Towards Practical Black-Box Accountable Authority IBE: Weak Black-Box Traceability with Short Ciphertexts and Private Keys

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

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

Abstract. At Crypto'07, Goyal introduced the concept of *Accountable Authority Identity-Based Encryption* (A-IBE) as a convenient tool to reduce the amount of trust in authorities in Identity-Based Encryption. In this model, if the Private Key Generator (PKG) maliciously re-distributes users' decryption keys, it runs the risk of being caught and prosecuted. Goyal proposed two constructions: the first one is efficient but can only trace well-formed decryption keys to their source; the second one allows tracing obfuscated decryption boxes in a model (called *weak black-box* model) where cheating authorities have no decryption oracle. The latter scheme is unfortunately far less efficient in terms of decryption cost and ciphertext size. The contribution of this paper is to describe a new construction that combines the efficiency of Goyal's first proposal with a simple weak black-box tracing mechanism. The proposed scheme is the first A-IBE that meets all security properties (although traceability is only guaranteed in the weak black-box model) in the adaptive-ID sense.

Keywords. Identity-Based Encryption, traceability, efficiency.

1 Introduction

Identity-based cryptography, first proposed by Shamir [43], alleviates the need for digital certificates used in traditional public-key infrastructures. In such systems, users' public keys are public identifiers (*e.g.* email addresses) and the matching private keys are derived by a trusted party called Private Key Generator (PKG). The first practical construction for *Identity-Based Encryption* (IBE) was put forth by Boneh and Franklin [10] – despite the bandwidth-demanding proposal by Cocks [19] – and, since then, a large body of work has been devoted to the design of schemes with additional properties or relying on different algorithmic assumptions [28, 7, 8, 39, 45, 9, 25, 15, 11].

In spite of its appealing advantages, Identity-Based Encryption has not undergone rapid adoption as a standard. The main reason is arguably the fact that it requires unconditional trust in the PKG: the latter can indeed decrypt any ciphertext or, even worse, re-distribute users' private keys. The key escrow problem can be mitigated as suggested in [10] by sharing the master secret among multiple PKGs, but this inevitably entails extra communication and infrastructure. Related paradigms [24, 3] strived to remove the key escrow problem but only did so at the expense of losing the benefit of human-memorizable public keys: these models get rid of escrow authorities but both involve traditional (though not explicitly certified) public keys that are usually less convenient to work with than easy-to-remember public identifiers.

In 2007, Goyal [29] explored a new approach to deter rogue actions from authorities. With the *Accountable Authority Identity-Based Encryption* (A-IBE) primitive, if the PKG discloses a decryption key associated with some identity over the Internet, it runs the risk of being caught and sued by the user. A-IBE schemes

⋆ 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 ICT Program under Contract ICT-2007-216676 ECRYPT II and by the French *Agence Nationale de la Recherche* through the PACE project.

⋆⋆ This is the full version of the paper *"Towards Black-Box Accountable Authority IBE with Short Ciphertexts and Private Keys"* presented in Public Key Cryptography 2009 [36]

achieve this goal by means of an interactive private key generation protocol between the user and the PKG. For each identity, there are exponentially-many families of possible decryption keys. The key generation protocol provides the user with a single decryption key while concealing to the PKG the family that this key belongs to. From this private key, the user is computationally unable to find one from a different family. Hence, for a given identity, a pair of private keys from distinct families serves as evidence of a fraudulent PKG. The latter remains able to passively eavesdrop communications but is discouraged to reveal users' private keys. Also, users cannot falsely accuse an honest PKG since they are unable to compute a new key from a different family using a given key.

Prior Works. Two constructions were given in [29]. The first one (that we call *Goyal-1* hereafter) builds on Gentry's IBE scheme [25] and, while efficient, only allows tracing well-formed decryption keys. This white-box model seems unlikely to suffice in practice since malicious parties can rather release an imperfect and/or obfuscated program that only decrypts with small but noticeable probability. The second scheme of [29] (let us call it *Goyal-2*), which is constructed from the Sahai-Waters fuzzy IBE scheme [39], has a variant providing weak black-box traceability: even an imperfect pirate decryption box can be traced (based on its input/output behavior) back to its source although traceability is only guaranteed against dishonest PKGs that have no decryption oracle in the attack game. However, *Goyal-2* is somewhat inefficient as decryption requires a number of pairing calculations that is linear in the security parameter. For the usually required security level, ciphertexts contain more than 160 group elements and decryption calculates a product of about 160 pairings.

Subsequently, Au *et al.* [4] described another A-IBE scheme providing retrievability (*i.e.*, a property that prevents the PKG from revealing more than one key for a given identity without exposing its master key) but remained in the white-box model. More recently, Goyal *et al.* [30] modified the *Goyal-2* system using attribute-based encryption techniques [39, 31] to achieve full black-box traceability: unlike *Goyal-2*, the scheme of [30] preserves security against dishonest PKGs that have access to a decryption oracle in the model. While definitely desirable in practice, this property is currently achievable only at the expense of the same significant penalty as in *Goyal-2* [29] in terms of decryption cost and ciphertext size.

Our Contributions. We present a very efficient and conceptually simple scheme with weak black-box traceability. We prove its security (in the standard model) under the same assumption as was used to prove the security of *Goyal-2*. Decryption keys and ciphertexts consist of a constant number of group elements and their length is thus linear in the security parameter λ (instead of quadratic as in *Goyal-2*). Encryption and decryption take $O(\lambda^3)$-time (compared to $O(\lambda^4)$ in *Goyal-2*) with only two pairing computations being needed for decryption (against more than 160 in *Goyal-2*).

The system is analyzed the adaptive-ID model of [10], as opposed to the selective-ID security model (where adversaries must choose the identity that will be their target at the outset of the game). In contrast, one of the security properties (*i.e.*, the infeasibility for users to frame innocent PKGs) was only established in the selective-ID setting for known schemes in the black-box model (*i.e.*, *Goyal-2* and its fully black-box extension [30]). Among such schemes, ours thus appears to be the first one that can be tweaked so as to achieve adaptive-ID security against dishonest users.

Our scheme performs almost as well as *Goyal-1* (the main overhead being a long master public key *à la* Waters [45] to obtain the adaptive-ID security). In comparison with *Goyal-1*, that was only analyzed in a white-box model of traceability, our system provides several other advantages.

As an extension to the proceedings version of this paper [36], we also show how to apply the idea of our weak black-box tracing mechanism to Gentry's IBE scheme. The resulting A-IBE system is obtained by making a simple modification to the key generation protocol of *Goyal-1* so as to perfectly hide the user's key family from the PKG's view while preserving the efficiency of the whole scheme. Since the resulting system inherits the efficiency of Gentry's IBE scheme and the *Goyal-1* white-box A-IBE scheme, it turns out to be the most efficient weakly black-box A-IBE construction to date. Its (adaptive-ID) security is moreover proved under a tight reduction (albeit under a strong assumption).

Finally, since detecting misbehaving PKGs is an equally relevant problem in IBE primitives and their generalizations, we show how the underlying idea of previous schemes can be applied to one of the most prac-

tical Identity-Based Broadcast Encryption (IBBE) realizations [12]. We also argue that the same technique similarly applies in the context of attribute-based encryption [39, 31].

Organization. In the rest of the paper, Section 2 recalls the A-IBE security model defined in [29]. We first analyze the basic version of our scheme in Section 3. Sections 4 and 5 describe and analyze the extensions of our method to Gentry's IBE scheme and the Boneh-Hamburg IBBE scheme, respectively.

2 Background and Definitions

Syntactic definition and security model. We recall the definition of A-IBE schemes and their security properties as defined in [29].

Definition 1. *An* Accountable Authority Identity-Based Encryption scheme *(A-IBE) is a tuple*

$$(\mathbf{Setup}, \mathbf{Keygen}, \mathbf{Encrypt}, \mathbf{Decrypt}, \mathbf{Trace})$$

of probabilistic polynomial-time algorithms or protocols such that:

- **Setup** *takes as input a security parameter and outputs a master public key* mpk *and a matching* master secret key msk.
- $\mathbf{Keygen}^{(\mathrm{PKG},\mathsf{U})}$ *is an interactive protocol between the public parameter generator* PKG *and the user* U*:*
  - *the common input to* PKG *and* U *are: the master public key* mpk *and an identity* ID *for which the decryption key has to be generated;*
  - *the private input to* PKG *is the master secret key* msk.

  Both parties may use a sequence of private coin tosses as additional inputs. The protocol ends with U *receiving a decryption key* d_{ID} *as his private output.*
- **Encrypt** *takes as input the master public key* mpk*, an identity* ID *and a message* m *and outputs a* ciphertext.
- **Decrypt** *takes as input the master public key* mpk*, a decryption key* d_{ID} *and a ciphertext* C *and outputs a message.*
- **Trace** *given the master public key* mpk*, a decryption key* d_{ID}*, this algorithm outputs a* key family number n_F *or the special symbol* $\perp$ *if* d_{ID} *is ill-formed.*

Correctness requires that, for any outputs $(\mathsf{mpk}, \mathsf{msk})$ *of* **Setup***, any plaintext* m *and any identity* ID*, whenever* $d_{\mathsf{ID}} \leftarrow \mathbf{Keygen}^{(\mathrm{PKG}(\mathsf{msk}),\mathsf{U})}(\mathsf{mpk}, \mathsf{ID})$*, we have*

$$\mathbf{Trace}\big(\mathsf{mpk}, d_{\mathsf{ID}}\big) \neq \perp,$$
$$\mathbf{Decrypt}\big(\mathsf{mpk}, d_{\mathsf{ID}}, \mathbf{Encrypt}(\mathsf{mpk}, \mathsf{ID}, m)\big) = m.$$

The above definition is for the white-box setting. In a black-box model, **Trace** takes as input an identity ID, the corresponding user's well-formed private key d_{ID} and a decryption box $\mathbb{D}$, modeled as a probabilistic polynomial time algorithm, that successfully opens a non-negligible fraction ε of ciphertexts encrypted under ID. The output of **Trace** is either "PKG" or "User" depending on which party is found guilty for having crafted $\mathbb{D}$.

Goyal formalized three security properties for A-IBE schemes. The first one is the standard notion of privacy [10] for IBE systems. As for the other ones, the $\mathsf{DishonestPKG}$ game captures the intractability for the PKG to create a decryption key of the same family as the one obtained by the user during the key generation protocol. Finally, the $\mathsf{DishonestUser}$ game models the infeasibility for users to generate a key $d^{(2)}_{\mathsf{ID}}$ outside the family of the legally obtained one $d^{(1)}_{\mathsf{ID}}$.

Definition 2. *An A-IBE scheme is deemed secure if all probabilistic polynomial time (PPT) adversaries have negligible advantage in the following games.*

1. **The IND-ID-CCA game.** For any PPT algorithm $\mathcal{A}$, the model considers the following game, where $\lambda \in \mathbb{N}$ is a security parameter:

$\boxed{\mathbf{Game}_{\mathcal{A}}^{\mathsf{IND\text{-}ID\text{-}CCA}}(\lambda)}$
$(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathbf{Setup}(\lambda)$
$(m_0, m_1, \mathsf{ID}^\star, s) \leftarrow \mathcal{A}^{\mathsf{Dec},\mathsf{KG}}(\mathsf{find}, \mathsf{mpk})$

Dec -	Input : (C, ID)
	Output : $\mathbf{Decrypt}\big(\mathsf{mpk}, d_{\mathsf{ID}}, \mathsf{ID}, C\big)$
KG -	Input : $\mathsf{ID} \neq \mathsf{ID}^\star$
	Output : $\mathbf{Keygen}^{(\mathrm{PKG}(\mathsf{msk}),\mathcal{A})}(\mathsf{mpk}, \mathsf{ID})$

$d^\star \xleftarrow{\$} \{0,1\}$
$C^\star \leftarrow \mathbf{Encrypt}(\mathsf{mpk}, \mathsf{ID}^\star, m_{d^\star})$
$d \leftarrow \mathcal{A}^{\mathsf{Dec},\mathsf{KG}}(\mathsf{guess}, s, C^\star)$

Dec -	Input : $(C, \mathsf{ID}) \neq (C^\star, \mathsf{ID}^\star)$
	Output : $\mathbf{Decrypt}\big(\mathsf{mpk}, d_{\mathsf{ID}}, \mathsf{ID}, C\big)$
KG -	Input : $\mathsf{ID} \neq \mathsf{ID}^\star$
	Output : $\mathbf{Keygen}^{(\mathrm{PKG}(\mathsf{msk}),\mathcal{A})}(\mathsf{mpk}, \mathsf{ID})$

`return` 1 `if` $d = d^\star$ `and` 0 `otherwise.`

$\mathcal{A}$'s advantage is

$$\mathbf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}ID\text{-}CCA}}(\lambda) = |\Pr[\mathbf{Game}_{\mathcal{A}}^{\mathsf{IND\text{-}ID\text{-}CCA}} = 1] - 1/2|.$$

The A-IBE scheme is termed IND-ID-CCA-secure if for all PPT algorithms $\mathcal{A}$, the advantage of $\mathcal{A}$ defined by the following experiment is a negligible function of λ.

The weaker definition of chosen-plaintext security (IND-ID-CPA) is formalized in the same way in [10] but $\mathcal{A}$ is not granted access to a decryption oracle. In [16], Canetti, Halevi and Katz suggested relaxed notions of IND-ID-CCA and IND-ID-CPA security where the adversary has to choose the target identity $\mathsf{ID}^\star$ ahead of time (even before seeing the master public key mpk). This relaxed model is called "selective-ID" model (or IND-sID-CCA and IND-sID-CPA for short).

2. **The DishonestPKG game.** Let $\mathcal{A}$ be a PPT algorithm. We consider the following games, where $\lambda \in \mathbb{N}$ is a security parameter and ε is a second parameter (also given as input):

$\boxed{\mathbf{Game}_{\mathcal{A}}^{\mathsf{DishonestPKG\text{-}WB\text{-}CPA}}(\lambda)}$
$(\mathsf{mpk}, \mathsf{ID}, s_1) \leftarrow \mathcal{A}(\mathsf{setup}, \lambda)$
$(d_{\mathsf{ID}}^{(1)}, s_2) \leftarrow \mathbf{Keygen}^{(\mathcal{A}(s_1),\cdot)}(\mathsf{mpk}, \mathsf{ID})$
$d_{\mathsf{ID}}^{(2)} \leftarrow \mathcal{A}(\mathsf{findkey}, s_1, s_2)$
`return` 1 `if` $\mathbf{Trace}(\mathsf{mpk}, d_{\mathsf{ID}}^{(1)}) = \mathbf{Trace}(\mathsf{mpk}, d_{\mathsf{ID}}^{(2)})$
0 `otherwise.`

$\boxed{\mathbf{Game}_{\mathcal{A}}^{\mathsf{DishonestPKG\text{-}wBB}}(\lambda)}$
$(\mathsf{mpk}, \mathsf{ID}, s_1) \leftarrow \mathcal{A}(\mathsf{setup}, \lambda)$
$(d_{\mathsf{ID}}, s_2) \leftarrow \mathbf{Keygen}^{(\mathcal{A}(s_1),\cdot)}(\mathsf{mpk}, \mathsf{ID})$
$\mathbb{D} \leftarrow \mathcal{A}(\mathsf{findkey}, s_1, s_2)$
`return` 1 `if` $\mathbf{Trace}^{\mathbb{D}}(\mathsf{mpk}, d_{\mathsf{ID}^\star}, \mathsf{ID}) =$ "User″ `and` $\mathbb{D}$ `is` ε`-useful for ID and mpk`
0 `otherwise.`

$\boxed{\mathbf{Game}_{\mathcal{A}}^{\mathsf{DishonestPKG\text{-}WB\text{-}CCA}}(\lambda)}$
$(\mathsf{mpk}, \mathsf{ID}, s_1) \leftarrow \mathcal{A}(\mathsf{setup}, \lambda)$
$(d_{\mathsf{ID}}^{(1)}, s_2) \leftarrow \mathbf{Keygen}^{(\mathcal{A}(s_1),\cdot)}(\mathsf{mpk}, \mathsf{ID})$
$d_{\mathsf{ID}}^{(2)} \leftarrow \mathcal{A}^{\mathsf{Dec}}(\mathsf{findkey}, s_1, s_2)$

Dec -	Input : C
	Output : $\mathbf{Decrypt}\big(\mathsf{mpk}, d_{\mathsf{ID}}^{(1)}, \mathsf{ID}, C\big)$

`return` 1 `if` $\mathbf{Trace}(\mathsf{mpk}, d_{\mathsf{ID}}^{(1)}) = \mathbf{Trace}(\mathsf{mpk}, d_{\mathsf{ID}}^{(2)})$
0 `otherwise.`

For $\omega \in \{\mathsf{WB\text{-}CPA}, \mathsf{WB\text{-}CCA}, \mathsf{wBB}\}$, $\mathcal{A}$'s advantage is

$$\mathbf{Adv}_{\mathcal{A}}^{\mathsf{DishonestPKG}\text{-}\omega}(\lambda) = \Pr[\mathbf{Game}_{\mathcal{A}}^{\mathsf{DishonestPKG}\text{-}\omega} = 1].$$

The A-IBE scheme is termed $\mathsf{DishonestPKG}$-ω-secure if for all PPT algorithms $\mathcal{A}$ and all $\varepsilon = 1/\mathsf{poly}(\lambda)$, the advantage of $\mathcal{A}$ defined by the corresponding experiment is a negligible function of λ.

