Adaptive-ID Secure Revocable Identity-Based Encryption

Benoît Libert[1] and Damien Vergnaud[2] *

[1] Université Catholique de Louvain, Microelectronics Laboratory, Crypto Group
Place du Levant, 3 – 1348 Louvain-la-Neuve – Belgium
[2] École Normale Supérieure – C.N.R.S. – I.N.R.I.A.
45, Rue d'Ulm – 75230 Paris CEDEX 05 – France

Abstract. Identity-Based Encryption (IBE) offers an interesting alternative to PKI-enabled encryption as it eliminates the need for digital certificates. While revocation has been thoroughly studied in PKIs, few revocation mechanisms are known in the IBE setting. Until quite recently, the most convenient one was to augment identities with period numbers at encryption. All non-revoked receivers were thus forced to obtain a new decryption key at discrete time intervals, which places a significant burden on the authority. A more efficient method was suggested by Boldyreva, Goyal and Kumar at CCS'08. In their *revocable* IBE scheme, key updates have logarithmic (instead of linear in the original method) complexity for the trusted authority. Unfortunately, security could only be proved in the selective-ID setting where adversaries have to declare which identity will be their prey at the very beginning of the attack game. In this work, we describe an adaptive-ID secure *revocable* IBE scheme and thus solve a problem left open by Boldyreva *et al.*.

Keywords. Identity-based encryption, revocation, provable security.

1 Introduction

Introduced by Shamir [35] and conveniently implemented by Boneh and Franklin [9], identity-based encryption (IBE) aims to simplify key management by using human-intelligible identifiers (e.g. email addresses) as public keys, from which corresponding private keys are derived by a trusted authority called Private Key Generator (PKG). Despite its many appealing advantages, it makes it difficult to accurately control users' decryption capabilities or revoke compromised identities. While IBE has been extensively studied using pairings (see [13] and references therein) or other mathematical tools [20, 10], little attention has been paid to the efficient implementation of identity revocation until very recently [5].

Related work. In public key infrastructures (PKI), revocation is taken care of either via certificate revocation lists (CRLs), by appending validity periods to certificates or using involved combinations of such techniques (e.g. [32, 1, 33, 24, 28]). However, the cumbersome management of certificates is precisely the burden that identity-based encryption strives to alleviate. Yet, the private key capabilities of misbehaving/compromised users should be promptly disabled after their detection. One of the cited reasons for the slow adoption of the IBE technology among standards is its lack of support for identity revocation. Since *only* the PKG's public key and the recipient's identity should be needed to encrypt, there is no way to notify senders that a specific identity was revoked.

To address this issue, Boneh and Franklin [9] suggested that users can periodically receive new private keys. Current validity periods are then appended to identities upon encryption so as to add timeliness to the decryption operation and provide automatic identity revocation: to revoke a specific user, the PKG simply stops issuing new keys for his identity. Unfortunately,

* The first author acknowledges the Belgian National Fund for Scientific Research (F.R.S.-F.N.R.S.) for their financial support and the BCRYPT Interuniversity Attraction Pole. The second author is supported by the European Commission through the IST Program under Contract ICT-2007-216646 ECRYPT II and by the French *Agence Nationale de la Recherche* through the PACE project.

this solution requires the PKG to perform linear work in the number of registered receivers and regularly generate fresh private keys for all users, which does not scale well as their number grows: each non-revoked user must obtain a new key at each period, which demands to prove his identity to the PKG and establish a secure channel to fetch the key.

Other solutions were suggested [8, 23, 30, 2] to provide immediate revocation but they require the cooperation of an online semi-trusted party (called mediator) at each decryption, which is not totally satisfactory either since it necessarily incurs communication between users and the mediator.

Recently, Boldyreva, Goyal and Kumar [5] (BGK) significantly improved the technique suggested by Boneh and Franklin [9] and reduced the authority's periodic workload to be logarithmic (instead of linear) in the number of users while keeping the scheme efficient for senders and receivers. Their *revocable* IBE primitive (or R-IBE for short) uses a binary tree data structure and also builds on Fuzzy Identity-Based Encryption (FIBE) schemes that were introduced by Sahai and Waters [34]. Unfortunately, their R-IBE scheme only offers security guarantees in the relaxed selective-ID model [17, 18] wherein adversaries must choose the target identity ahead of time (even before seeing the system-wide public key). The reason is that current FIBE systems are only secure in (a natural analogue of) the selective-ID model. Boldyreva *et al.* explicitly left open the problem of avoiding this limitation using their approach.

As noted in [6, 7], selective-ID secure schemes can give rise to fully secure ones, but only under an exponential reduction in the size of the identity space. Also, while a random-oracle-using [4] transformation was reported [6] to turn any selective-ID secure IBE scheme into an adaptive-ID secure one, it entails a degradation factor of q_H (*i.e.*, the number of random oracle queries) in the reduction and additionally fails to provide "real-world" security guarantees [16]. In the standard model, it has even been shown [25] that the strongest flavor of selective-ID security (*i.e.*, the IND-sID-CCA one that captures chosen-ciphertext adversaries) does not even imply the weakest form of adaptive-ID security (which is the one-wayness against chosen-plaintext attacks).

Our Contribution. We describe an IBE scheme endowed with a similar and equally efficient revocation mechanism as in the BGK system while reaching security in the stronger *adaptive*-ID sense (as originally defined by Boneh and Franklin [9]), where adversaries choose the target identity in the challenge phase. We emphasize that, although relatively loose, the reduction is polynomial in the number of adversarial queries. Our construction uses the same binary tree structure as [5] and applies the same revocation technique. Instead of FIBE systems, we utilize a recently considered variant [31] of the Waters IBE [36]. To obtain a fairly simple security reduction, we use the property that the simulator is able to compute at least one private key for each identity. This notably brings out the fact that ordinary (as opposed to fuzzy) IBE systems can supersede the particular instance of FIBE scheme considered in [5] to achieve revocation. From an efficiency standpoint, our R-IBE performs essentially as well as the BGK construction.

Organization. Section 2 first recalls the syntax and the security model of the R-IBE primitive. Section 3 explains the BGK revocation technique that we also use. Our scheme and its security analysis and then detailed in section 4.

2 Definitions

Model and Security Definitions. We recall the definition of R-IBE schemes and their security properties as defined in [5].

Definition 1. *An* identity-based encryption with efficient revocation*, or simply* Revocable IBE *(R-IBE) scheme is a 7-tuple* $(\mathcal{S}, \mathcal{SK}, \mathcal{KU}, \mathcal{DK}, \mathcal{E}, \mathcal{D}, \mathcal{R})$ *of efficient algorithms with associated message space* $\mathcal{M}$*, identity space* $\mathcal{I}$ *and time space* $\mathcal{T}$*:*

