Towards Black-Box Accountable Authority IBE with Short Ciphertexts and Private Keys*

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

[1] Université Catholique de Louvain, Microelectronics Laboratory
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* 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. In this work, we propose a new construction that combines the efficiency of Goyal's first proposal with a very simple weak black-box tracing mechanism. Our scheme is described in the selective-ID model but readily extends to meet all security properties in the adaptive-ID sense, which is not known to be true for prior black-box schemes.

Keywords. Identity-based encryption, traceability, efficiency.

1 Introduction

Identity-based cryptography, first proposed by Shamir [40], 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 [8] – despite the bandwidth-demanding proposal by Cocks [17] – 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 [23, 5, 6, 36, 43, 7, 22, 12, 9].

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 [8] by sharing the master secret among multiple PKGs, but this inevitably entails extra communication and infrastructure. Related paradigms [21, 2] 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 [24] 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

* This paper has appeared in *12th International Conference on Practice and Theory in Public-Key Cryptography - PKC 2009*, Lect. Notes Comput. Sci. 5443, S. Jarecki & G. Tsudik eds., Springer, 2009, pp. 235-255.

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

decryption key associated with some identity over the Internet, it runs the risk of being caught and sued by the user. A-IBE schemes 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 [24]. The first one (that we call *Goyal-1* hereafter) builds on Gentry's IBE [22] 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 [24] (let us call it *Goyal-2*), constructed on the Sahai-Waters fuzzy IBE [36], can be extended so as to provide 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.* [3] 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.* [25] modified the *Goyal-2* system using attribute-based encryption techniques [36, 26] to achieve full black-box traceability: unlike *Goyal-2*, the scheme of [25] preserves security against dishonest PKGs that have access to a decryption oracle in the model. While definitely desirable, this property is currently only achievable at the expense of the same significant penalty as in *Goyal-2* [24] in 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 *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 (w.r.t. $O(\lambda^4)$ in *Goyal-2*) with only two pairing computations as for the latter (against more than 160 in *Goyal-2*).

While presented in the selective-ID security model (where adversaries must choose the identity that will be their prey at the outset of the game) for simplicity, our scheme is easily adaptable to the adaptive-ID model of [8]. 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 [25]). 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 [43] to obtain the adaptive-ID security). In comparison with the latter, that was only analyzed in a white-box model of traceability, our system provides several other advantages:

- Its security relies on a weaker assumption. So far, the only fully practical A-IBE scheme was resting on assumptions whose strength grows with the number of adversarial queries, which can be as large as 2^{30} as commonly assumed in the literature. Such assumptions are subject to a limited attack [16] that requires a careful adjustment of group sizes (by as much as 50% additional bits) to guarantee a secure use of schemes.
- It remains secure when many users want to run the key generation protocol in a concurrent fashion. *Goyal-1* has a key generation protocol involving zero-knowledge proofs. As its security reductions require to rewind adversaries at each key generation query, security is only guaranteed when the PKG interacts with users sequentially. In inherently concurrent environments like the Internet, key generation protocols should remain secure when executed by many users willing to register at the same time. By minimizing the number of rewinds in reductions, we ensure that our scheme remains secure in a concurrent setting. In these regards, the key generation protocol of *Goyal-2* makes use of oblivious transfers (OT) in sub-protocols. It thus supports concurrency whenever the underlying OT protocol does. As already mentioned however, our scheme features a much better efficiency than *Goyal-2*.
- In a white-box model of traceability, it can be made secure against dishonest PKGs equipped with a decryption oracle[3]. In the following, we nevertheless focus on the (arguably more interesting) weak black-box traceability aspect.

Organization. In the rest of the paper, section 2 recalls the A-IBE security model defined in [24]. We first analyze the white-box version of our scheme in section 3 and then describe a weak black-box tracing mechanism in section 4.

2 Background and Definitions

Syntactic definition and security model. We recall the definition of A-IBE schemes and their security properties as defined in [24].

Definition 1. *An* Accountable Authority Identity-Based Encryption scheme *(A-IBE) is a tuple (***Setup**, **Keygen**, **Encrypt**, **Decrypt**, **Trace***) of efficient 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*

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

[3] We believe that the *Goyal-1* system can also be modified so as to obtain this property.

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 $\mathbb{D}$ 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 [8] for IBE systems. As for the other ones, the FindKey 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 ComputeNewKey game models the infeasibility for users to generate a key $d_{\mathsf{ID}}^{(2)}$ outside the family of the legally obtained one $d_{\mathsf{ID}}^{(1)}$.

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:

$$
\begin{array}{l}
\boxed{\mathbf{Game}_{\mathcal{A}}^{\text{IND-ID-CCA}}(\lambda)} \\
(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathbf{Setup}(\lambda) \\
(m_0, m_1, \mathsf{ID}^\star, s) \leftarrow \mathcal{A}^{\mathsf{Dec},\mathsf{KG}}(\mathsf{find}, \mathsf{mpk}) \\
\qquad\qquad \left| \begin{array}{l} \mathsf{Dec} : (C, \mathsf{ID}) \\ \quad \dashrightarrow \mathbf{Decrypt}\big(\mathsf{mpk}, \mathsf{msk}, \mathsf{ID}, C\big); \\ \mathsf{KG} : \mathsf{ID} \dashrightarrow \mathbf{Keygen}^{(\mathrm{PKG}(\mathsf{msk}),\mathcal{A})}(\mathsf{mpk}, \mathsf{ID}) \\ \qquad\quad // \quad \mathsf{ID} \neq \mathsf{ID}^\star \end{array} \right. \\
d^\star \xleftarrow{\$} \{0,1\} \\
C^\star \leftarrow \mathbf{Encrypt}(\mathsf{mpk}, \mathsf{ID}^\star, m_{d^\star}) \\
d \leftarrow \mathcal{A}^{\mathsf{Dec},\mathsf{KG}}(\mathsf{guess}, s, C^\star) \\
\quad \left| \begin{array}{l} \mathsf{Dec} : (C, \mathsf{ID}) \dashrightarrow \mathbf{Decrypt}\big(\mathsf{mpk}, \mathsf{msk}, \mathsf{ID}, C\big); \\ \qquad\qquad // \quad (C, \mathsf{ID}) \neq (C^\star, \mathsf{ID}^\star) \\ \mathsf{KG} : \mathsf{ID} \dashrightarrow \mathbf{Keygen}^{(\mathrm{PKG}(\mathsf{msk}),\mathcal{A})}(\mathsf{mpk}, \mathsf{ID}) \\ \qquad\quad // \quad \mathsf{ID} \neq \mathsf{ID}^\star \end{array} \right. \\
\texttt{return } 1 \texttt{ if } d = d^\star \text{ and } 0 \texttt{ otherwise}.
\end{array}
$$

$\mathcal{A}$'s advantage is measured by $\mathbf{Adv}_{\mathcal{A}}^{\mathrm{CCA}}(\lambda) = |\Pr[\mathbf{Game}_{\mathcal{A}}^{\mathrm{CCA}} = 1] - 1/2|$.

The weaker definition of chosen-plaintext security (IND-ID-CPA) is formalized in the same way in [8] but $\mathcal{A}$ is not granted access to a decryption oracle.

