Removing Escrow from Identity-Based Encryption

New Security Notions and Key Management Techniques

Sherman S.M. Chow*

Department of Computer Science
Courant Institute of Mathematical Sciences
New York University, NY 10012, USA
schow@cs.nyu.edu

Abstract. Key escrow is inherent in identity-based encryption (IBE). A curious key generation center (KGC) can simply generate the user's private key to decrypt a ciphertext. However, can a KGC still decrypt if it *does not* know the intended recipient of the ciphertext? We answer by formalizing KGC anonymous ciphertext indistinguishability ($\mathcal{ACI} - \mathcal{KGC}$).

We find that all existing pairing-based IBE schemes without random oracles, whether receipt-anonymous or not, do not achieve KGC one-wayness, a weaker notion of $\mathcal{ACI} - \mathcal{KGC}$. In view of this, we first show how to equip an IBE scheme by Gentry with $\mathcal{ACI} - \mathcal{KGC}$. Second, we propose a new system architecture with an anonymous private key generation protocol such that the KGC can issue a private key to an authenticated user without knowing the list of users identities. This also better matches the practice that authentication should be done with the local registration authorities instead of the KGC. Our proposal can be viewed as mitigating the key escrow problem in a different dimension than distributed KGCs approach.

1 Introduction

The feature that differentiates identity-based encryption (IBE) scheme from other public key encryption schemes lies in the way a public and private key pair is set up – every arbitrary string is a valid public key. There is a trusted authority, called the key generation center (KGC), responsible for the generation of private keys after user authentications. Private key generation applies the KGC's master secret key to the users' identities. The major benefit of this approach is to largely reduce the need for processing and storage of public key certificates under traditional public key infrastructure (PKI).

Nevertheless, the advantages come with a major drawback which is known as the *escrow problem*. The KGC could decrypt any message addressed to a user

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-3-642-00468-1_29

* The author would like to thank Yevgeniy Dodis for the inspiration of this research and many fruitful discussions, Kenneth Paterson for his invaluable assistance and suggestions, and Melissa Chase for her helpful comments.

S. Jarecki and G. Tsudik (Eds.): PKC 2009, LNCS 5443, pp. 256–276, 2009.

by generating that user's private key. To escape from the eye of the KGC, two users may execute an interactive key agreement protocol (e.g. [24]) to establish a session key known only to themselves, or the recipient can setup another key pair and employ certificateless encryption [2,23,25,26], which is a two-factor encryption method involving both IBE and public key encryption. However, one of the main benefits of IBE is lost – it is no longer true that a ciphertext can be prepared without any action by the recipient.

Can anonymity help confidentiality? Current study of IBE only considers anonymity against malicious users' attack, except a recent and independent work [34] which considers the application of KGC-anonymous IBE in password-authenticated key exchange but without any application in the context of IBE itself. We try to use anonymity against a malicious KGC to fight against the escrow problem. If the KGC *does not* know the intended recipient of the ciphertext, is it still possible for it to decrypt on behalf of the user? We answer this question by introducing the notions of KGC one-wayness ($\mathcal{OW} - \mathcal{KGC}$) and KGC anonymous ciphertext indistinguishability ($\mathcal{ACI} - \mathcal{KGC}$).

We find that (to the best of our knowledge) no existing pairing-based IBE schemes without random oracles can achieve the weakest notion of confidentiality $\mathcal{OW} - \mathcal{KGC}$, no matter whether it is user-anonymous. In view of this, we show to equip Gentry's IBE scheme [28] with $\mathcal{ACI} - \mathcal{KGC}$ in the standard model.

How can KGC *not* know the users' identities? Our notion of $\mathcal{ACI} - \mathcal{KGC}$ minimizes the damage of master secret key exposure, providing protection against adversaries who hold the master secret key but not the list of user identities. However, it is natural for the KGC to have this list. By generating all possible user private keys, the KGC can decrypt all ciphertexts. In view of this, we propose a new system architecture to prevent the KGC from knowing it.