Here, the adversary $\mathcal{A}$ acts as a cheating PKG and the challenger emulates the honest user. Both parties engage in a key generation protocol where the challenger obtains a private key for an identity ID chosen by $\mathcal{A}$. The latter aims at producing a private key corresponding to ID and belonging to the same family as the key obtained by the challenger in the key generation protocol. Such a successful dishonest PKG could disclose user keys without being caught.

Note that, at the beginning of the experiment, $\mathcal{A}$ generates mpk without revealing the master key msk and the challenger runs a sanity check on mpk.

As noted in [29, 30], it makes sense to provide $\mathcal{A}$ with a decryption oracle that undoes ciphertexts using $d_{\mathsf{ID}}^{(1)}$ (and could possibly leak information on the latter's family). We call this enhanced security notion $\mathsf{DishonestPKG}$-WB-CCA security (as opposed to the weaker one which we call $\mathsf{DishonestPKG}$-WB-CPA security).

Finally, in the black-box model, instead of outputting a new key $d_{\mathsf{ID}}^{(2)}$, the dishonest PKG comes up with a decryption box $\mathbb{D}$ which is *ε-useful for* ID *and* mpk, *i.e.* such that

$$\Pr[\mathbb{D}(\mathbf{Encrypt}(\mathsf{mpk}, \mathsf{ID}, m)] = m$$

with probability ε taken over the plaintext and the random coins used by the **Encrypt** algorithm. The dishonest PKG wins if the tracing algorithm returns "User" when run on $d_{\mathsf{ID}}^{(1)}$ and with oracle access to $\mathbb{D}$. We call this enhanced notion $\mathsf{DishonestPKG} - \mathsf{wBB}$ security when $\mathcal{A}$ is not[3] given access to a decryption oracle that undoes ciphertexts using $d_{\mathsf{ID}}^{(1)}$.

3. **The** $\mathsf{DishonestUser}$ **game.** Let $\mathcal{A}$ be a PPT algorithm. We consider the following games, where $\lambda \in \mathbb{N}$ is a security parameter and ε is a second parameter (also given as input):

$$\boxed{\mathbf{Game}_{\mathcal{A}}^{\mathsf{DishonestUser\text{-}ID\text{-}WB}}(\lambda)}$$
$$\begin{array}{l}
(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathbf{Setup}(\lambda) \\
(d_{\mathsf{ID}^\star}^{(1)}, d_{\mathsf{ID}^\star}^{(2)}, \mathsf{ID}^\star) \leftarrow \mathcal{A}^{\mathsf{KG}}(\mathsf{mpk}) \\
\qquad \left| \begin{array}{l} \mathsf{KG\ \text{-}\ Input} : \mathsf{ID} \\ \qquad \mathsf{Output} : \mathbf{Keygen}^{(\mathrm{PKG}(\mathsf{msk}), \mathcal{A})}(\mathsf{mpk}, \mathsf{ID}) \end{array} \right. \\
\texttt{return } 1 \texttt{ if } \mathbf{Trace}(\mathsf{mpk}, d_{\mathsf{ID}^\star}^{(1)}) \neq \perp \texttt{ and} \\
\qquad \mathbf{Trace}(\mathsf{mpk}, d_{\mathsf{ID}^\star}^{(2)}) \notin \{\perp, \mathbf{Trace}(\mathsf{mpk}, d_{\mathsf{ID}^\star}^{(1)})\} \\
\qquad 0 \texttt{ otherwise.}
\end{array}$$

$$\boxed{\mathbf{Game}_{\mathcal{A}}^{\mathsf{DishonestUser\text{-}ID\text{-}BB}}(\lambda)}$$
$$\begin{array}{l}
(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathbf{Setup}(\lambda) \\
(d_{\mathsf{ID}^\star}^{(1)}, \mathbb{D}, \mathsf{ID}^\star) \leftarrow \mathcal{A}^{\mathsf{KG}}(\mathsf{mpk}) \\
\qquad \left| \begin{array}{l} \mathsf{KG\ \text{-}\ Input} : \mathsf{ID} \\ \qquad \mathsf{Output} : \mathbf{Keygen}^{(\mathrm{PKG}(\mathsf{msk}), \mathcal{A})}(\mathsf{mpk}, \mathsf{ID}) \end{array} \right. \\
\texttt{return } 1 \texttt{ if } \mathbf{Trace}^{\mathbb{D}}(\mathsf{mpk}, d_{\mathsf{ID}^\star}^{(1)}, \mathsf{ID}^\star) = \text{“PKG”} \\
\qquad \texttt{and } \mathbb{D} \texttt{ is } \varepsilon\texttt{-useful for } \mathsf{ID}^\star \texttt{ and mpk} \\
\qquad 0 \texttt{ otherwise.}
\end{array}$$

For $\omega \in \{\mathsf{ID\text{-}WB}, \mathsf{ID\text{-}BB}\}$, $\mathcal{A}$'s advantage is $\mathbf{Adv}_{\mathcal{A}}^{\mathsf{DishonestUser}\text{-}\omega}(\lambda) = \Pr[\mathbf{Game}_{\mathcal{A}}^{\mathsf{DishonestUser}\text{-}\omega} = 1]$. The A-IBE scheme is termed $\mathsf{DishonestUser}$-secure if for all PPT algorithms $\mathcal{A}$ and all $\varepsilon = 1/\mathsf{poly}(\lambda)$, the advantage of $\mathcal{A}$ defined by the following experiment is a negligible function of λ.

[3] If $\mathcal{A}$ has access to the decryption oracle, one obtain the strong black-box security notion. Therefore, using intuitive naming conventions, the strong-security notion is the $\mathsf{DishonestPKG}$-BB-CCA whereas $\mathsf{DishonestPKG}$-wBB is the $\mathsf{DishonestPKG}$-BB-CPA security notion.

The DishonestUser-ID-WB game involves an adversary interacting with a PKG in executions of the key generation protocol and obtaining private keys associated with *distinct* identities of her choosing. The adversary is declared successful if, for some identity that may have been queried for key generation, she is able to find *two* private keys from *distinct* families. Such a pair would allow her to trick a judge into wrongly believing that the PKG has misbehaved.

In the black-box scenario (DishonestUser-ID-BB), the output of the dishonest user consist of a key $d^{(1)}_{\mathsf{ID}^\star}$ and a pirate decryption box $\mathbb{D}$ which is *ε-useful for* $\mathsf{ID}^\star$ *and* mpk, *i.e.* such that

$$\Pr[\mathbb{D}(\mathbf{Encrypt}(\mathsf{mpk}, \mathsf{ID}^\star, m)] = m$$

with probability ε taken over the plaintext and the random coins used by the **Encrypt** algorithm. In this case, the adversary wins if the output of $\mathbf{Trace}^{\mathbb{D}}(\mathsf{mpk}, d^{(1)}_{\mathsf{ID}^\star}, \mathsf{ID}^\star)$ is "PKG".

Finally, the relaxed "selective-ID" model can be naturally extended to the DishonestUser security notion (DishonestUser-sID-WB and DishonestUser-sID-BB).

Bilinear Maps and Complexity Assumptions. In the following, we review the definition of cryptographic bilinear maps and we do not pin down any particular generator, but instead parameterize definitions and security results by a choice of generator. For simplicity, we restrict our attention to so-called symmetric bilinear groups [23] however our constructions extend readily to the asymmetric bilinear group setting.

Definition 3. *A* bilinear-group generator *is a PPT that takes as input $\lambda \in \mathbb{N}$ and outputs a tuple $(\mathbb{G}, \mathbb{G}_T, e, p)$ satisfying the following conditions:*

1. *p is a prime with $2^{\lambda-1} < p < 2^\lambda$;*
2. *$(\mathbb{G}, \cdot)$ and $(\mathbb{G}_T, \cdot)$ are groups of order p;*
3. *$e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ satisfies the following properties:*
   (a) *$e(g^a, h^b) = e(g, h)^{ab}$ for any $(g, h) \in \mathbb{G} \times \mathbb{G}$ and $a, b \in \mathbb{Z}$;*
   (b) *e is non degenerate (*i.e. *$e(g, g) \neq 1_{\mathbb{G}_T}$ for some $g \in \mathbb{G}$);*
   (c) *there exists an efficient algorithm to compute e.*

In such *bilinear groups*, we assume the hardness of the (now classical) Decision Bilinear Diffie-Hellman problem that has been widely used in the recent years. The **Decision Bilinear Diffie-Hellman Problem** (DBDH) is to distinguish the distributions of tuples $(g, g^a, g^b, g^c, e(g, g)^{abc})$ and $(g, g^a, g^b, g^c, e(g, g)^z)$ in $\mathbb{G}^4 \times \mathbb{G}_T$ for random values $a, b, c, z \xleftarrow{\$} \mathbb{Z}_p^*$. The advantage of a distinguisher $\mathcal{A}$ is defined as follows:

Definition 4. *Let $\mathcal{G}$ be a bilinear-group generator and let $\mathcal{A}$ be a 0/1-valued PPT algorithm. We consider the following random experiments, where $\lambda \in \mathbb{N}$ is a security parameter:*

$\boxed{\mathbf{Game}^{\mathrm{DBDH}}_{\mathcal{A}}(\lambda)}$
$(\mathbb{G}, \mathbb{G}_T, e, p) \xleftarrow{\$} \mathcal{G}(\lambda)$
$g \xleftarrow{\$} \mathbb{G}$; $(a, b, c, z) \xleftarrow{\$} (\mathbb{Z}_p^*)^4$
$T_0 \leftarrow e(g, g)^{abc}$; $T_1 \leftarrow e(g, g)^z$
$d^\star \xleftarrow{\$} \{0, 1\}$
$d \leftarrow \mathcal{A}((\mathbb{G}, \mathbb{G}_T, e, p), g, g^a, g^b, g^c, T_{d^\star})$
return 1 *if* $d = d^\star$ *and* 0 *otherwise.*

$\mathcal{A}$'s advantage is defined as $\mathbf{Adv}^{\mathrm{DBDH}}_{\mathcal{A}}(\lambda) = \Pr[\mathbf{Game}^{\mathrm{DBDH}}_{\mathcal{A}} = 1]$. *The bilinear-group generator $\mathcal{G}$ is said* $DBDH$-secure *if, for all PPT algorithms $\mathcal{A}$, $\mathcal{A}$'s advantage is a negligible function of λ. In this case, we say that the* DBDH assumption *holds for $\mathcal{G}$.*

For convenience, we use an equivalent formulation – called *modified* DBDH – of the problem which is to distinguish $e(g, g)^{ab/c}$ from random given (g, g^a, g^b, g^c).

3 The Scheme

The scheme mixes ideas from the "commutative-blinding" [7] and "exponent-inversion" [40] frameworks. Private keys have the same shape as in commutative-blinding-based schemes [7, 8, 45, 15]. At the same time, their first element is a product of two terms, the first one of which is inspired from Gentry's IBE scheme [25].

Following a technique applied in [29], private keys contain a family number t that cannot be tampered with while remaining hidden from the PKG. This family number t is determined by combining two random values t_0 and t_1 respectively chosen by the user and the PKG in the key generation protocol. The latter begins with the user sending a commitment R to t_0. Upon receiving R, the PKG turns it into a commitment to $t_0 + t_1$ and uses the modified commitment to generate a "blinded" private key d'_{ID}. The user obtains his final key d_{ID} by "unblinding" d'_{ID} thanks to the randomness that was used to compute R.

A difference with *Goyal-1* is that, at the end of the key generation protocol, the private key component $t_0 + t_1$ is perfectly hidden from the PKG and the security against dishonest PKGs is unconditional. In the key generation protocol, the user's first message is a perfectly hiding commitment that comes along with a witness-indistinguishable (WI) proof of knowledge of its opening. In *Goyal-1*, users rather send a deterministic (and thus non-statistically hiding) commitment and knowledge of the underlying value must be proven in zero-knowledge because a proof of knowledge of a discrete logarithm must be simulated (by rewinding the cheating verifier) in the proof of security against dishonest PKGs. In the present scheme, the latter proof does not rely on a specific assumption and we do not need to simulate knowing the solution of a particular problem instance. Therefore, we can dispense with perfectly ZK proofs and settle for a more efficient 3-move WI proof (such as Okamoto's variant [37] of Schnorr [42]) whereas 4 rounds are needed using zero-knowledge proofs of knowledge.

3.1 Description of $\mathcal{A}$-IBE$_1$

Let $\mathcal{G}$ be a bilinear-group generator.

Setup(λ, n)**:** given $\lambda \in \mathbb{N}$, the PKG selects bilinear groups $(\mathbb{G}, \mathbb{G}_T, e, p)$ of prime order $p > 2^\lambda$ (by running $\mathcal{G}(\lambda)$) and a random generator $g \xleftarrow{\$} \mathbb{G}$. It chooses $h, Y \xleftarrow{\$} \mathbb{G}$, a vector $\mathbf{Z} = (Z_0, Z_1, \ldots, Z_n) \xleftarrow{\$} \mathbb{G}^{n+1}$ and $x \xleftarrow{\$} \mathbb{Z}_p^*$ at random. It defines the master public key as $\mathsf{mpk} := \big(X = g^x, Y, h, \{Z_i\}_{i=0}^n\big)$ while the master secret key is $\mathsf{msk} := x$.

Keygen$^{(\mathrm{PKG,U})}$ **:** to obtain a private key for his identity $\mathsf{ID} = i_1 \ldots i_n \in \{0,1\}^n$, a user U interacts with the PKG in the following key generation protocol, where the notation $H_{\mathbf{Z}}(\mathsf{ID})$ denotes $H_{\mathbf{Z}}(\mathsf{ID}) = Z_0 \cdot \prod_{j=1}^n Z_j^{i_j}$.

1. The user U draws $t_0, \theta \xleftarrow{\$} \mathbb{Z}_p^*$, provides the PKG with a commitment $R = h^{t_0} \cdot X^\theta$ and also runs an interactive witness indistinguishable proof of knowledge of the pair (t_0, θ) with the PKG, which he retains for later use.
2. The PKG outputs $\perp$ if the proof of knowledge fails to verify. Otherwise, it picks $r', t_1 \xleftarrow{\$} \mathbb{Z}_p^*$ and returns
$$d'_{\mathsf{ID}} = (d'_1, d'_2, d'_3) = \Big((Y \cdot R \cdot h^{t_1})^{1/x} \cdot H_{\mathbf{Z}}(\mathsf{ID})^{r'},\ X^{r'},\ t_1\Big). \tag{1}$$
3. U picks $r'' \xleftarrow{\$} \mathbb{Z}_p^*$ and computes $d_{\mathsf{ID}} = (d'_1/g^\theta \cdot H_{\mathbf{Z}}(\mathsf{ID})^{r''},\ d'_2 \cdot X^{r''},\ d'_3 + t_0)$ which should equal
$$d_{\mathsf{ID}} = (d_1, d_2, d_3) = \Big((Y \cdot h^{t_0+t_1})^{1/x} \cdot H_{\mathbf{Z}}(\mathsf{ID})^{r},\ X^{r},\ t_0 + t_1\Big) \tag{2}$$
where $r = r' + r''$. Then, U checks whether d_{ID} satisfies the relation
$$e(d_1, X) = e(Y, g) \cdot e(h, g)^{d_3} \cdot e(H_{\mathbf{Z}}(\mathsf{ID}), d_2). \tag{3}$$
If so, he sets his private key as d_{ID} and the latter belongs to the family of decryption keys identified by $d_3 = t_0 + t_1$. He outputs $\perp$ otherwise.