2. **The FindKey game.** Let $\mathcal{A}$ be a PPT algorithm. We consider the following game, where $\lambda \in \mathbb{N}$ is a security parameter:

$$
\begin{array}{l}
\boxed{\mathbf{Game}_{\mathcal{A}}^{\mathrm{FindKey}}(\lambda)} \\
(\mathsf{mpk}, \mathsf{ID}, s_1) \leftarrow \mathcal{A}(\mathsf{setup}, \lambda) \\
(d_{\mathsf{ID}}^{(1)}, s_2) \leftarrow \mathbf{Keygen}^{(\mathcal{A}(s_1),\cdot)}(\mathsf{mpk}, \mathsf{ID}) \\
d_{\mathsf{ID}}^{(2)} \leftarrow \mathcal{A}(\mathsf{findkey}, s_1, s_2) \\
\texttt{return } 1 \texttt{ if } \mathbf{Trace}(\mathsf{mpk}, d_{\mathsf{ID}}^{(1)}) = \mathbf{Trace}(\mathsf{mpk}, d_{\mathsf{ID}}^{(2)}) \\
\qquad\quad 0 \texttt{ otherwise}.
\end{array}
$$

$\mathcal{A}$'s advantage is now defined as $\mathbf{Adv}_{\mathcal{A}}^{\mathrm{FindKey}}(\lambda) = \Pr[\mathbf{Game}_{\mathcal{A}}^{\mathrm{FindKey}} = 1]$.

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 [24], 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) between steps 2 and 3 of the game. We call this enhanced notion FindKey-CCA (as opposed to the weaker one which we call FindKey-CPA).

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 $\mathbb{D}$ that correctly decrypts ciphertexts intended for ID with non-negligible probability ε and wins if the tracing algorithm returns "User" when run on $d_{\mathsf{ID}}^{(1)}$ and with oracle access to $\mathbb{D}$.

3. **The ComputeNewKey game.** For a PPT algorithm $\mathcal{A}$, the model finally considers the following game:

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

$\mathcal{A}$'s advantage is $\mathbf{Adv}_{\mathcal{A}}^{\text{ComputeNewKey}}(\lambda) = \Pr[\mathbf{Game}_{\mathcal{A}}^{\text{ComputeNewKey}} = 1]$.

The ComputeNewKey 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 in a misbehavior of the PKG.

In the black-box scenario, the output of the dishonest user consist of a key $d_{\mathsf{ID}^\star}^{(1)}$ and a pirate decryption box $\mathbb{D}$ that yields the correct answer with probability ε when provided with a ciphertext encrypted for $\mathsf{ID}^\star$. In this case, the adversary wins if the output of $\mathbf{Trace}^{\mathbb{D}}(\mathsf{mpk}, d_{\mathsf{ID}^\star}^{(1)})$ is "PKG".

In [14], 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, called "selective-ID" model (or IND-sID-CCA and IND-sID-CPA for short), can be naturally extended to the ComputeNewKey notion.

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

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

In such *bilinear groups*, we assume the hardness of the (now classical) Decision Bilinear Diffie-Hellman problem that has been widely used in the recent years.

Definition 3. *Let $(\mathbb{G}, \mathbb{G}_T)$ be bilinear groups of prime order p and $g \in \mathbb{G}$. The* **Decision Bilinear Diffie-Hellman Problem** *(DBDH) is to distinguish the distributions of tuples $(g^a, g^b, g^c, e(g,g)^{abc})$ and $(g^a, g^b, g^c, e(g,g)^z)$ for random values $a, b, c, z \xleftarrow{\$} \mathbb{Z}_p^*$. The advantage of a distinguisher $\mathcal{B}$ is measured by*

$$\mathbf{Adv}^{\mathrm{DBDH}}_{\mathbb{G},\mathbb{G}_T}(\lambda) = \big|\Pr[a,b,c \xleftarrow{\$} \mathbb{Z}_p^* : \mathcal{B}(g^a, g^b, g^c, e(g,g)^{abc}) = 1] \\ - \Pr[a,b,c,z \xleftarrow{\$} \mathbb{Z}_p^* : \mathcal{B}(g^a, g^b, g^c, e(g,g)^{z}) = 1]\big|.$$

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^a, g^b, g^c).

3 The Basic Scheme

The scheme mixes ideas from the "commutative-blinding" [5] and "exponent-inversion" [37] frameworks. Private keys have the same shape as in commutative-blinding-based schemes [5, 6, 43, 12]. At the same time, their first element is a product of two terms, the first one of which is inspired from Gentry's IBE [22].

According to a technique applied in [24], 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 the key family number is perfectly hidden to the PKG and the FindKey-CPA security 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 adversary) in the proof of FindKey-CPA security. In the present scheme, the latter 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 [34] of Schnorr [39]) whereas 4 rounds are needed[4] using zero-knowledge proofs of knowledge.

3.1 Description

Setup: given $\lambda \in \mathbb{N}$, the PKG selects bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order $p > 2^\lambda$ with a random generator $g \xleftarrow{\$} \mathbb{G}$. It chooses $h, Y, Z \xleftarrow{\$} \mathbb{G}$ and $x \xleftarrow{\$} \mathbb{Z}_p^*$ at random. It defines its master key as $\mathsf{msk} := x$ and the master public key is chosen as $\mathsf{mpk} := (X = g^x, Y, Z, h)$.

Keygen$^{(\mathsf{PKG},\mathsf{U})}$: to obtain a private key for his identity ID, a user U interacts with the PKG in the following key generation protocol.

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 gives an interactive witness indistinguishable proof of knowledge of the pair (t_0, θ), which he retains for later use.

[4] A similar modification can be brought to the key generation protocol of *Goyal-1* to statistically hide the key family number to the PKG and avoid the need for 4-round ZK proofs.

2. The PKG outputs $\perp$ if the proof of knowledge fails to verify.
   Otherwise, it picks $r', t_1 \stackrel{\$}{\leftarrow} \mathbb{Z}_p^*$ and returns

$$d'_{\mathsf{ID}} = (d'_1, d'_2, d'_3) = \Big((Y \cdot R \cdot h^{t_1})^{1/x} \cdot (g^{\mathsf{ID}} \cdot Z)^{r'},\ X^{r'},\ t_1\Big). \quad (1)$$

3. U picks $r'' \stackrel{\$}{\leftarrow} \mathbb{Z}_p^*$ and computes $d_{\mathsf{ID}} = (d'_1/g^{\theta} \cdot (g^{\mathsf{ID}} \cdot Z)^{r''},\ d'_2 \cdot X^{r''},\ d'_3 + t_0)$ which should equal

$$d_{\mathsf{ID}} = (d_1, d_2, d_3) = \Big((Y \cdot h^{t_0+t_1})^{1/x} \cdot (g^{\mathsf{ID}} \cdot Z)^{r},\ X^{r},\ t_0 + t_1\Big) \quad (2)$$

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

$$e(d_1, X) = e(Y, g) \cdot e(h, g)^{d_3} \cdot e(g^{\mathsf{ID}} \cdot Z, d_2). \quad (3)$$

   If so, he sets his private key as d_{ID} and the latter belongs to the family of decryption keys identified by $n_F = d_3 = t_0 + t_1$. He outputs $\perp$ otherwise.

Encrypt: to encrypt $m \in \mathbb{G}_T$ given mpk and ID, choose $s \stackrel{\$}{\leftarrow} \mathbb{Z}_p^*$ and compute

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

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

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

Trace: given a purported private key $d_{\mathsf{ID}} = (d_1, d_2, d_3)$ and an identity ID, check the validity of d_{ID} w.r.t. ID using relation (3). If valid, d_{ID} is declared as a member of the family identified by $n_F = d_3$.

The correctness of the scheme follows from the fact that well-formed private keys always satisfy relation (3). By raising both members 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 [5]. 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 to compute a quotient of two pairings which is significantly faster than two independent pairing evaluations when optimized in the same way as modular multi-exponentiations.

In comparison with the most efficient standard model scheme based on the same assumption (which is currently the first scheme of [5]), the only overhead is a slightly longer ciphertext and an extra exponentiation in $\mathbb{G}_T$ at both ends.

3.2 Security

Selective-ID Security. We first prove the IND-sID-CPA security under the modified DBDH assumption (mDBDH).