We acknowledge that the KGC can always try to derive all possible user private keys according to a certain "dictionary". It seems that there is not much we can do to protect ourselves against a strong adversary like the KGC in this situation. Nevertheless our notion is useful when there is some min-entropy from the identities (e.g. biometric identity [43]). On the other hand, nothing can be gained if one always stores the identity with the ciphertext.[1]

New Key Management Techniques. We separate the tasks of authentication and key issuing, hence our system architecture employs two parties, namely, an identity-certifying authority (or ICA in short) and a KGC. This setting is different from a typical ID-based cryptosystem, but actually better matches the practice that authentication should be done with the local registration authorities, especially when the KGC is not globally available to authenticate users.

The master secret is still solely owned by the KGC. In particular, it is not spilt across two authorities, in contrast with the distributed KGCs approach. The ICA is responsible for issuing some kind of certificates, but it does not need to store any of them, and only the KGC is required to verify the certificate.

[1] Don't write your address on a tag with your key to guide the thief who picked it up.

After obtaining the private key, users do not require any further interaction with these authorities for decryption. Last but not least, the certificate is not used anywhere else in the system, i.e. the encryption itself is still purely ID-based.

Under this model, we show that one can put anonymous ciphertext indistinguishability in practice. We give a design of the anonymous private key issuing protocol, and present a concrete protocol construction for Gentry-IBE.

1.1 Review of Identity-Based Encryption

The concept of IBE was formulated by Shamir in 1984 [47]. Satisfactory proposals for IBE did not exist until nearly two decades afterward, when Boneh and Franklin [12] and Sakai *et al.* [45] presented two IBE solutions based on pairing and full-domain hash to elliptic curve points (referred to as FDH-IBE).

Reduction Improvement. Since Boneh-Franklin's work (BF-IBE), there has been a flurry of variants. For improving the security reduction in the random oracle model, Attrapadung *et al.* [3] worked out an FDH-IBE having two public keys for an identity, an idea which was used to improve the security reduction of FDH signature. Galindo [27] gave a variant of BF-IBE using another transformation technique (different from the one in [12]) to get adaptive chosen-ciphertext security (CCA2). Modifying BF-IBE, Libert and Quisquater [39] gave an IBE without redundancy [42]. All these schemes share a similar $\mathcal{ACI} - \mathcal{KGC}$ analysis.

Multi-Recipient and Hierarchical ID-Based Encryption (HIBE). In HIBE, the workload of private key generation of a single root KGC is delegated to many lower-level KGCs. Gentry and Silverberg proposed the first full-blown (compared with [33]) HIBE (GS-HIBE) [29]. For encrypting to multiple recipients more efficiently than in the straightforward approach, multi-recipient IBE was proposed by Baek *et al.* (BSS-MIBE) [4]. An extension of [4] with shorter ciphertext was proposed in [39]. These schemes bear similarities to GS-HIBE.

Exponent-Inversion IBE. Sakai and Kasahara [44] proposed another IBE (SK-IBE) with a private key derivation algorithm based on exponent-inversion, which is different from FDH-IBE. The CCA2-security of SK-IBE is proven in another work [22], albeit in the random oracle model.

The first exponent-inversion IBE in the standard model was proposed by Boneh and Boyen [8] (hereinafter referred to as BB-EIIBE), which offers selective-ID security. Using the chameleon hashing technique due to Waters [49], an extension of [8] with adaptive-ID security was proposed in [36]. Since only the way of hashing the identity is changed, they share the same $\mathcal{ACI} - \mathcal{KGC}$ analysis.

Standard Model (Commutative-Blinding). Boneh and Boyen proposed selective-ID IBE and HIBE schemes in [8] (hereinafter referred to as BB-(H)IBE). Shortly afterward, they gave an adaptive-ID version [9]. Waters simplified [9] in [49], and gave a fuzzy version with Sahai in [43]. Extending from [49], Kiltz and Galindo [37] gave a CCA2 ID-based key encapsulation without using any transformation, and Kiltz and Vahlis [38] gave an efficient CCA2 ID-based

key encapsulation scheme using authenticated symmetric encryption. Extending from [43], Boldyreva *et al.* [7] gave an IBE with efficient revocation.

Regarding HIBE, [9] and [49] suggested HIBE extensions similar to the approach in [8]. An HIBE with constant-size ciphertext was proposed in [10], which was later made adaptive-ID secure in [20]. Generalizations of the selective-ID model for HIBE, with two HIBE constructions, were proposed in [17]. HIBE with short public parameters was proposed in [18]. A multi-recipient IBE and a parallel key-insulated IBE in standard model were proposed in [19] and [50].