Encrypt: to encrypt $m \in \mathbb{G}_T$ given mpk and $\mathsf{ID} = i_1 \ldots i_n \in \{0,1\}^n$, define $H_{\mathbf{Z}}(\mathsf{ID}) = Z_0 \cdot \prod_{j=1}^{n} Z_i^{i_j}$, choose $s \xleftarrow{\$} \mathbb{Z}_p^*$ and compute

$$C = \big(C_1, C_2, C_3, C_4\big) = \Big(X^s,\ H_{\mathbf{Z}}(\mathsf{ID})^s,\ e(g,h)^s,\ m \cdot e(g,Y)^s\Big).$$

Decrypt: given $C = \big(C_1, C_2, C_3, C_4\big)$ and $d_{\mathsf{ID}} = (d_1, d_2, d_3)$, compute

$$m = C_4 \cdot \Big(\frac{e(C_1, d_1)}{e(C_2, d_2) \cdot C_3^{d_3}}\Big)^{-1} \tag{4}$$

The correctness of the scheme follows from the fact that well-formed private keys always satisfy relation (3). By raising both sides of (3) to the power $s \in \mathbb{Z}_p^*$, we see that the quotient of pairings in (4) actually equals $e(g,Y)^s$.

The scheme features about the same efficiency as classical IBE schemes derived from the commutative-blinding framework [7]. Encryption demands no pairing calculation since $e(g,h)$ and $e(g,Y)$ can both be cached as part of the system parameters. Decryption requires the computation of a quotient of two pairings which is significantly faster than two independent pairing evaluations when optimized in the same way as modular multi-exponentiations [27].

In comparison with the most efficient standard model scheme based on the same assumption (which is currently the first scheme of [7]), the only overhead is a slightly longer ciphertext and an extra exponentiation in $\mathbb{G}_T$ in encryption and decryption processes.

Now, we describe a black-box tracing mechanism that protects the user from a dishonest PKG as long as the latter is withheld access to a decryption oracle. The tracing strategy is close to the one used by Kiayias and Yung [33] in 2-user traitor tracing schemes, where the tracer determines which one out of two subscribers produced a pirate decoder. In our setting, one rather has to decide whether an ε-useful decryption device stems from the PKG or the user himself.

Trace$^{\mathbb{D}}(\mathsf{mpk}, d_{\mathsf{ID}}, \varepsilon)$**:** given a well-formed private key $d_{\mathsf{ID}} = (d_1, d_2, d_3)$ belonging to a user of identity ID and oracle access to a decoder $\mathbb{D}$ that decrypts ciphertexts encrypted for ID with probability ε, conduct the following steps.

a. Initialize a counter $ctr \leftarrow 0$ and repeat the next steps $L = 8\lambda/\varepsilon$ times:
   1. Choose two distinct random exponents $s, s' \xleftarrow{\$} \mathbb{Z}_p^*$, compute $C_1 = X^s$, $C_2 = H_Z(\mathsf{ID})^s$ and $C_3 = e(g,h)^{s'}$.
   2. Calculate $C_4 = m \cdot e(C_1, d_1)/\big(e(C_2, d_2) \cdot C_3^{d_3}\big)$ for a randomly chosen message $m \in \mathbb{G}_T$.
   3. Feed the decryption device $\mathbb{D}$ with (C_1, C_2, C_3, C_4). If $\mathbb{D}$ outputs $m' \in \mathbb{G}_T$ such that $m' = m$, increment ctr.

b. If $ctr = 0$, incriminate the PKG. Otherwise, incriminate the user.

3.2 IND-ID-CPA Security

We first prove the IND-ID-CPA security of $\mathcal{A}$-$\mathcal{IBE}_1$ under the modified DBDH assumption (mDBDH).

Theorem 1. *The scheme $\mathcal{A}$-$\mathcal{IBE}_1$ is IND-ID-CPA secure under the mDBDH assumption in $\mathcal{G}$. More precisely, assuming that an adversary running in time t has advantage ε in the IND-ID-CPA game after q key generation queries, there exists an algorithm solving the mDBDH problem with advantage $\varepsilon/(16(n+1)q)$ within time $t + O(\varepsilon^{-2}\ln(\varepsilon^{-1})\eta^{-1}\ln(\eta^{-1}))$, where $\eta = 1/(4(n+1)q)$.*

Proof. We show how a simulator $\mathcal{B}$ can interact with the IND-ID-CPA adversary $\mathcal{A}$ to solve a mDBDH instance $(g, T_a = g^a, T_b = g^b, T_c = g^c, T \stackrel{?}{=} e(g,g)^{ab/c})$. To prepare the master public key mpk, $\mathcal{B}$ chooses $\gamma, t^* \xleftarrow{\$} \mathbb{Z}_p^*$ and sets $X = T_c = g^c$, $h = T_b = g^b$, $Y = X^\gamma \cdot h^{-t^*}$.

The vector $\mathbf{Z} \in \mathbb{G}^{n+1}$ remains to be defined. To do so, $\mathcal{B}$ picks $\kappa_z \in \{0, \ldots, n\}$. Let τ_z be an integer such that $\tau_z(n+1) < p$ (a convenient choice is $\tau_z = 2q$, where q is the number of key generation queries, as in [45]).

The simulator randomly selects a vector $(\alpha_{z,0}, \alpha_{z,1}, \ldots, \alpha_{z,n})$ of elements with $\alpha_{z,j} \in \mathbb{Z}_{\tau_z}$ for all $0 \leq j \leq n$. It also draws another vector $(\beta_{z,0}, \beta_{z,1}, \ldots, \beta_{z,n})$, with $\beta_{z,j} \stackrel{\$}{\leftarrow} \mathbb{Z}_p$ for all j. The vector $\mathbf{Z} = (Z_0, Z_1, \ldots, Z_n)$ is chosen to be

$$Z_0 = g^{\alpha_{z,0} - \kappa_z \tau_z} \cdot X^{\beta_{z,0}} \qquad Z_j = g^{\alpha_{z,j}} \cdot X^{\beta_{z,j}} \quad \text{for } 1 \leq j \leq n. \tag{5}$$

For any string $\mathsf{ID} = i_1 \ldots i_n \in \{0,1\}^n$, it will be convenient to define the functions

$$J(\mathsf{ID}) = \alpha_{z,0} + \sum_{j=1}^{n} i_j \alpha_{z,j} - \kappa_z \tau_z, \qquad K(\mathsf{ID}) = \beta_{z,0} + \sum_{j=1}^{n} i_j \beta_{z,j},$$

so that $H_{\mathbf{Z}}(\mathsf{ID}) = g^{J(\mathsf{ID})} \cdot X^{K(\mathsf{ID})}$, that will be useful in later games.

The adversary's view is then simulated as follows.

Queries: at any time, $\mathcal{A}$ may trigger an execution of the key generation protocol for an identity ID of her choosing. In the event that $J(\mathsf{ID}) = 0$, $\mathcal{B}$ aborts and outputs a random bit. Otherwise, the query can be answered as follows. First, $\mathcal{A}$ supplies an element $R = h^{t_0} \cdot X^{\theta}$ along with a WI proof of knowledge of (t_0, θ). The simulator $\mathcal{B}$ verifies the proof but does not need to rewind the adversary as it can answer the query without knowing (t_0, θ). To do so, it picks $t_1 \stackrel{\$}{\leftarrow} \mathbb{Z}_p^*$ at random and defines $W = Y \cdot R \cdot h^{t_1}$, $d'_3 = t_1$. Elements d'_1 and d'_2 are generated as

$$(d'_1, d'_2) = \left(H_{\mathbf{Z}}(\mathsf{ID})^{r'} \cdot W^{-\frac{K(\mathsf{ID})}{J(\mathsf{ID})}},\ X^{r'} \cdot W^{-\frac{1}{J(\mathsf{ID})}} \right) \tag{6}$$

using a random $r' \stackrel{\$}{\leftarrow} \mathbb{Z}_p^*$. If we set $\tilde{r}' = r' - \frac{w}{cJ(\mathsf{ID})}$, where $w = \log_g(W)$, we observe that (d'_1, d'_2) has the correct distribution since

$$\begin{aligned} W^{1/c} \cdot H_{\mathbf{Z}}(\mathsf{ID})^{\tilde{r}'} &= W^{1/c} \cdot (g^{J(\mathsf{ID})} \cdot X^{K(\mathsf{ID})})^{\tilde{r}'} \\ &= W^{1/c} \cdot H_{\mathbf{Z}}(\mathsf{ID})^{r'} \cdot (g^{J(\mathsf{ID})})^{-\frac{w}{cJ(\mathsf{ID})}} \cdot X^{-\frac{wK(\mathsf{ID})}{cJ(\mathsf{ID})}} \\ &= H_{\mathbf{Z}}(\mathsf{ID})^{r'} \cdot W^{-\frac{K(\mathsf{ID})}{J(\mathsf{ID})}} \end{aligned}$$

and $X^{\tilde{r}'} = X^{r'} \cdot (g^c)^{-\frac{w}{cJ(\mathsf{ID})}} = X^{r'} \cdot W^{-\frac{1}{J(\mathsf{ID})}}$. Finally, the "partial private key" (d'_1, d'_2, d'_3) is returned to $\mathcal{A}$. Note that the above calculation can be carried out without knowing $w = \log_g(W)$ or the representation (t_0, θ) of R w.r.t. to (h, X).

Challenge: when the first stage is over, $\mathcal{A}$ outputs messages $m_0, m_1 \in \mathbb{G}_T$ and a target identity $\mathsf{ID}^\star$. At this point, $\mathcal{B}$ aborts and outputs a random bit if $J(\mathsf{ID}^\star) \neq 0$. Otherwise, $\mathcal{B}$ picks $r^\star \stackrel{\$}{\leftarrow} \mathbb{Z}_p^*$ and defines a private key $(d_1, d_2, d_3) = (g^\gamma \cdot X^{K(\mathsf{ID}^\star) \cdot r^\star}, X^{r^\star}, t^*)$ for the identity ID^*. It flips a fair coin $d^\star \stackrel{\$}{\leftarrow} \{0,1\}$ and encrypts $m_{d^\star}$ as

$$C_1^\star = T_a = g^a \qquad C_2^\star = T_a^{K(\mathsf{ID}^\star)} \qquad C_3^\star = T \qquad C_4^\star = m_{d^\star} \cdot \frac{e(C_1^\star, d_1)}{e(C_2^\star, d_2) \cdot C_3^{\star d_3}}.$$

We see that (d_1, d_2, d_3) is a valid key for the identity $\mathsf{ID}^\star$. Since $H_{\mathbf{Z}}(\mathsf{ID}^\star) = X^{K(\mathsf{ID}^\star)} = T_c^{K(\mathsf{ID}^\star)}$ and $h = g^b$, $C^\star = (C_1^\star, C_2^\star, C_3^\star, C_4^\star)$ is a valid encryption of $m_{d^\star}$ (with the exponent $s = a/c$) if $T = e(g,g)^{ab/c}$. If T is random, we have $T = e(g,h)^{s'}$ for some random $s' \in \mathbb{Z}_p^*$ and thus $C_4^\star = m_{d^\star} \cdot e(Y,g)^s \cdot e(g,h)^{(s-s')t^*}$, which means that $m_{d^\star}$ is perfectly hidden since $t^\star$ is independent of $\mathcal{A}$'s view.

At this stage the adversary's probability of success could be correlated with the probability that $\mathcal{B}$ needs to "naturally" abort (*i.e.*, because $J(\mathsf{ID}) = 0$ in some key generation query or $J(\mathsf{ID}^\star) \neq 0$ in the challenge phase). As in [45], one way to compensate this possible dependency is to introduce an artificial abort step that forces $\mathcal{B}$ to always abort with the maximal probability, regardless of the particular set of queries made by $\mathcal{A}$.

Namely, with $\tau_z = 2q$, the same analysis as [45] shows that $\mathcal{B}$'s probability not to abort for any set of queries is at least $\eta = 1/(4(n+1)q)$.

Lemma 1. *The probability that the simulator does not abort for any set of queries is at least* $1/(4(n+1)q)$.

Proof. If $\mathsf{ID}^\star$ denotes the challenge identity and if $\mathcal{A}$ queries private keys for the identities $(\mathsf{ID}_1, \ldots, \mathsf{ID}_q)$, we have $\Pr[J(\mathsf{ID}^\star) = 0 \bmod p] = \frac{1}{\tau_z(n+1)} = \frac{1}{2q(n+1)}$. Indeed, recall that $\mathcal{A}$ has no information on the values $(\alpha_{z,0}, \alpha_{z,1}, \ldots, \alpha_{z,n})$ and she can only come up with $\mathsf{ID}^\star$ such that $J(\mathsf{ID}^\star) = 0 \bmod p$ by chance so that

$$\Pr[J(\mathsf{ID}^\star) = 0 \bmod p]$$
$$= \Pr[J(\mathsf{ID}^\star) = 0 \bmod p | J(\mathsf{ID}^\star) = 0 \bmod \tau_u] \cdot \Pr[J(\mathsf{ID}^\star) = 0 \bmod \tau_z] = \frac{1}{\tau_z(n+1)}.$$

Also, a sufficient condition to have $J(\mathsf{ID}_j) \neq 0 \bmod p$ is to have $J(\mathsf{ID}_j) \neq 0 \bmod \tau_z$ and we thus consider this condition. We have

$$\Pr\Big[\bigwedge_{j=1}^{q} J(\mathsf{ID}_j) \neq 0 \bmod \tau_z | \Pr[J(\mathsf{ID}^\star) = 0 \bmod \tau_z\Big] = 1 - \Pr\Big[\bigvee_{j=1}^{q} J(\mathsf{ID}_j) = 0 \bmod \tau_z | J(\mathsf{ID}^\star) = 0 \bmod \tau_z\Big]$$
$$\geq 1 - \sum_{j=1}^{q} \Pr\big[J(\mathsf{ID}_j) = 0 \bmod \tau_z | J(\mathsf{ID}^\star) = 0 \bmod \tau_z\big] \geq 1 - \frac{q}{\tau_z}.$$

□

At the end of the game, $\mathcal{B}$ considers the sequence of queries $(\mathsf{ID}_1, \ldots, \mathsf{ID}_q, \mathsf{ID}^\star)$ made by $\mathcal{A}$ and estimate the probability that it causes the simulation to abort. This does not require new executions of $\mathcal{A}$ but rather involves repeatedly sampling vectors $(\alpha_{z,0}, \alpha_{z,1}, \ldots, \alpha_{z,n}) \xleftarrow{\$} \mathbb{Z}_{\tau_z}^{n+1}$ and assess $J(\mathsf{ID}_1), \ldots, J(\mathsf{ID}_q)$ and $J(\mathsf{ID}^\star)$ accordingly. Once the estimated probability η' has been obtained after $O(\varepsilon^{-2}\ln(\varepsilon^{-1})\eta^{-1}\ln(\eta^{-1}))$ samples, if $\eta' > \eta$, the simulator $\mathcal{B}$ artificially aborts and outputs a random bit with probability $1 - \eta/\eta'$ (and continues with probability η/η').

Eventually, if $\mathcal{B}$ did not naturally or artificially abort, it outputs 1 (meaning that $T = e(g,g)^{ab/c}$) if $\mathcal{A}$ successfully guesses $d' = d^\star$ and 0 otherwise. Using exactly the same analysis as in [45], we obtain that, if $\mathcal{A}$'s advantage is ε, $\mathcal{B}$ breaks the mDBDH assumption with probability $\varepsilon/(16(n+1)q)$. □

As in [45], the proof of theorem 1 makes use of the artificial abort step to ensure that the simulator's probability to abort is independent of the particular set of queries made by the adversary. The technique of Bellare and Ristenpart [6] can be applied to avoid this step and obtain an improved concrete security.

