Security and Anonymity of Identity-Based Encryption with Multiple Trusted Authorities

Kenneth G. Paterson and Sriramkrishnan Srinivasan

Information Security Group,
Royal Holloway, University of London,
Egham, Surrey TW20 0EX, U.K.
{kenny.paterson,s.srinivasan}@rhul.ac.uk

Abstract. We consider the security of Identity-Based Encryption (IBE) in the setting of multiple Trusted Authorities (TAs). In this multi-TA setting, we envisage multiple TAs sharing some common parameters, but each TA generating its own master secrets and master public keys. We provide security notions and security models for the multi-TA setting which can be seen as natural extensions of existing notions and models for the single-TA setting. In addition, we study the concept of TA anonymity, which formally models the inability of an adversary to distinguish two ciphertexts corresponding to the same message and identity but generated using different TA master public keys. We argue that this anonymity property is a natural one of importance in enhancing privacy and limiting traffic analysis in multi-TA environments. We study a modified version of a Fujisaki-Okamoto conversion in the multi-TA setting, proving that our modification lifts security and anonymity properties from the CPA to the CCA setting. Finally, we apply these results to study the security of the Boneh-Franklin and Sakai-Kasahara IBE schemes in the multi-TA setting.

Keywords: identity-based encryption, multi-TA IBE, anonymity, multiple trusted authorities.

1 Introduction

The concept of Identity-Based Encryption (IBE) was first introduced by Shamir in [23]. In identity-based cryptography(IBC), arbitrary identifying strings such as e-mail addresses or IP addresses can be used to form public keys for users, with the corresponding private keys being created by a Trusted Authority (TA) who is in possession of a system-wide master secret. Then a party Alice who wishes, for example, to encrypt to a party Bob need only know Bob's identifier and the system-wide public parameters. This approach eliminates certificates and the associated processing and management overheads from public key cryptography. The first efficient and secure constructions for IBE were not forthcoming till the work of Cocks [12], and the pairing-based solutions of Sakai, Ohigishi and Kasahara [22] and Boneh and Franklin [6]. Boneh and Franklin [6] also proposed

S.D. Galbraith and K.G. Paterson (Eds.): Pairing 2008, LNCS 5209, pp. 354–375, 2008.

the first security models for IBE and gave schemes secure in the random oracle model [5]. Since the publication of these first results, there has been an explosion of interest in IBE and related cryptographic primitives.

1.1 Motivation and Contributions

Historically, anonymous encryption was motivated in the context of mobile communication. In the standard public key setting, an entity B sends a user A ciphertexts of messages encrypted under A's public key (and vice versa), over a wireless network. It is reasonable to assume that A and B will want to keep their identities hidden from an eavesdropper who can see all ciphertexts on the network. This is possible only when ciphertexts do not leak information about the public keys used to create them, a notion formalised as key-privacy in [4].

If an IBE scheme is used instead of a standard public key scheme, the equivalent notion is that of recipient anonymity: the ciphertext should not leak the identity of the (intended) recipient. In this setting, we assume that there is a single global TA issuing keys to all users in the system, and that all ciphertexts are created using the public parameters of that single global TA. With a small number of exceptions (upon which we elaborate in the related work section below), the security models proposed for IBE to date all consider such a single-TA setting.

It is however possible to envisage scenarios as above but with multiple, independent TAs (perhaps sharing some common system parameters). In some applications, each user may only have a single private key issued by one of the TAs, while in others, users could have multiple private keys for the same identity string with the different private keys being issued by different TAs. In both settings, in addition to the usual IBE security notions of indistinguishability and recipient anonymity, the notion of *TA anonymity* arises as being both natural and of fundamental importance. Here, we desire that an adversary should find it difficult to distinguish ciphertexts produced using different TA master public keys, even if the ciphertext is for the same message and identity string. As well as being a natural security notion for the multi-TA setting, TA anonymity may have practical significance. For example, we can imagine a coalition of TAs operating in a wireless setting where all ciphertexts can be captured from the network by an adversary. In such a scenario, if the ciphertext were to somehow leak the identity of the TA, then this would open up avenues for traffic analysis. In a hostile environment, traffic analysis can lead to the leaking of information relating to which entities are communicating and how frequently, which can often reveal important intelligence about the nature of operations.

In this paper we extend the usual indistinguishability and recipient anonymity notions for IBE security to the multi-TA setting, and, in addition, formalize the notion of TA anonymity. We introduce a modified version of the Fujisaki-Okamoto conversion for the multi-TA setting, proving that our modified transformation lifts security and anonymity properties from the CPA to the CCA setting. We then apply these results to study the security and anonymity of the Boneh-Franklin [6] and the Sakai-Kasahara [21] IBE schemes in the multi-TA setting.

As well as formalising the notion of TA anonymity, our work also establishes new results concerning the recipient anonymity of important IBE schemes. For example, to the best of our knowledge, no CCA-secure variant of the Boneh-Franklin IBE scheme was previously known to have recipient anonymity. Moreover, we show that the Sakai-Kasahara scheme (and a CCA-secure variant of it) enjoys recipient anonymity, contradicting a claim of [7].

1.2 Related Work

Anonymity. In the standard public key setting, the notion of key-privacy [4] captures the requirement that an adversary in possession of a ciphertext cannot tell which public key was used to create the ciphertext, i.e the ciphertext should not leak information about the public key. The equivalent notion in the IBE setting is the notion of recipient anonymity, i.e the ciphertext should not leak the identity of the recipient. The systematic study of recipient anonymity was initiated in [1], motivated both by its intrinsic interest in IBE and for its application in constructing PEKS (Public Key Encryption with Keyword Search) schemes from IBE schemes. Since then, recipient anonymity has quickly become a standard security property for IBE schemes. IBE schemes known to offer recipient anonymity include the CPA-secure `BasicIdent` scheme of Boneh and Franklin [6] and the IBE schemes of Gentry [16].

Multi-TA Security for IBE. Holt [18] also considered security of IBE in the multi-TA setting, motivated by earlier work on anonymous credential systems [19,9]. Two notions of key privacy for IBE were outlined in [18]. The first, termed "identity-based indistinguishability of identity under chosen plaintext attack" (ID-II-CPA), is just the standard single-TA recipient anonymity notion. The second is termed "identity-based indistinguishability of key generator under chosen plaintext attack" (ID-IKG-CPA), and is roughly similar to our notion of multi-TA TA anonymity under chosen plaintext attack (m-TAA-CPA). However, the ID-IKG-CPA security model in [18], while allowing corruption of TAs, does not allow the adversary to extract any user private keys at all. Our m-TAA-CPA model is strictly stronger, allowing both corruption of TAs and extraction of private keys (even for the challenge TA)[1]. Moreover, [18] only considers the CPA setting, showing that the `BasicIdent` scheme of [6] has ID-II-CPA and ID-IKG-CPA security. However, even the proofs for these CPA cases are at best informal. In this paper, we consider the CCA setting, use stronger security notions, and give rigorous proofs.

Wang and Cao [24] gave examples of IBE schemes enjoying reduced ciphertext expansion and reduced computation when the sender sends the same message to a single identity using multiple, different master public keys belonging to different TAs, such that the message can be recovered with a private key issued

[1] Holt's work allows the adversary to dynamically instantiate new TAs during its attack but without any adversarial input to the set up process, while we set up all the TAs at the start of the security games. These two approaches are easily seen to have equivalent strength.

for that identity by any one of the TAs. However, the security models presented in [24] are the standard single-TA, indistinguishability-based security models, and no consideration is given to how security may be affected by encrypting the same message using multiple master public keys. In addition, the schemes of [24] reuse randomness to enhance efficiency, and this is not formally addressed in the security analysis. Barbosa and Farshim [3] consider the security of multi-recipient IBE with randomness re-use, but only in the single-TA setting.

Chase [10] has considered Attribute Based Encryption (ABE), a generalisation of IBE, in the setting of multiple authorities. In her work, a user is equipped with private keys corresponding to attributes from different TAs and the user is only able to decrypt a ciphertext if he possesses a threshold of attributes from different TAs. Chase does not seem to consider the issue of TA anonymity.

Anonymity for Hierarchical IBE. Anonymity properties for IBE have already been studied in the hierarchical setting [1,8]. Anonymous Hierarchical IBE (AHIBE) is related to, but different from, our notion of TA anonymity for IBE. In AHIBE, a single root TA generates public parameters and a master secret, using which the master secrets of all sub-TAs are produced. Ciphertexts are then anonymous, in that an adversary cannot distinguish which identity was used when producing a ciphertext, where now identities are comprised of a vector of strings identifying a hierarchy of TAs and a final user. On other hand, in our multi-TA setting, there is no single root authority, but rather a group of independent TAs (who may share some common parameters). The "right" generalisation of our multi-TA IBE concept to the hierarchical setting would then involve multiple, independent root TAs, each being the root of a tree of TAs and users. Thus we would have a forest of trees, and would then wish to study anonymity properties of ciphertexts in this multi-HIBE setting. We leave further development of this line of research to future work.

Fujisaki-Okamoto Conversions. Yang *et al.* [25] and Kitagawa *et al.* [20] considered the adaptation of the Fujisaki-Okamoto conversions of [14] and [13] to the IBE setting, showing that simple modifications of the original Fujisaki-Okamoto approaches can be used to build IBE schemes with IND-CCA security from schemes having only OW-CPA and IND-CPA security, respectively, in the random oracle model. We adapt the Fujisaki-Okamoto technique of [13] to the multi-TA setting, showing how it lifts security and anonymity properties from the CPA to the CCA setting.