- *The **Setup** algorithm $\mathcal{S}$ is run by a key authority*[3]*. Given a security parameter λ and a maximal number of users N, it outputs a master public/secret key pair $(\mathsf{mpk}, \mathsf{msk})$, an initial state st and an empty revocation list RL.*
- *The stateful **Private Key Generation** algorithm $\mathcal{SK}$ is run by the key authority that takes as input the system master key pair $(\mathsf{mpk}, \mathsf{msk})$, an identity $id \in \mathcal{I}$ and state st and outputs a private key d_{id} and an updated state st.*
- *The **Key Update Generation** algorithm $\mathcal{KU}$ is used by the key authority. Given the master public and secret keys $(\mathsf{mpk}, \mathsf{msk})$, a key update time $t \in \mathcal{T}$, a revocation list RL and a state st, it publishes a key update ku_t.*
- *The **Decryption Key Generation** algorithm $\mathcal{DK}$ is run by the user. Given a private key d_{id} and a key update ku_t, it outputs a decryption key $d_{id,t}$ to be used during period t or a special symbol $\perp$ indicating that id was revoked.*
- *The randomized **Encryption** algorithm $\mathcal{E}$ takes as input the master public key mpk, an identity $id \in \mathcal{I}$, an encryption time $t \in \mathcal{T}$, and a message $m \in \mathcal{M}$ and outputs a ciphertext c. For simplicity and w.l.o.g. we assume that id and t are efficiently computable from c.*
- *The deterministic **Decryption** algorithm $\mathcal{D}$ takes as input a decryption key $d_{id,t}$ and a ciphertext c, and outputs a message $m \in \mathcal{M}$ or a special symbol $\perp$ indicating that the ciphertext is invalid.*
- *The stateful **Revocation** algorithm $\mathcal{R}$ takes as input an identity to be revoked $id \in \mathcal{I}$, a revocation time $t \in \mathcal{T}$, a revocation list RL and state st, and outputs an updated revocation list RL.*

Correctness requires that, for any outputs $(\mathsf{mpk}, \mathsf{msk})$ of $\mathcal{S}$, any $m \in \mathcal{M}$, any $id \in \mathcal{I}$ and $t \in \mathcal{T}$, all possible states st and revocation lists RL, if id is not revoked by time t, then for $(d_{id}, st) \leftarrow \mathcal{SK}(\mathsf{mpk}, \mathsf{msk}, id, st)$, $ku_t \leftarrow \mathcal{KU}(\mathsf{mpk}, \mathsf{msk}, t, RL, st)$, $d_{id,t} \leftarrow \mathcal{DK}(d_{id}, ku_t)$ we have $\mathcal{D}(d_{id,t}, \mathcal{E}(\mathsf{mpk}, id, t, m)) = m$.

Boldyreva *et al.* formalized the *selective-revocable-ID* security property that captures the usual notion of selective-ID[4] security but also takes revocations into account. In addition to a private key generation oracle $\mathcal{SK}(.)$ that outputs private keys for identities of her choosing, the adversary is allowed to revoke users at will using a dedicated oracle $\mathcal{R}(.,.)$ (taking as input identities id and period numbers t) and can obtain key update information (which is assumed to be public) for any period t via queries $\mathcal{KU}(t)$ to another oracle. The following definition extends the security property expressed in [5] to the adaptive-ID setting.

Definition 2. *A R-IBE scheme is* revocable-ID *secure if any probabilistic polynomial time (PPT) adversary $\mathcal{A}$ has negligible advantage in this experiment:*

```
$\boxed{\mathbf{Expt}_{\mathcal{A}}^{\text{IND-RID-CPA}}(\lambda)}$
$(\mathsf{mpk}, \mathsf{msk}, RL, st) \leftarrow \mathcal{S}(\lambda, n)$
$(m_0, m_1, id^\star, t^\star, s) \leftarrow \mathcal{A}^{\mathcal{SK}(\cdot), \mathcal{KU}(\cdot), \mathcal{R}(\cdot,\cdot)}(\mathsf{find}, \mathsf{mpk})$
$d^\star \xleftarrow{R} \{0, 1\}$
$c^\star \leftarrow \mathcal{E}(\mathsf{mpk}, id^\star, t^\star, m_{d^\star})$
$d \leftarrow \mathcal{A}^{\mathcal{SK}(\cdot), \mathcal{KU}(\cdot), \mathcal{R}(\cdot,\cdot)}(\mathsf{guess}, s, c^\star)$
$\textit{return } 1 \textit{ if } d = d^\star \textit{ and } 0 \textit{ otherwise.}$
```

Beyond $m_0, m_1 \in \mathcal{M}$ and $|m_0| = |m_1|$, the following restrictions are made:

[3] We follow [5] and call the trusted authority "key authority" instead of "PKG".

[4] Considered by Canetti, Halevi and Katz [17, 18], this relaxed notion forces the adversary to choose the target identity before seeing the master public key.

1. *$\mathcal{KU}(\cdot)$ and $\mathcal{R}(\cdot,\cdot)$ can be queried on time which is greater than or equal to the time of all previous queries i.e. the adversary is allowed to query only in non-decreasing order of time. Also, $\mathcal{R}(\cdot,\cdot)$ cannot*[5] *be queried on time t if $\mathcal{KU}(\cdot)$ was queried on t.*
2. *If $\mathcal{SK}(\cdot)$ was queried on identity $id^\star$ then $\mathcal{R}(\cdot,\cdot)$ must be queried on $(id^\star, t)$ for some $t \leq t^\star$.*

$\mathcal{A}$'s advantage is $\mathbf{Adv}_{\mathcal{A}}^{\text{IND-RID-CPA}}(\lambda) = \big|\Pr[\mathbf{Expt}_{\mathcal{A}}^{\text{IND-RID-CPA}}(\lambda) = 1] - \frac{1}{2}\big|$.

This definition naturally extends to the *chosen-ciphertext* scenario where the adversary is further granted access to a decryption oracle $\mathcal{D}(\cdot)$ that, on input of a ciphertext c and a pair (id, t), runs $\mathcal{D}(d_{id,t}, c)$ to return some $m \in \mathcal{M}$ or $\perp$. Of course, $\mathcal{D}(\cdot)$ cannot be queried on the ciphertext $c^\star$ for the pair $(id^\star, t^\star)$.

Bilinear Maps and Hardness Assumptions. We use prime order groups $(\mathbb{G}, \mathbb{G}_T)$ endowed with an efficiently computable map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ such that:

1. $e(g^a, h^b) = e(g, h)^{ab}$ for any $(g, h) \in \mathbb{G} \times \mathbb{G}$ and $a, b \in \mathbb{Z}$;
2. $e(g, h) \neq 1_{\mathbb{G}_T}$ whenever $g, h \neq 1_{\mathbb{G}}$.

In such *bilinear groups*, we rely on a variant of the (now classical) Decision Bilinear Diffie-Hellman (DBDH) problem.

Definition 3. *Let $(\mathbb{G}, \mathbb{G}_T)$ be bilinear groups of prime order $p > 2^\lambda$ and $g \in \mathbb{G}$. The* **modified Decision Bilinear Diffie-Hellman Problem** *(mDBDH) is to distinguish the distributions $(g^a, g^b, g^c, e(g, g)^{bc/a})$ and $(g^a, g^b, g^c, e(g, g)^d)$ for random values $a, b, c, d \xleftarrow{R} \mathbb{Z}_p^*$. The advantage of a distinguisher $\mathcal{B}$ is*

$$\begin{aligned}\mathbf{Adv}_{\mathbb{G},\mathbb{G}_T}^{\text{mDBDH}}(\lambda) = \big|&\Pr[a, b, c \xleftarrow{R} \mathbb{Z}_p^* : \mathcal{B}(g^a, g^b, g^c, e(g, g)^{bc/a}) = 1] \\ &- \Pr[a, b, c, d \xleftarrow{R} \mathbb{Z}_p^* : \mathcal{B}(g^a, g^b, g^c, e(g, g)^d) = 1]\big|.\end{aligned}$$

This problem is equivalent (see [19, Lemma 3.1] for a proof) to the original DBDH problem which is to tell apart $e(g, g)^{abc}$ from random given (g^a, g^b, g^c).