Theorem 1. *The scheme is IND-sID-CPA under the mDBDH assumption.*

Proof. We show how a simulator $\mathcal{B}$ can interact with a selective-ID adversary $\mathcal{A}$ to solve a mDBDH instance $(T_a = g^a, T_b = g^b, T_c = g^c, T \stackrel{?}{=} e(g, g)^{ab/c})$. At the outset of the game, $\mathcal{A}$ announces the target identity $\mathsf{ID}^\star$. To prepare mpk, $\mathcal{B}$ chooses $\alpha, \gamma, t^* \stackrel{\$}{\leftarrow} \mathbb{Z}_p^*$ and sets $X = T_c = g^c$, $h = T_b = g^b$, $Y = X^{\gamma} \cdot h^{-t^*}$, and $Z = g^{-\mathsf{ID}^\star} \cdot X^{\alpha}$. The adversary's view is simulated as follows.

Queries: at any time, $\mathcal{A}$ may trigger an execution of the key generation protocol for an identity $\mathsf{ID} \neq \mathsf{ID}^\star$ of her choosing. She then 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 $t_1 \xleftarrow{\$} \mathbb{Z}_p^*$ 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

$$(d_1', d_2') = \Big((g^{\mathsf{ID}} \cdot Z)^{r'} \cdot W^{-\frac{\alpha}{\mathsf{ID}-\mathsf{ID}^\star}},\ X^{r'} \cdot W^{-\frac{1}{\mathsf{ID}-\mathsf{ID}^\star}} \Big) \tag{5}$$

using a random $r' \xleftarrow{\$} \mathbb{Z}_p^*$. If we set $\tilde{r}' = r' - \frac{w}{c(\mathsf{ID}-\mathsf{ID}^\star)}$, where $w = \log_g(W)$, we observe that (d_1', d_2') has the correct distribution since

$$\begin{aligned} W^{1/c} \cdot (g^{\mathsf{ID}} \cdot Z)^{\tilde{r}'} &= W^{1/c} \cdot (g^{\mathsf{ID}-\mathsf{ID}^\star} \cdot X^\alpha)^{\tilde{r}'} \\ &= W^{1/c} \cdot (g^{\mathsf{ID}-\mathsf{ID}^\star} \cdot X^\alpha)^{r'} \cdot (g^{\mathsf{ID}-\mathsf{ID}^\star})^{-\frac{w}{c(\mathsf{ID}-\mathsf{ID}^\star)}} \cdot X^{-\frac{w\alpha}{c(\mathsf{ID}-\mathsf{ID}^\star)}} \\ &= (g^{\mathsf{ID}} \cdot Z)^{r'} \cdot W^{-\frac{\alpha}{\mathsf{ID}-\mathsf{ID}^\star}} \end{aligned}$$

and $X^{\tilde{r}'} = X^{r'} \cdot (g^c)^{-\frac{w}{c(\mathsf{ID}-\mathsf{ID}^\star)}} = X^{r'} \cdot W^{-\frac{1}{\mathsf{ID}-\mathsf{ID}^\star}}$. 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) and $\mathcal{B}$ does *not* need to rewind $\mathcal{A}$.

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

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

We see that (d_1, d_2, d_3) is a valid key for $\mathsf{ID}^\star$. Since $g^{\mathsf{ID}^\star} \cdot Z = X^\alpha = T_c^\alpha$ 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.

As usual, $\mathcal{B}$ outputs 1 (meaning that $T = e(g,g)^{ab/c}$) if $\mathcal{A}$ successfully guesses $d' = d^\star$ and 0 otherwise. □

In the above proof, the simulator does not rewind the adversary at any time. The scheme thus remains IND-sID-CPA in concurrent environments, where a batch of users may want to simultaneously run the key generation protocol.

Also, the simulator knows a valid private key for each identity. This allows using Cramer-Shoup-like techniques [19] as in [22, 29] to secure the scheme against chosen-ciphertext attacks. The advantage of this approach, as we show in appendix A, is to provide FindKey-CCA security in a white-box setting.

Unlike the *Goyal-1* scheme, the basic system provides unconditional FindKey-CPA security: after an execution of the key generation protocol, even an all powerful PKG does not have any information on the component d_3 that is eventually part of the private key obtained by the new user.

Theorem 2. *In the information theoretic sense, no adversary has an advantage in the* FindKey-CPA *game.*

Proof. The proof directly follows from the perfect hiding property of Pedersen's commitment [35] and the perfect witness indistinguishability of the protocol [34] 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. □

Appendix A describes a hybrid variant of the scheme that provides white-box FindKey-CCA security using authenticated symmetric encryption in the fashion of [30, 41, 27] so as to reject all invalid ciphertexts with high probability.

Theorem 3. *In the selective-ID* ComputeNewKey *game, any PPT adversary has negligible advantage assuming that the Diffie-Hellman assumption holds.*

Proof. For simplicity, we prove the result using an equivalent formulation of the Diffie-Hellman problem which is to find $h^{1/x}$ given $(g, h, X = g^x)$.

At the outset of the game, $\mathcal{A}$ declares the identity $\mathsf{ID}^\star$ for which she aims at finding two private keys $d_{\mathsf{ID}^\star}^{(1)}, d_{\mathsf{ID}^\star}^{(2)}$ comprising distinct values of $d_3 = t$. Then, the simulator $\mathcal{B}$ prepares the PKG's public key as follows. Elements h and X are taken from the modified Diffie-Hellman instance (g, h, X). As in the proof of theorem 1, $\mathcal{B}$ defines $Z = g^{-\mathsf{ID}^\star} \cdot X^{\alpha}$ for a randomly chosen $\alpha \stackrel{\$}{\leftarrow} \mathbb{Z}_p^*$. To define Y, it chooses random values $\gamma, t_1' \stackrel{\$}{\leftarrow} \mathbb{Z}_p^*$ and sets $Y = X^{\gamma} \cdot h^{-t_1'}$.

Queries: in this game, $\mathcal{A}$ is allowed to query executions of the key generation protocol w.r.t. any identity, including $\mathsf{ID}^\star$. The only requirement is that queried identities be distinct.

- For an identity $\mathsf{ID} \neq \mathsf{ID}^\star$, $\mathcal{B}$ can proceed *exactly* as suggested by relation (5) in the proof of theorem 1 and does not need to rewind $\mathcal{A}$.
- When $\mathsf{ID} = \mathsf{ID}^\star$, $\mathcal{B}$ conducts the following steps. When $\mathcal{A}$ supplies a group element $R = h^{t_0} \cdot X^{\theta}$ along with a WI proof of knowledge of (t_0, θ), $\mathcal{B}$ uses the knowledge extractor of the proof of knowledge that allows extracting a representation (t_0, θ) of R by rewinding $\mathcal{A}$. Next, $\mathcal{B}$ computes $t_1 = t_1' - t_0$ picks $r \stackrel{\$}{\leftarrow} \mathbb{Z}_p^*$ and returns

$$(d_1', d_2', d_3') = \big(g^{\gamma+\theta} \cdot (g^{\mathsf{ID}^\star} \cdot Z)^r,\ X^r,\ t_1\big). \tag{6}$$

To see that the above tuple has the appropriate shape, we note that

$$(Y \cdot R \cdot h^{t_1})^{1/x} = (Y \cdot h^{t_0+t_1} \cdot X^{\theta})^{1/x} = (Y \cdot h^{t_1'} \cdot X^{\theta})^{1/x} = g^{\gamma+\theta}.$$