2 Background and Definitions

In this section, we provide basic definitions needed for the remainder of the paper.

Definition 1. *A pairing-friendly group generator* `PairingGen` *is a polynomial time algorithm with input* 1^k *and output a tuple* (G, G_T, e, q, P)*. Here* G, G_T *are groups of prime order* q*,* P *generates* G*, and* $e : G \times G \rightarrow G_T$ *is a bilinear,*

non-degenerate and efficiently computable map. By convention, G is an additive group and G_T multiplicative.

For ease of presentation, we work exclusively in the setting where e is symmetric; our definitions and results can be generalised to the asymmetric setting where $e : G_1 \times G_2 \rightarrow G_T$, with G_1 and G_2 being different groups. Further details concerning the basic choices that are available when using pairings in cryptography can be found in [15].

Definition 2. *A function $\epsilon(k)$ is said to be negligible if, for every c, there exists k_c such that $\epsilon(k) \leq k^{-c}$ for every $k \geq k_c$.*

Definition 3. *We define the advantage of an algorithm $\mathcal{A}$ in solving the Bilinear Diffie-Hellman (BDH) problem in (G, G_T) to be:*

$$\boldsymbol{Adv}_{\mathcal{A}}^{BDH}(k) = \Pr(\mathcal{A}(aP, bP, cP) = e(P,P)^{abc})$$

where $a, b, c \leftarrow \mathbb{Z}_q$. Here, we implicitly assume that parameters (G, G_T, e, q, P) are given to $\mathcal{A}$ as additional inputs. We say that the BDH problem is hard *in (G, G_T) if no polynomial-time algorithm that solves the BDH problem in (G, G_T) has a non-negligible advantage.*

Definition 4. *We define the advantage of an algorithm $\mathcal{A}$ in solving the ℓ-Bilinear Diffie-Hellman Inversion (ℓ-BDHI) problem in (G, G_T) to be:*

$$\boldsymbol{Adv}_{\mathcal{A}}^{\ell\text{-}BDHI}(k) = \Pr(\mathcal{A}(xP, x^2P, \ldots, x^\ell P) = e(P,P)^{1/x})$$

where $x \leftarrow \mathbb{Z}_q$. Here, we implicitly assume that parameters (G, G_T, e, q, P) are given to $\mathcal{A}$ as additional inputs. We say that the ℓ-BDHI problem is hard *in (G, G_T) if no polynomial-time algorithm that solves the ℓ-BDHI problem in (G, G_T) has a non-negligible advantage.*

Definition 5. *A (single-TA) IBE scheme is defined in terms of four algorithms:*

- `Setup`: On input 1^k, outputs a master public key *mpk* which includes system parameters *params*, and a master secret key *msk*. We assume that *params* contains descriptions of the message and ciphertext spaces, MsgSp and CtSp, and that $\mathsf{MsgSp} \subset \{0,1\}^*$.
- `KeyDer`: A key derivation algorithm that on input *mpk*, *msk* and identifier $id \in \{0,1\}^*$, returns a private key usk_{id}. This algorithm may or may not be randomized.
- `Enc`: An encryption algorithm that on input *mpk*, identifier $id \in \{0,1\}^*$ and message $m \in \mathsf{MsgSp}$, returns a ciphertext $c \in \mathsf{CtSp}$. This algorithm is usually randomized; in subsequent descriptions, we will write $c = \texttt{Enc}(mpk, id, m; r)$ when we wish to emphasize that randomness r (drawn from some space RSp) is used when performing an encryption.
- `Dec`: A decryption algorithm that on input *mpk*, a private key usk_{id} and a ciphertext $c \in \mathsf{CtSp}$, returns either a message $m \in \mathsf{MsgSp}$ or a failure symbol $\perp$.

These algorithms must satisfy the standard consistency requirement that decryption undoes encryption, i.e. $\forall m \in \mathsf{MsgSp}, \mathtt{Dec}(mpk, usk_{id}, c) = m$ where $c = \mathtt{Enc}(mpk, id, m)$.

3 Multi-TA Security

We formalize IBE in the multi-TA setting and the associated notions of security. A multi-TA IBE scheme is defined in terms of five algorithms:

- `CommonSetup`: On input 1^k, outputs *params*, a set of system parameters shared by all TAs; $\mathcal{TA} = \{ta_i : 1 \leq i \leq n\}$ will represent the set of (labels of) TAs, where $n = n(k) \in \mathbb{N}$.
- `TASetup`: On input *params*, outputs a master public key *mpk* (which includes *params*), and a master secret key *msk*. This algorithm is randomized and executed independently for each TA in $\mathcal{TA}$.
- `KeyDer`, `Enc`, `Dec`: These are all as per a normal IBE scheme.

Note that we explicitly include a `CommonSetup` algorithm which outputs *params*, a set of system parameters shared by all TAs. The different TAs will of course have different master public keys and master secret keys. Our model is capable of handling situations where no such common system parameters are used, simply by setting *params* to be the security parameter 1^k. Nevertheless, it is not unreasonable to assume that the different TAs may share some common system parameters (e.g. the output of a pairing parameter generator in the Boneh-Franklin IBE scheme), since cryptographic schemes and related parameters are often standardised by bodies like ISO, NIST or IEEE P1363, and then used in multiple domains by different authorities. Indeed, the IEEE P1363.3 working group aims to produce a set of standards specific to identity based cryptography and we may expect specific recommendations for cryptographic parameters to be produced by this group in due course. For the concrete schemes considered in this paper, common parameters are needed in order to achieve our notion of TA anonymity; doing so without having some (non-trivial) common parameters is an interesting open problem.

We also need a standard consistency requirement on such a scheme. In addition, in applications, we may require a robustness condition – decrypting a ciphertext created using an identity and the master public key of one TA should fail to decrypt using a private key for that (or any other) identity issued by another TA. We return to this issue in Section 5.

In the security games defined below, $TASet$ represents the set of TAs that have been compromised, i.e queried for their master secret keys, $IDSet_{ta}$ represents the set of identities queried for private keys for each $ta \in \mathcal{TA}$, while $CSet_{ta}$ represents the set of identity/ciphertext pairs on which decryption queries have been performed for each $ta \in \mathcal{TA}$. In these games, $MPK = \{mpk_{ta} : ta \in \mathcal{TA}\}$ and $MSK = \{msk_{ta} : ta \in \mathcal{TA}\}$ represent the set of all master public keys and all master secret keys, respectively. For each experiment defined below,

we associate to an adversary $\mathcal{A}$ and a bit $b \in \{0,1\}$, the advantage of the adversary for a given "notion-attack" combination, which is defined as:

$$\mathbf{Adv}_{\mathcal{A}}^{\text{notion-atk}}(k) = \left|\Pr[\mathbf{Exp}_{\mathcal{A}}^{\text{notion-atk-1}}(k) = 1] - \Pr[\mathbf{Exp}_{\mathcal{A}}^{\text{notion-atk-0}}(k) = 1]\right|$$

A scheme is said to be "notion-atk"-secure if the advantage of all PPT adversaries is negligible as a function of the security parameter k.

We focus below on Chosen Ciphertext Attacks (CCA) for three different security notions: indistinguishability, recipient anonymity and TA anonymity. Removing adversarial access to decryption oracles gives the same notions of security against a Chosen Plaintext Attack (CPA).

In each of the first two cases (namely, indistinguishability of messages and recipient anonymity), setting $n = 1$ and removing access to the `Corrupt` oracle gives us a security notion that coincides with a known (single-TA) IBE security notion. Formally, to obtain a (single-TA) IBE scheme, we need to combine the `CommonSetup` and `TASetup` algorithms of the multi-TA scheme into a single `Setup` algorithm. In what follows, we will refer to this scheme as being the *corresponding single-TA IBE scheme*. In the third case, TA anonymity, the security notion is inappropriate for the single-TA setting.

3.1 m-IND-CCA Security

We first define the m-IND-CCA security notion that captures indistinguishability of messages under chosen ciphertext attacks in the multi-TA setting.

Experiment $\mathbf{Exp}_{\mathcal{A}}^{\text{m-IND-CCA-b}}(k)$
$params \leftarrow \texttt{CommonSetup}(1^k)$
$TASet \leftarrow \emptyset$
$\forall ta \in \mathcal{TA}$, $(mpk_{ta}, msk_{ta}) \leftarrow \texttt{TASetup}(params)$
$IDSet_{ta} \leftarrow \emptyset$, $CSet_{ta} \leftarrow \emptyset$
$(ta, id, m_0, m_1, state) \leftarrow$
$\quad \mathcal{A}^{\texttt{Corrupt},\texttt{KeyDer},\texttt{Dec}}(\texttt{find}, MPK)$
$c^* \leftarrow \texttt{Enc}(mpk_{ta}, id, m_b)$
$b' \leftarrow \mathcal{A}^{\texttt{Corrupt},\texttt{KeyDer},\texttt{Dec}}(\texttt{guess}, c^*, state)$
If $\{m_0, m_1\} \nsubseteq \mathsf{MsgSp}$ or $|m_0| \neq |m_1|$ or $m_0 = m_1$ then return 0
If $ta \notin TASet$, $id \notin IDSet_{ta}$ and $(id, c^*) \notin CSet_{ta}$ then return b' else return 0

Oracle $\texttt{Corrupt}(ta)$
$TASet \leftarrow TASet \cup \{ta\}$
Return msk_{ta}

Oracle $\texttt{KeyDer}(ta, id)$
$IDSet_{ta} \leftarrow IDSet_{ta} \cup \{id\}$
$usk_{id,ta} \leftarrow \texttt{KeyDer}(msk_{ta}, id)$
Return $usk_{id,ta}$

Oracle $\texttt{Dec}(ta, id, c)$
$CSet_{ta} \leftarrow CSet_{ta} \cup (id, c)$
$usk_{id,ta} \leftarrow \texttt{KeyDer}(msk_{ta}, id)$
$m \leftarrow \texttt{Dec}(mpk_{ta}, usk_{id,ta}, c)$
Return m

The following theorem relates the m-IND-CCA security of a multi-TA IBE scheme to the IND-CCA security of the corresponding single-TA IBE scheme.