3.3 DishonestPKG and DishonestUser Security

The soundness of the tracing algorithm is proved using a similar technique to [1]. To ensure the independence of iterations, we assume (as in [1]) that pirate devices are stateless, or resettable, and do not retain information from prior queries: each decryption query is answered as if it were the first one and, in particular, the pirate device cannot self-destruct.

Theorem 2. *The scheme $\mathcal{A}$-IBE$_1$ is* DishonestUser-ID-BB*-secure under the mDBDH assumption in $\mathcal{G}$. More precisely, the advantage of any adversary $\mathcal{A}$, running in time t, in building a $\varepsilon(\lambda)$-useful decryption box, after q key generation queries, is at most* $\mathbf{Adv}_{\mathcal{A}}^{\text{DishonestUser-ID-BB}}(\lambda) \leq 16 \cdot q^2 \cdot (n+1) \cdot (\mathbf{Adv}^{\text{mDBDH}}(\lambda) + \exp(-\lambda))$ *for all algorithms $\mathcal{B}$ running in time at most* $t + O(\mathbf{Adv}_{\mathcal{A}}^{-2}\ln(\mathbf{Adv}_{\mathcal{A}}^{-1})\eta^{-1}\ln(\eta^{-1}))$*, where* $\eta = 1/(4(n+1)q)$.

Proof. We consider a DishonestUser-ID-BB adversary $\mathcal{A}$ and we construct a mDBDH algorithm $\mathcal{B}$ that will play the role of the DishonestUser-ID-BB challenger. Algorithm $\mathcal{B}$ gets a mDBDH instance (g, g^a, g^b, g^c, T) and generates the master public key as $X = g^c$, $h = g^b$, $Y = X^\gamma \cdot h^{-t^\star}$, for some $\gamma, t^\star \xleftarrow{\$} \mathbb{Z}_p$, and the vector $\mathbf{Z}$ is set up so as to have $H_{\mathbf{Z}}(\mathsf{ID}) = g^{J(\mathsf{ID})} \cdot X^{K(\mathsf{ID})}$ for efficiently computable functions $J, K : \{0,1\}^n \to \mathbb{G}$. Then, $\mathcal{A}$ is given the master public key and starts making key generation queries that the simulator $\mathcal{B}$ handles as follows. It will have to guess upfront (with probability $1/q$) which key generation query will involve the target identity $\mathsf{ID}^\star$. At the outset of the game, $\mathcal{B}$ thus picks a random index $j^\star \xleftarrow{\$} \{1, \ldots, q\}$ and eventually aborts if the target identity did not appear in the $j^{\star\text{th}}$ key generation query. During the game, it also aborts if one of the following events occurs.

A. The j^{th} query (with $j \neq j^\star$) involves an identity ID_j such that $J(\mathsf{ID}_j) = 0$.
B. The $j^{\star\text{th}}$ query involves an identity $\mathsf{ID}_{j^\star}$ such that $J(\mathsf{ID}_{j^\star}) \neq 0$.

For each query $j \in \{1, \ldots, q\} \backslash \{j^\star\}$, $\mathcal{B}$ can generate a private key as in the proof of Theorem 3.2 as long as event A does not occur. At the $j^{\star\text{th}}$ query, $\mathcal{B}$ first checks that $J(\mathsf{ID}_{j^\star}) = 0$ (*i.e.*, that event B does not occur), in which case it computes a private key by first rewinding $\mathcal{A}$ to extract (t_0, θ) such that $R = h^{t_0} X^\theta$. Then, $\mathcal{B}$ picks a random $r^\star \xleftarrow{\$} \mathbb{Z}_p$, defines $d'_3 = t^\star - t_0$ and can compute a partial private key $d'_{\mathsf{ID}^\star} = (d'_1, d'_2, d'_3)$ as

$$(d'_1, d'_2, d'_3) = \left(g^{\gamma+\theta} \cdot X^{K(\mathsf{ID}^\star)\cdot r^\star}, X^{r^\star}, t^* - t_0\right)$$

for the identity ID_{j^*}.

At the end of the game, $\mathcal{A}$ outputs a decryption box $\mathbb{D}$ that correctly decrypts a fraction ε of ciphertexts for the identity $\mathsf{ID}^\star$ and the master public key mpk. At this point, $\mathcal{B}$ aborts and outputs a random bit if $\mathsf{ID}^\star \neq \mathsf{ID}_{j^\star}$. Otherwise, it necessarily knows a valid full private key $d_{\mathsf{ID}^\star} = (d_1, d_2, d_3) = (g^\gamma \cdot H_{\mathbf{Z}}(\mathsf{ID}^\star)^r, X^r, t^\star)$ for the identity $\mathsf{ID}^\star$. At this stage, an artificial abort step is needed to make sure that $\mathcal{B}$ always aborts with the maximal probability regardless of the specific set of queries $(\mathsf{ID}_1, \ldots, \mathsf{ID}_q)$ made by $\mathcal{A}$. This time, the lower bound for $\mathcal{B}$'s probability not to abort for any set of queries is $\eta = 1/(4q^2(n+1))$ (in comparison with the proof of Theorem 1, an additional factor of $1/q$ is lost due to the random choice of $j^\star \xleftarrow{\$} \{1, \ldots, q\}$ at the beginning of the game).

Algorithm $\mathcal{B}$ then holds a ε-useful decryption box $\mathbb{D}$ for the identity $\mathsf{ID}^\star$ and mpk and it will use it to determine whether T is equal to $e(g,g)^{ab/c}$ or random.

It uses the decryption key $d_{\mathsf{ID}^\star}$ to construct $L = 8\lambda/\varepsilon$ random ciphertexts $C^{(i)} = (C_1^{(i)}, C_2^{(i)}, C_3^{(i)}, C_4^{(i)})$ for $i \in \{1, \ldots, L\}$ as

$$C_1^{(i)} = g^{a\rho_i} \cdot g^{c\nu_i}, \quad C_2^{(i)} = (g^{a\rho_i} \cdot g^{c\nu_i})^{K(\mathsf{ID}^\star)}, \quad C_3^{(i)} = T^{\rho_i} \cdot e(g, g^b)^{\nu_i}, \quad C_4^{(i)} = m^{(i)} \cdot \frac{e(C_1^{(i)}, d_1)}{e(C_2^{(i)}, d_2) \cdot (C_3^{(i)})^{t^\star}}$$

where $T \in \mathbb{G}_T$ is part of the mDBDH instance and $(m^{(i)}, \rho^{(i)}, \nu^{(i)}) \in \mathbb{G}_T \times (\mathbb{Z}_p^*)^2$ are picked independently and uniformly at random for each $i \in \{1, \ldots, L\}$. Algorithm $\mathcal{B}$ simulates the tracing algorithm with these ciphertexts $C^{(1)}, \ldots, C^{(L)}$. If $T = e(g,g)^{ab/c}$, all ciphertexts are properly formed encryptions of plaintexts $m^{(i)}$ with the encryption exponents $s_i = \nu_i + (a/c) \cdot \rho_i$ and $\mathbb{D}$ correctly decrypts with probability ε. If $T \neq e(g,g)^{ab/c}$ (say, $T = e(g,g)^{\delta + ab/c}$ for some random $\delta \neq 0$), $\mathbb{D}$ is given ciphertexts $C^{(i)}$ where each $C_3^{(i)}$ has been tampered with and $C^{(i)}$ thus corresponds to a ciphertext produced by the tracing algorithm with the encryption exponents $s_i = \nu_i + (a/c) \cdot \rho_i$ and $s'_i = \nu_i + (\delta + a/c) \cdot \rho_i$ (observe that, since $\delta \neq 0$, these look independent to the adversary).

The tracing algorithm (simulated by $\mathcal{B}$) points to the PKG if it ends up with $ctr = 0$. If $T = e(g,g)^{ab/c}$, the variable ctr can be seen as the sum of L independent random variables $X_i \in \{0, 1\}$ having the same expected value ε. We have $\mu = \mathbf{E}[ctr] = L\varepsilon = 8\lambda$. The Chernoff bound tells us that, for any real number ω such that $0 \leq \omega \leq 1$, $\Pr[ctr < (1-\omega)\mu] < \exp(-\mu\omega^2/2)$. With $\omega = 1/2$, the Chernoff bound guarantees that

$$\Pr[ctr < 1] < \Pr[ctr < 4\lambda] = \Pr[ctr < \mu/2] < \exp(-\mu/8) = \exp(-\lambda).$$

If $T = e(g,g)^{ab/c}$, conditionally on the simulator not aborting, the decoder $\mathbb{D}$ must output the correct plaintext $m^{(i)}$ at some iteration with overwhelming probability $1 - \exp(-\lambda)$. In other words, if we call E the event of the tracing procedure ending up with $ctr = 0$, we have $\Pr[E] < \exp(-\lambda)$ when $T = e(g,g)^{ab/c}$. Moreover, if E occurs with substantially higher probability when $T = e(g,g)^{ab/c}$ is replaced by $T \in_R \mathbb{G}_T$, there must be a distinguisher for the mDBDH assumption. Since the advantage of $\mathcal{A}$ is precisely the probability $\Pr[E]$ when $T \in_R \mathbb{G}_T$, it comes that $\mathcal{A}$ cannot frame the PKG if the mDBDH assumption holds.

Taking the artificial abort step (which is conducted by $\mathcal{B}$ exactly as in the proof of theorem 1) into account, it eventually comes that $\mathbf{Adv}_{\mathcal{A}}^{\mathsf{DishonestUser\text{-}ID\text{-}BB}}(\lambda) \leq 16 \cdot q^2 \cdot (n+1) \cdot (\mathbf{Adv}^{\text{mDBDH}}(\lambda) + \exp(-\lambda))$. □

The system turns out to be the first scheme that achieves weak black-box traceability against dishonest users in the adaptive-ID sense. Due to their reliance on attribute-based encryption techniques (for which

only selective-ID adversaries were dealt with until very recently), earlier (weak) black-box A-IBE proposals [29, 30] are only known to provide selective-ID security against dishonest users.

As for the security against dishonest PKGs, we observe that, in the DishonestPKG-wBB game, the last part $d_3 = t$ of the user's private key is perfectly hidden to the malicious PKG after the key generation protocol. Then, a pirate decoder $\mathbb{D}$ made by the PKG has negligible chance of decrypting ciphertexts where C_3 is random in the same way as the user would. When the user comes across $\mathbb{D}$ and takes it to the court, the latter runs the tracing algorithm using $\mathbb{D}$ and the user's well-formed key $d_{\mathsf{ID}} = (d_1, d_2, d_3)$ for which d_3 is independent of $\mathbb{D}$.

Lemma 2. *In the* DishonestPKG-wBB *game, one iteration of the tracing algorithm increases ctr with probability at most* $1/p$.

Proof. After the key generation protocol, a dishonest PKG has no information on part $d_3 \in \mathbb{Z}_p$ of the user's private key. This follows from the perfectly hiding property of Pedersen's commitment [38] and the perfect witness indistinguishability of the protocol [37] for proving knowledge of a discrete logarithm representation. Since the commitment $R = h^{t_0} \cdot X^{\theta}$ and the proof of knowledge of (t_0, θ) perfectly hide t_0 to the PKG, all elements of $\mathbb{Z}_p^*$ are equally likely values of $d_3 = t_0 + t_1$ as for the last part of the user's eventual private key.

In an iteration of the tracing stage, $\mathbb{D}$ is given $C = (C_1, C_2, C_3, C_4)$ such that $C_1 = X^s$, $C_2 = (g^{\mathsf{ID}} \cdot Z)^s$, $C_3 = e(g,h)^{s'}$ and $C_4 = m \cdot e(g,Y)^s \cdot e(g,h)^{(s-s')t}$ for distinct $s, s' \xleftarrow{\$} \mathbb{Z}_p^*$. Since $\mathbb{D}$ has no information on $d_3 = t$, for any plaintext $m \in \mathbb{G}_T$, there is a value d_3 that explains C_4 and it comes that $\mathbb{D}$ returns the one chosen by the tracer with probability $1/p$. □

We note that a pirate device $\mathbb{D}$ generated by the dishonest PKG is able to recognize invalid ciphertexts in the tracing stage (as it may contain the master secret x). However, as long as $\mathbb{D}$ is assumed stateless, it cannot shutdown or self-destruct when detecting a tracing attempt. Moreover, with all but negligible probability, it will never be able to decrypt such invalid ciphertexts in the same way as the owner of d_{ID} would.

Theorem 3. *The scheme* $\mathcal{A}$-*IBE*$_1$ *is statistically* DishonestPKG-wBB*-secure. More precisely, the advantage of any adversary* $\mathcal{A}$ *in building a* $\varepsilon(\lambda)$*-useful decryption box is at most* $\mathbf{Adv}^{\mathsf{DishonestPKG\text{-}wBB}}(\lambda) \leq 8\lambda/(2^{\lambda}\varepsilon(\lambda))$.

Proof. The dishonest PKG is not detected if it outputs a decryption box for which the tracing algorithm ends with a non-zero value of *ctr*. However, this can only happen with negligible probability. Indeed, from Lemma 2, it easily comes that $\Pr[ctr \neq 0] = \Pr[ctr \geq 1] \leq L/p = 8\lambda/(\varepsilon p) \leq 8\lambda/(2^{\lambda}\varepsilon)$. □

To secure the scheme against chosen-ciphertext attacks and preserve the weak black-box property, we can use the Canetti-Halevi-Katz [17] technique or its optimizations [13, 14] that do not affect the tracing algorithm.

4 Extension to Gentry's IBE scheme

In this section, we show how to apply the weak black-box tracing mechanism of Section 3 to Gentry's IBE scheme. The resulting A-IBE scheme, called $\mathcal{A}$-*IBE*$_2$, system is obtained by bringing a simple modification to the key generation protocol of Goyal's first scheme [29] so as to perfectly hide the user's key family from the PKG's view while preserving the efficiency of the whole scheme.

The advantage of this scheme is to directly provide adaptive-ID security against dishonest users and under reductions that are just as tight as in Gentry's system. On the other hand, as in [25], a stronger assumption is needed in security proofs.

The q**-Decision Augmented Bilinear Diffie-Hellman Exponent Problem** (q-ADBDHE) is to distinguish $e(g,h)^{(\alpha^{q+1})}$ from a random element in $\mathbb{G}_T$ given $\left(g, g^{\alpha}, \ldots, g^{(\alpha^q)}, h, h^{(\alpha^{q+2})}\right)$ for a random triple $(g, h, \alpha) \in \mathbb{G}^2 \times \mathbb{Z}_p^*$.

Definition 5 ([25]). *Let* $\mathcal{G}$ *be a bilinear-group generator and let* $\mathcal{A}$ *be a* 0/1*-valued PPT algorithm. We consider the following experiment, where* $\lambda \in \mathbb{N}$ *is a security parameter:*

$\boxed{\mathbf{Game}_{\mathcal{A}}^{q\text{-ADBDHE}}(\lambda)}$
$(\mathbb{G}, \mathbb{G}_T, e, p) \xleftarrow{\$} \mathcal{G}(\lambda)$
$(g, h) \xleftarrow{\$} \mathbb{G}^2$; $(\alpha, \beta) \xleftarrow{\$} (\mathbb{Z}_p^*)^2$
$T_0 \leftarrow e(g,h)^{(\alpha^{q+1})}$; $T_1 \leftarrow e(g,h)^{\beta}$
$d^\star \xleftarrow{\$} \{0,1\}$
$d \leftarrow \mathcal{A}\big((\mathbb{G}, \mathbb{G}_T, e, p), g, g^{\alpha}, \cdots, g^{(\alpha^q)}, h, h^{(\alpha^{q+2})}, T_{d^\star}\big)$
`return` 1 `if` $d = d^\star$ `and` 0 `otherwise`.

$\mathcal{A}$'s advantage is measured by $\mathbf{Adv}_{\mathcal{A}}^{q\text{-ADBDHE}}(\lambda) = \Pr[\mathbf{Game}_{\mathcal{A}}^{q\text{-ADBDHE}} = 1]$. *Analogously to definition 4, the bilinear-group generator $\mathcal{G}$ is said* q-ADBDHE-secure *if, for all PPT algorithms $\mathcal{A}$, the advantage of $\mathcal{A}$ is a negligible function of λ. In this case, we say that the* q-ADBDHE assumption *holds for $\mathcal{G}$.*

4.1 Description of $\mathcal{A}$-IBE_2

In the description hereafter, the encryption and decryption algorithms are exactly as in [25]. Since the key generation protocol perfectly conceals the user's key family, we can apply the same weak black-box tracing mechanism as in Section 3. The resulting system turns out to be the most efficient adaptive-ID secure weakly black-box A-IBE scheme to date.