Output: upon its termination, $\mathcal{A}$ is expected to come up with distinct valid private keys $d_{\mathsf{ID}^\star}^{(1)} = (d_1^{(1)}, d_2^{(1)}, d_3^{(1)})$ and $d_{\mathsf{ID}^\star}^{(2)} = (d_1^{(2)}, d_2^{(2)}, d_3^{(2)})$, such that $t = d_3^{(1)} \neq d_3^{(2)} = t'$, for the identity $\mathsf{ID}^\star$. Given that we must have

$$\begin{aligned} d_1^{(1)} &= (Y \cdot h^{t})^{1/x} \cdot X^{\alpha r} \qquad & d_2^{(1)} &= X^{r} \\ d_1^{(2)} &= (Y \cdot h^{t'})^{1/x} \cdot X^{\alpha r'} \qquad & d_2^{(2)} &= X^{r'} \end{aligned}$$

for some values $r, r' \in \mathbb{Z}_p$, $\mathcal{B}$ can extract $h^{1/x} = \left(\frac{d_1^{(1)} / {d_2^{(1)}}^{\alpha}}{d_1^{(2)} / {d_2^{(2)}}^{\alpha}}\right)^{\frac{1}{t-t'}}$. □

We note that, in the above proof, the simulator does not have to rewind all executions of the key generation protocol but only one, when the adversary asks for a private key corresponding to the target identity $\mathsf{ID}^\star$ (recall that all queries involve distinct identities). Given that the number of rewinds is constant, the proof still goes through when the simulator is presented with many concurrent key generation queries. If other executions of the protocol (that necessarily involve identities $\mathsf{ID} \neq \mathsf{ID}^\star$) are nested within the one being rewinded when dealing with $\mathsf{ID}^\star$, the simulator simply runs them as an honest verifier would in the proof of knowledge and calculates the PKG's output as per relation (5) in the proof of theorem 1. Thus, the initial rewind does not trigger any other one and the simulation still takes polynomial time in a concurrent setting.

Adaptive-ID Security. The scheme can obviously be made IND-ID-CPA if Waters' "hash function" $F(\mathsf{ID}) = u' \prod_{j=1}^{n} u_i^{i_j}$ – where $\mathsf{ID} = i_1 \dots i_n \in \{0,1\}^n$ and $(u', u_1, \dots, u_n) \in \mathbb{G}^{n+1}$ is part of mpk – supersedes the Boneh-Boyen identity hashing $F(\mathsf{ID}) = g^{\mathsf{ID}} \cdot Z$. The function F is chosen so as to equal $F(\mathsf{ID}) = g^{J_1(\mathsf{ID})} \cdot X^{J_2(\mathsf{ID})}$ for integer-valued functions J_1, J_2 that are computable by the simulator. The security proof relies on the fact that J_1 is small in absolute value and cancels with non-negligible probability proportional to $1/q(n+1)$, where q is the number of key generation queries.

When extending the proof of theorem 3 to the adaptive setting, an adversary with advantage ε allows solving CDH with probability $O(\varepsilon/q^2(n+1))$. The reason is that the simulator has to guess beforehand which key generation query will involve the target identity $\mathsf{ID}^\star$. If $\mathsf{ID}^\star$ is expected to appear in the j^{th} query, when the latter is made, $\mathcal{B}$ rewinds $\mathcal{A}$ to extract (t_0, θ) and uses the special value t_1' to answer the query as per (6). With probability $1/q$, $\mathcal{B}$ is fortunate when choosing $j \xleftarrow{\$} \{1, \dots, q\}$ at the beginning and, again, $J_1(\mathsf{ID}^\star)$ happens to cancel with probability $O(1/q(n+1))$ for the target identity.

4 Weak Black-Box Traceability

Theorem 3 showed the infeasibility for users to compute another key from a different family given their private key. In these regards, a decryption key implements a "1-copyrighted function" – in the terminology of [33, 28] – for the matching identity. Using this property and the perfect white-box FindKey-CPA security, 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 the one used by Kiayias and Yung [28] 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 $L = 16\lambda/\varepsilon$ times:
   1. Choose distinct exponents $s, s' \xleftarrow{\$} \mathbb{Z}_p^*$ at random, compute $C_1 = X^s$, $C_2 = (g^{\mathsf{ID}} \cdot Z)^s$ 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 $ctr < 4\lambda$, incriminate the PKG. Otherwise, incriminate the user.

The soundness of this 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 query is answered as if it were the first one.

Theorem 4. *Under the mDBDH assumption, dishonest users have negligible chance to produce a decryption device $\mathbb{D}$ that makes the tracing algorithm incriminate the PKG in the selective-ID ComputeNewKey game.*

Proof. The tracing algorithm points to the PKG if it ends up with a too small value of ctr. The latter can be seen as the sum of $L = 16\lambda/\varepsilon$ independent random variables $X_i \in \{0, 1\}$ having the same expected value p_1. We have $\mu = \mathbf{E}[ctr] = Lp_1$. The Chernoff bound tells us that, for any real number ω such that $0 \leq \omega \leq 1$, $\Pr[ctr < (1-\omega)\mu] < \exp(-\mu\omega^2/2)$. Under the mDBDH assumption, we certainly have $\mathbf{Adv}^{\mathrm{mDBDH}}(\lambda) \leq \varepsilon/2$ (since $\varepsilon/2$ is presumably non-negligible). Lemma 1 shows that $p_1 \geq \varepsilon - \mathbf{Adv}^{\mathrm{mDBDH}}(\lambda)$, which implies

$$\mu = Lp_1 \geq L(\varepsilon - \mathbf{Adv}^{\mathrm{mDBDH}}(\lambda)) \geq \frac{L\varepsilon}{2} = 8\lambda. \tag{7}$$

With $\omega = 1/2$, the Chernoff bound guarantees that

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

□

Lemma 1. *In the selective-ID ComputeNewKey game, if $\mathbb{D}$ correctly opens well-formed ciphertexts with probability ε, the probability that an iteration of the tracing algorithm increases ctr is at least $p_1 \geq \varepsilon - \mathbf{Adv}^{\mathsf{mDBDH}}(\lambda)$.*

Proof. We consider two games called Game_0 and Game_1 where the adversary $\mathcal{A}$ is faced with a ComputeNewKey challenger $\mathcal{B}$ and produces a decryption device $\mathbb{D}$ which is provided with ciphertexts during a tracing stage. In Game_0, $\mathbb{D}$ is given a properly formed encryption of some plaintext m whereas it is given a ciphertext C where C_3 has been changed in Game_1. In either case, we call p_i (with $i \in \{0, 1\}$) the probability that $\mathbb{D}$ returns the plaintext m chosen by $\mathcal{B}$.

In the beginning of Game_0, $\mathcal{A}$ chooses a target identity $\mathsf{ID}^\star$ and the challenger $\mathcal{B}$ defines the system parameters as $X = g^c$, $h = g^b$, $Y = X^\gamma \cdot h^{-t^\star}$ and $Z = g^{-\mathsf{ID}^\star} \cdot X^\alpha$ for random $\alpha, \gamma, t^\star \xleftarrow{\$} \mathbb{Z}_p^*$. Then, $\mathcal{A}$ starts making key generation queries that are treated using the same technique as in the proof of theorem 3. Again, $\mathcal{B}$ only has to rewind the WI proof when the query pertains to $\mathsf{ID}^\star$.

At the end of the game, $\mathcal{A}$ outputs a decryption box $\mathbb{D}$ that correctly decrypts a fraction ε of ciphertexts. Then, $\mathcal{B}$ constructs a ciphertext C as

$$C_1 = g^a, \qquad C_2 = (g^a)^\alpha, \qquad C_3 = T, \qquad C_4 = m \cdot \frac{e(C_1, d_1)}{e(C_2, d_2) \cdot C_3^{t^\star}}$$

where $T \in \mathbb{G}_T$.