Theorem 1. *Let $atk \in \{CPA, CCA\}$. Then for any m-IND-atk adversary $\mathcal{A}$ against a multi-TA IBE scheme with n TAs having advantage ε and running in time t, there exists an IND-atk adversary $\mathcal{B}$ against the corresponding single-TA IBE scheme with advantage $\frac{\varepsilon}{n}$ and running in time $O(time(\mathcal{A}))$.*

Proof. Suppose there is an m-IND-atk adversary $\mathcal{A}$ against a multi-TA IBE scheme having advantage ε and running in time t. We show how to construct an algorithm $\mathcal{B}$ that uses $\mathcal{A}$ to break the IND-atk security of the corresponding single-TA IBE scheme.

$\mathcal{B}$'s input from its challenger is the public key mpk of the single-TA scheme which, by our definitions, includes some public parameters *params* that are output by the `CommonSetup` part of the `Setup` algorithm of the single-TA scheme. $\mathcal{B}$'s task is to break the IND-atk property of the scheme and it does this by acting as a challenger for $\mathcal{A}$.

$\mathcal{B}$ first sets up a multi-TA IBE scheme. It does this by first taking *params* from the public key of the single-TA scheme. If n is the number of TAs in the multi-TA setting, it first picks $i \stackrel{\$}{\leftarrow} \{1, \ldots n\}$ and sets $mpk_{ta_i} = mpk$ (note it does not know the corresponding master secret key for this TA). For the remaining $n-1$ TAs it generates the master public keys and master secret keys itself using the `TASetup` algorithm. $\mathcal{B}$ now gives the set of n master public keys to $\mathcal{A}$.

$\mathcal{A}$ then makes a series of TA corrupt queries, extraction queries (and decryption queries in the CCA setting) which $\mathcal{B}$ answers using either its knowledge of the relevant master secret key or by relaying queries to its own challenger. If $\mathcal{A}$ makes a corrupt query on ta_i then $\mathcal{B}$ aborts the simulation.

$\mathcal{A}$ also makes a single query in the challenge phase; if $\mathcal{A}$'s selected TA in this phase is not ta_i, then $\mathcal{B}$ aborts, otherwise $\mathcal{B}$ again uses its own challenger to answer the query. When $\mathcal{A}$ terminates by outputting a bit b', $\mathcal{B}$ simply relays this bit to its challenger.

This completes our description of $\mathcal{B}$'s simulation. Note that $\mathcal{A}$'a view of the simulation is identical to its view in a real attack, unless $\mathcal{B}$ aborts. Moreover $\mathcal{B}$'s output b' is correct if $\mathcal{A}$'s is. It is easy to see that $\mathcal{B}$ aborts with probability $1/n$ and that $\mathcal{B}$ runs in time $O(time(\mathcal{A}))$. The result follows.

3.2 m-RA-CCA Security

Our m-RA-CCA security notion captures the notion of recipient anonymity in the presence of chosen ciphertext attackers, in the multi-TA setting. The single-TA version of the m-RA-CPA security notion was studied in detail in [1], where it was named IBE-ANO-CPA security.

Halevi [17] provides a simple sufficient condition for an IND-CPA public key encryption scheme to have key-privacy: given public keys pk_0 and pk_1 and the encryption of a random message under pk_b for a bit b chosen at random, even a computationally unbounded adversary should have negligible advantage in determining which public key was used. Abdalla *et al.* [1] extended this condition to study recipient anonymity of IND-CPA-secure IBE schemes. We further extend these ideas to study multi-TA IBE schemes in the following sections.

Here, as throughout, we suppress "IBE", since all of our work is in the ID-based setting. We use "RA' in place of "ANO" because we wish to study two forms of anonymity, *viz* recipient anonymity (RA) and TA anonymity (TAA).

Experiment $\mathbf{Exp}^{\text{m-RA-CCA-b}}_{\mathcal{A}}(k)$
$params \leftarrow \texttt{CommonSetup}(1^k)$
$TASet \leftarrow \emptyset$
$\forall ta \in \mathcal{TA}$, $(mpk_{ta}, msk_{ta}) \leftarrow \texttt{TASetup}(params)$,
$IDSet_{ta} \leftarrow \emptyset$ and $CSet_{ta} \leftarrow \emptyset$
$(ta, id_0, id_1, m, state) \leftarrow$
$\mathcal{A}^{\texttt{Corrupt},\texttt{KeyDer},\texttt{Dec}}(\texttt{find}, MPK)$
$c^* \leftarrow \texttt{Enc}(mpk_{ta}, id_b, m)$
$b' \leftarrow \mathcal{A}^{\texttt{Corrupt},\texttt{KeyDer},\texttt{Dec}}(\texttt{guess}, c^*, state)$
If $m \notin \mathsf{MsgSp}$ or $id_0 = id_1$ then return 0
If $ta \notin TASet$, $id_0 \notin IDSet_{ta}$, $id_1 \notin IDSet_{ta}$, $(id_0, c^*) \notin CSet_{ta}$ and $(id_1, c^*) \notin CSet_{ta}$ then return b' else return 0

Oracle $\texttt{Corrupt}(ta)$
$TASet \leftarrow TASet \cup \{ta\}$
Return msk_{ta}

Oracle $\texttt{KeyDer}(ta, id)$
$IDSet_{ta} \leftarrow IDSet_{ta} \cup \{id\}$
$usk_{id,ta} \leftarrow \texttt{KeyDer}(msk_{ta}, id)$
Return $usk_{id,ta}$

Oracle $\texttt{Dec}(ta, id, c)$
$CSet_{ta} \leftarrow CSet_{ta} \cup (id, c)$
$usk_{id,ta} \leftarrow \texttt{KeyDer}(msk_{ta}, id)$
$m \leftarrow \texttt{Dec}(mpk_{ta}, usk_{id,ta}, c)$
Return m

Theorem 2. *Let atk* $\in \{CPA, CCA\}$. *Then for any m-RA-atk adversary* $\mathcal{A}$ *against a multi-TA IBE scheme with n TAs having advantage* ε *and running in time t, there exists an RA-atk adversary* $\mathcal{B}$ *against the corresponding single-TA IBE scheme with advantage* $\frac{\varepsilon}{n}$ *and running in time* $O(time(\mathcal{A}))$.

The proof is similar to that of Theorem 1 and is omitted.

3.3 m-RA-RE-CCA Security

In order to establish the m-RA-CPA/m-RA-CCA security of concrete schemes, it is helpful to work with a related notion, m-RA-RE-CPA/m-RA-RE-CCA security. Our treatment here follows that of [1], with appropriate modifications for the multi-TA setting.

In handling the challenge phase in the following game, the challenger encrypts a random message m' in place of the adversary's choice of message m, hence the choice "RE" in m-RA-RE-CCA to signify "randomized encryption".

Experiment $\mathbf{Exp}^{\text{m-RA-RE-CCA-b}}_{\mathcal{A}}(k)$
$params \leftarrow \texttt{CommonSetup}(1^k)$
$TASet \leftarrow \emptyset$
$\forall ta \in \mathcal{TA}$, $(mpk_{ta}, msk_{ta}) \leftarrow \texttt{TASetup}(params)$,
$IDSet_{ta} \leftarrow \emptyset$ and $CSet_{ta} \leftarrow \emptyset$
$(ta, id_0, id_1, m, state) \leftarrow$
$\mathcal{A}^{\texttt{Corrupt},\texttt{KeyDer},\texttt{Dec}}(\texttt{find}, MPK)$
$m' \xleftarrow{\$} \mathsf{MsgSp}$ with $|m'| = |m|$;
$c^* \leftarrow \texttt{Enc}(mpk_{ta}, id_b, m')$
$b' \leftarrow \mathcal{A}^{\texttt{Corrupt},\texttt{KeyDer},\texttt{Dec}}(\texttt{guess}, c^*, state)$
If $m \notin \mathsf{MsgSp}$ or $id_0 = id_1$ then return 0
If $ta \notin TASet$, $id_0 \notin IDSet_{ta}$, $id_1 \notin IDSet_{ta}$, $(id_0, c^*) \notin CSet_{ta}$ and $(id_1, c^*) \notin CSet_{ta}$ then return b' else return 0

Oracle $\texttt{Corrupt}(ta)$
$TASet \leftarrow TASet \cup \{ta\}$
Return msk_{ta}

Oracle $\texttt{KeyDer}(ta, id)$
$IDSet_{ta} \leftarrow IDSet_{ta} \cup \{id\}$
$usk_{id,ta} \leftarrow \texttt{KeyDer}(msk_{ta}, id)$
Return $usk_{id,ta}$

Oracle $\texttt{Dec}(ta, id, c)$
$CSet_{ta} \leftarrow CSet_{ta} \cup (id, c)$
$usk_{id,ta} \leftarrow \texttt{KeyDer}(msk_{ta}, id)$
$m \leftarrow \texttt{Dec}(mpk_{ta}, usk_{id,ta}, c)$
Return m

The following result relates the notions of m-RA-atk security and m-RA-RE-atk security; a single-TA version of this result for atk = CPA was given in [1].