3 The BGK Construction

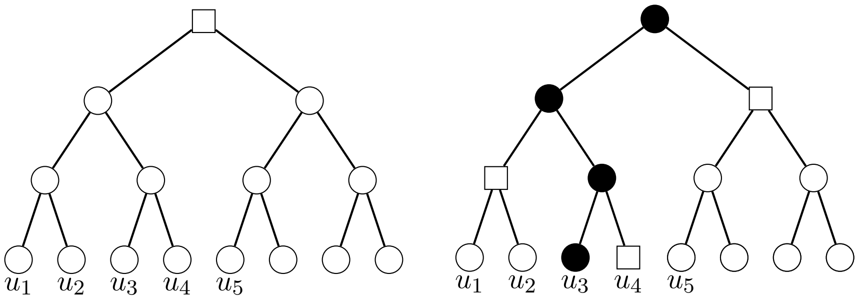
The idea of the scheme described by Boldyreva, Goyal and Kumar consists in assigning users to the leaves of a complete binary tree. Upon registration, the key authority provides them with a set of distinct private keys (all corresponding to their identity) for each node on the path from their associated leaf to the root of the tree. During period t, a given user's decryption key can be obtained by suitably combining any one of its node private keys with a key update for period t and associated with the *same* node of the tree.

At period t, the key authority publishes key updates for a set Y of nodes that contains no ancestors of revoked users and exactly one ancestor of any non-revoked one (so that, when no user is revoked, Y contains only the root node as illustrated on the figure where the nodes of Y are the squares). Then, a user assigned to leaf v is able to form an effective decryption key for period t if the set Y contains a node on the path from the root to v. By doing so, every update of the revocation list RL only requires the key authority to perform logarithmic work in the overall number of users. The size of users' private keys also logarithmically depends on the maximal number of users but, when the number of revoked users is reasonably small (as is likely to be the case in practice since one can simply re-initialize the whole system otherwise),

[5] As in [5], we assume that revocations are made effective before that key updates are published at each time period. Otherwise, $\mathcal{A}$ could trivially win the game by corrupting and revoking $id^\star$ at period $t^\star$ but *after* having queried $\mathcal{KU}(t^\star)$.

the revocation method is much more efficient than the one initially suggested in [9].

Another attractive feature of this technique is that it can be used for temporary revocation. When a key is suspected of being compromised, the matching identity can be temporarily revoked while an investigation is conducted, and then reinstated if necessary.



No user is revoked

User u_3 is revoked

The scheme of Boldyreva *et al.* builds on the fuzzy identity-based encryption (FIBE) primitive [34]. In FIBE systems, identities are seen as sets of descriptive attributes and users' keys can decrypt ciphertexts for which a certain threshold (called the "error tolerance") of attributes match between the ciphertext and the key. The private key of an identity (*i.e.*, a set of attributes) is generated using a new polynomial (of degree one less than the error tolerance) whose constant term is part of the master key of the scheme. The revocable IBE scheme of [5] uses a special kind of fuzzy IBE where ciphertexts are encrypted using the receiver's identity and the period number as "attributes". The decryption key of the receiver has to match both attributes to decrypt the ciphertext. For each node on the path from the root to its assigned leaf, the user is given a key attribute that is generated using a new polynomial of degree 1 for which the constant term is always the master secret. The same polynomials are used, for each node, to generate key updates. To compute a decryption key for period t, each user thus needs to combine two key attributes associated with the *same* node of the tree.

To date, existing FIBE schemes are only provably secure in the selective-ID sense and the construction of [5] has not been extended to the adaptive-ID model. As we will see, classical pairing-based IBE systems actually allow instantiating the same underlying revocation mechanism in the adaptive-ID setting.

4 An Adaptive-ID Secure Scheme

4.1 Intuition

We start from the same general idea as Boldyreva *et al.* but, instead of using fuzzy identity-based cryptosystems, we build on a recently suggested [31] variant of Waters' IBE [36] where, somewhat in the fashion of Gentry's IBE [26], the simulator is able to compute a decryption key for any identity in the security proof. In this variant, the master public key consists of $(X = g^x, Y, h) \in \mathbb{G}^3$ and a vector $\overline{u} = (u_0, u_1, \ldots, u_n) \in \mathbb{G}_1^{n+1}$ implementing Waters' "hashing" technique that maps strings $id = i_1 \ldots i_n \in \{0,1\}^n$ onto $F_u(id) = u_0 \cdot \prod_{j=1}^n u_i^{i_j}$. To derive a private key for the identity id, the authority picks $r, s \xleftarrow{R} \mathbb{Z}_p^*$ and sets

$$d_{id} = (d_1, d_2, d_3) = \big((Y \cdot h^r)^{1/x} \cdot F_u(id)^s,\ X^s,\ r\big)$$

so that $e(d_1, X) = e(Y, g) \cdot e(h, g)^{d_3} \cdot e(F(id), d_2)$. Ciphertexts are encrypted as

$$C = (C_0, C_1, C_2, C_3) = \big(m \cdot e(Y, g)^z,\ X^z,\ F_u(id)^z,\ e(g, h)^z\big)$$

and decrypted by computing $m = C_0 \cdot e(C_2, d_2) \cdot C_3^{d_3} / e(C_1, d_1)$ (the correctness can be checked by noting that $e(d_1, X)^z = e(Y, g)^z \cdot e(h, g)^{zd_3} \cdot e(F(id), d_2)^z$).

We consider a two-level hierarchical extension of the above system where the second level identity is the period number. The shape of private keys thus becomes $(d_1, d_2, d_3, d_4) = \big((Y \cdot h^r)^{1/x} \cdot F_u(id)^{s_1} \cdot F_v(t)^{s_2},\ X^{s_1},\ X^{s_2},\ r\big)$ for some function $F_v(t)$. Since we only need a polynomial number of time periods, we can settle for the Boneh-Boyen selective-ID secure identity hashing $F_v(id) = v_0^{id} \cdot v_1$ [6], for some $v_0, v_1 \in \mathbb{G}$, at level 2 (instead of Waters' technique).

Then, we also assign users to the leaves of a binary tree T. For each node $\theta \in \mathsf{T}$, the key authority splits $Y \in \mathbb{G}$ into new shares $Y_{1,\theta}, Y_{2,\theta}$ such that $Y = Y_{1,\theta} \cdot Y_{2,\theta}$. To derive users' private keys, the key authority computes a triple $(d_{1,\theta}, d_{2,\theta}, d_{3,\theta}) = \big((Y_{1,\theta} \cdot h^{r_{1,\theta}})^{1/x} \cdot F_u(id)^{s_{1,\theta}},\ X^{s_{1,\theta}},\ r_{1,\theta}\big)$ for each node θ on the path from the root to the leaf corresponding to the user. Key updates are triples $(ku_{1,\theta}, ku_{2,\theta}, ku_{3,\theta}) = \big((Y_{2,\theta} \cdot h^{r_{2,\theta}})^{1/x} \cdot F_v(t)^{s_{2,\theta}},\ X^{s_{2,\theta}},\ r_{2,\theta}\big)$ associated with non-revoked nodes $\theta \in \mathsf{T}$ during period t. Users' decryption keys can be obtained by combining any two such triples $(d_{1,\theta}, d_{2,\theta}, d_{3,\theta})$, $(ku_{1,\theta}, ku_{2,\theta}, ku_{3,\theta})$ for the same node θ. Revocation is handled as in [5], by having the key authority stop issuing key updates for nodes outside the set Y.