In Game_0, $\mathcal{B}$ sets $T = e(g, g)^{ab/c}$ so that we have $C_3 = e(g, h)^{a/c}$ and C is a valid ciphertext (for the encryption exponent $s = a/c$) that $\mathbb{D}$ correctly decrypts with probability ε. In this case, $\mathbb{D}$ thus outputs $m' = m \in \mathbb{G}_T$ with probability $p_0 = \varepsilon$. In Game_1, T is chosen as a random element of $\mathbb{G}_T$ and $C = (C_1, C_2, C_3, C_4)$ has the distribution of a ciphertext produced by the tracing stage and $\mathbb{D}$ must output a plaintext $m' = m$ with probability p_1. It is clear that $|p_0 - p_1| \leq \mathbf{Adv}^{\mathrm{mDBDH}}(\lambda)$ and we thus have $p_1 \geq \varepsilon - \mathbf{Adv}^{\mathrm{mDBDH}}(\lambda)$. □

The proofs of theorem 4 and lemma 1 readily extend to the adaptive-ID setting using the same arguments as in the last paragraph of section 3. The system thus turns out to be the first scheme that is amenable for 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 so far), earlier black-box or weakly black-box A-IBE proposals [24, 25] are only known to provide selective-ID security against dishonest users.

As for the security against dishonest PKGs, we observed that, in the FindKey-CPA game, the last part $d_3^{(1)} = t$ 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 $d_{\mathsf{ID}}^{(1)} = (d_1^{(1)}, d_2^{(1)}, d_3^{(1)})$ for which $d_3^{(1)}$ is independent of $\mathbb{D}$.

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

Proof. 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 $s, s' \stackrel{\$}{\leftarrow} \mathbb{Z}_p^*$. Since $\mathbb{D}$ has no information on $d_3^{(1)} = t$, for any plaintext $m \in \mathbb{G}_T$, there is a value $d_3^{(1)}$ that explains C_4 and it comes that $\mathbb{D}$ returns the one chosen by the tracer with probability $1/p$. $\square$

Theorem 5. *In the black-box FindKey-CPA game, a dishonest PKG has negligible advantage.*

Proof. The dishonest PKG is not detected if it outputs a decryption box for which the tracing ends with a sufficiently large ctr. From lemma 2, it easily comes that $\Pr[ctr \geq 4\lambda] \leq \Pr[ctr \geq 1] \leq L/p = 16\lambda/(\varepsilon p) \leq 16\lambda/(2^\lambda \varepsilon)$. $\square$

To secure the scheme against chosen-ciphertext attacks and preserve the weak black-box property, we can use the Canetti-Halevi-Katz [15] technique or its optimizations [10, 11] that do not affect the tracing algorithm.

5 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 dwells 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.

Acknowledgements

We thank Duong Hieu Phan and the anonymous referees for their comments.

References

1. M. Abdalla, A. W. Dent, J. Malone-Lee, G. Neven, D. H. Phan, and N. P. Smart, *Identity-Based Traitor Tracing.*, 10th International Workshop on Practice and Theory in Public Key Cryptography, PKC 2007 (T. Okamoto and X. Wang, eds.), Lect. Notes Comput. Sci., vol. 4450, Springer, 2007, pp. 361–376.
2. S. S. Al-Riyami and K. G. Paterson, *Certificateless Public Key Cryptography.*, Advances in Cryptology - Asiacrypt 2003 (C.-S. Laih, ed.), Lect. Notes Comput. Sci., vol. 2894, Springer, 2003, pp. 452–473.
3. M. H. Au, Q. Huang, J. K. Liu, W. Susilo, D. S. Wong, and G. Yang, *Traceable and Retrievable Identity-Based Encryption.*, Applied Cryptography and Network Security, ACNS 2008 (S. M. Bellovin, R. Gennaro, A. D. Keromytis, and M. Yung, eds.), Lect. Notes Comput. Sci., vol. 5037, 2008, pp. 94–110.
4. E. Biham (ed.), *Advances in Cryptology - Eurocrypt 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, Lect. Notes Comput. Sci., vol. 2656, Springer, 2003.
5. D. Boneh and X. Boyen, *Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles.*, in Cachin and Camenisch [13], pp. 223–238.
6. ———, *Secure Identity Based Encryption Without Random Oracles.*, in Franklin [20], pp. 443–459.
7. D. Boneh, X. Boyen, and E.-J. Goh, *Hierarchical Identity Based Encryption with Constant Size Ciphertext.*, in Cramer [18], pp. 440–456.
8. D. Boneh and M. Franklin, *Identity-Based Encryption from the Weil Pairing.*, SIAM J. Comput. **32** (2003), no. 3, 586–615.

9. D. Boneh, C. Gentry, and M. Hamburg, *Space-Efficient Identity Based Encryption Without Pairings.*, Proceedings of the 48th IEEE Symposium on Foundations of Computer Science (FOCS 2007), IEEE Computer Society, 2007, pp. 647–657.
10. D. Boneh and J. Katz, *Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity-Based Encryption.*, Topics in Cryptology - CT-RSA 2005 (A. J. Menezes, ed.), Lect. Notes Comput. Sci., vol. 3376, Springer, 2005, pp. 87–103.
11. X. Boyen, Q. Mei, and B. Waters, *Direct Chosen Ciphertext Security from Identity-Based Techniques.*, Proceedings of the 12th ACM Conference on Computer and Communications Security (V. Atluri, B. Pfitzmann, and P. McDaniel, eds.), ACM Press, 2005, 320-329.
12. X. Boyen and B. Waters, *Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles).*, Advances in Cryptology - Crypto 2006, pp. 290–307.
13. C. Cachin and J. Camenisch (eds.), *Advances in Cryptology* - Eurocrypt *2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*, Lect. Notes Comput. Sci., vol. 3027, Springer, 2004.
14. R. Canetti, S. Halevi, and J. Katz, *A Forward-Secure Public-Key Encryption Scheme.*, in Biham [4], pp. 255–271.
15. ———, *Chosen-Ciphertext Security from Identity-Based Encryption.*, in Cachin and Camenisch [13], pp. 207–222.
16. J. H. Cheon, *Security Analysis of the Strong Diffie-Hellman Problem.*, in Vaudenay [42], pp. 1–11.
17. C. Cocks, *An Identity Based Encryption Scheme Based on Quadratic Residues.*, Cryptography and Coding, 8th IMA International Conference (B. Honary, ed.), Lect. Notes Comput. Sci., vol. 2260, Springer, 2001, pp. 360–363.
18. R. Cramer (ed.), *Advances in Cryptology* - Eurocrypt *2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, Lect. Notes Comput. Sci., vol. 3494, Springer, 2005.
19. R. Cramer and V. Shoup, *Design and Analysis of Practical Public-Key Encryption Schemes Secure Against Adaptive Chosen Ciphertext Attack.*, SIAM J. Comput. **33** (2003), no. 1, 167–226.
20. M. K. Franklin (ed.), *Advances in Cryptology* - Crypto *2004, 24th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, Lect. Notes Comput. Sci., vol. 3152, Springer, 2004.
21. C. Gentry, *Certificate-Based Encryption and the Certificate Revocation Problem.*, in Biham [4], pp. 272–293.
22. ———, *Practical Identity-Based Encryption Without Random Oracles.*, in Vaudenay [42], pp. 445–464.
23. C. Gentry and A. Silverberg, *Hierarchical ID-Based Cryptography.*, Advances in Cryptology - Asiacrypt 2002 (Y. Zheng, ed.), Lect. Notes Comput. Sci., vol. 2501, Springer, 2002, pp. 548–566.
24. V. Goyal, *Reducing Trust in the PKG in Identity Based Cryptosystems.*, in Menezes [32], pp. 430–447.
25. V. Goyal, S. Lu, A. Sahai, and B. Waters, *Black-box accountable authority identity-based encryption.*, Proceedings of the 2008 ACM Conference on Computer and Communications Security, CCS 2008 (P. Ning, P. F. Syverson, and S. Jha, eds.), ACM Press, 2008, pp. 427–436.
26. V. Goyal, O. Pandey, A. Sahai, and B. Waters, *Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data.*, Proceedings of the 2006 ACM Conference on Computer and Communications Security, CCS 2006 (A. Juels, R. N. Wright, and S. De Capitani di Vimercati, eds.), ACM Press, 2006, pp. 89–98.
27. D. Hofheinz and E. Kiltz, *Secure Hybrid Encryption from Weakened Key Encapsulation.*, in Menezes [32], pp. 553–571.
28. A. Kiayias and M. Yung, *Traitor Tracing with Constant Transmission Rate.*, Advances in Cryptology - Eurocrypt 2002 (L. R. Knudsen, ed.), Lect. Notes Comput. Sci., vol. 2332, Springer, 2002, pp. 450–465.
29. E. Kiltz and Y. Vahlis, *CCA2 Secure IBE: Standard Model Efficiency through Authenticated Symmetric Encryption.*, Topics in Cryptology - CT-RSA 2008 (T. Malkin, ed.), Lect. Notes Comput. Sci., vol. 4964, Springer, 2008, pp. 221–238.
30. K. Kurosawa and I. Desmedt, *A New Paradigm of Hybrid Encryption Scheme.*, in Franklin [20], pp. 426–442.
31. B. Libert and D. Vergnaud, *Towards Black-Box Accountable Authority IBE with Short Ciphertexts and Private Keys.*, Tech. Report 0807.1775, Computing Research Repository, 2008.
32. A. Menezes (ed.), *Advances in cryptology - crypto 2007, 27th annual international cryptology conference, santa barbara, ca, usa, august 19-23, 2007, proceedings*, Lect. Notes Comput. Sci., vol. 4622, Springer, 2007.
33. D. Naccache, A. Shamir, and J. Stern, *How to Copyright a Function?*, 2nd International Workshop on Practice and Theory in Public Key Cryptography, PKC 1999 (H. Imai and Y. Zheng, eds.), Lect. Notes Comput. Sci., vol. 1560, Springer, 1999, pp. 188–196.
34. T. Okamoto, *Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes.*, Advances in Cryptology - Crypto'92 (E. F. Brickell, ed.), Lect. Notes Comput. Sci., vol. 740, Springer, 1993, pp. 31–53.
35. T. P. Pedersen, *Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing.*, Advances in Cryptology - Crypto'91 (J. Feigenbaum, ed.), Lect. Notes Comput. Sci., vol. 576, Springer, 1992, pp. 129–140.