Despite their apparent versatility (e.g. different ways of generating public keys from identities), all these schemes use a similar implicit key encapsulation method. As a result, they share a similar $\mathcal{ACI} - \mathcal{KGC}$ analysis. Finally, [21,41] studied the tradeoff between key size and security reduction for [49].

Standard Model (with User Anonymity). Boyen and Waters [15] proposed an anonymous IBE scheme (BW-IBE) and the first anonymous HIBE (AHIBE). It has been suggested in [15] that AHIBE can obtain adaptive security by the hashing technique of Waters [49]. Similar to the extension of [8] in [36], it does not affect the $\mathcal{ACI} - \mathcal{KGC}$ analysis. Recently, [10] has been made anonymous in [46]. Although these schemes are anonymous, they can be shown to be not $\mathcal{OW} - \mathcal{KGC}$-secure in a similar way to BB-(H)IBE.

Gentry's scheme also provides anonymity in the standard model [28]. It has been extended by Kiltz and Vahlis using authenticated symmetric encryption for better efficiency (KV-IBE) [38], and by Libert and Vergnaud for more efficient weak black-box accountable IBE (LV-IBE) [40]. We will show that Gentry-IBE can be made $\mathcal{ACI} - \mathcal{KGC}$ secure, but interestingly, its extensions [38,40] are not. Actually, LV-IBE mixes commutative-blinding and exponent-inversion – its $\mathcal{OW} - \mathcal{KGC}$ can be broken similar to breaking BB-EIIBE or BB-(H)IBE.

Generalizations of IBE. Recently, there have been many generalizations of IBE, such as hidden-vector encryption [14], predicate encryption [35] and spatial encryption [13]. However, it can be shown that they are not $\mathcal{OW} - \mathcal{KGC}$-secure.

1.2 Attempts in Reducing Trust in the KGC

Accountable IBE. In accountable IBE [30] (AIBE), the trust in the KGC is reduced in another dimension, such that the KGC is discouraged from leaking or selling any user secret key. Consider an IBE scheme with an exponential number of user secret keys for any given identity, such that deriving any other secret key from any one of them (without the knowledge of the master secret key) is intractable; if the key issuing protocol ensures that the user can obtain a user private key without letting the KGC know which one it is, we can conclude that the KGC must be the one who leaks the user private key if a user can show the existence of two private keys for the same identity. Goyal [30] showed that Gentry-IBE satisfies the aforementioned properties, and proposed the corresponding key issuing protocol, which also works with our modified Gentry-IBE. Another AIBE scheme that is based on Waters IBE [49] and Sahai-Waters fuzzy

IBE [43] was also proposed in [30]. Goyal *et al.* [31] later proposed a black-box accountable IBE (BBAIBE). However, these schemes are not $\mathcal{OW} - \mathcal{KGC}$-secure.

KGC-Anonymous ID-based KEM. Independent of our work, anonymity against an honest but curious KGC attack was considered by Izabachène and Pointcheval [34]. Their notion of key anonymity with respective to authority (KwrtA), given in the context of identity-based KEM (IB-KEM), requires the adversary to guess between the two possibilities of recipient identity, with the master secret key and the challenge ciphertext, but *without* the ephemeral session key. In the context of IBE, the ciphertext always contain a component which encrypts the message by this session key. Taking it away means that the challenge is "incomplete" since partial knowledge of it can be seen in the ciphertext produced by IBE. Hence, the real-world impact on IBE given by their security notion may be unclear. Nevertheless, they showed that an IB-KEM with this KwrtA-anonymity and ID-based non-malleability (another new notion in [34]) is a useful tool for constructing password-authenticated key exchange protocols. Relationships between our notion and theirs will be given in §5.4.

Distributed KGCs. A standard method to avoid the inherent key escrow is to split the master secret key to multiple KGCs. The user private key generation is then done in a threshold manner, where each KGC uses a share of the master secret key to generate a private key component for a user. In our approach, the master secret key is not distributed. It is always possible to have this key distribution on top of our idea if an extra layer of protection is desirable.