In the selective-ID sense, the binary tree technique of [5] can be applied to a 2-level extension of the Boneh-Boyen HIBE by sharing the master secret key in a two-out-of-two fashion, using new shares for each node. Directly extending the technique to the adaptive-ID setting with Waters' IBE is not that simple. In the security reduction of [36], the simulator does not know the master key or the private key of the target identity. The difficulty that we are faced with is that, at the first time that a tree node is involved in a private key query or a key update query, the simulator has to decide which one of the two master key shares it will have to know for that node. This is problematic when the target identity $id^\star$ is not known and has not been assigned a leaf yet: which share should be known actually depends on whether the considered node lies on the path connecting the target identity to the root of the tree. To address this issue, we used a variant of the Waters IBE where the simulator knows at least one valid decryption key for each identity[6] and can answer queries regardless of whether nodes are on the path from $id^\star$ to the root.

4.2 Description

The scheme uses the same binary tree structure as in [5] and we employ similar notations. Namely, root denotes the root node of the tree T. If v is a leaf node, we let $\mathsf{Path}(v)$ stand for the set of nodes on the path from v to root. Whenever θ is a non-leaf node, θ_l and θ_r respectively denote its left and right children.

In the description hereafter, we use the same node selection algorithm (called $\mathsf{KUNodes}$) as in [5]. At each time period, this algorithm determines the smallest subset $\mathsf{Y} \subset \mathsf{T}$ of nodes that contains an ancestor of all leaves corresponding to non-revoked users. This minimal set precisely contains nodes for which key updates have to be publicized in such a way that only non-revoked users will be able to generate the appropriate decryption key for the matching period.

To identify the set Y, $\mathsf{KUNodes}$ takes as input the tree T, the revocation list RL and a period number t. It first marks (in black on the figure) all ancestors of users that were revoked by time t as revoked nodes. Then, it inserts in Y the non-revoked children of revoked nodes. Its formal specification is the following:

[6] After the completion of the paper, we noticed that a 2-level instance of the original Waters HIBE can be used and allows for shorter ciphertexts. As will be shown in an updated version of this work, it unfortunately ends up with an equally loose reduction since the simulator has to guess upfront which private key query (if any) will involve the target identity.

```
$\mathsf{KUNodes}(\mathsf{T}, RL, t)$
  $\mathsf{X}, \mathsf{Y} \leftarrow \emptyset$
  $\forall (v_i, t_i) \in RL$
    if $t_i \leq t$ then add $\mathsf{Path}(v_i)$ to $\mathsf{X}$
  $\forall \theta \in \mathsf{X}$
    if $\theta_l \notin \mathsf{X}$ then add $\theta_l$ to $\mathsf{Y}$
    if $\theta_r \notin \mathsf{X}$ then add $\theta_r$ to $\mathsf{Y}$
  If $\mathsf{Y} = \emptyset$ then add $\mathsf{root}$ to $\mathsf{Y}$
  Return $\mathsf{Y}$
```

As in [5], we assume that the number of time periods t_{max} is polynomial in the security parameter λ, so that a degradation of $O(1/t_{max})$ in the security reduction is acceptable.

Setup $\mathcal{S}(\lambda, n, N)$: given security parameters $\lambda, n \in \mathbb{N}$ and a maximal number of users $N \in \mathbb{N}$ that the scheme must be prepared for, the key authority defines $\mathcal{I} = \{0,1\}^n$, $\mathcal{T} = \{1, \ldots, t_{max}\}$ and does the following.

1. Select bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order $p > 2^\lambda$ with $g \xleftarrow{R} \mathbb{G}^*$.
2. Randomly choose $x \xleftarrow{R} \mathbb{Z}_p^*$, $h, Y \xleftarrow{R} \mathbb{G}^*$ as well as two random vectors $\overline{u} = (u_0, u_1, \ldots, u_n) \in \mathbb{G}^{*n+1}$ and $\overline{v} = (v_0, v_1) \in \mathbb{G}^{*2}$ that define functions $F_u : \mathcal{I} \to \mathbb{G}$, $F_v : \mathcal{T} \to \mathbb{G}$ such that, when $id = i_1 \ldots i_n \in \mathcal{I} = \{0,1\}^n$,
$$F_u(id) = u_0 \cdot \prod_{j=1}^{n} u_j^{i_j} \qquad\qquad F_v(t) = v_0^t \cdot v_1$$
3. Set the master key as $\mathsf{msk} := x$ and initialize a revocation list $RL := \emptyset$ and a state $st = \mathsf{T}$ consisting of a binary tree T with $N < 2^n$ leaves.
4. Define the master public key to be $\mathsf{mpk} := (X = g^x, Y, h, \overline{u}, \overline{v})$.

Private Key Generation $\mathcal{SK}(\mathsf{mpk}, \mathsf{msk}, id, st)$: Parse mpk as $(X, Y, h, \overline{u}, \overline{v})$, msk as x and st as T.

1. Choose an unassigned leaf v from T and associate it with $id \in \{0,1\}^n$.
2. For all nodes $\theta \in \mathsf{Path}(v)$ do the following:
   a. Retrieve $Y_{1,\theta}$ from T if it was defined[7]. Otherwise, choose it at random $Y_{1,\theta} \xleftarrow{R} \mathbb{G}$, set $Y_{2,\theta} = Y/Y_{1,\theta}$ and store the pair $(Y_{1,\theta}, Y_{2,\theta}) \in \mathbb{G}^2$ at node θ in $st = \mathsf{T}$.
   b. Pick $s_{1,\theta}, r_{1,\theta} \xleftarrow{R} \mathbb{Z}_p^*$ and set
$$d_{id,\theta} = (d_{1,\theta}, d_{2,\theta}, r_{1,\theta}) = \Big((Y_{1,\theta} \cdot h^{r_{1,\theta}})^{1/x} \cdot F_u(id)^{s_{1,\theta}},\ X^{s_{1,\theta}},\ r_{1,\theta} \Big).$$
3. Return $d_{id} = \{(\theta, d_{id,\theta})\}_{\theta \in \mathsf{Path}(v)}$ and the updated state $st = \mathsf{T}$.

Key Update Generation $\mathcal{KU}(\mathsf{mpk}, \mathsf{msk}, t, RL, st)$: Parse mpk as $(X, Y, h, \overline{u}, \overline{v})$, msk as x and st as T. For all nodes $\theta \in \mathsf{KUNodes}(\mathsf{T}, RL, t)$,

1. Fetch $Y_{2,\theta}$ from T if it was previously defined. If not, choose a fresh pair $(Y_{1,\theta}, Y_{2,\theta}) \in \mathbb{G}^2$ such that $Y = Y_{1,\theta} \cdot Y_{2,\theta}$ and store it in θ.
2. Choose $s_{2,\theta}, r_{2,\theta} \xleftarrow{R} \mathbb{Z}_p^*$ and compute
$$ku_{t,\theta} = (ku_{1,\theta}, ku_{2,\theta}, r_{2,\theta}) = \Big((Y_{2,\theta} \cdot h^{r_{2,\theta}})^{1/x} \cdot F_v(t)^{s_{2,\theta}},\ X^{s_{2,\theta}},\ r_{2,\theta} \Big).$$

Then, return $ku_t = \{(\theta, ku_{t,\theta})\}_{\theta \in \mathsf{KUNodes}(\mathsf{T}, RL, t)}$ and the updated $st = \mathsf{T}$.

[7] To avoid having to store $Y_{1,\theta}$ for each node, the authority can derive it from a pseudo-random function of θ using a shorter seed and re-compute it when necessary.