36. A. Sahai and B. Waters, *Fuzzy Identity-Based Encryption.*, in Cramer [18], pp. 457–473.
37. R. Sakai and M. Kasahara, *ID based Cryptosystems with Pairing on Elliptic Curve.*, Tech. Report 2003/054, IACR eprint, 2003.
38. P. Sarkar and S. Chatterjee, *Construction of a Hybrid HIBE Protocol Secure Against Adaptive Attacks.*, Provable Security, First International Conference, ProvSec 2007 (W. Susilo, J. K. Liu, and Y. Mu, eds.), Lect. Notes Comput. Sci., vol. 4784, Springer, 2007, pp. 51–67.
39. C. P. Schnorr, *Efficient signature generation by smart cards.*, J. Cryptology **4** (1991), no. 3, 161–174.
40. A. Shamir, *Identity-Based Cryptosystems and Signature Schemes.*, Advances in Cryptology - CRYPTO'84 (G. R. Blakley and D. Chaum, eds.), Lect. Notes Comput. Sci., vol. 196, Springer, 1985, pp. 47–53.
41. V. Shoup and R. Gennaro, *A Note on An Encryption Scheme of Kurosawa and Desmedt.*, Tech. Report 2004/194, IACR eprint, 2004.
42. S. Vaudenay (ed.), *Advances in Cryptology* - EUROCRYPT *2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, Lect. Notes Comput. Sci., vol. 4004, Springer, 2006.
43. B. Waters, *Efficient Identity-Based Encryption Without Random Oracles.*, in Cramer [18], pp. 114–127.

A A Variant with White-Box FindKey-CCA security

To achieve IND-sID-CCA2 security, we can hybridize the scheme using an authenticated symmetric encryption scheme (as defined in appendix B) as previously considered in [38, 29] in the context of identity-based encryption. The obtained variant is reminiscent of a version of Gentry's IBE described in [29].

Setup: is the same as in section 3 except that the PKG now chooses two elements $Y_A, Y_B \xleftarrow{\$} \mathbb{G}$ instead of a single one Y. An authenticated symmetric encryption scheme (E, D) of keylength $\ell \in \mathbb{N}$, a secure key derivation function $KDF : \mathbb{G}_T \to \{0,1\}^\ell$ and a target collision-resistant hash function $H : \{0,1\}^* \to \mathbb{Z}_p^*$ are also needed. The master key is set as $\mathsf{msk} := x$ and the global public key is $\mathsf{mpk} := (X = g^x, h, Y_A, Y_B, Z, H, KDF, (\mathsf{E}, \mathsf{D}))$.

Keygen$^{(\mathrm{PKG},\mathsf{U})}$: to obtain a private key for his identity ID, a user U interacts with the PKG as follows.

1. U sends $R = h^{t_0} \cdot X^\theta$ to the PKG and proves his knowledge of the underlying pair $(t_0, \theta) \xleftarrow{\$} (\mathbb{Z}_p^*)^2$ in a witness indistinguishable fashion.
2. The PKG outputs $\perp$ if the proof is incorrect.
   Otherwise, it picks random values $r'_A, t_{A,1}, r'_B, t_B \xleftarrow{\$} \mathbb{Z}_p^*$ and returns
$$d'_{\mathsf{ID},A} = (d'_{A,1}, d'_{A,2}, d'_{A,3}) = \Big((Y \cdot R \cdot h^{t_{A,1}})^{1/x} \cdot (g^{\mathsf{ID}} \cdot Z)^{r'_A},\ X^{r'_A},\ t_{A,1}\Big)$$
$$d'_{\mathsf{ID},B} = (d'_{B,1}, d'_{B,2}, d'_{B,3}) = \Big((Y_B \cdot h^{t_B})^{1/x} \cdot (g^{\mathsf{ID}} \cdot Z)^{r'_B},\ X^{r'_B},\ t_B\Big)$$
3. U computes $d_{\mathsf{ID},A} = (d'_{A,1}/g^\theta \cdot (g^{\mathsf{ID}} \cdot Z)^{r''_A},\ d'_{A,2} \cdot X^{r''_A},\ d'_{A,3} + t_0)$ as well as $d_{\mathsf{ID},B} = (d'_{B,1} \cdot (g^{\mathsf{ID}} \cdot Z)^{r''_B},\ d'_{B,2} \cdot X^{r''_B},\ d_{B,3})$, for randomly chosen $r''_A, r''_B \xleftarrow{\$} \mathbb{Z}_p^*$ so that
$$d_{\mathsf{ID},A} = (d_{A,1}, d_{A,2}, d_{A,3}) = \Big((Y_A \cdot h^{t_A})^{1/x} \cdot (g^{\mathsf{ID}} \cdot Z)^{r_A},\ X^{r_A},\ t_A\Big) \tag{8}$$
$$d_{\mathsf{ID},B} = (d_{B,1}, d_{B,2}, d_{B,3}) = \Big((Y_B \cdot h^{t_B})^{1/x} \cdot (g^{\mathsf{ID}} \cdot Z)^{r_B},\ X^{r_B},\ t_B\Big) \tag{9}$$
   where $t_A = t_0 + t_{A,1}$, $r_A = r'_A + r''_A$ and $r_B = r'_B + r''_B$. He checks whether $d_{\mathsf{ID},A}$ and $d_{\mathsf{ID},B}$ respectively satisfy
$$e(d_{A,1}, X) = e(Y_A, g) \cdot e(h, g)^{d_{A,3}} \cdot e(g^{\mathsf{ID}} \cdot Z, d_{A,2}) \tag{10}$$
$$e(d_{B,1}, X) = e(Y_B, g) \cdot e(h, g)^{d_{B,3}} \cdot e(g^{\mathsf{ID}} \cdot Z, d_{B,2}). \tag{11}$$
   If so, he sets his private key as $(d_{\mathsf{ID},A}, d_{\mathsf{ID},B})$ and the latter belongs to the family of decryption key identified by $n_F = d_{A,3} = t_A$.