Let $\mathcal{G}$ be a bilinear-group generator.

Setup: given a security parameter $\lambda \in \mathbb{N}$, the PKG selects bilinear groups $(\mathbb{G}, \mathbb{G}_T, e, p)$ of prime order $p > 2^\lambda$ (by running $\mathcal{G}(\lambda)$) and a generator $g \xleftarrow{\$} \mathbb{G}$. It picks $h, g \xleftarrow{\$} \mathbb{G}$ and $\alpha \xleftarrow{\$} \mathbb{Z}_p^*$ at random. It defines the master key as $\mathsf{msk} := \alpha$ and the master public key is defined to be $\mathsf{mpk} := (g, g_1 = g^\alpha, h)$.

Keygen$^{(\mathrm{PKG,U})}$ **:** the user U and the PKG interact in the following protocol.

1. U picks $t_0, \theta \xleftarrow{\$} \mathbb{Z}_p^*$ and sends a commitment $R = g^{-t_0} \cdot (g_1 \cdot g^{-\mathsf{ID}})^\theta$ to the PKG. He also gives an interactive witness indistinguishable proof of knowledge of the pair (t_0, θ).
2. The PKG outputs $\perp$ if the proof of knowledge is invalid. Otherwise, it picks $t_1 \xleftarrow{\$} \mathbb{Z}_p^*$ and returns
$$d'_{\mathsf{ID}} = (d', t'_{\mathsf{ID}}) = \Big((h \cdot R \cdot g^{-t_1})^{1/(\alpha - \mathsf{ID})},\ t_1\Big). \tag{7}$$
3. U computes $d_{\mathsf{ID}} = (d'/g^\theta,\ t'_{\mathsf{ID}} + t_0)$ which should equal
$$d_{\mathsf{ID}} = (d, t_{\mathsf{ID}}) = \Big((h \cdot g^{-(t_0+t_1)})^{1/(\alpha - \mathsf{ID})},\ t_0 + t_1\Big). \tag{8}$$
Then, U checks whether d_{ID} satisfies the relation
$$e(d, g_1 \cdot g^{-\mathsf{ID}}) = e(h, g) \cdot e(g, g)^{-t_{\mathsf{ID}}}. \tag{9}$$
If so, he sets his private key as d_{ID}, which belongs to the key family identified by $t_{\mathsf{ID}} = t_0 + t_1$. He outputs $\perp$ otherwise.

Encrypt: to encrypt $m \in \mathbb{G}_T$ given mpk and ID, choose $s \xleftarrow{\$} \mathbb{Z}_p^*$ and compute
$$C = \big(C_1, C_2, C_3\big) = \Big(\big(g_1 \cdot g^{-\mathsf{ID}}\big)^s,\ e(g,g)^s,\ m \cdot e(g,h)^s\Big).$$

Decrypt: given $C = \big(C_1, C_2, C_3\big)$ and $d_{\mathsf{ID}} = (d, t_{\mathsf{ID}})$, compute
$$m = C_3 \cdot \Big(e(C_1, d) \cdot C_2^{t_{\mathsf{ID}}}\Big)^{-1}$$

Trace$^{\mathbb{D}}(\mathsf{mpk}, d_{\mathsf{ID}}, \varepsilon)$**:** given a valid private key $d_{\mathsf{ID}} = (d, t_{\mathsf{ID}})$ belonging to user ID and a ε-useful pirate decoder $\mathbb{D}$, conduct the following steps.

a. Set $ctr \leftarrow 0$ and repeat the next steps $L = 8\lambda/\varepsilon$ times:
   1. Choose $s, s' \xleftarrow{\$} \mathbb{Z}_p^*$ such that $s \neq s'$ and set $C_1 = (g_1 \cdot g^{-\mathsf{ID}})^s$ and $C_2 = e(g,g)^{s'}$.
   2. Compute $C_3 = m \cdot e(C_1, d) \cdot C_2^{t_{\mathsf{ID}}}$ for a random message $m \in \mathbb{G}_T$.
   3. Feed the decryption device $\mathbb{D}$ with (C_1, C_2, C_3). If $\mathbb{D}$ outputs $m' \in \mathbb{G}_T$ such that $m' = m$, increment ctr.

b. If $ctr = 0$, incriminate the PKG. Otherwise, incriminate the user.

4.2 Security

The IND-ID-CPA security of the scheme $\mathcal{A}$-IBE_2 can be simply reduced to that of Gentry's IBE scheme as shown in the proof of the next theorem.

Theorem 4. *Any IND-ID-CPA adversary against $\mathcal{A}$-IBE_2 implies an IND-ID-CPA attacker against Gentry's IBE scheme.*

Proof. Let us assume an IND-ID-CPA adversary $\mathcal{A}$ in the game described by definition 2. We show that $\mathcal{A}$ gives rise to an IND-ID-CPA adversary $\mathcal{B}$ against Gentry's IBE scheme.

Our adversary $\mathcal{B}$ receives a master public key $\mathsf{mpk} = (g, g_1, h)$ from her challenger. When the A-IBE adversary $\mathcal{A}$ makes a key generation request for an identity ID, $\mathcal{B}$ queries her own challenger to extract a private key $d_{\mathsf{ID}} = (d, t_{\mathsf{ID}}) = \big((h \cdot g^{-t_{\mathsf{ID}}})^{1/(\alpha - \mathsf{ID})}, t_{\mathsf{ID}}\big)$ and starts executing the key generation protocol with in interaction with $\mathcal{A}$. The latter first supplies a commitment $R = g^{-t_0} \cdot (g_1 \cdot g^{-\mathsf{ID}})^\theta$ and an interactive WI proof of knowledge of the pair (t_0, θ). Using the knowledge extractor of the proof of knowledge, $\mathcal{B}$ extracts (t_0, θ) by rewinding $\mathcal{A}$ and returns $d_{\mathsf{ID}} = (d', t'_{\mathsf{ID}})$, where $t'_{\mathsf{ID}} = t_{\mathsf{ID}} - t_0$ and $d' = d_{\mathsf{ID}} \cdot g^\theta$.

In the challenge phase, $\mathcal{A}$ chooses a target identity $\mathsf{ID}^\star$ and messages (m_0, m_1), which $\mathcal{B}$ forwards to her own challenger. The latter provides $\mathcal{B}$ with a challenge ciphertext (C_1, C_2, C_3) which is relayed to $\mathcal{A}$. After a second series of key generation queries, $\mathcal{A}$ outputs a bit $d \in \{0,1\}$, which is also $\mathcal{B}$'s output. It is easy to see that, if $\mathcal{A}$ is successful, so is $\mathcal{B}$. □

We now turn to prove the weak black-box traceability property.

Theorem 5. *In the Adaptive-ID* DishonestUser-ID-BB *game and for a ε-useful device $\mathbb{D}$, the probability that the tracing algorithm accuses the PKG is at most* $\mathbf{Adv}_{\mathcal{A}}^{\mathsf{DishonestUser\text{-}ID\text{-}BB}}(\lambda) < \mathbf{Adv}_{\mathbb{G},\mathbb{G}_T}^{q\text{-ADBDHE}}(\lambda) + \exp(-\lambda)$, *where q is the number of key generation queries.*

Proof. The proof is very similar to the proof of IND-ID-CPA security in [25]. For the sake of contradiction, let us assume that the dishonest user gets the tracing algorithm to accuse the PKG with non-negligible probability. Then, we can construct a distinguisher $\mathcal{B}$ for the q-ADBDHE assumption.

The distinguisher $\mathcal{B}$ takes as input $(g, g^\alpha, \ldots, g^{(\alpha^q)}, h, h^{(\alpha^{q+2})}, T)$ and aims at deciding if $T = e(g,h)^{(\alpha^{q+1})}$. It generates the master public key in such a way that $g_1 = g^\alpha$ and $h = g^{f(\alpha)}$, for some random polynomial $f(X) \in \mathbb{Z}_p[X]$ of degree q. At each key generation query, $\mathcal{B}$ first computes a valid private key $d_{\mathsf{ID}} = (d, t_{\mathsf{ID}})$ for the identity ID, by setting $t_{\mathsf{ID}} = f(\mathsf{ID})$ as in the proof of Theorem 1 in [25]. Then, in the interactive key generation protocol, $\mathcal{A}$ sends a commitment $R = g^{-t_0} \cdot (g_1 \cdot g^{-\mathsf{ID}})^\theta$ and proves knowledge of the pair (t_0, θ), which $\mathcal{B}$ extracts by rewinding $\mathcal{A}$ as in the proof of Theorem 4. As in the latter, $\mathcal{B}$ replies with a well-distributed pair $d'_{\mathsf{ID}} = (d', t'_{\mathsf{ID}})$, where $t'_{\mathsf{ID}} = t_{\mathsf{ID}} - t_0$ and $d' = d \cdot g^\theta$.

The game ends with $\mathcal{A}$ outputting an identity ID^*, a private key $d_{\mathsf{ID}^\star} = (d^\star, t^\star_{\mathsf{ID}^\star})$ and a ε-useful device. In the tracing stage, $\mathcal{B}$ first expands $F(X) = (X^{q+2} - \mathsf{ID}^{\star q+2})/(X - \mathsf{ID}^\star) = X^{q+1} + F_q X^q + \cdots + F_1 X + F_0$. Then, $\mathcal{B}$ chooses a plaintext $m^{(1)}, \ldots, m^{(L)} \xleftarrow{\$} \mathbb{G}_T$ and, for $i = 1$ to L, computes $C^{(i)} = (C_1^{(i)}, C_2^{(i)}, C_3^{(i)})$ as

$$C_1^{(i)} = \Big(\frac{h^{(\alpha^{q+2})}}{h^{(\mathsf{ID}^{\star} q+2)}}\Big)^{\rho_i} \cdot (g_1 \cdot g^{-\mathsf{ID}})^{\nu_i} \qquad C_2^{(i)} = T^{\rho_i} \cdot e\big(h^{\rho_i}, \prod_{j=0}^{q} (g^{(\alpha_j) F_j})\big) \cdot e(g,g)^{\nu_i}$$

$$C_3^{(i)} = m^{(i)} \cdot e(C_1^{(i)}, d^\star) \cdot {C_2^{(i)}}^{t^\star_{\mathsf{ID}^\star}}.$$

As in the security proof of [25], $(C_1^{(i)}, C_2^{(i)}, C_3^{(i)})$ is a well-formed ciphertext with the encryption exponent $s_i = \nu_i + \rho_i \cdot \log_g(h)F(\alpha)$ if $T = e(g,h)^{(\alpha^{q+1})}$. In this case, $\mathbb{D}$ should return m_i with probability ε. In contrast, if $T = e(g,h)^{\delta+(\alpha^{q+1})}$ for some random $\delta \neq 0$, the i^{th} ciphertext $C^{(i)} = (C_1^{(i)}, C_2^{(i)}, C_3^{(i)})$ can be written as $C^{(i)} = \big((g_1 \cdot g^{-\mathsf{ID}^\star})^{s_i}, e(g,g)^{s'_i}, m \cdot e(C_1^{(i)}, d^\star) \cdot C_2^{(i)^{t^\star_{\mathsf{ID}^\star}}}\big)$, where $s_i = \nu_i + \rho_i \cdot \log_g(h)F(\alpha)$ and $s'_i = s_i + \rho_i \cdot \delta \cdot \log_g(h)$, which corresponds to a ciphertext produced by the tracing algorithm.

Using the same arguments as in the proof of theorem 2, we find that, if $T = e(g,h)^{(\alpha^{q+1})}$, the probability that $\mathbb{D}$ never manages to return the correct plaintext $m^{(i)}$ is smaller than $\exp(-\lambda)$. Moreover, if the probability of the latter event becomes non-negligible when $T \in_R \mathbb{G}_T$, there must be a distinguisher for the q-ADBDHE assumption. In summary, if $\mathbb{D}$ eventually frames the PKG, it should be able to somehow distinguish valid ciphertexts from those produced by the tracing algorithm and the q-ADBDHE assumption is broken. □

The weak black-box security against dishonest PKGs follows from the information theoretic secrecy of the user's private key element t_{ID} upon termination of the key generation protocol.

Lemma 3. *In the* DishonestPKG-wBB *game, each iteration of the tracing procedure increases ctr with probability at most* $1/p$.

Proof. As in the proof of lemma 2, during the key generation protocol, the dishonest PKG obtains no information on part $t_{\mathsf{ID}} \in \mathbb{Z}_p$ of the user's key thanks to the unconditional hiding property of Pedersen's commitment [38] and the perfect witness indistinguishability of the interactive proof of knowledge of a discrete logarithm representation [37].

Let us consider what happens in one iteration of the tracing algorithm. The pirate device $\mathbb{D}$ is given $C = (C_1, C_2, C_3)$ such that $C_1 = (g_1 \cdot g^{-\mathsf{ID}})^s$, $C_2 = e(g,g)^{s'}$ and $C_3 = m \cdot e(g,h)^s \cdot e(g,h)^{(s-s')t_{\mathsf{ID}}}$ for distinct exponents $s, s' \xleftarrow{\$} \mathbb{Z}_p^*$. Since the pirate device $\mathbb{D}$ has no information on t_{ID}, for any message $m \in \mathbb{G}_T$, there exists a value t_{ID} that explains C_3. Hence, $\mathbb{D}$ has probability at most $1/p$ to return the particular plaintext $m \in \mathbb{G}_T$ that was chosen at random by the tracer. □

Theorem 6. *In the information theoretic sense, no (computationally unbounded) adversary has non-negligible advantage in the* DishonestPKG-wBB *game.*

Proof. The dishonest PKG wins the DishonestPKG-wBB game if it outputs a decryption box $\mathbb{D}$ for which the tracing procedure increases *ctr* at least once. However, this only happens with negligible probability. Indeed, from Lemma 3, we find that $\Pr[ctr \neq 0] = \Pr[ctr \geq 1] \leq L/p = 8\lambda/(\varepsilon p) \leq 8\lambda/(2^\lambda \varepsilon)$. □

To secure the scheme against chosen-ciphertext attacks, we cannot use hash proof systems as suggested in [25, 34]. This technique would indeed cause the decryption algorithm to reject all invalid ciphertexts with high probability, which would not be compatible with our weak black-box tracing mechanism.

Fortunately, CCA-security can be acquired by applying the Canetti-Halevi-Katz transformation to a two-receiver variant of the Gentry-Waters Identity-Based Broadcast Encryption (IBBE) scheme [26], which is very similar to Gentry's IBE in the shape of its ciphertexts and private keys. In this section, we chose to illustrate how the weak black-box technique can be applied to Gentry's IBE for the sake of simplicity since the Gentry-Waters system is substantially more complex to describe.

An IBBE scheme is an IBE scheme where the sender can encrypt a message for several receivers using their identities (a formal definition is given in section A): the sender takes as input the master public key mpk and a set $S = \{\mathsf{ID}_1, \ldots, \mathsf{ID}_s\}$ of identities and computes a ciphertext C which can be decrypted using a private key d_{ID} for any identity $\mathsf{ID} \in S$. The IND-ID-CPA security of IBBE schemes is defined by a game where the adversary can obtain private keys for arbitrary identities as in the usual notion of IND-ID-CPA security. In the challenge phase, the adversary chooses an identity set $S^\star = \{\mathsf{ID}_1^\star, \ldots, \mathsf{ID}_s^\star\}$ o and obtains an encryption of a message $m_{d^\star} \in \{m_0, m_1\}$, for a random bit $d^\star \xleftarrow{\$} \{0,1\}$ which the adversary has to guess without obtaining private keys for identities in $S^\star$ at any time.

