., Boneh, D., Boyen, X.: Efficient Lattice (H)IBE in the Standard Model. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 553–572. Springer, Heidelberg (2010)
2. Aiello, W., Lodha, S., Ostrovsky, R.: Fast Digital Identity Revocation (Extended Abstract). In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 137–152. Springer, Heidelberg (1998)
3. Attrapadung, N., Imai, H.: Attribute-Based Encryption Supporting Direct/Indirect Revocation Modes. In: Parker, M.G. (ed.) Cryptography and Coding 2009. LNCS, vol. 5921, pp. 278–300. Springer, Heidelberg (2009)
4. Attrapadung, N., Imai, H.: Conjunctive Broadcast and Attribute-Based Encryption. In: Shacham, H., Waters, B. (eds.) Pairing 2009. LNCS, vol. 5671, pp. 248–265. Springer, Heidelberg (2009)
5. Baek, J., Zheng, Y.: Identity-Based Threshold Decryption. In: Bao, F., Deng, R., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 262–276. Springer, Heidelberg (2004)
6. Bellare, M., Palacio, A.: Protecting against key exposure: strongly key-insulated encryption with optimal threshold. IACR Cryptology ePrint Archive 2002:064 (2002)
7. Boldyreva, A., Goyal, V., Kumar, V.: Identity-based encryption with efficient revocation. In: ACM CCS 2008, pp. 417–426 (2008)
8. Boneh, D., Boyen, X.: Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004)
9. Boneh, D., Canetti, R., Halevi, S., Katz, J.: Chosen-ciphertext security from identity-based encryption. SIAM J. Comput. 36(5), 1301–1328 (2007)
10. Boneh, D., Ding, X., Tsudik, G., Wong, C.-M.: A method for fast revocation of public key certificates and security capabilities. In: USENIX Security Symposium 2001. USENIX (2001)
11. Boneh, D., Franklin, M.K.: Identity-based encryption from the weil pairing. SIAM J. Comput. 32(3), 586–615 (2003)
12. Canetti, R., Halevi, S., Katz, J.: A forward-secure public-key encryption scheme. Journal of Cryptology 20, 265–294 (2007)
13. Chen, J., Lim, H.W., Ling, S., Wang, H., Nguyen, K.: Revocable Identity-Based Encryption from Lattices. In: Susilo, W., Mu, Y., Seberry, J. (eds.) ACISP 2012. LNCS, vol. 7372, pp. 390–403. Springer, Heidelberg (2012)
14. Ding, X., Tsudik, G.: Simple Identity-Based Cryptography with Mediated RSA. In: Joye, M. (ed.) CT-RSA 2003. LNCS, vol. 2612, pp. 193–210. Springer, Heidelberg (2003)
15. Dodis, Y., Franklin, M., Katz, J., Miyaji, A., Yung, M.: A Generic Construction for Intrusion-Resilient Public-Key Encryption. In: Okamoto, T. (ed.) CT-RSA 2004. LNCS, vol. 2964, pp. 81–98. Springer, Heidelberg (2004)
16. Dodis, Y., Katz, J., Xu, S., Yung, M.: Key-Insulated Public Key Cryptosystems. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 65–82. Springer, Heidelberg (2002)
17. Elwailly, F.F., Gentry, C., Ramzan, Z.: QuasiModo: Efficient Certificate Validation and Revocation. In: Bao, F., Deng, R., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 375–388. Springer, Heidelberg (2004)
18. Gentry, C.: Certificate-Based Encryption and the Certificate Revocation Problem. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 272–293. Springer, Heidelberg (2003)

19. Gentry, C.: Practical Identity-Based Encryption Without Random Oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445–464. Springer, Heidelberg (2006)
20. Goyal, V.: Certificate Revocation Using Fine Grained Certificate Space Partitioning. In: Dietrich, S., Dhamija, R. (eds.) FC 2007 and USEC 2007. LNCS, vol. 4886, pp. 247–259. Springer, Heidelberg (2007)