Lemma 1. *Let* `m-IBE` *be a multi-TA IBE scheme that is m-IND-atk-secure and m-RA-RE-atk-secure. Then* `m-IBE` *is also m-RA-atk-secure. Here* $atk \in \{CPA, CCA\}$.

Proof. Let $\mathcal{A}$ be a poly-time algorithm (PTA) attacking the m-RA-atk security of a scheme `m-IBE`. It is easy to construct PTAs $\mathcal{A}_1$, $\mathcal{A}_3$ attacking the m-IND-atk security of `m-IBE`, and a PTA $\mathcal{A}_2$ attacking m-RA-RE-atk security of `m-IBE` such that:

$$\begin{aligned}
& \mathbf{Adv}_{\mathcal{A}}^{\text{m-RA-atk}}(k) \\
= \;& |\Pr[\mathbf{Exp}_{\mathcal{A}}^{\text{m-RA-atk-1}}(k)=1] - \Pr[\mathbf{Exp}_{\mathcal{A}}^{\text{m-RA-atk-0}}(k)=1]| \\
= \;& |\Pr[\mathbf{Exp}_{\mathcal{A}}^{\text{m-RA-atk-1}}(k)=1] - \Pr[\mathbf{Exp}_{\mathcal{A}}^{\text{m-RA-RE-atk-1}}(k)=1] \\
& + \Pr[\mathbf{Exp}_{\mathcal{A}}^{\text{m-RA-RE-atk-1}}(k)=1] - \Pr[\mathbf{Exp}_{\mathcal{A}}^{\text{m-RA-RE-atk-0}}(k)=1] \\
& + \Pr[\mathbf{Exp}_{\mathcal{A}}^{\text{m-RA-RE-atk-0}}(k)=1] - \Pr[\mathbf{Exp}_{\mathcal{A}}^{\text{m-RA-atk-0}}(k)=1]| \\
\leq \;& |\Pr[\mathbf{Exp}_{\mathcal{A}_1}^{\text{m-RA-atk-1}}(k)=1] - \Pr[\mathbf{Exp}_{\mathcal{A}_1}^{\text{m-RA-RE-atk-1}}(k)=1]| \\
& + |\Pr[\mathbf{Exp}_{\mathcal{A}_2}^{\text{m-RA-RE-atk-1}}(k)=1] - \Pr[\mathbf{Exp}_{\mathcal{A}_2}^{\text{m-RA-RE-atk-0}}(k)=1]| \\
& + |\Pr[\mathbf{Exp}_{\mathcal{A}_3}^{\text{m-RA-RE-atk-0}}(k)=1] - \Pr[\mathbf{Exp}_{\mathcal{A}_3}^{\text{m-RA-atk-0}}(k)=1]| \\
\leq \;& \mathbf{Adv}_{\mathcal{A}_1}^{\text{m-IND-atk}}(k) + \mathbf{Adv}_{\mathcal{A}_2}^{\text{m-RA-RE-atk}}(k) + \mathbf{Adv}_{\mathcal{A}_3}^{\text{m-IND-atk}}(k)
\end{aligned}$$

3.4 m-TAA-CCA Security

The m-TAA-CCA security notion formalizes TA anonymity: a ciphertext should not leak which TA's master public key was used to compute the ciphertext. We work with chosen ciphertext adversaries in the multi-TA setting. As explained above, TA anonymity is a necessary condition to achieve fully private communication thwarting adversarial activity like traffic analysis in the multi-TA setting.

Experiment $\mathbf{Exp}_{\mathcal{A}}^{\text{m-TAA-CCA-b}}(k)$
$params \leftarrow \texttt{CommonSetup}(1^k)$
$TASet \leftarrow \emptyset$
$\forall ta \in \mathcal{TA}$, $(mpk_{ta}, msk_{ta}) \leftarrow \texttt{TASetup}(params)$,
$IDSet_{ta} \leftarrow \emptyset$ and $CSet_{ta} \leftarrow \emptyset$
$(ta_0, ta_1, id, m, state) \leftarrow$
$\quad \mathcal{A}^{\texttt{Corrupt},\texttt{KeyDer},\texttt{Dec}}(\texttt{find}, MPK)$
$c^* \leftarrow \texttt{Enc}(mpk_{ta_b}, id, m)$
$b' \leftarrow \mathcal{A}^{\texttt{Corrupt},\texttt{KeyDer},\texttt{Dec}}(\texttt{guess}, c^*, state)$
If $m \notin \mathsf{MsgSp}$ or $ta_0 = ta_1$ then return 0
If $ta_0 \notin TASet$, $ta_1 \notin TASet$, $id \notin IDSet_{ta_0}$, $id \notin IDSet_{ta_1}$, $(id, c^*) \notin CSet_{ta_0}$ and $(id, c^*) \notin CSet_{ta_1}$ then return b' else return 0

Oracle $\texttt{Corrupt}(ta)$
$TASet \leftarrow TASet \cup \{ta\}$
Return msk_{ta}

Oracle $\texttt{KeyDer}(ta, id)$
$IDSet_{ta} \leftarrow IDSet_{ta} \cup \{id\}$
$usk_{id,ta} \leftarrow \texttt{KeyDer}(msk_{ta}, id)$
Return $usk_{id,ta}$

Oracle $\texttt{Dec}(ta, id, c)$
$CSet_{ta} \leftarrow CSet_{ta} \cup (id, c)$
$usk_{id,ta} \leftarrow \texttt{KeyDer}(msk_{ta}, id)$
$m \leftarrow \texttt{Dec}(mpk_{ta}, usk_{id,ta}, c)$
Return m

3.5 m-TAA-RE-CCA Security

Again, when proving m-TAA-RE-CCA security for a concrete scheme it is sometimes easier to work with the related m-TAA-RE-CCA security notion, which we define next.

Experiment $\mathbf{Exp}_{\mathcal{A}}^{\text{m-TAA-CCA-b}}(k)$
$params \leftarrow \texttt{CommonSetup}(1^k)$
$TASet \leftarrow \emptyset$
$\forall ta \in \mathcal{TA}$, $(mpk_{ta}, msk_{ta}) \leftarrow \texttt{TASetup}(params)$,
$IDSet_{ta} \leftarrow \emptyset$ and $CSet_{ta} \leftarrow \emptyset$
$(ta_0, ta_1, id, m, state) \leftarrow$
$\quad \mathcal{A}^{\texttt{Corrupt},\texttt{KeyDer},\texttt{Dec}}(\texttt{find}, MPK)$
$m' \xleftarrow{\$} \mathsf{MsgSp}$ with $|m'| = |m|$;
$c^* \leftarrow \texttt{Enc}(mpk_{ta_b}, id, m')$
$b' \leftarrow \mathcal{A}^{\texttt{Corrupt},\texttt{KeyDer},\texttt{Dec}}(\texttt{guess}, c^*, state)$
If $m \notin \mathsf{MsgSp}$ or $ta_0 = ta_1$ then return 0
If $ta_0 \notin TASet$, $ta_1 \notin TASet$, $id \notin IDSet_{ta_0}$, $id \notin IDSet_{ta_1}$, $(id, c^*) \notin CSet_{ta_0}$ and $(id, c^*) \notin CSet_{ta_1}$ then return b' else return 0.

Oracle $\texttt{Corrupt}(ta)$
$TASet \leftarrow TASet \cup \{ta\}$
Return msk_{ta}

Oracle $\texttt{KeyDer}(ta, id)$
$IDSet_{ta} \leftarrow IDSet_{ta} \cup \{id\}$
$usk_{id,ta} \leftarrow \texttt{KeyDer}(msk_{ta}, id)$
Return $usk_{id,ta}$

Oracle $\texttt{Dec}(ta, id, c)$
$CSet_{ta} \leftarrow CSet_{ta} \cup (id, c)$
$usk_{id,ta} \leftarrow \texttt{KeyDer}(msk_{ta}, id)$
$m \leftarrow \texttt{Dec}(mpk_{ta}, usk_{id,ta}, c)$
Return m

Lemma 2. *Let* `m-IBE` *be a multi-TA IBE scheme that is m-IND-atk-secure and m-TAA-RE-atk-secure. Then* `m-IBE` *is also m-TAA-atk-secure. Here* $atk \in \{CPA, CCA\}$.

The proof is similar to that of Lemma 1 and is omitted.

3.6 A Combined Security Notion: m-IND-TAA-RA-CCA Security

Finally, we define an m-IND-RA-TAA-CCA experiment that simultaneously captures message indistinguishability, recipient anonymity, and TA anonymity in the multi-TA setting for chosen ciphertext adversaries.