From an IND-ID-CPA security secure IBBE scheme $\Pi_1^{\text{IBBE}} = (\text{Setup}, \text{Keygen}, \text{Encrypt}, \text{Decrypt})$ where the sender can encrypt a ciphertext for up to n identities, the Canetti-Halevi-Katz transform gives a CCA2-secure IBBE scheme $\Pi_2^{\text{IBBE}} = (\mathbf{Setup}, \mathbf{Keygen}, \mathbf{Encrypt}, \mathbf{Decrypt})$ where ciphertexts can be encrypted for

at most $n-1$ receivers. The setup algorithms are identical in both schemes whereas Π_2^{IBBE} derives keys using the key generation algorithm of Π_1^{IBBE} as $d_{\mathsf{ID}} = \Pi_2^{\text{IBBE}}.\mathbf{Keygen}(\mathsf{msk}, \mathsf{ID}) = \Pi_1^{\text{IBBE}}.\mathbf{Keygen}(\mathsf{msk}, (0||\mathsf{ID}))$. In order to encrypt a message M for the receiver set $S = \{\mathsf{ID}_1, \ldots, \mathsf{ID}_s\}$, the encryption algorithm of Π_2^{IBBE} proceeds by first generating a one-time signature key pair $(\mathsf{VK}, \mathsf{SK})$ and computing the ciphertext $C = \Pi_1^{\text{IBBE}}.\mathbf{Encrypt}(\mathsf{mpk}, S)$ for the identity set $S = \{\mathsf{ID}'_0 = (1||\mathsf{VK}), \mathsf{ID}'_1 = (0||\mathsf{ID}_1), \ldots, \mathsf{ID}'_s = (0||\mathsf{ID}_s)\}$. The final ciphertext consists of $C' = (\mathsf{VK}, C, \sigma)$, where $\sigma = \text{Sig}_{\mathsf{SK}}(C)$ is a one-time signature of the message C. It is easy to see (as previously reported in [22] for instance) that the resulting IBBE Π_2^{IBBE} is IND-ID-CCA secure as long as Π_1^{IBBE} IND-ID-CPA secure and the one-time signature is strongly unforgeable.

From a two-receiver variant of the Gentry-Waters IBBE, we can thus construct an IND-ID-CCA (single receiver) IBE in a very simple way: one of the two receivers' identities is set to be the verification key VK of a strongly unforgeable one-time signature and the matching private key SK is used to sign the whole ciphertext.

Our tracing algorithm can be combined with the latter approach since, in the Gentry-Waters IBBE scheme [26], private keys have the same shape as in Gentry's IBE scheme and one of the ciphertext components lives in the group $\mathbb{G}_T$. As already mentioned, the CHK technique does not affect traceability as, upon decryption, ill-formed ciphertexts only get rejected when the one-time signature verification fails. The computational/bandwidth cost of the resulting system exceeds that of the above A-IBE construction only by a small factor.

5 Extension to Identity-Based Broadcast Encryption

As already stressed in [29, 30], reducing the required amount of trust in PKGs is an equally important problem in IBE schemes and their extensions such as attributed-based encryption or IBBE.

In this section, we thus show how the underlying idea of previous schemes can be applied to one of the most efficient IBBE realizations to date.

In [12], Boneh and Hamburg showed how to turn the Boneh-Boyen-Goh hierarchical IBE scheme [9] into an efficient IBBE system which is recalled in appendix A, where we also recall the syntax of the IBBE primitive. This scheme features constant-size ciphertexts and linear-size private keys in the bound N on the number of receivers per ciphertext. Their construction was shown to derive from a more general primitive termed "spatial encryption".

Its security (in the selective-ID sense) was established under the **ℓ-Decision Bilinear Diffie-Hellman Exponent** assumption (ℓ-DBDHE) introduced in [9].

Definition 6. *Let $\mathcal{G}$ be a bilinear-group generator and let $\mathcal{A}$ be a 0/1-valued PPT algorithm. We consider the following random experiments, where $\lambda \in \mathbb{N}$ is a security parameter:*

$\boxed{\mathbf{Game}_{\mathcal{A}}^{\ell\text{-DBDHE}}(\lambda)}$
$(\mathbb{G}, \mathbb{G}_T, e, p) \xleftarrow{\$} \mathcal{G}(\lambda)$
$(g, h) \xleftarrow{\$} \mathbb{G}^2$; $(\alpha, \beta) \xleftarrow{\$} (\mathbb{Z}_p^*)^2$
$T_0 \leftarrow e(g,h)^{(\alpha^{\ell+1})}$; $T_1 \leftarrow e(g,h)^{\beta}$
$d^\star \xleftarrow{\$} \{0,1\}$
$d \leftarrow \mathcal{A}((\mathbb{G}, \mathbb{G}_T, e, p), g, g^{\alpha}, \ldots, g^{(\alpha^{\ell})}, g^{(\alpha^{\ell+2})}, \ldots, g^{(\alpha^{2\ell})}, h, T_{d^\star})$
return 1 *if* $d = d^\star$ *and* 0 *otherwise.*

$\mathcal{A}$'s advantage is $\mathbf{Adv}_{\mathcal{A}}^{\ell\text{-DBDHE}}(\lambda) = \Pr[\mathbf{Game}_{\mathcal{A}}^{\ell\text{-DBDHE}} = 1]$. *The bilinear-group generator $\mathcal{G}$ is said* ℓ-DBDHE-secure *if, for any PPT distinguisher $\mathcal{A}$, $\mathcal{A}$'s advantage is a negligible function of λ. In this case, we say that the* ℓ-DBDHE assumption *holds for $\mathcal{G}$.*

In the following, we use the same notations as in [12] and, for any vector $\mathbf{a} = (a_0, \ldots, a_N) \in \mathbb{Z}_p^{N+1}$, $g^{\mathbf{a}}$ stands for the vector $(g^{a_0}, \ldots, g^{a_N}) \in \mathbb{G}^{N+1}$.

5.1 A weak Black-Box Accountable Authority IBBE scheme

The idea of the scheme in Section 3 applies to construct an IBBE scheme with short ciphertexts and accountable authorities. The syntax of accountable authority IBBE (A-IBBE) schemes extends that of IBBE systems in the same way as the A-IBE primitive extends IBE schemes. The resulting construction, termed *A-IBBE*, goes as follows.

Setup(λ, N)**:** given a security parameter $\lambda \in \mathbb{N}$ and the maximal number of receivers $N \in \mathbb{N}$ per ciphertext, choose bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order $p > 2^\lambda$ and a generator $g \xleftarrow{\$} \mathbb{G}$. Choose $z \xleftarrow{\$} \mathbb{G}$ as well a $(N+1)$-vector $\mathbf{h} = (h_0, h_1, \ldots, h_N) \xleftarrow{\$} \mathbb{G}^{N+1}$ of random generators so that $h_i = g^{a_i}$, for $i = 0$ to N, with a randomly chosen $\mathbf{a} = (a_0, \ldots, a_N) \xleftarrow{\$} \mathbb{Z}_p^{N+1}$. Finally, pick $\alpha \xleftarrow{\$} \mathbb{Z}_p^*$, $g_2, g_3 \xleftarrow{\$} \mathbb{G}$ and compute $g_1 = g^\alpha$. The master public key is $\mathsf{mpk} = (g, g_1 = g^\alpha, g_2, g_3, z, \mathbf{h} = g^{\mathbf{a}})$ while the master secret is $\mathsf{msk} = (\mathbf{a}, \alpha)$.

Keygen$^{(\mathrm{PKG,U})}$ **:** the two parties conduct the following interactive steps.

1. U picks $t_0, \theta \xleftarrow{\$} \mathbb{Z}_p^*$ and sends a commitment $R = g_2^{t_0} \cdot g^\theta$ to the PKG and provides an interactive WI proof of knowledge of (t_0, θ).
2. The PKG outputs $\perp$ if the proof of knowledge is invalid. Otherwise, it picks $r, t_1 \xleftarrow{\$} \mathbb{Z}_p^*$ and returns

$$\begin{aligned} K'_{\mathsf{ID}} &= (K'_1, K'_2, T'_0, \ldots, T'_{N-1}, t'_{\mathsf{ID}}) \\ &= \big((g_2^{t_1} \cdot R \cdot g_3)^\alpha \cdot z^r,\ g^r,\ h_1^r \cdot h_0^{-\mathsf{ID}\cdot r},\ h_2^r \cdot h_1^{-\mathsf{ID}\cdot r}, \ldots,\ h_N^r \cdot h_{N-1}^{-\mathsf{ID}\cdot r},\ t_1\big) \end{aligned}$$

3. U picks $r' \xleftarrow{\$} \mathbb{Z}_p^*$ and computes $K_{\mathsf{ID}} = (K_1, K_2, T_0, \ldots, T_{N-1}, t_{\mathsf{ID}})$, where $K_1 = (K'_1/g_1^\theta) \cdot z^{r'}$, $K_2 = K'_2 \cdot g^{r'}$, $T_i = T'_i \cdot (h_{i+1} \cdot h_i^{-\mathsf{ID}})^{r'}$ for indices $i = 0, \ldots, N-1$ and $t'_{\mathsf{ID}} + t_0$, so that

$$\begin{aligned} K_{\mathsf{ID}} &= (K_1, K_2, T_0, \ldots, T_{N-1}, t_{\mathsf{ID}}) \\ &= \Big((g_2^{t_0+t_1} \cdot g_3)^\alpha \cdot z^{r''},\ g^{r''},\ h_1^{r''} \cdot h_0^{-\mathsf{ID}\cdot r''}, \ldots,\ h_N^{r''} \cdot h_{N-1}^{-\mathsf{ID}\cdot r''},\ t_0 + t_1\Big), \end{aligned}$$

where $r'' = r + r'$. Then, U checks whether d_{ID} satisfies the relation

$$e(K_1, g) = e(g_1, g_2)^{t_{\mathsf{ID}}} \cdot e(g_1, g_3) \cdot e(z, K_2),$$

and $e(g, T_i) = e(K_2, h_{i+1} \cdot h_i^{-\mathsf{ID}})$ for each $i \in \{0, \ldots, N-1\}$.

Encrypt(mpk, S, m)**:** to encrypt $m \in \mathbb{G}_T$ for the receiver set $S = \{\mathsf{ID}_1, \ldots, \mathsf{ID}_n\}$, where $n \leq N$,

1. Expand $P(X) \in \mathbb{Z}_p[X]$ as

$$P(X) = \prod_{i \in S} (X - \mathsf{ID}_i) = \rho_n X^n + \rho_{n-1} X^{n-1} + \cdots + \rho_1 X + \rho_0.$$

2. Choose $s \xleftarrow{\$} \mathbb{Z}_p^*$ and compute

$$\begin{aligned} C &= (C_0, C_1, C_2, C_3) \\ &= \Big(m \cdot e(g_1, g_3)^s,\ g^s,\ \big(z \cdot h_0^{\rho_0} \cdot h_1^{\rho_1} \cdots h_n^{\rho_n}\big)^s,\ e(g_1, g_2)^s\Big). \end{aligned}$$

Decrypt$(\mathsf{mpk}, K_{\mathsf{ID}}, C, S)$**:** parse C as (C_0, C_1, C_2, C_3) and K_{ID} as

$$K_{\mathsf{ID}} = (K_1, K_2, T_0, \ldots, T_{N-1}, t_{\mathsf{ID}}) \in \mathbb{G}^{N+2} \times \mathbb{Z}_p.$$

1. Expand $P_{\mathsf{ID}}(X) \in \mathbb{Z}_p[X]$ as

$$P_{\mathsf{ID}}(X) = \prod_{\mathsf{ID}_j \in S \setminus \{\mathsf{ID}\}} (X - \mathsf{ID}_j) = y_{n-1}^{(\mathsf{ID})} X^{n-1} + y_{n-2}^{(\mathsf{ID})} X^{n-2} + \cdots + y_1^{(\mathsf{ID})} X + y_0^{(\mathsf{ID})}$$

and compute the decryption key

$$(D_{\mathsf{ID}}, d_{\mathsf{ID}}, t_{\mathsf{ID}}) = \big(K_1 \cdot T_0^{y_0^{(\mathsf{ID})}} \cdot T_1^{y_1^{(\mathsf{ID})}} \cdots T_{n-1}^{y_{n-1}^{(\mathsf{ID})}},\ K_2,\ t_{\mathsf{ID}}\big)$$
$$= \Big((g_2^{t_{\mathsf{ID}}} \cdot g_3)^{\alpha} \cdot \big(z \cdot h_0^{\rho_0} \cdot h_1^{\rho_1} \cdots h_n^{\rho_n}\big)^{r},\ g^r,\ t_{\mathsf{ID}}\Big).$$

2. Recover the plaintext as

$$m = C_0 \cdot e\big(C_1, D_{\mathsf{ID}}\big)^{-1} \cdot e\big(C_2,\ d_{\mathsf{ID}}\big) \cdot C_3^{t_{\mathsf{ID}}}.$$

Trace$^{\mathbb{D}}(\mathsf{mpk}, K_{\mathsf{ID}}, \varepsilon)$**:** given a valid private key K_{ID} for the identity ID and a ε-useful decoder $\mathbb{D}$, the tracing algorithm proceeds using $L = 8 \cdot \lambda/\varepsilon$ iterations in a similar fashion to previous schemes, by feeding $\mathbb{D}$ with ciphertexts $C^{(i)} = (C_0^{(i)}, C_1^{(i)}, C_2^{(i)}, C_3^{(i)})$, for $i = 1$ to L, and receiver sets $S^{(i)}$ containing ID and other randomly chosen identities. In the generation of $C^{(i)}$, $C_1^{(i)}$ and $C_2^{(i)}$ are calculated as specified by the encryption algorithm. On the other hand, $C_3^{(i)}$ is chosen as a random element of $\mathbb{G}_T$ and $C_0^{(i)}$ is obtained by applying the decryption algorithm to $S^{(i)}$ and $(C_1^{(i)}, C_2^{(i)}, C_3^{(i)})$.

The correctness of the scheme is implied the fact that the decryption key $(D_{\mathsf{ID}}, d_{\mathsf{ID}}, t_{\mathsf{ID}})$ always satisfies the relation $e(D_{\mathsf{ID}}, g) = e(g_1, g_2)^{t_{\mathsf{ID}}} \cdot e(g_1, g_3) \cdot e(z \cdot \prod_{i=0}^{n} h_i^{\rho_i}, d_{\mathsf{ID}})$ and raising both members to the power s as in previous schemes.

To avoid repeating the work of Boneh and Hamburg, we prove the security properties of the above A-IBBE system by reducing them to the IND-sID-CPA security of the underlying IBBE scheme.

Theorem 7. *The above A-IBBE scheme is secure under the $(N+1)$-DBDHE assumption. More precisely, any IND-sID-CPA adversary against it implies an equally successful IND-sID-CPA attacker against the Boneh-Hamburg IBBE scheme.*

Proof. We show that an IND-sID-CPA adversary $\mathcal{A}$ against the A-IBBE scheme gives rise to a "real-or-random" IND-sID-CPA adversary $\mathcal{B}$ (*i.e.*, in which the adversary $\mathcal{A}$ outputs a single message m and has to decide whether the challenge ciphertext $C^\star$ encrypts m or a random message) against the Boneh-Hamburg IBBE scheme. Hence, the security of the latter implies the security of our scheme.

When $\mathcal{A}$ chooses her set of target identities $S^\star = \{\mathsf{ID}_1^\star, \ldots, \mathsf{ID}_{n^\star}^\star\}$, with $n^\star \leq N$, our adversary $\mathcal{B}$ forwards $S^\star$ to her own challenger and receives a master public key $\mathsf{mpk}^{\mathrm{BH}} = (g, g_1 = g^\alpha, g_2, z, \mathbf{h} = g^{\mathbf{a}})$. Then, $\mathcal{B}$ picks $t^*, \beta \xleftarrow{\$} \mathbb{Z}_p^*$, computes $g_3 = g_2^{-t^*} g^\beta$ and provides $\mathcal{A}$ with $\mathsf{mpk} = (g, g_1, g_2, g_3, z, \mathbf{h})$.