Decryption Key Generation $\mathcal{DK}(\mathsf{mpk}, d_{id}, ku_t)$**:** Parse d_{id} into $\{(i, d_{id,i})\}_{i\in \mathsf{I}}$ and ku_t as $\{(j, ku_{t,j})\}_{j\in \mathsf{J}}$ for some sets of nodes $\mathsf{I}, \mathsf{J} \in \mathsf{T}$. If there exists no pair $(i,j) \in \mathsf{I} \times \mathsf{J}$ such that $i = j$, return $\perp$. Otherwise, choose an arbitrary such pair $i = j$, parse $d_{id,i} = (d_{1,i}, d_{2,i}, r_{1,i})$, $ku_{t,i} = (ku_{1,i}, ku_{2,i}, r_{2,i})$ and set the updated decryption key as

$$\begin{aligned} d_{id,t} &= \big(d_{t,1},\ d_{t,2},\ d_{t,3},\ d_{t,4}\big) = \big(d_{1,i} \cdot ku_{1,i},\ d_{2,i},\ ku_{2,i},\ r_{1,i} + r_{2,i}\big) \\ &= \Big((Y \cdot h^{d_{t,4}})^{1/x} \cdot F_u(id)^{s_{1,i}} \cdot F_v(t)^{s_{2,i}},\ X^{s_{1,i}},\ X^{s_{2,i}}, d_{t,4}\Big). \end{aligned}$$

Finally, check that $d_{id,t}$ satisfies

$$e(d_{t,1}, X) = e(Y, g) \cdot e(g, h)^{d_{t,4}} \cdot e(F_u(id), d_{t_2}) \cdot e(F_v(t), d_{t,3}) \qquad (1)$$

and return $\perp$ if the above condition fails to hold. Otherwise return $d_{id,t}$.

Encryption $\mathcal{E}(\mathsf{mpk}, id, t, m)$**:** to encrypt $m \in \mathbb{G}_T$ for $id = i_1 \ldots i_n \in \{0,1\}^n$ during period t, choose $z \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and compute

$$\begin{aligned} C &= \big(id, t, C_0, C_1, C_2, C_3, C_4\big) \\ &= \Big(id,\ t,\ m \cdot e(g, Y)^z,\ X^z,\ F_u(id)^z,\ F_v(t)^z,\ e(g, h)^z\Big). \end{aligned}$$

Decryption $\mathcal{D}(\mathsf{mpk}, d_{id,t}, C)$**:** Parse C as $\big(id, t, C_0, C_1, C_2, C_3, C_4\big)$ and the decryption key $d_{id,t}$ as $(d_{t,1}, d_{t,2}, d_{t,3}, d_{t,4})$. Then, compute and return

$$m = C_0 \cdot \Big(\frac{e(C_1, d_{t,1})}{e(C_2, d_{t,2}) \cdot e(C_3, d_{t,3}) \cdot C_4^{d_{t,4}}}\Big)^{-1}. \qquad (2)$$

Revocation $\mathcal{R}(\mathsf{mpk}, id, t, RL, st)$**:** let v be the leaf node associated with id. To revoke the latter at period t, add (v, t) to RL and return the updated RL.

Correctness. We know that well-formed decryption keys always satisfy relation (1). If we raise both members of (1) to the power $z \in \mathbb{Z}_p^*$ (*i.e.*, the encryption exponent), we see that the quotient of pairings in (2) actually equals $e(g, Y)^z$.

Efficiency. The efficiency of the scheme is comparable to that of the revocable IBE described in [5]: ciphertexts are only slightly longer (by an extra element of $\mathbb{G}_T$) and decryption is even slightly faster since it incurs the evaluation of a product of only 3 pairings (against 4 in [5]). Both schemes feature the same logarithmic complexity in the number of users in terms of private key size and space/computational cost for issuing key updates.

4.3 Security

The security proof is based on the one of [31] with the difference that we have to consider the case where the challenge identity is compromised at some point but revoked for the period during which the challenge ciphertext is created.

Theorem 1. *Let us assume that an IND-RID-CPA adversary $\mathcal{A}$ runs in time ζ and makes at most q private key queries over t_{max} time periods. Then, there exists an algorithm $\mathcal{B}$ solving the mDBDH problem with advantage $\mathbf{Adv}_{\mathcal{B}}^{\mathrm{mDBDH}}(\lambda)$ and within running time $O(\zeta) + O(\varepsilon^{-2} \ln \delta^{-1})$ for sufficiently small ε and δ. The advantage of $\mathcal{A}$ is then bounded by*

$$\mathbf{Adv}_{\mathcal{A}}^{\text{IND-RID-CPA}}(\lambda) \leq 4 \cdot t_{max} \cdot q^2 \cdot (n+1) \cdot \Big(4 \cdot \mathbf{Adv}^{\mathrm{mDBDH}}(\lambda) + \delta\Big). \qquad (3)$$

Proof (sketch). The complete proof is deferred to the full version of the paper due to space limitation but we give its intuition here. We construct a simulator $\mathcal{B}$ that is given a tuple (g^a, g^b, g^c, T) and uses the adversary $\mathcal{A}$ to decide if $T = e(g,g)^{bc/a}$. The master public key is prepared as $X = g^a$, $h = g^b$ and $Y = X^{\gamma} \cdot h^{-r^\star}$ for random $\gamma, r^\star \xleftarrow{R} \mathbb{Z}_p^*$. The vector $\overline{v} = (v_0, v_1)$ is chosen so that $F_v(t) = g^{\beta(t-t^\star)} \cdot X^{\alpha}$ for random values $\alpha, \beta \xleftarrow{R} \mathbb{Z}_p^*$ and where $t^\star \xleftarrow{R} \{1, \ldots, t_{max}\}$ is chosen at random as a guess for the time period of the challenge phase. Finally, the $(n+1)$-vector $\overline{u}$ is chosen so as to have $F_u(id) = g^{J(id)} \cdot X^{K(id)}$ for some integer-valued functions $J, K : \{0,1\}^n \rightarrow \mathbb{Z}$ chosen by the simulator according to Waters' technique [36].

To be successful, $\mathcal{B}$ needs to have $J(id^\star) = 0$ in the challenge phase and, by choosing $\overline{u}$ such that $J(.)$ is relatively small in absolute value, this will be the case with probability $O(1/q(n+1))$. The simulator also hopes that $\mathcal{A}$ will indeed make her challenge query for period $t^\star$, which occurs with probability $1/t_{max}$. The security proof relies on the fact that, with non-negligible probability, $\mathcal{B}$ can compute a valid decryption key for each identity $id \in \{0,1\}^n$. If $J(id) \neq 0$, $\mathcal{B}$ can do it using the Boneh-Boyen technique [6] while, in the case $J(id) = 0$, a valid key $d_{id,t}$ for period t is obtained by choosing $s_1, s_2 \xleftarrow{R} \mathbb{Z}_p^*$ and setting

$$(d_{t,1}, d_{t,2}, d_{t,3}, d_{t,4}) = \big(g^{\gamma} \cdot F_u(id)^{s_1} \cdot F_v(t)^{s_2},\ X^{s_1},\ X^{s_2},\ r^\star\big), \tag{4}$$

which has the required shape since $(Y \cdot h^{r^\star})^{1/a} = g^{\gamma}$.