Experiment $\mathbf{Exp}_{\mathcal{A}}^{\text{m-IND-RA-TAA-CCA-b}}(k)$
$params \leftarrow \texttt{CommonSetup}(1^k)$
$TASet \leftarrow \emptyset$
$\forall ta \in \mathcal{TA}$, $(mpk_{ta}, msk_{ta}) \leftarrow \texttt{TASetup}(params)$,
$IDSet_{ta} \leftarrow \emptyset$ and $CSet_{ta} \leftarrow \emptyset$
$(ta_0, ta_1, id_0, id_1, m_0, m_1, state) \leftarrow$
$\quad \mathcal{A}^{\texttt{Corrupt},\texttt{KeyDer},\texttt{Dec}}(\texttt{find}, MPK)$
$c^* \leftarrow \texttt{Enc}(mpk_{ta_b}, id_b, m_b)$
$b' \leftarrow \mathcal{A}^{\texttt{Corrupt},\texttt{KeyDer},\texttt{Dec}}(\texttt{guess}, c^*, state)$
If $\{m_0, m_1\} \not\subseteq \mathsf{MsgSp}$ or $|m_0| \neq |m_1|$
then return 0
If $(ta_0 = ta_1$ and $id_0 = id_1$ and $m_0 = m_1)$
then return 0
If $ta_0 \notin TASet$, $ta_1 \notin TASet$, $id_0 \notin IDSet_{ta_0}$, $id_1 \notin IDSet_{ta_1}$, $(id_0, c^*) \notin CSet_{ta_0}$ and $(id_1, c^*) \notin CSet_{ta_1}$ then return b' else return 0.

Oracle $\texttt{Corrupt}(ta)$
$TASet \leftarrow TASet \cup \{ta\}$
Return msk_{ta}

Oracle $\texttt{KeyDer}(ta, id)$
$IDSet_{ta} \leftarrow IDSet_{ta} \cup \{id\}$
$usk_{id,ta} \leftarrow \texttt{KeyDer}(msk_{ta}, id)$
Return $usk_{id,ta}$

Oracle $\texttt{Dec}(ta, id, c)$
$CSet_{ta} \leftarrow CSet_{ta} \cup (id, c)$
$usk_{id,ta} \leftarrow \texttt{KeyDer}(msk_{ta}, id)$
$m \leftarrow \texttt{Dec}(mpk_{ta}, usk_{id,ta}, c)$
Return m

Lemma 3. *Let* `m-IBE` *be a multi-TA IBE scheme that is m-IND-atk-secure, m-RA-atk-secure and m-TAA-atk-secure. Then* `m-IBE` *is also m-IND-RA-TAA-atk-secure. Here* $atk \in \{CPA, CCA\}$.

Proof. The proof (informally) follows by noting that if `m-IBE` is m-TAA-atk-secure, then the challenger may replace the triple (ta_0, id_0, m_0) with (ta_1, id_0, m_0) in its response to the challenge query without the adversary being able to detect the change. Likewise, using m-RA-atk security, the challenger may then replace (ta_1, id_0, m_0) with (ta_1, id_1, m_0). Finally, using m-IND-atk security, the challenger can replace (ta_1, id_1, m_0) with (ta_1, id_1, m_1), again, without the adversary being able to detect the change. This informal argument can be made rigorous using a sequence of games.

A combined m-IND-RA-CCA security notion can also be defined and it is easy to show that m-IND-RA-CCA security holds for a scheme that has both m-IND-CCA and m-RA-CCA security, using a similar strategy as above. In the single-TA setting, we obtain IND-RA-CCA and IND-RA-CPA security notions. The latter security notion for IBE was used to prove the security of PEKS schemes in [1]. Similarly, we define combined m-IND-TAA-CPA and m-IND-TAA-CCA security notions.

4 Extending the Fujisaki-Okamoto Conversion to Multi-TA IBE Schemes

In two separate but related strands of work, Fujisaki and Okamoto studied the problem of building Public Key Encryption (PKE) schemes which are secure in a very strong sense (IND-CCA) from PKE schemes which are secure in a weaker sense.

In [14], Fujisaki and Okamoto gave a generic conversion that takes any OW-CPA-secure PKE scheme satisfying a mild technical condition (γ-uniformity) and outputs a PKE scheme that is IND-CCA-secure in the Random Oracle Model. Yang *et al.* [25] investigated how to adapt this particular Fujisaki-Okamoto (FO) technique to the ID-based setting.

Similarly, in [13], Fujisaki and Okamoto gave a generic conversion that takes any IND-CPA-secure PKE scheme and outputs a PKE scheme that is IND-CCA-secure in the Random Oracle Model. The security analysis in [13] is significantly simpler than that of [14]. Kitagawa *et al.* [20] investigated how to modify this particular FO technique for the ID-based setting.

We now describe a modified FO conversion for IBE in the multi-TA setting. We are able to show that in the multi-TA setting, we can apply this modified conversion to build an IBE scheme that has m-IND-RA-TAA-CCA security from an IBE scheme that is m-IND-RA-TAA-CPA-secure and γ-uniform. We extend the ideas of [13,20]. In particular, we include additional parameters in the input to the hash function used in the scheme. This allows us to efficiently respond to hash queries, simplifies book-keeping in the proof, and yields a simulation that has a reduced running time in comparison to an application of the unmodified Fujisaki-Okamoto transformation.

We begin by defining a suitable notion of γ-uniformity for the multi-TA setting.

Definition 6. *Let Π be a multi-TA IBE scheme with space of randomness RSp. Then Π is said to be γ-uniform if, for any fixed choice of $c \in \mathsf{CtSp}$, $m \in \mathsf{MsgSp}$, $id \in \{0,1\}^*$ and $ta \in \mathcal{TA}$, we have:*

$$\Pr\left[c = \mathtt{Enc}(mpk_{ta}, id, m; r) : r \xleftarrow{\$} \mathsf{RSp}\right] \leq \gamma.$$

Now let $\Pi = \{\mathtt{CommonSetup}, \mathtt{TASetup}, \mathtt{KeyDer}, \mathtt{Enc}, \mathtt{Dec}\}$ be a multi-TA IBE scheme. Then $\Pi' = \{\mathtt{CommonSetup}', \mathtt{TASetup}', \mathtt{KeyDer}', \mathtt{Enc}', \mathtt{Dec}'\}$ denotes a new multi-TA IBE scheme with algorithms defined as follows.

Let $l_0 + l_1$ be the bit length of messages in Π, where l_0 will be the bit length of messages in Π', and let RSp be the space of randomness used by $\mathtt{Enc}$.

- $\mathtt{CommonSetup}'$: As in $\mathtt{CommonSetup}$, but in addition, we pick a hash function $H : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^{l_0} \times \{0,1\}^{l_1} \rightarrow \mathsf{RSp}$.
- $\mathtt{TASetup}'$:As in $\mathtt{TASetup}$.
- $\mathtt{KeyDer}'$: As in $\mathtt{KeyDer}$.
- $\mathtt{Enc}'$: This algorithm takes as input mpk_{ta} for $ta \in \mathcal{TA}$, $id \in \{0,1\}^*$, and a message $m \in \{0,1\}^{l_0}$. Its output is:

$$\mathtt{Enc}'(mpk_{ta}, id, m) = \mathtt{Enc}(mpk_{ta}, id, m||\sigma; H(mpk_{ta}, id, m, \sigma))$$

  where $\sigma \xleftarrow{\$} \{0,1\}^{l_1}$. So Π' has randomness space $\{0,1\}^{l_1}$.
- $\mathtt{Dec}'$: Let c denote a ciphertext to be decrypted using a private key $usk_{id,ta}$ issued by TA ta with master public key mpk_{ta} for identity id. This algorithm works as follows:
  1. Compute $m' = \mathtt{Dec}(mpk_{ta}, usk_{id,ta}, c)$.
  2. Let $m = [m']^{l_0}$ and $\sigma = [m']_{l_1}$ where $[a]^b$ and $[a]_b$ denote the first and last b bits of a string a respectively.
  3. Test if $\mathtt{Enc}(mpk_{ta}, id, m||\sigma; H(mpk_{ta}, id, m, \sigma)) = c$. If not output $\perp$; otherwise output m as the decryption of c.

Theorem 3. *Modelling H as a random oracle, if Π is a multi-TA IBE scheme that is m-IND-RA-TAA-CPA-secure and γ-uniform for some negligible γ, then Π' is m-IND-RA-TAA-CCA-secure.*

In more detail, suppose Π is a γ-uniform IBE encryption scheme. Let $\mathcal{A}$ be an m-IND-RA-TAA-CCA adversary which has advantage $\epsilon(k)$ against Π' and which runs in time $t(k)$. Suppose $\mathcal{A}$ makes at most q_H queries to H, at most q_E extraction queries, and at most q_D decryption queries. Suppose further that executing $\mathtt{Enc}$ once needs at most time τ. Then there is an m-IND-RA-TAA-CPA adversary $\mathcal{B}$ which has advantage at least $\epsilon'(k)$ against Π, with running time $t'(k)$, such that

$$\epsilon'(k) = 2\left(\frac{\epsilon + 1}{2} - \frac{q_h}{2^{l_1} - 1}\right)(1 - \gamma)^{q_d} - 1$$

and

$$t'(k) = O(t(k) + q_h \tau).$$

Proof. Suppose there is an m-IND-RA-TAA-CCA adversary $\mathcal{A}$ against Π' with advantage $\epsilon(k)$ and running in time $t(k)$. We show how to construct an adversary $\mathcal{B}$ that uses $\mathcal{A}$ to break the m-IND-RA-TAA-CPA-security of Π

$\mathcal{B}$'s input is the set of all master public keys MPK. $\mathcal{B}$ gives $\mathcal{A}$ the set MPK. $\mathcal{A}$ also has access to random oracle H that is controlled by $\mathcal{B}$. $\mathcal{A}$ then makes a series of queries which $\mathcal{B}$ answers as follows.