Encrypt: to encrypt m given mpk and ID, choose $s \xleftarrow{\$} \mathbb{Z}_p^*$ and compute

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

where $K = KDF(e(g, Y_A)^s \cdot e(g, Y_B)^{\kappa s})$ and $\kappa = H(C_1, C_2, C_3)$.

Decrypt: given $C = \big(C_1, C_2, C_3, C_4\big)$ and $d_{\mathsf{ID}} = (d_{\mathsf{ID},A}, d_{\mathsf{ID},B})$, compute the plaintext $m = \mathsf{D}_K(C_4)$ (which may just be $\perp$ if C_4 is not a valid authenticated encryption) using the key

$$K = KDF\Big(\frac{e(C_1, d_{A,1} \cdot d_{B,1}^{\kappa})}{e(C_2, d_{A,2} \cdot d_{B,2}^{\kappa}) \cdot C_3^{d_{A,3} + \kappa d_{B,3}}}\Big) \tag{12}$$

with $\kappa = H(C_1, C_2, C_3)$.

Trace: given an alleged private key $(d_{\mathsf{ID},A}, d_{\mathsf{ID},B})$, with $d_{\mathsf{ID},A} = (d_{A,1}, d_{A,2}, d_{A,3})$, for an identity ID, check the validity of d_{ID} w.r.t. ID using relations (10)-(11). If valid, the key is declared as a member of the family $n_F = d_{3,A} = t_A$.

To prove the IND-sID-CCA security, we can apply the technique of [29], which in turn borrows ideas from [30, 41, 27].

In the chosen-ciphertext scenario, the white-box FindKey security is no longer unconditional but relies on the ciphertext integrity of the symmetric encryption scheme.

Theorem 6. *The scheme is IND-sID-CCA secure in the standard model if the modified DBDH assumption holds, if the symmetric scheme is a secure authenticated encryption scheme, if H is target collision-resistant and if the key derivation function is secure. More precisely, we have*

$$\begin{aligned}\mathbf{Adv}_{\mathcal{A}}^{\mathrm{CCA}}(\lambda, \ell) \leq \frac{q_d + 2q_d^2}{p} + \mathbf{Adv}^{\mathsf{TCR}}(\lambda) + \mathbf{Adv}^{\mathsf{mDBDH}}(\lambda) + 3q_d \cdot \mathbf{Adv}^{\mathsf{CT\text{-}INT}}(\ell) \\ + (2q_d + 1) \cdot \mathbf{Adv}^{\mathsf{KDF}}(\lambda, \ell) + \mathbf{Adv}^{\mathsf{IND\text{-}SYM}}(\ell)\end{aligned}$$

where q_d denotes the number of decryption queries allowed to the adversary $\mathcal{A}$ and the advantage functions against (E, D) *are defined in appendix B.*

Proof. Given in the full version of the paper [31]. □

Theorem 7. *The scheme is* FindKey-CCA *secure assuming the security of the key derivation function and the (weak) ciphertext integrity of the symmetric encryption scheme. The advantage of an adversary $\mathcal{A}$ making at most q_d decryption queries is bounded by*

$$\begin{aligned}\mathbf{Adv}_{\mathcal{A}}^{\text{FindKey-CCA}}(\lambda, \ell) \leq 2 \cdot q_d \cdot \mathbf{Adv}^{\mathsf{CT\text{-}INT}}(\ell) \\ + 2 \cdot q_d \cdot \mathbf{Adv}^{\mathsf{KDF}}(\lambda, \ell) + \frac{2q_d^2 + q_d + 1}{p}.\end{aligned}$$

Proof. Given in appendix C. □

B Authenticated Symmetric Encryption

A symmetric encryption scheme is specified by a pair (E, D), where E is the encryption algorithm and D is the decryption procedure, and a key space $\mathcal{K}(\ell)$ where $\ell \in \mathbb{N}$ is a security parameter. The security of authenticated symmetric encryption is defined by means of two games that capture the ciphertext indistinguishability and ciphertext (one-time) integrity properties.

Definition 4. *An symmetric encryption scheme is secure in the sense of authenticated encryption if any PPT adversary has negligible advantage in the following games.*

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

$$\boxed{\mathbf{Game}_{\mathcal{A}}^{\mathsf{IND\text{-}SYM}}(\ell)}$$
$$\begin{array}{l} K \xleftarrow{\$} \mathcal{K}(\ell) \\ (m_0, m_1, s) \leftarrow \mathcal{A}(\mathsf{find}, \ell) \\ d^\star \xleftarrow{\$} \{0,1\} \\ c^\star \leftarrow \mathsf{E}_K(m_{d^\star}) \\ d \leftarrow \mathcal{A}(\mathsf{guess}, s, c^\star) \\ \texttt{return } 1 \texttt{ if } d = d^\star \texttt{ and } 0 \texttt{ otherwise.} \end{array}$$

   $\mathcal{A}$'s advantage is $\mathbf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}SYM}}(\ell) = |\Pr[\mathbf{Game}_{\mathcal{A}}^{\mathsf{IND\text{-}SYM}} = 1] - 1/2|$.
2. **The CT-INT game.** Let $\mathcal{A}$ be a PPT algorithm. We consider the following game, where $\ell \in \mathbb{N}$ is a security parameter:

$$\boxed{\mathbf{Game}_{\mathcal{A}}^{\mathsf{CT\text{-}INT}}(\ell)}$$
$$\begin{array}{l} K \xleftarrow{\$} \mathcal{K}(\ell) \\ (m, s) \leftarrow \mathcal{A}(\mathsf{find}, \ell) \\ c \leftarrow \mathsf{E}_K(m) \\ c' \leftarrow \mathcal{A}(\mathsf{create}, \ell, c) \\ \texttt{return } 1 \texttt{ if } c' \neq c \texttt{ and } \mathsf{D}_K(c') \neq \perp \\ \qquad\qquad 0 \texttt{ otherwise.} \end{array}$$

   $\mathcal{A}$'s advantage is now defined as $\mathbf{Adv}_{\mathcal{A}}^{\mathsf{CT\text{-}INT}}(\ell) = \Pr[\mathbf{Game}_{\mathcal{A}}^{\mathsf{CT\text{-}INT}} = 1]$.

The notion of weak ciphertext integrity is defined in the same way but the adversary is not allowed to see an encryption c under the challenge key K.

C Proof of Theorem 7

The proof proceeds again with a sequence of games, in all of which S_i denotes the event that the adversary $\mathcal{A}$ wins.