In the challenge phase, when $\mathcal{A}$ hopefully comes up with a pair $(id^\star, t^\star)$ such that $J(id^\star) = 0$ and $t^\star$ is the expected time period, $\mathcal{B}$ flips a coin $d^\star \xleftarrow{R} \{0,1\}$ and constructs the ciphertext $C^\star$ as follows:

$$C_1^\star = g^c \qquad C_2^\star = (g^c)^{K(id^\star)} \qquad C_3^\star = (g^c)^{\alpha} \qquad C_4^\star = T$$

$$C_0^\star = m_{d^\star} \cdot \frac{e(C_1^\star, d_{t^\star,1})}{e(C_2^\star, d_{t^\star,2}) \cdot e(C_3^\star, d_{t^\star,3}) \cdot C_4^{\star d_{t^\star,4}}} \tag{5}$$

where $d_{id^\star,t^\star} = (d_{t^\star,1}, d_{t^\star,2}, d_{t^\star,3}, d_{t^\star}, 4)$ is a valid decryption key calculated as per (4) for the pair $(id^\star, t^\star)$. If T actually equals $e(g,g)^{bc/a}$, $C^\star$ is easily seen to be a valid encryption of $m_{d^\star}$ using the encryption exponent $z = c/a$. If T is random on the other hand (say $T = e(g,h)^{z'}$ for a random $z' \in_R \mathbb{Z}_p^*$), we can check that $C_0^\star = m_{d^\star} \cdot e(Y,g)^z \cdot e(g,h)^{(z-z')r^\star}$, which means that $m_{d^\star}$ is perfectly hidden from $\mathcal{A}$'s view as long as $r^\star$ is so.

We now have to make sure that no information on $r^\star$ ever leaks during the game. To do so, we distinguish two kinds of adversaries:

- Type I adversaries choose to be challenged on an identity $id^\star$ that is corrupted at some point of the game but is revoked at period $t^\star$ or before.
- Type II adversaries do not corrupt the target identity $id^\star$ at any time.

At the outset of the game, the simulator $\mathcal{B}$ flips a coin $c_{mode} \xleftarrow{R} \{0,1\}$ as a guess for the type of adversarial behavior that it will be faced with. In the expectation of Type I adversary (*i.e.*, $c_{mode} = 0$), $\mathcal{B}$ additionally has to guess which private key query will involve the identity $id^\star$ that $\mathcal{A}$ chooses to be challenged upon. If $c_{mode} = 0$, it thus draws $j^\star \xleftarrow{R} \{1, \ldots, q\}$ at the beginning of the game and the input id_j of the j^{th} private key query happens to be $id^\star$ with probability $1/q$.

Regardless of the value of c_{mode}, for each tree node $\theta \in \mathsf{T}$, $\mathcal{B}$ splits the public key element $Y \in \mathbb{G}$ into two node-specific multiplicative shares $(Y_{1,\theta}, Y_{2,\theta})$ such that $Y = Y_{1,\theta} \cdot Y_{2,\theta}$. That is, at the first time that a node $\theta \in \mathsf{T}$ is involved in some query, $\mathcal{B}$ defines and stores exponents $\gamma_{1,\theta}, \gamma_{2,\theta}, r^\star_{1,\theta}, r^\star_{2,\theta}$ such that $\gamma = \gamma_{1,\theta} + \gamma_{2,\theta}$, $r^\star = r^\star_{1,\theta} + r^\star_{2,\theta}$ and defines $Y_{1,\theta} = X^{\gamma_{1,\theta}} \cdot h^{-r^\star_{1,\theta}}$,

$Y_{2,\theta} = X^{\gamma_{2,\theta}} \cdot h^{-r^\star_{2,\theta}}$.

From here on, we assume that $\mathcal{B}$ is fortunate in the random guesses that it makes (*i.e.*, $c_{mode} \in \{0,1\}$ and $j^\star \xleftarrow{R} \{1,\ldots,q\}$ if $c_{mode} = 0$). Then, the treatment of $\mathcal{A}$'s queries is the following. Revocation queries are dealt with by following the specification of the revocation algorithm that simply inserts the appropriate node trees in the revocation list RL. The way to answer other queries now depends on the bit c_{mode}.

- If $c_{mode} = 0$, $\mathcal{B}$ uses the following strategy.
  - $\mathcal{SK}(.)$ queries: let id_j be the input of the j^{th} private key query and let $v \in \mathsf{T}$ be the node that $\mathcal{B}$ assigns to id_j.
    - If $j \neq j^\star$, for each node $\theta \in \mathsf{Path}(v)$, $\mathcal{B}$ re-computes $Y_{1,\theta} = X^{\gamma_{1,\theta}} \cdot h^{-r^\star_{1,\theta}}$ using the shares $(\gamma_{1,\theta}, \gamma_{2,\theta}, r^\star_{1,\theta}, r^\star_{2,\theta})$. It picks $r_{1,\theta}, s_{1,\theta} \xleftarrow{R} \mathbb{Z}_p^*$, defines $W = Y_{1,\theta} \cdot h^{r_{1,\theta}}$ and calculates
$$(d_{1,\theta}, d_{2,\theta}) = \Big(F_u(id_j)^{s_{1,\theta}} \cdot W^{-\frac{K(id_j)}{J(id_j)}},\ X^{s_{1,\theta}} \cdot W^{-\frac{1}{J(id_j)}}\Big) \qquad (6)$$
which is well-defined since $J(id_j) \neq 0$ and can be checked to provide a correctly-shaped triple $d_{id_j,\theta} = (d_{1,\theta}, d_{2,\theta}, r_{1,\theta})$ for node θ if we set $\tilde{s_{1,\theta}} = s_{1,\theta} - w/(aJ(id_j))$ where $w = \log_g(W)$. Indeed,
$$\begin{aligned} W^{1/a} \cdot F_u(id_j)^{\tilde{s_{1,\theta}}} &= W^{1/a} \cdot F_u(id_j)^{s_{1,\theta}} \cdot (g^{J(id_j)} \cdot X^{K(id_j)})^{-\frac{w}{aJ(id_j)}} \\ &= F_u(id_j)^{s_{1,\theta}} \cdot W^{-\frac{K(id_j)}{J(id_j)}} \end{aligned}$$
and $X^{\tilde{s_{1,\theta}}} = X^{s_{1,\theta}} \cdot W^{-\frac{1}{J(id_j)}}$. In this case, for all nodes $\theta \in \mathsf{Path}(v)$, the share $r^\star_{1,\theta}$ remains perfectly hidden from $\mathcal{A}$'s view.
    - If $j = j^\star$ (and thus $id_j = id^\star$ if $\mathcal{B}$ was lucky when choosing $j^\star$), for each node $\theta \in \mathsf{Path}(v)$, $\mathcal{B}$ picks a random $s_{1,\theta} \xleftarrow{R} \mathbb{Z}_p^*$ and uses the shares $(\gamma_{1,\theta}, \gamma_{2,\theta}, r^\star_{1,\theta}, r^\star_{2,\theta})$ to compute a triple $d_{id_j,\theta} = (d_{1,\theta}, d_{2,\theta}, r^\star_{1,\theta})$ where
$$(d_{1,\theta}, d_{2,\theta}) = (g^{\gamma_{1,\theta}} \cdot F_u(id_j)^{s_{1,\theta}},\ X^{s_{1,\theta}})$$
We see that $d_{id_j,\theta}$ is well-formed since $(Y_{1,\theta} \cdot h^{r^\star_{1,\theta}})^{1/a} = g^{\gamma_{1,\theta}}$. In this case, the shares $\{r^\star_{1,\theta}\}_{\theta \in \mathsf{Path}(v)}$ are revealed to $\mathcal{A}$ as part of $d_{id_j,\theta}$.
  - $\mathcal{KU}(.)$ queries:
    - For periods $t \neq t^\star$, $\mathcal{B}$ runs $\mathsf{KUNodes}(\mathsf{T}, RL, t)$ to find the right set Y of non-revoked nodes. For each $\theta \in \mathsf{Y}$, $\mathcal{B}$ re-constructs $Y_{2,\theta} = X^{\gamma_{2,\theta}} \cdot h^{-r^\star_{2,\theta}}$ using the shares $(\gamma_{1,\theta}, \gamma_{2,\theta}, r^\star_{1,\theta}, r^\star_{2,\theta})$. It sets $W = Y_{2,\theta} \cdot h^{r_{2,\theta}}$ for a random $r_{2,\theta} \xleftarrow{R} \mathbb{Z}_p^*$. Then, it picks $s_{2,\theta} \xleftarrow{R} \mathbb{Z}_p^*$ and computes
$$(ku_{1,\theta}, ku_{2,\theta}) = \big(F_v(t)^{s_{2,\theta}} \cdot W^{-\frac{\alpha}{\beta(t-t^\star)}},\ X^{s_{2,\theta}} \cdot W^{-\frac{1}{\beta(t-t^\star)}}\big),$$
which is well-defined since $F_v(t) = g^{\beta(t-t^\star)} \cdot X^\alpha$ and $t \neq t^\star$ and, if we define $\tilde{s_{2,\theta}} = s_{2,\theta} - w/(\beta a(t-t^\star))$ (with $w = \log_g(W)$), we have
$$\begin{aligned} W^{1/a} \cdot F_v(t)^{\tilde{s_{2,\theta}}} &= W^{1/a} \cdot F_v(t)^{s_{2,\theta}} \cdot (g^{\beta(t-t^\star)} \cdot X^\alpha)^{-\frac{w}{\beta a(t-t^\star)}} \\ &= F_v(t)^{s_{2,\theta}} \cdot W^{-\frac{\alpha}{\beta(t-t^\star)}} \end{aligned}$$
and $X^{\tilde{s_{2,\theta}}} = X^{s_{2,\theta}} \cdot W^{-\frac{1}{\beta(t-t^\star)}}$. Finally, $\mathcal{B}$ returns $\{(ku_{1,\theta}, ku_{2,\theta}, r_{2,\theta})\}_{\theta \in \mathsf{Y}}$ and, for all nodes $\theta \in \mathsf{Y}$, the share $r^\star_{2,\theta}$ remains perfectly hidden.