- **H-queries:** $\mathcal{B}$ maintains a list of tuples $\langle mpk_i, id_i, m_i, \sigma_i, g_i, c_i\rangle$. We refer to this list as the H^{list}. The list is initially empty.
  When $\mathcal{A}$ makes a H query on (mpk, id, m, σ), $\mathcal{B}$ responds as follows:
  - If the query (mpk, id, m, σ) already appears in a tuple $\langle mpk_i, id_i, m_i, \sigma_i, g_i, c_i\rangle$ then $\mathcal{B}$ responds with $H(mpk, id, m, \sigma) = g_i$.
  - Otherwise $\mathcal{B}$ picks $g \xleftarrow{\$} \mathsf{RSp}$, generates $c = \mathtt{Enc}(mpk_{ta}, id, m||\sigma; g)$, adds the tuple $\langle mpk, id, m, \sigma, g, c\rangle$ to the H^{list} and responds to $\mathcal{A}$ with $H(mpk, id, m, \sigma) = g$.
- **Corrupt Queries:** If $\mathcal{A}$ issues a TA corrupt query on $ta \in \mathcal{TA}$, then $\mathcal{B}$ simply relays this query to its challenger, which responds with the corresponding master secret key msk_{ta}. $\mathcal{B}$ then passes the resulting key to $\mathcal{A}$.
- **Extraction Queries:** If $\mathcal{A}$ issues an extraction query on (ta, id), then $\mathcal{B}$ forwards (ta, id) to its challenger, which responds with the private key $usk_{id,ta}$. $\mathcal{B}$ forwards this key to $\mathcal{A}$.
- **Decryption Queries:** If $\mathcal{A}$ issues a decryption query on (ta, id, c), $\mathcal{A}$ responds as follows:
  - Searches for a tuple $\langle mpk_i, id_i, m_i, \sigma_i, g_i, c_i\rangle$ from the H^{list} such that $mpk_{ta} = mpk_i$, $id = id_i$ and $c = c_i$.
  - If such a tuple exists, then outputs m, else outputs $\perp$.
- **Challenge:** $\mathcal{A}$ outputs data $(ta_0, ta_1, id_0, id_1, m_0, m_1)$ on which it wishes to be challenged. This data is subject to the usual restrictions (see Section 3.6). $\mathcal{B}$ chooses two l_1 bit strings σ_0 and σ_1 uniformly at random, subject to the condition that they be distinct, and sends $(ta_0, ta_1, id_0, id_1, m_0||\sigma_0, m_1||\sigma_1)$ to its challenger. $\mathcal{B}$'s challenger picks a random bit b and sets

$$c^* = \mathtt{Enc}(mpk_{ta_b}, id_b, m_b||\sigma_b; r)$$

  where $r \in \mathsf{RSp}$. $\mathcal{B}$ forwards c^* to $\mathcal{A}$.

After the Challenge query has been issued, if the adversary $\mathcal{A}$ makes a hash oracle query on either $(ta_0, id_0, m_0, \sigma_0)$ or $(ta_1, id_1, m_1, \sigma_1)$ then the adversary $\mathcal{B}$ simply outputs $b' = 0$ or $b' = 1$, respectively, as its guess for the value of the bit b. If neither hash query is made then, at the end of $\mathcal{A}$'s attack, $\mathcal{B}$ simply outputs the same bit b' that $\mathcal{A}$ outputs. $\mathcal{B}$ wins if $b' = b$. This completes our description of the simulation.

Our analysis now follows closely the analysis in [13]. We define the following events and probabilities.

Let $\Pr[\mathtt{Succ}\mathcal{A}]$ be the probability that adversary $\mathcal{A}$ outputs a bit $b' = b$. Similarly, let $\Pr[\mathtt{Succ}\mathcal{B}]$ be the probability that adversary $\mathcal{B}$ outputs a bit $b' = b$. For notational convenience, we let ϵ denote $\mathcal{A}$'s advantage in the simulation.

Let $\mathtt{Ask}_b$ be the event that $\mathcal{A}$ asks a hash query that coincides with$(mpk_{ta_b}, id_b, m_b, \sigma_b)$ and $\mathtt{Ask}_{\bar{b}}$ be the event that $\mathcal{A}$ asks a hash query that coincides with $(mpk_{ta_{\bar{b}}}, id_{\bar{b}}, m_{\bar{b}}, \sigma_{\bar{b}})$. Notice that these two queries are distinct because $\sigma_0 \neq \sigma_1$.

We define $\mathcal{F}$ to be the event that $\mathcal{B}$ fails to answer a decryption query correctly at some point during the game so that $\Pr[\neg\mathcal{F}]$ is the probability that $\mathcal{B}$ answers all decryption queries correctly during the simulation. Now,

$$\begin{aligned}\Pr[\mathtt{Succ}\mathcal{A}] = &\Pr[\mathtt{Succ}\mathcal{A}|\mathtt{Ask}_b] \cdot \Pr[\mathtt{Ask}_b] \\ &+ \Pr[\mathtt{Succ}\mathcal{A}|(\neg\mathtt{Ask}_b) \wedge \mathtt{Ask}_{\bar{b}}] \cdot \Pr[(\neg\mathtt{Ask}_b) \wedge \mathtt{Ask}_{\bar{b}})] \\ &+ \Pr[\mathtt{Succ}\mathcal{A}|(\neg\mathtt{Ask}_b) \wedge (\neg\mathtt{Ask}_{\bar{b}})] \cdot \Pr[(\neg\mathtt{Ask}_b) \wedge (\neg\mathtt{Ask}_{\bar{b}})].\end{aligned}$$

Similarly,

$$\begin{aligned}\Pr[\mathtt{Succ}\mathcal{B}] = &\Pr[\mathtt{Succ}\mathcal{B}|\mathtt{Ask}_b] \cdot \Pr[\mathtt{Ask}_b] \\ &+ \Pr[\mathtt{Succ}\mathcal{B}|(\neg\mathtt{Ask}_b) \wedge \mathtt{Ask}_{\bar{b}}] \cdot \Pr[(\neg\mathtt{Ask}_b) \wedge \mathtt{Ask}_{\bar{b}})] \\ &+ \Pr[\mathtt{Succ}\mathcal{B}|(\neg\mathtt{Ask}_b) \wedge (\neg\mathtt{Ask}_{\bar{b}})] \cdot \Pr[(\neg\mathtt{Ask}_b) \wedge (\neg\mathtt{Ask}_{\bar{b}})].\end{aligned}$$

From the conditions of the simulation, we have the following:

$$\begin{aligned}\Pr[\mathtt{Succ}\mathcal{B}|\mathtt{Ask}_b] &= 1, \\ \Pr[\mathtt{Succ}\mathcal{B}|(\neg\mathtt{Ask}_b) \wedge \mathtt{Ask}_{\bar{b}}] &= 0, \\ \Pr[\mathtt{Succ}\mathcal{A}|(\neg\mathtt{Ask}_b) \wedge (\neg\mathtt{Ask}_{\bar{b}})] &= \Pr[\mathtt{Succ}\mathcal{B}|(\neg\mathtt{Ask}_b) \wedge (\neg\mathtt{Ask}_{\bar{b}})].\end{aligned}$$

Therefore,

$$\begin{aligned}\Pr[\mathtt{Succ}\mathcal{B}] - \Pr[\mathtt{Succ}\mathcal{A}] &= \Pr[\mathtt{Ask}_b](1 - \Pr[\mathtt{Succ}\mathcal{A}|\mathtt{Ask}_b]) \\ &\quad + \Pr[(\neg\mathtt{Ask}_b) \wedge \mathtt{Ask}_{\bar{b}}](0 - \Pr[\mathtt{Succ}\mathcal{A}|(\neg\mathtt{Ask}_b \wedge \mathtt{Ask}_{\bar{b}})]) \\ &\geq -\Pr[(\neg\mathtt{Ask}_b) \wedge \mathtt{Ask}_{\bar{b}}].\end{aligned}$$

Since even a computationally unbounded adversary has no information about what the string $\sigma_{\bar{b}}$ is (except that it is distinct from σ_b and so is uniformly distributed on a set of size $2^{l_1} - 1$), and our adversary makes at most q_h queries to the oracle H, we infer that $\Pr[(\neg\mathtt{Ask}_b) \wedge \mathtt{Ask}_{\bar{b}}] \leq \frac{q_h}{2^{l_1}-1}$. Hence,

$$\begin{aligned}\Pr[\mathtt{Succ}\mathcal{B}] &\geq \Pr[\mathtt{Succ}\mathcal{A}] - \Pr[(\neg\mathtt{Ask}_b) \wedge \mathtt{Ask}_{\bar{b}}] \\ &\geq \tfrac{\epsilon+1}{2} - \tfrac{q_h}{2^{l_1}-1}.\end{aligned}$$

The event $\mathcal{F}$ occurs only when $\mathcal{A}$ submits a decryption query (ta, id, c) such that

$$c = \mathtt{Enc}(mpk_{ta}, id, m||\sigma; H(mpk_{ta}, id, m, \sigma))$$

without first querying H on input $(mpk_{ta}, id, m, \sigma)$. Now observe that, given values ta, id, c, there is at most one possible message $m' = m||\sigma$ that could result from decrypting ciphertext c under the private key $usk_{id,ta}$, namely $m' = \mathtt{Dec}(mpk_{ta}, usk_{id,ta}, c)$. Applying the definition of γ-uniformity, and noting that the randomness r that would be used to form c for the scheme Π' is still uniformly distributed whenever the relevant hash query has not been made, we see that $\mathcal{B}$ fails to properly answer each decryption query with probability at most γ. Therefore $\Pr[\neg\mathcal{F}] \leq (1-\gamma)^{q_d}$.