2 Definitions

2.1 Notations and Complexity Assumptions

We use $x \in_R S$ to denote the operation of picking an element x at random and uniformly from a finite set S. For a probabilistic algorithm $\mathcal{A}$, $x \xleftarrow{\$} \mathcal{A}$ assigns the output of $\mathcal{A}$ to the variable x. If x is a string, $|x|$ denotes its length. If $\lambda \in \mathbb{N}$, 1^λ denotes a string of λ ones. A function $\epsilon : \mathbb{N} \rightarrow \mathbb{R}$ is negligible ($\mathsf{negl}(k)$) if for every constant $c \geq 0$ there exists k_c such that $\epsilon(k) < k^{-c}$ for all $k > k_c$.

Definition 1 (Bilinear Map). *Let $\mathbb{G}$ and $\mathbb{G}_T$ be two (multiplicative) cyclic groups of prime order p. A bilinear map $e(\cdot, \cdot) : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ satisfies:*

1. *Bilinearity: For all $u, v \in \mathbb{G}$, $a, b \in \mathbb{Z}$, $e(u^a, v^b) = e(u, v)^{ab}$.*
2. *Non-degeneracy: $e(g, g) \neq 1$ where g is a generator of $\mathbb{G}$.*

Definition 2. *(Decisional) Bilinear Diffie-Hellman Problem (DBDHP): Given $g, g^a, g^b, g^c \in \mathbb{G}$, and $\hat{t} \in \mathbb{G}_T$, output 'yes' if $\hat{t} = e(g, g)^{abc}$ and 'no' otherwise.*

We introduce two problems whose names are inspired by the decisional linear problem [11]. An oracle for solving the first one makes solving DBDHP easily.

Definition 3. *Decisional Bilinear Problem (DBP): Given two* $\mathbb{G}$ *elements* g *and* g^a*, two* $\mathbb{G}_T$ *elements* $e(g,g)^b$ *and* $\hat{t}$*, output '*yes*' if* $\hat{t} = e(g,g)^{ab}$ *and '*no*' otherwise. We name* $(g, g^a, e(g,g)^b, e(g,g)^{ab})$ *as a decisional bilinear tuple.*

Definition 4. *Modified Decisional Bilinear Problem (MDBP): Given* $g, g^a, g^{b^{-1}} \in \mathbb{G}$*, and* $e(g,g)^b, \hat{t} \in \mathbb{G}_T$*, output '*yes*' if* $\hat{t} = e(g,g)^{ab}$ *and '*no*' otherwise.*

Lemma 1. *DBDH assumption implies Decisional Bilinear assumption.*

Proof. Given $(g, g^a, g^b, g^c, \hat{t})$, computes $e(g,g)^{b'} = e(g^b, g^c)$ where $b' = bc$, feeds $(g, g^a, e(g,g)^{b'}, \hat{t})$ to the DBP oracle and outputs its answer. □

Definition 5. *(Decisional)* q*-Bilinear Diffie-Hellman Exponent Problem (*q*-BDHEP): Given* $(q+2)$ $\mathbb{G}$ *elements* $(g', g, g^\alpha, \cdots, g^{\alpha^q})$*, and one* $\mathbb{G}_T$ *element* $\hat{t}$*, output '*yes*' if* $\hat{t} = e(g^{\alpha^{q+1}}, g')$ *and '*no*' otherwise.*

A stronger version of q-BDHEP is assumed difficult for the security of Gentry-IBE. We remark that the hard problem considered in [28] is augmented with $g'^{\alpha^{q+2}}$ and q equals to the number of users compromised by the adversary.

Lemma 2. *Decisional 2-Bilinear Diffie-Hellman Exponent assumption implies Modified Decisional Bilinear assumption.*

Proof. Given $(g', g, g^\alpha, g^{\alpha^2}, \hat{t})$, set $\theta_1 = g^\alpha$, $\theta_2 = g'$, $\theta_3 = g$, $\hat{\theta} = e(g^\alpha, g^{\alpha^2})$ and feed $(\theta_1, \theta_2, \theta_3, \hat{\theta}, \hat{t})$ to the MDBP oracle. The input is valid since $\theta_3 = (\theta_1)^{\alpha^{-1}}$ and $\hat{\theta} = e(\theta_1, \theta_1)^\alpha$. Let $\theta_2 = \theta_1^\gamma$ where $\gamma \in \mathbb{Z}_p$, the MDBP oracle outputs 'yes' if and only if $\hat{t} = e(\theta_1, \theta_1)^{\gamma\alpha}$, since $e(\theta_1, \theta_1)^{\gamma\alpha} = e(g^\alpha, g^\alpha)^{\gamma\alpha} = e(g^{\alpha^3}, g')$. □