- For period $t = t^\star$, $\mathcal{B}$ determines the set $\mathsf{Y} \in \mathsf{T}$ of non-revoked nodes using $\mathsf{KUNodes}(\mathsf{T}, RL, t)$. For each $\theta \in \mathsf{Y}$, $\mathcal{B}$ uses the shares $(\gamma_{1,\theta}, \gamma_{2,\theta}, r^\star_{1,\theta}, r^\star_{2,\theta})$ to construct $ku_{t^\star,\theta}$ as the triple $ku_{t^\star,\theta} = (ku_{1,\theta}, ku_{2,\theta}, r^\star_{2,\theta})$ where
$$(ku_{1,\theta}, ku_{2,\theta}) = \big(g^{\gamma_{2,\theta}} \cdot F_v(t^\star)^{s_{2,\theta}},\ X^{s_{2,\theta}}\big)$$
for a random $s_{2,\theta} \xleftarrow{R} \mathbb{Z}_p^*$. This pair has the correct distribution since $(Y_{2,\theta} \cdot h^{r^\star_{2,\theta}})^{1/a} = g^{\gamma_{2,\theta}}$. In this case, shares $\{r^\star_{2,\theta}\}_{\theta \in \mathsf{Y}}$ are given away.

By inspection, we check that, with non-negligible probability, $\mathcal{B}$ never has to reveal two complementary shares $r^\star_{1,\theta}, r^\star_{2,\theta}$ of $r^\star$ for any node $\theta \in \mathsf{T}$. Let $v^\star$ be the leaf that $\mathcal{B}$ assigns to the target identity $id^\star$ (which is also $id_{j^\star}$ with probability $1/q$). For all $\theta \in \mathsf{Path}(v^\star)$, $\mathcal{A}$ never sees both $r^\star_{1,\theta}$ and $r^\star_{2,\theta}$ because, according to the rules of definition 2, $id^\star$ must be revoked by period $t^\star$ if $\mathcal{A}$ decides to corrupt it at some point. Then, no ancestor of $v^\star$ lies in the set Y determined by $\mathsf{KUNodes}$ at period $t^\star$.

• The case $c_{mode} = 1$ is easier to handle. Recall that, if $\mathcal{A}$ indeed behaves as a Type II adversary, it does not query the private key of $id^\star$ at any time.

- $\mathcal{SK}(.)$ queries: let id be the queried identity. We must have $J(id) \neq 0$ with non-negligible probability and $\mathcal{B}$ can compute a private key as suggested by relation (6) in the case $c_{mode} = 0$. In particular, the value $r^\star_{1,\theta}$ does not leak for any $\theta \in \mathsf{Path}(v)$ where v is the leaf associated with id.
- $\mathcal{KU}(.)$ queries are processed exactly as in the case $c_{mode} = 0$. Namely, $\mathcal{B}$ distinguishes the same situations $t \neq t^\star$ and $t = t^\star$ and only reveals $r^\star_{2,\theta}$, for non-revoked nodes $\theta \in \mathsf{Y}$, when generating updates for period $t = t^\star$.

Again, the simulator does not reveal both $r^\star_{1,\theta}$ and $r^\star_{2,\theta}$ for any node since $r^\star_{1,\theta}$ is never used to answer private key queries.

With non-negligible probability, the value $r^\star$ thus remains independent of $\mathcal{A}$'s view for either value of $c_{mode} \in \{0, 1\}$. This completes the outline of the proof, which is more thoroughly detailed the full paper. □

As we mentioned earlier, the reduction leaves room for improvement as its quadratic degradation factor q^2 becomes cubic since we must have $t_{max} \geq q$ to tolerate a polynomial number $O(q)$ of revocation queries. Although loose, the reduction is polynomial and thus solves the problem left open in [5].

Chosen-ciphertext security can be efficiently achieved using the usual techniques [18, 12, 14] or, since the outlined simulator knows a valid private key for each identity as in [26], in the fashion of Cramer-Shoup [22].

5 Conclusion

We showed that regular IBE schemes can be used to implement the efficient revocation mechanism suggested by Boldyreva *et al.* and notably provide the first adaptive-ID secure revocable IBE. The latter was obtained by sharing the key generation process of a 2-level HIBE system from the "commutative-blinding family" (initiated with the first scheme of [6]). As another extension, the same ideas make it possible to construct revocable identity-based broadcast encryption schemes (using the recent Boneh-Hamburg constructions [11] for instance) in the selective-ID model.

An open problem is to devise adaptive-ID secure R-IBE systems with a tighter reduction than what we could obtain. It would also be interesting to see how revocation can be handled in the context of hierarchical IBE [29, 27], where each entity of the hierarchy should be responsible for revoking its children.

Acknowledgements

We thank the reviewers for their comments.