Hence, we have

$$\mathbf{Adv}_{\mathcal{B}}(k) = 2\Pr[\mathtt{Succ}\mathcal{B}] \cdot \Pr[\neg\mathcal{F}] - 1 \geq 2(\frac{\epsilon+1}{2} - \frac{q_h}{2^{l_1}-1})(1-\gamma)^{q_d} - 1.$$

For the running time analysis, note that in addition to the running time of $\mathcal{A}$, the adversary $\mathcal{B}$ has to run the encryption algorithm `Enc` at most q_h times. Therefore $t'(k) = O(t(k) + q_h\tau)$. □

Notice that the above theorem as stated requires the initial scheme Π to have all three security properties (IND, RA and TAA) in order to convert from CPA-security to CCA-security. In fact, it is easy to prove versions of Theorem 3 that convert IND-RA-CPA security to IND-RA-CCA security and IND-TAA-CPA security to IND-TAA-CCA security. However, the proof technique does not allow us to prove that the conversion preserves either of our anonymity properties in isolation – we need the base scheme Π to also be IND-secure.

We leave as an open problem to find a modified version of the "other" FO conversion (from [14]) that preserves anonymity properties in the multi-TA setting.

4.1 Applying the Modified FO Conversion to `BasicIdent`

We describe and analyse a multi-TA scheme `m-BasicIdent` that is based on the scheme `BasicIdent` from [6]. This scheme is defined as follows:

`CommonSetup`(1^k):

- $(G, G_T, e, q, P) \leftarrow$ `PairingGen`(1^k).
- Output $params = (G, G_T, e, q, P, H_1, H_2, n)$ where $H_1 : \{0,1\}^* \rightarrow G$, $H_2 : G_T \rightarrow \{0,1\}^n$ for some $n = n(k)$.
- $\mathsf{MsgSp} = \{0,1\}^n$, $\mathsf{CtSp} = G_1 \times \{0,1\}^n$, $\mathsf{RSp} = \mathbb{Z}_q$.

`TASetup`$(params)$

- Set $s \xleftarrow{\$} \mathbb{Z}_q, Q = sP$.
- Set $mpk = (params, Q)$.
- Set $msk = s$.
- Output (mpk, msk).

`KeyDer`$^{H_1}(ta, id)$:

- Set $usk_{id,ta} = msk_{ta} \cdot H_1(id)$.
- Output $usk_{id,ta}$.

`Enc`$^{H_1,H_2}(ta, id, m)$:

- Parse mpk_{ta} as $(params, Q_{ta})$.
- Set $r \xleftarrow{\$} \mathbb{Z}_q$.
- Set $T = e(H_1(id), Q_{ta})^r$.
- Output $c = (rP, m \oplus H_2(T))$.

`Dec`$^{H_2}(ta, usk_{id,ta}, c)$:

- Parse c as (U, V).
- Set $T = e(usk_{id,ta}, U)$.
- Output $m = V \oplus H_2(T)$.

The scheme `m-BasicIdent`.

We next show the scheme that results from applying the modified Fujisaki-Okamoto tranformation to the `m-BasicIdent` scheme above.

`CommonSetup`$'(1^k)$:

- $(G, G_T, e, q, P) \leftarrow$ `PairingGen`(1^k).
- Output $params = (G, G_T, e, q, P, H_1, H_2, H_3, l_0, l_1, n)$ where $H_1 : \{0,1\}^* \rightarrow G$, $H_2 : G_T \rightarrow \{0,1\}^n$ for some $n = n(k)$, $l_0 + l_1 = n$, and $H_3 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^{l_0} \times \{0,1\}^{l_1} \rightarrow \mathbb{Z}_q$.
- $\mathsf{MsgSp} = \{0,1\}^{l_0}$, $\mathsf{CtSp} = G_1 \times \{0,1\}^n$, $\mathsf{RSp} = \{0,1\}^{l_1}$.

`TASetup`$'$: As in `TASetup`

`KeyDer`$'$: As in `KeyDer`

`Enc`$^{H_1,H_2,H_3}(ta, id, m)$:

- Parse mpk_{ta} as $(params, Q_{ta})$.
- Set $\sigma \xleftarrow{\$} \{0,1\}^{l_1}$.
- Set $r = H_3(mpk_{ta}, id, m, \sigma)$.
- Set $T = e(H_1(id), Q_{ta})^r$.
- Output $c = (rP, (m||\sigma) \oplus H_2(T))$.

`Dec`$^{H_2,H_3}(ta, usk_{id,ta}, c)$:

- Parse c as (U, V).
- Set $T = e(usk_{id,ta}, U)$.
- Set $m' = V \oplus H_2(T)$.
- Set $m = [m']^{l_0}$ and $\sigma = [m']_{l_1}$.
- Test if $r = H_3(mpk_{ta}, id, m, \sigma)$. If not, output $\perp$; otherwise output m as the decryption of c.

The scheme `FO-m-BasicIdent`.

Lemma 4. *The multi-TA scheme `m-BasicIdent` is m-IND-CPA-secure, assuming the hardness of the BDH problem in groups output by `PairingGen`.*

Proof. The single-TA scheme corresponding to `m-BasicIdent` is nothing other than the Boneh-Franklin `BasicIdent` scheme, whose IND-CPA security is known to rest on the hardness of the BDH problem in groups output by `PairingGen` [6]. Now apply Theorem 1.

The following result is an extension of a result from [1] that showed that the `BasicIdent` scheme has recipient anonymity against CPA attackers.

Lemma 5. *The multi-TA scheme `m-BasicIdent` is m-RA-CPA-secure and m-TAA-CPA-secure, assuming the hardness of the BDH problem in groups output by `PairingGen`.*

Proof. Ciphertexts c in the `m-BasicIdent` scheme have two parts, namely $U = rP$ and $V = m \oplus H_2(T)$. The value U is chosen uniformly at random from G. If the message m is chosen uniformly at random from $\{0,1\}^n$ then V is also distributed uniformly in $\{0,1\}^n$ and is independent of $H_2(T)$. Thus, in both 0 and 1 worlds of the m-RA-RE-CPA and m-TAA-RE-CPA games, the ciphertext c has exactly the same distribution and any adversary in these RE games will have zero advantage. By Lemma 4, `m-BasicIdent` is m-IND-CPA-secure. Applying Lemmas 1 and 2 yields m-RA-CPA and m-TAA-CPA security for `m-BasicIdent`, assuming the hardness of the BDH problem in groups output by `PairingGen`.

Lemma 6. *The* `m-BasicIdent` *scheme is* γ*-uniform for* $\gamma = 1/q$.

Proof. In the `m-BasicIdent` scheme, the first component of the ciphertext is $U = rP$ where $r \xleftarrow{\$} \mathbb{Z}_q$. It is them immediate that `m-BasicIdent` is γ uniform with $\gamma = 1/q$.

Theorem 4. *The scheme* `FO-m-BasicIdent` *obtained by applying the modified FO conversion to the scheme* `m-BasicIdent` *is m-IND-RA-TAA-CCA-secure, assuming the hardness of the BDH problem in groups output by* `PairingGen`.

Proof. We obtain the above result by combining Lemmas 4, 5 with Lemmas 3, 6 and Theorem 3.

Thus we have obtained an efficient multi-TA IBE scheme enjoying indistinguishability, recipient anonymity and TA anonymity for the CCA setting, in the random oracle model. We note as a corollary of our analysis that the single-TA version of our scheme offers recipient anonymity. To the best of our knowledge, this is the first such result for a CCA-secure variant of `BasicIdent`.

4.2 Applying the Modified FO Conversion to the Sakai-Kasahara IBE Scheme

The Sakai-Kasahara IBE scheme [21] has an alternative (and attractive) private key extraction algorithm compared to the Boneh-Franklin scheme. We define `m-BasicSK`, a multi-TA version of this scheme using symmetric pairings, immediately below, and then provide a sketch security analysis.

`CommonSetup`(1^k):

- $(G, G_T, e, q, P) \leftarrow$ `PairingGen`(1^k).
- Output $params = (G, G_T, e, q, P, Z, H_1, H_2, n)$ where $Z = e(P, P) \in G_T$, $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q$, $H_2 : G_T \rightarrow \{0,1\}^n$ for some $n = n(k)$.
- $\mathsf{MsgSp} = \{0,1\}^n$, $\mathsf{CtSp} = G_1 \times \{0,1\}^n$, $\mathsf{RSp} = \mathbb{Z}_q$.

`TASetup`$(params)$

- Set $s \xleftarrow{\$} \mathbb{Z}_q, Q = sP$.
- Set $mpk = (params, Q)$.
- Set $msk = s$.
- Output (mpk, msk).

`KeyDer`$^{H_1}(ta, id)$:

- Output $usk_{id,ta} = \frac{1}{msk_{ta} + H_1(id)} \cdot P$.