2.2 Identity Based Encryption

Under the standard definition, an IBE scheme consists of four algorithms:

1. via $(mpk, msk) \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$ the randomized key generation algorithm outputs the system parameters mpk and the master secret key msk;
2. via $usk[\mathsf{ID}] \xleftarrow{\$} \mathsf{KeyDer}(msk, \mathsf{ID})$ the KGC outputs[2] a secret key for user ID;
3. via $\mathfrak{C} \xleftarrow{\$} \mathsf{Enc}(mpk, \mathsf{ID}, m)$ anyone can encrypt a message m to user ID in $\mathfrak{C}$;
4. via $m \leftarrow \mathsf{Dec}(mpk, usk[\mathsf{ID}], \mathfrak{C})$ user ID uses secret key usk to get m from $\mathfrak{C}$.

Consistency requires that for all $\lambda \in \mathbb{N}$, all identities ID, all messages $m \in \mathsf{MsgSp}$ (defined by mpk) and all $\mathfrak{C} \xleftarrow{\$} \mathsf{Enc}(mpk, \mathsf{ID}, m)$, $\Pr[\mathsf{Dec}(\mathsf{KeyDer}(msk, \mathsf{ID}), \mathfrak{C}) = m] = 1$, where the probability is taken over the coins of all the above algorithms.

In our definition, we separate the master key generation from the Setup.

Definition 6. *An IBE scheme consists of the following five PPT algorithms:*

[2] This algorithm is deterministic for most schemes stemmed from FDH-IBE.

1. *via* $param \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$ *the setup algorithm outputs the system parameters* $param$ *for security parameter* $\lambda \in \mathbb{N}$*, with message space* $\mathsf{MsgSp}(\lambda)$ *included.*
2. *via* $(mpk, msk) \xleftarrow{\$} \mathsf{MKeyGen}(param)$ *the key generation algorithm outputs the master public/secret key* (mpk, msk) *conforming to* $param$*;*
3. KeyDer*,* Enc *and* Dec *are defined as in the standard definition.*

We can view Setup as a trusted initializer for choosing the system parameters (for examples, the choice of elliptic cure) which are implicitly included in the input of KeyDer, Enc and Dec. The KGC generates a master public/private key pair only via $\mathsf{MKeyGen}$. We assume it is efficient to check if a message m is in $\mathsf{MsgSp}(\lambda)$ or if mpk comes from a group that matches with what is specified in $param$. We denote the latter check by (an abused notation) $mpk \in param$.

3 Anonymity and Indistinguishability against the KGC

3.1 Anonymity against User Attack

User-anonymity is defined by the game below [1]. The adversarial goal is to distinguish the intended recipient of a ciphertext between two chosen identities[3].

Experiment $\mathbf{Exp}^{\mathrm{ano-cpa}}_{\mathcal{IBE},\mathcal{A}}(\lambda)$
$\mathsf{IDset} \leftarrow \emptyset$; $(param) \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$; $(mpk, msk) \xleftarrow{\$} \mathsf{MKeyGen}(param)$;
$(\mathsf{ID}_0, \mathsf{ID}_1, m^*, st) \xleftarrow{\$} \mathcal{A}^{\textsc{KeyDerO}(\cdot)}(\text{`find'}, param, mpk)$;
If $m^* \notin \mathsf{MsgSp}(\lambda)$ then return 0;
$b \xleftarrow{\$} \{0,1\}$; $\mathfrak{C} \xleftarrow{\$} \mathsf{Enc}(mpk, \mathsf{ID}_b, m^*)$; $b' \xleftarrow{\$} \mathcal{A}^{\textsc{KeyDerO}(\cdot)}(\text{`guess'}, \mathfrak{C}, st)$;
If $b \neq b'$ or $(\{\mathsf{ID}_0, \mathsf{ID}_1\} \cap \mathsf{IDset} \neq \emptyset)$ then return 0 else return 1;

where the private key derivation oracle $\textsc{KeyDerO}(\mathsf{ID})$ is defined as:

$$\mathsf{IDset} \leftarrow \mathsf{IDset} \cup \{\mathsf{ID}\}; usk[\mathsf{ID}] \leftarrow \mathsf{KeyDer}(msk, \mathsf{ID});\ \text{return } usk[\mathsf{ID}]$$

and st denotes the state information maintained by the adversary $\mathcal{A}$.