At any time, $\mathcal{A}$ may request an execution of the key generation protocol for an arbitrary identity $\mathsf{ID} \notin S^\star$. At the beginning of each such protocol, $\mathcal{A}$ sends a commitment $R = g_2^{t_0} \cdot g^\theta$ and interactively proves knowledge of (t_0, θ), which $\mathcal{B}$ extracts by rewinding $\mathcal{A}$. Then, $\mathcal{B}$ chooses $t_1 \xleftarrow{\$} \mathbb{Z}_p^*$, sets $t = t_0 + t_1$ and queries her own IND-sID-CPA challenger to obtain a private key

$$\tilde{K}_{\mathsf{ID}} = (\tilde{K}_1, \tilde{K}_2, \tilde{T}_0, \ldots, \tilde{T}_{N-1}) = \big(g_2^\alpha \cdot z^r,\ g^r,\ h_1^r \cdot h_0^{-\mathsf{ID} \cdot r},\ h_2^r \cdot h_1^{-\mathsf{ID} \cdot r}, \ldots,\ h_N^r \cdot h_{N-1}^{-\mathsf{ID} \cdot r}\big)$$

for the identity ID chosen by $\mathcal{A}$. The latter is turned into an A-IBBE private key and re-randomized by setting

$$K_{\mathsf{ID}} = (K_1, K_2, T_0, \ldots, T_{N-1}) = \big(g_1^\beta \cdot \tilde{K}_1^{(t-t^\star)} \cdot z^{r'},$$
$$\tilde{K}_2^{(t-t^\star)} \cdot g^{r'}, \tilde{T}_0^{(t-t^\star)} \cdot (h_1 \cdot h_0^{-\mathsf{ID}})^{r'}, \ldots, \tilde{T}_{n-1}^{(t-t^\star)} \cdot (h_N \cdot h_{N-1}^{-\mathsf{ID}})^{r'}\big),$$

where $r' \xleftarrow{\$} \mathbb{Z}_p^*$. The new key K_{ID} is easily seen to have the same distribution as those obtained in step 3 of the key generation protocol. Finally, $\mathcal{A}$ obtains the "blinded key" $K'_{\mathsf{ID}} = (K'_1, K'_2, T'_0, \ldots, T'_{N-1})$, where $K'_1 = K_1 \cdot g_1^\theta$.

In the challenge phase, $\mathcal{A}$ chooses a pair of target messages (m_0, m_1). The adversary $\mathcal{B}$ chooses a random

plaintext $m^\star \xleftarrow{\$} \mathbb{G}_T$, which she sends to her own "real-or-random" challenger. The latter replies with a challenge ciphertext

$$C^\star = (C_0, C_1, C_2) = \Big(m \cdot e(g_1, g_2)^{s^\star},\ g^{s^\star},\ \big(z \cdot h_0^{\rho_0} \cdot h_1^{\rho_1} \cdots h_{n^\star}^{\rho_{n^\star}}\big)^{s^\star}\Big).$$

for the receiver set $S^\star = \{\mathsf{ID}_1^*, \ldots, \mathsf{ID}_{n^\star}^*\}$, where m is either $m^\star$ or a random element of $\mathbb{G}_T$. The adversary $\mathcal{B}$ picks a random bit $d \xleftarrow{\$} \{0,1\}$ and computes $C' = (C'_0, C_1, C_2, C_0/m^\star)$ where $C'_0 = m_d \cdot (C_0/m^\star)^{-t^*} \cdot e(g_1, C_1)^\beta$ and C' is relayed to $\mathcal{A}$ as a challenge ciphertext. After a second series of key generation queries, $\mathcal{A}$ outputs a bit $d' \in \{0,1\}$, and $\mathcal{B}$ outputs "real" if $d' = d$ and "random" otherwise. It is easy to see that, if $C^\star$ encrypts a random plaintext, then $C_0/m^\star$ can be expressed as $C_0/m^\star = e(g_1, g_2)^{s^\star - s'}$, where $s^\star = \log_g(C_1)$ and for some $s' \neq 0$. In this case, we obtain that $C'_0 = m_d \cdot e(g_1, g_3)^{s^\star} \cdot e(g_1, g_2)^{s' t^\star}$ statistically hides m_d (and thus $\Pr[d' = d] = 1/2$) since $\mathcal{A}$ has no information on t^*. In contrast, if $C^\star$ encrypts $m^\star$, then C' is a valid encryption of m_d for the A-IBBE scheme, so that $\Pr[d' = d] = 1/2 + \mathbf{Adv}^{\text{BH-IND-sID-CPA}}_{\mathbb{G},\mathbb{G}_T}(\lambda)$, where the latter advantage function denotes the maximal "real-or-random" advantage of any IND-sID-CPA adversary against the Boneh-Hamburg IBBE. It comes that $\mathcal{B}$'s advantage in the real-or-random game is exactly $\mathbf{Adv}^{\text{BH-IND-sID-CPA}}_{\mathbb{G},\mathbb{G}_T}(\lambda)$. □

Theorem 8. *In the selective-ID* DishonestUser-ID-BB *game, any PPT adversary has negligible advantage assuming that the $(N+1)$-DBDHE assumption holds. More precisely, the probability that the honest user outputs a ε-useful device that frames the PKG after the tracing procedure is at most*

$$\mathbf{Adv}^{\mathsf{DishonestUser\text{-}ID\text{-}BB}}_{\mathcal{A}}(\lambda) < L \cdot \mathbf{Adv}^{(N+1)\text{-DBDHE}}_{\mathbb{G},\mathbb{G}_T}(\lambda) + \exp(-\lambda).$$

with $L = 8\lambda/\varepsilon$.

Proof. Let us assume that, at the end of the selective-ID DishonestUser game, the dishonest user $\mathcal{A}$ outputs a device $\mathbb{D}$ for which the tracing algorithm declares the PKG guilty. Then, we show how to obtain an IND-sID-CPA adversary $\mathcal{B}$ against the Boneh-Hamburg IBBE scheme in the sense of a real-or-random definition of IND-sID-CPA security[4].

The adversary $\mathcal{B}$ plays the IND-sID-CPA game against a challenger $\mathcal{C}^{\text{BH}}$ for the Boneh-Hamburg IBBE and plays $\mathcal{A}$'s challenger in the selective-ID DishonestUser game. At the outset of the latter, $\mathcal{A}$ chooses a target identity ID^* and $\mathcal{B}$ then chooses her own sets $S_1^\star, \ldots, S_L^\star$ of target identities as follows: for each $i \in \{1, \ldots, L\}$, $S_i^\star$ is chosen as a set containing $\mathsf{ID}^\star$ and at most $N-1$ other random identities. When seeing the description of $S_1^\star, \ldots, S_L^\star$, the IBBE challenger $\mathcal{C}^{\text{BH}}$ generates a master public key $\mathsf{mpk}^{\text{BH}} = (g, g_1, g_2, z, \mathbf{h})$. Then, $\mathcal{B}$ chooses $t^\star, \beta \xleftarrow{\$} \mathbb{Z}_p^*$ and sets $g_3 = g_2^{-t^\star} \cdot g^\beta$. The master public key of the A-IBBE system is defined as $\mathsf{mpk} = (g, g_1, g_2, g_3, z, \mathbf{h})$ and given to $\mathcal{A}$.

Then, $\mathcal{A}$ starts making a number of key generation queries. For each key generation query involving an identity $\mathsf{ID} \neq \mathsf{ID}^\star$, $\mathcal{B}$ proceeds by invoking her own challenger $\mathcal{C}^{\text{BH}}$, exactly as in the proof of Theorem 7. When $\mathcal{A}$ queries a private key $K_{\mathsf{ID}^\star}$ for the target identity $\mathsf{ID}^\star$, $\mathcal{B}$ first rewinds the proof of knowledge so as to extract the pair (t_0, θ) such that $R = g_2^{t_0} \cdot g^\theta$ in the commitment. Then, it sets $t_1 = t^\star - t_0$ (in such a way that $t = t_0 + t_1 = t^\star$). In this case, $\mathcal{B}$ can compute an A-IBBE private key $K_{\mathsf{ID}^\star}$ on her own (without having to query $\mathcal{C}^{\text{BH}}$) as

$$(K_1, K_2, T_0, \ldots, T_{N-1}, t_{\mathsf{ID}^\star}) = \big(g_1^\beta \cdot z^r,\ g^r,\ (h_1 \cdot h_0^{-\mathsf{ID}^\star})^r, \ldots,\ (h_N \cdot h_{N-1}^{-\mathsf{ID}^\star})^r,\ t^\star\big),$$

[4] Namely, the IND-sID-CPA adversary chooses L sets of challenge identities $S_1^\star, \ldots, S_L^\star$ upfront and starts invoking a key generation oracle (that returns private keys for arbitrary identities) and a challenge oracle that, at its i^{th} invocation (for $i \in \{1, \ldots, L\}$), takes as input a plaintext $m_i^\star$ and returns an IBBE encryption under the set $S_i^\star$ of either $m_i^\star$ or a random plaintext depending on the value of some secret bit $d^\star$ that remains constant across all challenge queries. The adversary's goal is then to guess $d^\star$ without obtaining the private key of any identity belonging to a set $S_i^\star$ at any time. Using a classical hybrid argument (*e.g.* see [5, *Theorem 3*]), this notion is easily shown equivalent (with a $1/L$ loss in the security reduction) to the standard IND-sID-CPA security notion for IBBE schemes.

which is well-formed since $g_2^{t^\star} \cdot g_3 = g^\beta$. Finally, $\mathcal{B}$ returns the "blinded key" $K'_{\mathsf{ID}^\star} = \big(g_1^\theta \cdot K_1, K_2, T_0, \ldots, T_{N-1}, t_1\big)$ to $\mathcal{A}$.

At the end of the game, $\mathcal{A}$ outputs a private key $K_{\mathsf{ID}^\star}$ and a ε-useful device for the identity $\mathsf{ID}^\star$. In the tracing stage, $\mathcal{B}$ invokes L times her challenger $\mathcal{C}^{\mathrm{BH}}$ to obtain L challenge cipherexts $\{C_i^\star\}_{i=1}^L$. At each challenge request, $\mathcal{B}$ chooses a random plaintext $m_i^\star \stackrel{\$}{\leftarrow} \mathbb{G}_T$ and a receiver set $S^{(i)} = S_i^\star$ to the real-or-random challenger $\mathcal{C}^{\mathrm{BH}}$. For each plaintext $m_i^\star$, $\mathcal{C}^{\mathrm{BH}}$ replies with a challenge ciphertexts $C_i^\star = (C_{i,0}^\star, C_{i,1}^\star, C_{i,2}^\star)$ for $i = 1$ to L.

If the real-or-random challenger $\mathcal{C}^{\mathrm{BH}}$ is playing the "real" game, the obtained ciphertexts $\{C_i^\star\}_{i=1}^L$ are such that $C_{i,0}^\star = m_i^\star \cdot e(g_1, g_2)^{s_i^\star}$ and $C_{i,1} = g^{s_i^\star}$, with $s_i^\star \in_R \mathbb{Z}_p$, for $i = 1$ to L. On the other hand, if $\mathcal{C}^{\mathrm{BH}}$ decides to play the "random" game, each $C_i^\star$ encrypts a randomly chosen element of $\mathbb{G}_T$. To construct L ciphertexts for the tracing stage of the A-IBBE scheme, $\mathcal{B}$ proceeds as follows. For each $i \in \{1, \ldots, L\}$, it sets $C_3^{(i)} = C_{i,0}^\star / m_i^\star$ (which equals $e(g_1, g_2)^{s_i^\star}$ in the "real" game and $e(g_1, g_2)^{s'_i}$, with $s'_i \neq s_i^\star$ in the "random" game), $C_1^{(i)} = C_{i,1}^\star$ and $C_2^{(i)} = C_{i,2}^\star$. To compute $C_0^{(i)}$, $\mathcal{B}$ chooses a random plaintext $m^{(i)} \stackrel{\$}{\leftarrow} \mathbb{G}_T$ and calculates

$$C_0^{(i)} = m^{(i)} \cdot e\big(C_1^{(i)}, D_{\mathsf{ID}^\star}\big)^{-1} \cdot e\big(C_2^{(i)},\ d_{\mathsf{ID}^\star}\big) \cdot {C_3^{(i)}}^{t^\star}, \tag{10}$$

where $(D_{\mathsf{ID}^\star}, d_{\mathsf{ID}^\star}, t^\star)$ is the decryption key for the identity $\mathsf{ID}^\star$ and the receiver set $S^{(i)}$, which is obtained from $K_{\mathsf{ID}^\star}$. It is easy to see that, if $\mathcal{C}^{\mathrm{BH}}$ is playing the "real" game, $C^{(i)} = (C_0^{(i)}, C_1^{(i)}, C_2^{(i)}, C_3^{(i)})$ forms a valid encryption of $m^{(i)}$. If $\mathcal{C}^{\mathrm{BH}}$ is playing the "random" game, $C^{(i)}$ is distributed as a ciphertext produced by the tracing algorithm.

Similarly to the proof of theorem 2, we can show that, if $\mathcal{C}^{\mathrm{BH}}$ is playing the "real" game, the probability that $\mathbb{D}$ never outputs the correct plaintext $m^{(i)}$ at any iteration is smaller than $\exp(-\lambda)$. If this probability significantly increases when $\mathcal{C}^{\mathrm{BH}}$ switches to play the "random" game, algorithm $\mathcal{B}$ must be able to break the IND-sID-CPA security of the underlying IBBE scheme: at the end of the game that $\mathcal{B}$ plays against $\mathcal{C}^{\mathrm{BH}}$, it says "random" whenever the tracing algorithm points to the PKG and "real" otherwise. Since the result of [12] implies that $\mathbf{Adv}^{\text{BH-IND-sID-CPA}}_{\mathbb{G},\mathbb{G}_T}(\lambda) \leq \mathbf{Adv}^{(N+1)\text{-DBDHE}}_{\mathbb{G},\mathbb{G}_T}(\lambda)$, the claimed result follows from the $1/L$ security loss coming from the hybrid argument. □

As in previous schemes, as long as pirate devices are stateless, no dishonest PKG can create one that gets the tracing procedure to accuse the user and the result holds unconditionally. The proof of the following theorem is omitted since it is completely similar to the proofs of theorems 3 and 6.

Theorem 9. *In the information theoretic sense, no adversary has an advantage in the* DishonestPKG-wBB *game.*

It is noteworthy that other IBE-related primitives can be made accountable using the same technique. Due to their algebraic similarities with the "commutative blinding" IBE family, the "large-universe" attribute-based encryption schemes described in [39, 31] can easily be tweaked to support accountability in the weak black-box model.

6 Conclusion

We described the first A-IBE system allowing for weak black-box traceability while retaining short ciphertexts and private keys. We also suggested a white-box variant that remains secure against dishonest PKGs equipped with a decryption oracle. In the black-box setting, it remains an open problem to achieve the latter property without significantly degrading the efficiency.

In the setting of hierarchical IBE schemes, it would also be desirable to see how the problem can be addressed. When a pirate decoder is found to decrypt ciphertexts intended for a node, one should be able to determine which ancestor(s) of that node should be blamed.