Game$_0$: is the FindKey-CCA experiment. The dishonest PKG $\mathcal{A}$ generates the master public key, chooses an identity ID that she wishes to be challenged upon. She interacts with the challenger in a key generation protocol, upon completion of which the challenger $\mathcal{B}$ obtains a decryption key consisting of two triples $d_{\mathsf{ID},A}^{(1)} = (d_{A,1}{}^{(1)}, d_{A,2}{}^{(1)}, d_{A,3}{}^{(1)})$, $d_{\mathsf{ID},B}^{(1)} = (d_{B,1}{}^{(1)}, d_{B,2}{}^{(1)}, d_{B,3}{}^{(1)})$ that should pass the key sanity check (otherwise, $\mathcal{B}$ aborts). At this stage, $\mathcal{A}$ knows $t_B^{(1)} = d_{B,3}^{(1)}$ but has no information on $d_{A,3}^{(1)} = t_A^{(1)}$ or on the values $r_A = \log_X(d_{A,2}^{(1)})$ and $r_B = \log_X(d_{B,2}^{(1)})$ (by the construction of the key generation protocol). In the next phase, $\mathcal{A}$ starts making a number of decryption queries that the challenger handles using $(d_{\mathsf{ID},A}^{(1)}, d_{\mathsf{ID},B}^{(1)})$. Namely, when queried on a ciphertext $C = (C_1, C_2, C_3, C_4)$, $\mathcal{B}$ calculates

$$\psi = \frac{e\big(C_1, d_{A,1}^{(1)} \cdot d_{B,1}^{(1)}{}^{\kappa}\big)}{e\big(C_2, d_{A,2}^{(1)} \cdot d_{B,2}^{(1)}{}^{\kappa}\big) \cdot C_3^{d_{A,3}^{(1)} + \kappa d_{B,3}{}^{(1)}}},$$

where $\kappa = H(C_1, C_2, C_3)$, $K = KDF(\psi)$ and $m = \mathsf{D}_K(C_4)$ which is returned to $\mathcal{A}$ (and may be $\perp$ if C is declared invalid).

At the end of the game, $\mathcal{A}$ outputs a key $(d^{(2)}_{\mathsf{ID},A}, d^{(2)}_{\mathsf{ID},B})$ and wins if $d^{(2)}_{\mathsf{ID},A}$ parses into $({d_{A,1}}^{(2)}, {d_{A,2}}^{(2)}, {d_{A,3}}^{(2)})$ such that ${d_{A,3}}^{(1)} = t^{(1)}_A = t^{(2)}_A = {d_{A,3}}^{(2)}$.

We note that decryption queries on well-formed ciphertexts do not reveal any information to $\mathcal{A}$ (since all well-formed keys yield the same result). We will show that, provided all ill-formed ciphertexts are rejected by $\mathcal{B}$, $\mathcal{A}$ still has negligible information on $t^{(1)}_A$ in the end of the game. For convenience, we distinguish two types of invalid ciphertexts: type I ciphertexts (C_1, C_2, C_3, C_4) are such that $\log_X(C_1) \neq \log_{F(\mathsf{ID})}(C_2)$ (and can be told apart from valid ones by checking if $e(C_1, F(\mathsf{ID})) \neq e(X, C_2)$), where $F(\mathsf{ID}) = g^{\mathsf{ID}} \cdot Z$, whereas type II ciphertexts are those for which $\log_X(C_1) = \log_{F(\mathsf{ID})}(C_2) \neq \log_{e(g,h)}(C_3)$.

Game$_1$: is as Game$_0$ but $\mathcal{B}$ rejects all type I invalid ciphertexts (that are publicly recognizable). Such a malformed ciphertext comprises elements $C_1 = X^{s_1}$, $C_2 = F(\mathsf{ID})^{s_1 - s_1'}$ and $C_3 = e(g,h)^{s_1 - s_1''}$ where $s_1' > 0$ and $s_1'' \geq 0$. Hence, the symmetric key K that $\mathcal{B}$ calculates is derived from

$$\psi = e(g, Y_A^{s_1} \cdot Y_B^{\kappa s_1}) \cdot e(F(\mathsf{ID}), X)^{s_1'(r_A + \kappa r_B)} \cdot e(g,h)^{s_1''(t^{(1)}_A + \kappa t^{(1)}_B)} \tag{13}$$

where $\kappa = H(C_1, C_2, C_3)$. Upon termination of the key generation protocol, $\mathcal{A}$ has no information on r_A, r_B (as $\mathcal{B}$ re-randomizes its key). Even if κ was the same in all decryption queries (which may happen if these queries all involve identical (C_1, C_2, C_3)), the second term of the product (13) remains almost uniformly random to $\mathcal{A}$ at each new query. Indeed, for each failed one, $\mathcal{A}$ learns at most one value that is not $r_A + \kappa r_B$. After i attempts, $p - i$ candidates are left and the distance between the uniform distribution on $\mathbb{G}_T$ and that of $e(F(\mathsf{ID}), X)^{s_1'(r_A + \kappa r_B)}$ becomes at most $i/p \leq q_d/p$. Then, the only way for $\mathcal{A}$ to cause the new rejection rule to apply is to forge a symmetric authenticated encryption for an essentially random key K. A standard argument shows that, throughout all queries, the probability of $\mathcal{B}$ not rejecting a type I ciphertext is smaller than $q_d \cdot (\mathbf{Adv}^{\mathsf{CT\text{-}INT}}(\ell) + \mathbf{Adv}^{\mathsf{KDF}}(\lambda, \ell) + q_d/p)$. It easily comes that $|\Pr[S_1] - \Pr[S_0]| \leq q_d \cdot (\mathbf{Adv}^{\mathsf{CT\text{-}INT}}(\lambda) + \mathbf{Adv}^{\mathsf{KDF}}(\lambda, \ell) + q_d/p)$.

We now consider type II invalid queries. While $\mathcal{A}$ knows $t^{(1)}_B$, she has initially no information on $t^{(1)}_A$ and the last term of the product (13) is unpredictable to her at the first type II query. Each such rejected query allows $\mathcal{A}$ to rule out at most one candidate as for the value $t^{(1)}_A$. After $i \leq q_d$ unsuccessful type II queries, she is left with at least $p - i$ candidates at the next type II query, where the distance between the uniform distribution on $\mathbb{G}_T$ and that of ψ (calculated as per (13)) becomes smaller than $i/p \leq q_d/p$. Again, one can show that, throughout all queries, the probability of $\mathcal{B}$ not rejecting a type II ciphertext is at most $q_d \cdot (\mathbf{Adv}^{\mathsf{CT\text{-}INT}}(\ell) + \mathbf{Adv}^{\mathsf{KDF}}(\lambda, \ell) + q_d/p)$. Let us call `type-2` the latter event. If all invalid ciphertexts are rejected, $\mathcal{A}$'s probability of success is given by $\Pr[S_1 | \neg\texttt{type-2}] \leq 1/(p - q_d) \leq (q_d + 1)/p$. Since

$$\begin{aligned}
\Pr[S_1] &= \Pr[S_1 \wedge \texttt{type-2}] + \Pr[S_1 \wedge \neg\texttt{type-2}] \\
&\leq \Pr[\texttt{type-2}] + \Pr[S_1 | \neg\texttt{type-2}]\Pr[\neg\texttt{type-2}] \\
&\leq \Pr[\texttt{type-2}] + \Pr[S_1 | \neg\texttt{type-2}] \\
&\leq q_d \cdot \big(\mathbf{Adv}^{\mathsf{CT\text{-}INT}}(\ell) + \mathbf{Adv}^{\mathsf{KDF}}(\lambda, \ell) + \frac{q_d}{p}\big) + \frac{q_d + 1}{p}
\end{aligned}$$

and $|\Pr[S_0] - \Pr[S_1]| \leq q_d \cdot (\mathbf{Adv}^{\mathsf{CT\text{-}INT}}(\lambda) + \mathbf{Adv}^{\mathsf{KDF}}(\lambda, \ell) + q_d/p)$, the claimed upper bound follows. □