3.2 Anonymous Ciphertext Indistinguishability

We use the term "anonymous ciphertext" to refer a ciphertext that the KGC holds without the knowledge of who is the intended recipient. We do not model the case where the KGC maliciously generates the system parameters (e.g. the choice of elliptic curve), but we provide a new "embedded-identity encryption" oracle, which lets the adversary adaptively get many ciphertexts designated to the same person, without knowing the real identity. The absence of such an oracle gives the adversary no way to see more than one ciphertext for the unknown recipient. For the ease of discussion, we suppose an identity is of n-bit length.

[3] IBE's ciphertext does not mean to reveal the recipient's identity. We omit anonymity revocation oracle which is present in some cryptographic schemes (e.g. [11]).

Definition 7. *An IBE scheme is* (t, q_E, ϵ) $\mathcal{ACI} - \mathcal{KGC}$ *secure if all* t*-time adversaries making at most* q_E *embedded-identity encryption oracle queries have advantage at most* ϵ *in winning the game below (i.e. the experiment returns* 1*).*

Experiment $\mathbf{Exp}^{\text{aci-kgc}}_{\mathcal{IBE},\mathcal{A}}(\lambda)$
$(param) \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$; $\mathsf{ID}^* \xleftarrow{\$} \{0,1\}^n$;
$(mpk, st) \xleftarrow{\$} \mathcal{A}(\text{'gen'}, param)$; If $mpk \notin param$ then return 0;
$(m_0^*, m_1^*, st) \xleftarrow{\$} \mathcal{A}^{\text{ENCO}_{(mpk,\mathsf{ID}^*)}(\cdot)}(\text{'find'}, mpk, st)$;
If $\{m_0^*, m_1^*\} \nsubseteq \mathsf{MsgSp}(\lambda)$ or $|m_0^*| \neq |m_1^*|$ then return 0;
$b \xleftarrow{\$} \{0,1\}$; $\mathfrak{C} \xleftarrow{\$} \mathsf{Enc}(mpk, \mathsf{ID}^*, m_b^*)$; $b' \xleftarrow{\$} \mathcal{A}^{\text{ENCO}_{(mpk,\mathsf{ID}^*)}(\cdot)}(\text{'guess'}, \mathfrak{C}, st)$;
If $b \neq b'$ then return 0 else return 1;

where the embedded-identity oracle $\text{ENCO}_{(mpk,\mathsf{ID}^*)}(m)$ returns $\mathsf{Enc}(mpk, \mathsf{ID}^*, m)$ and the advantage of $\mathcal{A}$ is defined as $|\Pr[\mathbf{Exp}^{\text{aci-kgc}}_{\mathcal{IBE},\mathcal{A}}(\lambda) = 1] - \frac{1}{2}|$.

One may define semantic security of the hidden identity in a similar way; but we omitted it to keep our focus on whether the KGC can decrypt the ciphertext.

Embedded-Identity Decryption. The above game just considers chosen-plaintext attack (CPA). One may consider giving the adversary adaptive access to a decryption oracle, or even an "embedded-identity decryption oracle". We consider this stronger notion from both the theory and practice perspectives.

Our security notion is actually quite strong in the sense that the adversary is not required to reveal the master secret key to the challenger. We start our discussion with a weakened definition such that the adversary is instead required to do so. While it is possible that the decryption oracle could help the adversary to deduce information about the challenge ciphertext, this happens when a maliciously formed ciphertext is presented to the decryption oracle. If we are able to put some validity tag in the ciphertext such that the challenger, with the master secret key, can do a sanity check before the actual decryption; only "invalid" will be returned for any malformed ciphertext or those not encrypted for the challenge identity, i.e. CCA2-security against user also helps in here.