References

1. M. Abdalla, A. Dent, J. Malone-Lee, G. Neven, D.-H. Phan, N. Smart. Identity-Based Traitor Tracing. In *PKC'07*, *LNCS* 4450, pp. 361–376, 2007.
2. M. Abdalla, E. Kiltz, G. Neven. Generalized Key Delegation for Hierarchical Identity-Based Encryption. In *ESORICS'07*, *LNCS* 4734, pp. 139–154. Springer, 2007.
3. S. Al-Riyami, K. Paterson. Certificateless Public Key Cryptography. In *Asiacrypt'03*, *LNCS* 2894, pp. 452–473, 2003.
4. M.-H. Au, Q. Huang, J.-K. Liu, W. Susilo, D.-S. Wong, G. Yang. Traceable and Retrievable Identity-Based Encryption. In *ACNS'08*, *LNCS* 5037, pp. 94–110, 2008.
5. O. Baudron, D. Pointcheval, J. Stern. Extended Notions of Security for Multicast Public Key Cryptosystems. In *ICALP'00*, *LNCS* 1853, pp. 499–511, 2000.
6. M. Bellare, T. Ristenpart. Simulation without the Artificial Abort: Simplified Proof and Improved Concrete Security for Waters' IBE Scheme. In *Eurocrypt'09*, *LNCS* 5479, pp. 407–424, 2009.
7. D. Boneh, X. Boyen. Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In *Eurocrypt'04*, *LNCS* 3027, pp. 223–238, 2004.
8. D. Boneh, X. Boyen. Secure Identity-Based Encryption Without Random Oracles. In *Crypto'04*, *LNCS* 3152, pp. 443–459, 2004.
9. D. Boneh, X. Boyen, E.-J. Goh. Hierarchical Identity-Based encryption with Constant Size Ciphertext. In *Eurocrypt'05*, *LNCS* 3494, pp. 440–456, 2005.
10. D. Boneh, M. Franklin. Identity-Based Encryption from the Weil Pairing. In *SIAM* Journal of Computing 32(3), pp. 586–615, 2003, earlier version in *Crypto'01*, *LNCS* 2139, pp. 213–229, 2001.
11. D. Boneh, C. Gentry, M. Hamburg Space-Efficient Identity-Based Encryption Without Pairings. In *FOCS'07*, pp. 647–657, 2007.
12. D. Boneh, M. Hamburg. Generalized Identity Based and Broadcast Encryption Schemes. In *Asiacrypt'08*, *LNCS* 5350, pp. 455–470, 2008
13. D. Boneh, J. Katz. Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity-Based Encryption. In *CT-RSA'05*, *LNCS* 3376, pp. 87–103, 2005.
14. X. Boyen, Q. Mei, B. Waters. Direct Chosen Ciphertext Security from Identity-Based Techniques. in *ACM CCS'05*, pp. 320–329, 2005.
15. X. Boyen, B. Waters. Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles). In *Crypto'06*, *LNCS* 4117, pages 290–307, 2006.
16. R. Canetti, S. Halevi, J. Katz. A Forward-Secure Public-Key Encryption Scheme. In *Eurocrypt'03*, *LNCS* 2656, pp. 254–271, 2003.
17. R. Canetti, S. Halevi, J. Katz. Chosen-Ciphertext Security from Identity-Based Encryption. In *Eurocrypt'04*, *LNCS* 3027, pp. 207–222, 2004.
18. J. H. Cheon. Security Analysis of the Strong Diffie-Hellman Problem. In *Eurocrypt'06*, *LNCS* 4004, pp. 1–11, 2006.
19. C. Cocks. An Identity-Based Encryption Scheme Based on Quadratic Residues. In *8th IMA International Conference*, *LNCS* 2260, pp. 360–363, 2001.
20. R. Cramer, V. Shoup. A Practical Public-Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack. In *Crypto'98*, *LNCS* 1462, pp. 13–25, 1998.
21. R. Cramer, V. Shoup. Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption. In *Eurocrypt'02*, *LNCS* 2332, pp. 45–64, 2002.
22. C. Delerablée. Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys. In *Asiacrypt'07*, *LNCS* 4833, pp. 200–215, 2007.
23. S. D. Galbraith, K. G. Paterson, and N. P. Smart. Pairings for cryptographers. *Discrete Applied Mathematics*, 156(16):3113–3121, 2008.
24. C. Gentry. Certificate-Based Encryption and the Certificate Revocation Problem. In *Eurocrypt'03*, volume 2656 of *LNCS*, pp. 272–293, 2003.
25. C. Gentry. Practical Identity-Based Encryption Without Random Oracles. In *Eurocrypt'06*, *LNCS* 4004, pp. 445–464, 2006.
26. C. Gentry, B. Waters. Adaptive Security in Broadcast Encryption Systems (with Short Ciphertexts). In *Eurocrypt'09*, *LNCS* 5479, pp. 171–188, 2009.
27. R. Granger, N. P. Smart. On Computing Products of Pairings. Cryptology ePrint Archive: Report 2006/172, 2006.

28. C. Gentry, A. Silverberg. Hierarchical ID-Based Cryptography. In *Asiacrypt'02*, *LNCS* 2501, pp. 548–566, 2002.
29. V. Goyal. Reducing Trust in the PKG in Identity-Based Cryptosystems. In *Crypto'07*, *LNCS* 4622, pp. 430–447, 2007.
30. V. Goyal, S. Lu, A. Sahai, B. Waters. Black-Box Accountable Authority Identity Based Encryption. In *ACM-CCS'08*, 2008.
31. V. Goyal, O. Pandey, A. Sahai, B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *ACM CCS'06*, pp. 89–98, 2006.
32. D. Hofheinz, E. Kiltz. Secure Hybrid Encryption from Weakened Key Encapsulation. In *Crypto'07*, *LNCS* 4622, pp. 553–571, 2007.
33. A. Kiayias, M. Yung. Traitor Tracing with Constant Transmission Rate. In *Eurocrypt'02*, *LNCS* 2332, pp. 450–465, 2002. Updated version available as Cryptology ePrint Archive: Report 2006/458, 2006.
34. E. Kiltz, Y. Vahlis. CCA2 Secure IBE: Standard Model Efficiency through Authenticated Symmetric Encryption In *CT-RSA'08*, *LNCS* 4964, pp. 221–238, 2008.
35. K. Kurosawa, Y. Desmedt. A New Paradigm of Hybrid Encryption Scheme. In *Crypto'04*, *LNCS* 3152, pp. 445–456, 2004.
36. B. Libert, D. Vergnaud. Towards Black-Box Accountable Authority IBE with Short Ciphertexts and Private Keys. In *PKC'09*, *LNCS* 5443, pp. 235–255, 2009.
37. T. Okamoto. Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes. In *Crypto'92*, *LNCS* 740, pp. 31–53, 2002.
38. T. Pedersen. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. In *Crypto'91*, *LNCS* 576, pp. 129–140, 1991.
39. A. Sahai, B. Waters. Fuzzy Identity-Based Encryption In *Eurocrypt'05*, *LNCS* 3494, pp. 457–473, 2005.
40. R. Sakai, M. Kasahara. ID-based Cryptosystems with Pairing on Elliptic Curve. In *SCIS'03*, `http://eprint.iacr.org/2003/054`, 2003.
41. P. Sarkar, S. Chatterjee. Construction of a Hybrid HIBE Protocol Secure Against Adaptive Attacks. In *ProvSec'07*, *LNCS* 4784, pp. 51–67, 2007.
42. C. P. Schnorr. Efficient Identification and Signatures for Smart Cards. In *Crypto'89*, *LNCS* 435, pp. 239–252, 1989.
43. A. Shamir. Identity-Based Cryptosystems and Signature Schemes. In *Crypto'84*, *LNCS* 196, pp. 47–53, 1984.
44. V. Shoup, R. Gennaro. A Note on An Encryption Scheme of Kurosawa and Desmedt. Cryptology ePrint Archive: Report 2004/194, 2004.
45. B. Waters. Efficient Identity-Based Encryption Without Random Oracles. In *Eurocrypt'05*, *LNCS* 3494, pp. 114–127, 2005.

A The Boneh-Hamburg IBBE scheme

An Identity-Based Broadcast Encryption scheme, as formalized in [2], can be seen as an IBE scheme where ciphertexts can be decrypted by more than one receiver. Syntactically, it consists of four algorithms:

- **Setup:** given a security parameter and a bound N on the number of receivers per ciphertext, this algorithm outputs a master key pair $(\mathsf{mpk}, \mathsf{msk})$.
- **KeyGen:** is used by the PKG to derive a private key K_{ID} for an identity ID.
- **Encrypt:** takes as input a plaintext m, a master public key mpk and a set $S = \{\mathsf{ID}_1, \ldots, \mathsf{ID}_n\}$ of receivers' identities, where $n \leq N$. It outputs a ciphertext C.
- **Decrypt:** takes as input the master public key mpk, a ciphertext C, a set of receivers $S = \{\mathsf{ID}_1, \ldots, \mathsf{ID}_n\}$ and a private key d_{ID} corresponding to some identity $\mathsf{ID} \in S$. It outputs a plaintext m or $\perp$.

The description of the Boneh-Hamburg IBBE scheme is as follows.

Setup(λ, N)**:** given a security parameter $\lambda \in \mathbb{N}$ and the maximal number of receivers $N \in \mathbb{N}$ per ciphertext, choose bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order $p > 2^\lambda$ and a generator $g \xleftarrow{\$} \mathbb{G}$. Choose $z \xleftarrow{\$} \mathbb{G}$ as well a $(N+1)$-vector $\mathbf{h} = (h_0, h_1, \ldots, h_N) \xleftarrow{\$} \mathbb{G}^{N+1}$ of random generators so that $h_i = g^{a_i}$ for $i = 0, \ldots, N$ with a randomly chosen $\mathbf{a} = (a_0, \ldots, a_N) \xleftarrow{\$} \mathbb{Z}_p^{N+1}$. Finally, pick $\alpha \xleftarrow{\$} \mathbb{Z}_p^*$, $g_2 \xleftarrow{\$} \mathbb{G}$ and compute $g_1 = g^\alpha$. The master public key is $\mathsf{mpk} = (g, g_1 = g^\alpha, g_2, z, \mathbf{h} = g^{\mathbf{a}})$ while the master secret key is $\mathsf{msk} = (\mathbf{a}, \alpha)$.

Keygen$(\mathsf{msk}, \mathsf{ID})$**:** to generate a private key for an identity ID, choose a random $r \xleftarrow{\$} \mathbb{Z}_p^*$ and compute

$$\begin{aligned} K_{\mathsf{ID}} &= (K_1, K_2, T_0, \ldots, T_{N-1}) \\ &= \left(g_2^{\alpha} \cdot z^r,\ g^r,\ h_1^r \cdot h_0^{-\mathsf{ID}\cdot r},\ h_2^r \cdot h_1^{-\mathsf{ID}\cdot r}, \ldots,\ h_N^r \cdot h_{N-1}^{-\mathsf{ID}\cdot r}\right) \end{aligned}$$

for which the "delegation component" $(T_0, \ldots, T_{N-1}) \in \mathbb{G}^N$ can be expressed as $g^{r \cdot M_1^t \cdot \mathbf{a}}$, for some matrix $M_1 \in \mathbb{Z}_p^{(N+1)\times N}$, which will be defined below.

Encrypt(mpk, S, m)**:** to encrypt $m \in \mathbb{G}_T$ for the receiver set $S = \{\mathsf{ID}_1, \ldots, \mathsf{ID}_n\}$, where $n \leq N$,

1. Expand the polynomial

$$P(X) = \prod_{i \in S} (X - \mathsf{ID}_i) = \rho_n X^n + \rho_{n-1} X^{n-1} + \cdots + \rho_1 X + \rho_0. \tag{11}$$

2. Pick $s \xleftarrow{\$} \mathbb{Z}_p^*$ and compute

$$C = (C_0, C_1, C_2) = \left(m \cdot e(g_1, g_2)^s,\ g^s,\ \left(z \cdot h_0^{\rho_0} \cdot h_1^{\rho_1} \cdots h_n^{\rho_n}\right)^s\right).$$

Decrypt$(\mathsf{mpk}, K_{\mathsf{ID}}, C, S)$**:** parse S as $\{\mathsf{ID}_1, \ldots, \mathsf{ID}_n\}$, C as (C_0, C_1, C_2) and K_{ID} as

$$K_{\mathsf{ID}} = (K_1, K_2, T_0, \ldots, T_{N-1}) \in \mathbb{G}^{N+2}.$$

1. Expand the polynomial

$$P_{\mathsf{ID}}(X) = \prod_{\mathsf{ID}_j \in S \setminus \{\mathsf{ID}\}} (X - \mathsf{ID}_j) = y_{n-1}^{(\mathsf{ID})} X^{n-1} + y_{n-2}^{(\mathsf{ID})} X^{n-2} + \cdots + y_1^{(\mathsf{ID})} X + y_0^{(\mathsf{ID})}$$

and use its coefficients to compute

$$\begin{aligned} (D_{\mathsf{ID}}, d_{\mathsf{ID}}) &= \left(K_1 \cdot T_0^{y_0^{(\mathsf{ID})}} \cdot T_1^{y_1^{(\mathsf{ID})}} \cdots T_{n-1}^{y_{n-1}^{(\mathsf{ID})}},\ K_2\right) &(12)\\ &= \left(g_2^{\alpha} \cdot \left(z \cdot h_0^{\rho_0} \cdot h_1^{\rho_1} \cdots h_n^{\rho_n}\right)^r,\ g^r\right) &(13)\end{aligned}$$

where $\rho_0, \ldots, \rho_n$ are the coefficients of $P(X)$ (calculated as per (11)).

2. Recover the plaintext as

$$m = C_0 \cdot e\big(C_1, D_{\mathsf{ID}}\big)^{-1} \cdot e\big(C_2,\ d_{\mathsf{ID}}\big). \tag{14}$$

To see why step 1 of the decryption algorithm works, one observes that, for any polynomials $(X - \mathsf{ID})$ and $P_{\mathsf{ID}}(X) = y_{n-1}^{(\mathsf{ID})} X^{n-1} + y_{n-2}^{(\mathsf{ID})} X^{n-2} + \cdots + y_1^{(\mathsf{ID})} X + y_0^{(\mathsf{ID})}$, the coefficients of $P(X) = (X - \mathsf{ID}) P_{\mathsf{ID}}(X) = \rho_n X^n + \cdots + \rho_1 X + \rho_0$ are given by

$$\rho = \begin{pmatrix} \rho_0 \\ \rho_1 \\ \rho_2 \\ \vdots \\ \rho_n \end{pmatrix} = M_1 \cdot \mathbf{y} = \begin{pmatrix} -\mathsf{ID} & & & & \\ 1 & -\mathsf{ID} & & & \\ & 1 & -\mathsf{ID} & & \\ & & \ddots & \ddots & \\ & & & 1 & -\mathsf{ID} \\ & & & & 1 \end{pmatrix} \cdot \begin{pmatrix} y_0^{(\mathsf{ID})} \\ y_1^{(\mathsf{ID})} \\ \vdots \\ y_{n-1}^{(\mathsf{ID})} \end{pmatrix},$$

where $M_1 \in \mathbb{Z}_p^{(n+1)\times n}$. Since the latter matrix is such that

$$M_1^t \cdot \mathbf{a}|_{n+1} = M_1^t \cdot \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} a_1 - \mathsf{ID} \cdot a_0 \\ a_2 - \mathsf{ID} \cdot a_1 \\ \vdots \\ a_n - \mathsf{ID} \cdot a_{n-1} \end{pmatrix},$$

for each private key K_{ID}, the first n delegation components satisfy

$$(T_0, \ldots, T_{n-1}) = \left(h_1^r \cdot h_0^{-\mathsf{ID}\cdot r},\ h_2^r \cdot h_1^{-\mathsf{ID}\cdot r}, \ldots,\ h_n^r \cdot h_{n-1}^{-\mathsf{ID}\cdot r}\right) = g^{rM_1^t\cdot\mathbf{a}}.$$

Therefore, since $\rho = M_1 \cdot \mathbf{y}$, we have

$$(z \cdot \prod_{k=0}^{n} h_k^{\rho_k})^r = z^r \cdot g^{r\cdot\rho^t\cdot\mathbf{a}} = z^r \cdot g^{r\mathbf{y}^t\cdot M_1^t\cdot\mathbf{a}} = z^r \cdot T_0^{y_0^{(\mathsf{ID})}} \cdots T_{n-1}^{y_{n-1}^{(\mathsf{ID})}}$$

which explains the transition between relations (12) and (13). To explain the second step of the decryption algorithm, we note that, for each $\mathsf{ID} \in S$, the pair $(D_{\mathsf{ID}}, d_{\mathsf{ID}})$ satisfies

$$e(D_{\mathsf{ID}}, g) = e(g_1, g_2) \cdot e(z \cdot h_0^{\rho_0} \cdot h_1^{\rho_1} \cdots h_n^{\rho_n}, d_{\mathsf{ID}}) \tag{15}$$

By raising both sides of (15) to the power $s \in \mathbb{Z}_p^*$, where s is the random encryption exponent, we see why m can be recovered as per (14).

The security of this scheme was proved [12] under the $(N+1)$-DBDHE assumption in the selective-ID model. In the context of IBBE schemes, the $\mathsf{IND\text{-}sID\text{-}CPA}$ model was formalized in [2]. It requires the adversary to choose upfront (*i.e.*, before seeing mpk) the set $S^\star = \{\mathsf{ID}_1^\star, \ldots, \mathsf{ID}_{n^\star}^\star\}$ of identities under which the challenge ciphertext $C^\star$ will be generated. The adversary is then allowed to query private keys for identities $\mathsf{ID}_i \notin S^\star$ and eventually aims at guessing which one out of two messages of her choice was encrypted in the generation of $C^\star$.