`Enc`$^{H_1,H_2}(ta, id, m)$:

- Parse mpk_{ta} as $(params, Q_{ta})$.
- Set $r \xleftarrow{\$} \mathbb{Z}_q$.
- Set $U = rQ_{ta} + rH_1(id)P$.
- Output $c = (U, m \oplus H_2(Z^r))$.

`Dec`$^{H_2}(ta, usk_{id,ta}, c)$:

- Parse c as (U, V).
- Set $T = e(usk_{id,ta}, U)$.
- Output $m = V \oplus H_2(T)$.

The scheme `m-BasicSK`.

The IND-CPA security of the single-TA scheme corresponding to `m-BasicSK` can be proved by making small modifications to the proof of [11, Theorem 2], which established the OW-CPA security of a closely related scheme based on the hardness of the ℓ-BDHI problem in groups output by `PairingGen` (for some value ℓ related to the number of queries made by the adversary). Using Theorem 1, we can deduce that `m-BasicSK` is m-IND-CPA-secure under the same assumption. It is then easy to establish that `m-BasicSK` is m-RA-CPA-secure and m-TAA-CPA-secure; this requires a similar analysis as in Lemma 5. Moreover, `m-BasicSK` is γ-uniform for $\gamma = 1/q$. We may now apply Theorem 3 to deduce that the scheme `FO-m-BasicSK` that is obtained by applying our modified FO conversion to `m-BasicSK` is m-IND-RA-TAA-CCA-secure, assuming the hardness of the ℓ-BDHI problem in groups output by `PairingGen`.

Thus we have obtained a second efficient multi-TA IBE scheme enjoying indistinguishability, recipient anonymity and TA anonymity for the CCA setting, in the random oracle model. Our CCA-secure scheme has roughly the same performance as the KEM-DEM-derived scheme of [11], but offers stronger proven anonymity guarantees. We also note that even the recipient anonymity of the single-TA version of `m-BasicSK` was not previously known – indeed this is explicitly claimed *not* to hold in [7].

5 Conclusion and Future Work

We have given a formal analysis of various security and anonymity notions for multi-TA IBE schemes and the relationships between them. We have also investigated a modified Fujisaki-Okamoto transformation for IBE and shown that this transformation preserves our security and anonymity notions when building a CCA-secure scheme from a CPA-secure one. We investigated the application of this transformation to the Boneh-Franklin `BasicIdent` scheme and to the Sakai-Kasahara scheme.

In future work, we will investigate further specific IBE schemes and see if they meet the multi-TA security notions introduced in this paper. In particular, it will be interesting to examine the IND-RA-atk-secure IBE schemes of Gentry [16] and see if they can also be proven to be TAA-atk-secure We raised the possibility of adapting the "other" FO conversion of [14] so as to preserve our multi-TA security notions. Another open problem suggested by this work is its generalization to the hierarchical IBE (HIBE) setting, where the anonymity properties of ciphertexts generated using different root TA master public keys could be studied.

Finally, the subject of robustness of IBE in the single-TA and multi-TA settings requires further investigation: when using an IND-RA-TA-CCA-secure scheme in practice in a fully anonymous communications system, users will need to be able to decide whether or not a ciphertext is intended for their consumption. Seemingly the only way for a user to do this is to attempt a trial decryption using his private key, relying on the decryption algorithm to reject the ciphertext if the wrong private key has been used. However, there is nothing intrinsic to our

formal definitions or security models that guarantees that decryption will always output "$\perp$" when the wrong private key is used, though such a robustness property is clearly desirable (as it would prevent attacks where an adversary fooled a user into decrypting a ciphertext intended for another party to obtain a meaningful message upon which the decrypting party might then act). Robustness in this sense for standard public key encryption and IBE schemes is the subject of a recent paper of Abdalla *et al.* [2]. It would be interesting to attempt to extend their results to the multi-TA setting, but it should be noted that the authors of [2] have already established that the FO conversion of [14] does not preserve robustness in general.

Acknowledgements

This research was sponsored in part by the US Army Research Laboratory and the UK Ministry of Defence and was accomplished under Agreement Number W911NF-06-3-0001. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the US Army Research Laboratory, the US Government, the UK Ministry of Defense, or the UK Government. The US and UK Governments are authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon.

The second author is supported by a Dorothy Hodgkin Postgraduate Award, funded by EPSRC and Vodafone and administered by Royal Holloway, University of London.

We are grateful to Nigel Smart for initiating a discussion concerning the anonymity properties of the Sakai-Kasahara IBE scheme and to the anonymous referees for many valuable comments and references.

References

1. Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T., Malone-Lee, J., Neven, G., Paillier, P., Shi, H.: Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 205–222. Springer, Heidelberg (2005)
2. Abdalla, M., Bellare, M., Namprempre, C., Neven, G.: Robust public-key and identity-based encryption (unpublished manuscript, 2008)
3. Barbosa, M., Farshim, P.: Efficient identity-based key encapsulation to multiple parties. In: Smart, N. (ed.) Cryptography and Coding 2005. LNCS, vol. 3796, pp. 428–441. Springer, Heidelberg (2005)
4. Bellare, M., Boldyreva, A., Desai, A., Pointcheval, D.: Key-privacy in public-key encryption. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 566–582. Springer, Heidelberg (2001)
5. Bellare, M., Rogaway, P.: Random oracles are practical: A paradigm for designing efficient protocols. In: ACM Conference on Computer and Communications Security, pp. 62–73 (1993)

6. Boneh, D., Franklin, M.K.: Identity-based encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
7. Boyen, X.: The $\mathtt{BB}_1$ identity-based cryptosystem: A standard for encryption and key encapsulation. IEEE P1363.3 (submission, 2006), http://grouper.ieee.org/groups/1363/IBC/submissions/Boyen-bb1_ieee.pdf
8. Boyen, X., Waters, B.: Anonymous hierarchical identity-based encryption (without random oracles). In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 290–307. Springer, Heidelberg (2006)
9. Bradshaw, R.W., Holt, J.E., Seamons, K.E.: Concealing complex policies with hidden credentials. In: Atluri, V., Pfitzmann, B., McDaniel, P.D. (eds.) ACM Conference on Computer and Communications Security, pp. 146–157. ACM, New York (2004)
10. Chase, M.: Multi-authority attribute based encryption. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 515–534. Springer, Heidelberg (2007)
11. Chen, L., Cheng, Z., Malone-Lee, J., Smart, N.P.: An efficient ID-KEM based on the Sakai-Kasahara key construction. Cryptology ePrint Archive, Report 2005/224 (2005), http://eprint.iacr.org/
12. Cocks, C.: An identity based encryption scheme based on quadratic residues. In: Honary, B. (ed.) Cryptography and Coding 2001. LNCS, vol. 2260, pp. 360–363. Springer, Heidelberg (2001)
13. Fujisaki, E., Okamoto, T.: How to enhance the security of public-key encryption at minimum cost. In: Imai, H., Zheng, Y. (eds.) PKC 1999. LNCS, vol. 1560, pp. 53–68. Springer, Heidelberg (1999)
14. Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 537–554. Springer, Heidelberg (1999)
15. Galbraith, S.D., Paterson, K.G., Smart, N.P.: Pairings for cryptographers. Cryptology ePrint Archive, Report 2006/165 (2006), http://eprint.iacr.org/
16. Gentry, C.: Practical identity-based encryption without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445–464. Springer, Heidelberg (2006)
17. Halevi, S.: A sufficient condition for key-privacy. Cryptology ePrint Archive, Report 2005/005 (2005), http://eprint.iacr.org/
18. Holt, J.E.: Key privacy for identity based encryption. Cryptology ePrint Archive, Report 2006/120 (2006), http://eprint.iacr.org/
19. Holt, J.E., Bradshaw, R.W., Seamons, K.E., Orman, H.K.: Hidden credentials. In: Jajodia, S., Samarati, P., Syverson, P.F. (eds.) WPES, pp. 1–8. ACM, New York (2003)
20. Kitagawa, T., Yang, P., Hanaoka, G., Zhang, R., Watanabe, H., Matsuura, K., Imai, H.: Generic transforms to acquire CCA-security for identity based encryption: The cases of FOpkc and REACT. In: Batten, L.M., Safavi-Naini, R. (eds.) ACISP 2006. LNCS, vol. 4058, pp. 348–359. Springer, Heidelberg (2006)
21. Sakai, R., Kasahara, M.: ID based cryptosystems with pairing on elliptic curve. Cryptology ePrint Archive, Report 2003/054 (2003), http://eprint.iacr.org/
22. Sakai, R., Ohgishi, K., Kasahara, M.: Cryptosystems based on pairing. In: The 2000 Sympoium on Cryptography and Information Security, Okinawa, Japan, January, pp. 26–28 (2000)
23. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)

24. Wang, S., Cao, Z.: Practical identity-based encryption (IBE) in multiple PKG environments and its applications. Cryptology ePrint Archive, Report 2007/100 (2007), http://eprint.iacr.org/
25. Yang, P., Kitagawa, T., Hanaoka, G., Zhang, R., Matsuura, K., Imai, H.: Applying Fujisaki-Okamoto to identity-based encryption. In: Fossorier, M.P.C., Imai, H., Lin, S., Poli, A. (eds.) AAECC 2006. LNCS, vol. 3857, pp. 183–192. Springer, Heidelberg (2006)