21. Hanaoka, G., Weng, J.: Generic Constructions of Parallel Key-Insulated Encryption. In: Garay, J.A., De Prisco, R. (eds.) SCN 2010. LNCS, vol. 6280, pp. 36–53. Springer, Heidelberg (2010)
22. Hanaoka, Y., Hanaoka, G., Shikata, J., Imai, H.: Identity-Based Hierarchical Strongly Key-Insulated Encryption and Its Application. In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 495–514. Springer, Heidelberg (2005)
23. Katz, J., Sahai, A., Waters, B.: Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 146–162. Springer, Heidelberg (2008)
24. Lewko, A.: Tools for Simulating Features of Composite Order Bilinear Groups in the Prime Order Setting. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 318–335. Springer, Heidelberg (2012)
25. Lewko, A., Waters, B.: New Techniques for Dual System Encryption and Fully Secure HIBE with Short Ciphertexts. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 455–479. Springer, Heidelberg (2010)
26. Libert, B., Quisquater, J.-J.: Efficient revocation and threshold pairing based cryptosystems. In: PODC 2003, pp. 163–171. ACM (2003)
27. Libert, B., Quisquater, J.-J., Yung, M.: Parallel Key-Insulated Public Key Encryption Without Random Oracles. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 298–314. Springer, Heidelberg (2007)
28. Libert, B., Vergnaud, D.: Adaptive-ID Secure Revocable Identity-Based Encryption. In: Fischlin, M. (ed.) CT-RSA 2009. LNCS, vol. 5473, pp. 1–15. Springer, Heidelberg (2009)
29. Libert, B., Vergnaud, D.: Towards Black-Box Accountable Authority IBE with Short Ciphertexts and Private Keys. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 235–255. Springer, Heidelberg (2009)
30. Micali, S.: Efficient certificate revocation. Technical Report MIT/LCS/TM-542b (1996)
31. Micali, S.: Novomodo: Scalable certificate validation and simplified PKI management. In: PKI Research Workshop (2002)
32. Naor, D., Naor, M., Lotspiech, J.: Revocation and Tracing Schemes for Stateless Receivers. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 41–62. Springer, Heidelberg (2001)
33. Naor, M., Nissim, K.: Certificate revocation and certificate update. IEEE Journal on Selected Areas in Communications 18, 561–570 (2000)
34. González-Nieto, J.M., Manulis, M., Sun, D.: Fully Private Revocable Predicate Encryption. In: Susilo, W., Mu, Y., Seberry, J. (eds.) ACISP 2012. LNCS, vol. 7372, pp. 350–363. Springer, Heidelberg (2012)
35. Okamoto, T., Takashima, K.: Hierarchical Predicate Encryption for Inner-Products. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 214–231. Springer, Heidelberg (2009)
36. Sahai, A., Waters, B.: Fuzzy Identity-Based Encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005)

37. Seo, J.H., Emura, K.: Efficient Delegation of Key Generation and Revocation Functionalities in Identity-Based Encryption. In: Dawson, E. (ed.) CT-RSA 2013. LNCS, vol. 7779, pp. 343–358. Springer, Heidelberg (2013)
38. Waters, B.: Efficient Identity-Based Encryption Without Random Oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005)
39. Weng, J., Liu, S., Chen, K., Ma, C.: Identity-Based Parallel Key-Insulated Encryption Without Random Oracles: Security Notions and Construction. In: Barua, R., Lange, T. (eds.) INDOCRYPT 2006. LNCS, vol. 4329, pp. 409–423. Springer, Heidelberg (2006)
40. Weng, J., Liu, S., Chen, K., Zheng, D., Qiu, W.: Identity-Based Threshold Key-Insulated Encryption without Random Oracles. In: Malkin, T. (ed.) CT-RSA 2008. LNCS, vol. 4964, pp. 203–220. Springer, Heidelberg (2008)