References

1. W. Aiello, S. Lodha, and R. Ostrovsky, *Fast Digital Identity Revocation (Extended Abstract).*, Advances in Cryptology - Crypto'98 (H. Krawczyk, ed.), Lect. Notes Comput. Sci., vol. 1462, Springer, 1998, pp. 137–152.
2. J. Baek and Y. Zheng, *Identity-Based Threshold Decryption.*, in Bao et al. [3], pp. 262–276.
3. F. Bao, R. H. Deng, and J. Zhou (eds.), *Public Key Cryptography - PKC 2004, 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004*, Lect. Notes Comput. Sci., vol. 2947, Springer, 2004.
4. M. Bellare and P. Rogaway, *Random Oracles are Practical: A Paradigm for Designing Efficient Protocols.*, Proceedings of the First ACM Conference on Computer and Communications Security (D. Denning, R. Pyle, R. Ganesan, R. Sandhu, and V. Ashby, eds.), ACM Press, 1993, pp. 62–73.
5. A. Boldyreva, V. Goyal, and Kumar V., *Identity-based encryption with efficient revocation.*, Proceedings of the 2008 ACM Conference on Computer and Communications Security, CCS 2008 (P. Ning, P. F. Syverson, and S. Jha, eds.), ACM Press, 2008, pp. 417–426.
6. D. Boneh and X. Boyen, *Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles.*, in Cachin and Camenisch [15], pp. 223–238.
7. ———, *Secure Identity Based Encryption Without Random Oracles.*, Advances in Cryptology - Crypto 2004 (M. K. Franklin, ed.), Lect. Notes Comput. Sci., vol. 3152, Springer, 2004, pp. 443–459.
8. D. Boneh, X. Ding, G. Tsudik, and C. M. Wong, *A Method for Fast Revocation of Public Key Certificates and Security Capabilities.*, 10th USENIX Security Symposium (D. S. Wallach, ed.), USENIX Association, 2001, pp. 297–310.
9. D. Boneh and M. Franklin, *Identity-Based Encryption from the Weil Pairing.*, SIAM J. Comput. **32** (2003), no. 3, 586–615.
10. D. Boneh, C. Gentry, and M. Hamburg, *Space-Efficient Identity Based Encryption Without Pairings.*, Proceedings of the 48th IEEE Symposium on Foundations of Computer Science (FOCS 2007), IEEE Computer Society, 2007, pp. 647–657.
11. D. Boneh and M. Hamburg, *Generalized Identity Based and Broadcast Encryption Schemes.*, Advances in Cryptology - Asiacrypt 2008 (J. Pieprzyk, ed.), Lect. Notes Comput. Sci., vol. 5350, Springer, 2008, pp. 455–470.
12. D. Boneh and J. Katz, *Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity-Based Encryption.*, Topics in Cryptology - CT-RSA 2005 (A. J. Menezes, ed.), Lect. Notes Comput. Sci., vol. 3376, Springer, 2005, pp. 87–103.
13. X. Boyen, *A Tapestry of Identity-Based Encryption: Practical Frameworks Compared*, Int. J. of Applied Cryptography **1** (2008), no. 1, 3–21.
14. X. Boyen, Q. Mei, and B. Waters, *Direct Chosen Ciphertext Security from Identity-Based Techniques.*, Proceedings of the 12th ACM Conference on Computer and Communications Security (V. Atluri, B. Pfitzmann, and P. McDaniel, eds.), ACM Press, 2005, 320-329.
15. C. Cachin and J. Camenisch (eds.), *Advances in Cryptology* - Eurocrypt *2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*, Lect. Notes Comput. Sci., vol. 3027, Springer, 2004.
16. R. Canetti, O. Goldreich, and S. Halevi, *The Random Oracle Methodology, Revisited.*, J. Assoc. Comput. Mach. **51** (2004), no. 4, 557–594.
17. R. Canetti, S. Halevi, and J. Katz, *A Forward-Secure Public-Key Encryption Scheme.*, Advances in Cryptology - Eurocrypt 2003 (E. Biham, ed.), Lect. Notes Comput. Sci., vol. 2656, Springer, 2003, pp. 255–271.
18. ———, *Chosen-Ciphertext Security from Identity-Based Encryption.*, in Cachin and Camenisch [15], pp. 207–222.
19. R. Canetti and S. Hohenberger, *Chosen-Ciphertext Secure Proxy Re-Encryption.*, Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007 (P. Ning, S. De Capitani di Vimercati, and P. F. Syverson, eds.), ACM Press, 2007, pp. 185–194.
20. C. Cocks, *An Identity Based Encryption Scheme Based on Quadratic Residues.*, Cryptography and Coding, 8th IMA International Conference (B. Honary, ed.), Lect. Notes Comput. Sci., vol. 2260, Springer, 2001, pp. 360–363.
21. R. Cramer (ed.), *Advances in Cryptology* - Eurocrypt *2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, Lect. Notes Comput. Sci., vol. 3494, Springer, 2005.

22. R. Cramer and V. Shoup, *Design and Analysis of Practical Public-Key Encryption Schemes Secure Against Adaptive Chosen Ciphertext Attack.*, SIAM J. Comput. **33** (2003), no. 1, 167–226.
23. X. Ding and G. Tsudik, *Simple Identity-Based Cryptography with Mediated RSA.*, Topics in Cryptology - CT-RSA 2003 (M. Joye, ed.), Lect. Notes Comput. Sci., vol. 2612, Springer, 2003, pp. 193–210.
24. F. F. Elwailly, C. Gentry, and Ramzan Z., *QuasiModo: Efficient Certificate Validation and Revocation.*, in Bao et al. [3], pp. 375–388.
25. D. Galindo, *A Separation Between Selective and Full-Identity Security Notions for Identity-Based Encryption.*, Computational Science and Its Applications - ICCSA 2006, International Conference (M. L. Gavrilova, O. Gervasi, V. Kumar, C. J. Kenneth Tan, D. Taniar, A. Laganà, Y. Mun, and H. Choo, eds.), Lect. Notes Comput. Sci., vol. 3982, Springer, 2006, pp. 318–326.
26. C. Gentry, *Practical Identity-Based Encryption Without Random Oracles.*, Advances in Cryptology - Eurocrypt 2006 (S. Vaudenay, ed.), Lect. Notes Comput. Sci., vol. 4004, Springer, 2006, pp. 445–464.
27. C. Gentry and A. Silverberg, *Hierarchical ID-Based Cryptography.*, Advances in Cryptology - Asiacrypt 2002 (Y. Zheng, ed.), Lect. Notes Comput. Sci., vol. 2501, Springer, 2002, pp. 548–566.
28. V. Goyal, *Certificate Revocation Using Fine Grained Certificate Space Partitioning.*, Financial Cryptography and Data Security, 11th International Conference, FC 2007 (S. Dietrich and R. Dhamija, eds.), Lect. Notes Comput. Sci., vol. 4886, Springer, 2008, pp. 247–259.
29. J. Horwitz and B. Lynn, *Toward Hierarchical Identity-Based Encryption.*, Advances in Cryptology - Eurocrypt 2002 (L. R. Knudsen, ed.), Lect. Notes Comput. Sci., vol. 2332, Springer, 2002, pp. 466–481.
30. B. Libert and J.-J. Quisquater, *Efficient Revocation and Threshold Pairing Based Cryptosystems.*, Proceedings of the Twenty-Second Annual ACM Symposium on Principles of Distributed Computing, PODC 2003 (E. Borowsky and S. Rajsbaum, eds.), ACM, 2003, pp. 163–171.
31. B. Libert and D. Vergnaud, *Towards Black-Box Accountable Authority IBE with Short Ciphertexts and Private Keys.*, 12th International Workshop on Practice and Theory in Public Key Cryptography, PKC 2009 (H. Imai and Y. Zheng, eds.), Lect. Notes Comput. Sci., vol. 1751, Springer, 2000, pp. 235–255.
32. S. Micali, *Efficient Certificate Revocation.*, Tech. Report 542-b, MIT/LCS/TM, 1996.
33. ______, *Novomodo: Scalable Certificate Validation and Simplified PKI Management.*, 1st Annual PKI Research Workshop (S. Smith, ed.), NIST, 2002, pp. 15–25.
34. A. Sahai and B. Waters, *Fuzzy Identity-Based Encryption.*, in Cramer [21], pp. 457–473.
35. A. Shamir, *Identity-Based Cryptosystems and Signature Schemes.*, Advances in Cryptology - Crypto'84 (G. R. Blakley and D. Chaum, eds.), Lect. Notes Comput. Sci., vol. 196, Springer, 1985, pp. 47–53.
36. B. Waters, *Efficient Identity-Based Encryption Without Random Oracles.*, in Cramer [21], pp. 114–127.