If the challenger does not know the master secret, it may sound impossible to simulate the decryption oracle. Nevertheless, our definition assumes trusted parameter generation, which possibly allows us to solve the problem with approaches similar to simulating the strong decryption oracle in certificateless encryption [2,23,25,26], such as a knowledge-extractor with the help of the random oracle, or a non-interactive zero-knowledge proof system setup according to the trusted parameters. Due to the lack of space, we do not delve into details.

In practice, while it makes sense to trick a user into encrypting some predefined messages (as modeled by the embedded-identity encryption oracle); it may not make much sense to consider the case that the KGC gained accesses to an embedded-identity decryption oracle – which possibly means the KGC has identified this user already. Due to these complications, we keep our focus on the CPA notion. Nevertheless, this does not preclude the possibility of achieving $\mathcal{ACI} - \mathcal{KGC}$-security and CCA2-security against user attack simultaneously.

3.3 Comparison of User Anonymity and KGC One-Wayness

A KGC is a powerful adversary. We consider KGC one-wayness ($\mathcal{OW} - \mathcal{KGC}$), a notion strictly weaker than $\mathcal{ACI} - \mathcal{KGC}$, to better reflect the security of IBE against KGC attacks. We also present two separation results.

Definition 8. *An IBE is* $\mathcal{OW} - \mathcal{KGC}$ *secure if* $\Pr[\mathbf{Exp}^{\mathrm{ow-kgc}}_{\mathcal{IBE},\mathcal{A}}(\lambda)=1] < \mathsf{negl}(\lambda)$.

Experiment $\mathbf{Exp}^{\mathrm{ow-kgc}}_{\mathcal{IBE},\mathcal{A}}(\lambda)$
$(param) \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$, $\mathsf{ID}^* \xleftarrow{\$} \{0,1\}^n$;
$(mpk, st) \xleftarrow{\$} \mathcal{A}(\text{`}\mathsf{gen}\text{'}, param)$; If $mpk \notin param$ then return 0;
$m^* \xleftarrow{\$} \mathsf{MsgSp}(\lambda)$; $\mathfrak{C} \xleftarrow{\$} \mathsf{Enc}(mpk, \mathsf{ID}^*, m^*)$; $m' \xleftarrow{\$} \mathcal{A}(\text{`}\mathsf{guess}\text{'}, \mathfrak{C}, st)$;
If $m^* \neq m'$ then return 0 else return 1;

Theorem 1. *User anonymity does not imply* $\mathcal{OW} - \mathcal{KGC}$.

Proof. Given any user-anonymous IBE scheme with encryption algorithm Enc, define a new IBE with encryption algorithm $\mathsf{Enc}'(mpk, \mathsf{ID}, m) = (\mathsf{Enc}(mpk, \mathsf{ID}, m), \mathsf{Enc}(mpk, \text{“0”}, \mathsf{ID}))$, where “0” is a dummy identity and the corresponding user secret key is never released by the KGC. If the IBE scheme is semantically secure, the ciphertext produced by Enc' is still user-anonymous. But it is not $\mathcal{OW} - \mathcal{KGC}$ since the KGC can just generate the user secret key for “0”, decrypt the second component of the ciphertext and then decrypt the first component.

Theorem 2. $\mathcal{ACI} - \mathcal{KGC}$ *does not imply user anonymity.*

Proof. Given any $\mathcal{ACI} - \mathcal{KGC}$ with encryption algorithm Enc, define a new IBE with encryption algorithm which appends the first bit of identity to the ciphertext. Any adversary can just choose two identities which differ at the first bit to break the user-anonymity. On the other hand, the notion of $\mathcal{ACI} - \mathcal{KGC}$ depends on the number of random bits in the identity; essentially only one bit of security is lost and $\mathcal{ACI} - \mathcal{KGC}$ is still preserved.

In next section, we will see they are also orthogonal to each other in practice.

4 Analysis

Table 1 gives a concise and unified review of existing IBE schemes in the context of $\mathcal{ACI} - \mathcal{KGC}$ analysis. Seven (H)IBE schemes representing a large class of IBE schemes in the literature are selected. Note that we made many simplifications and omitted many elegant components of the IBE schemes being analyzed. We do not intend to give a complete review of the constructions of all these schemes (it seems we are reducing these IBE schemes to ID-based key encapsulations or even just public key encryption schemes), but we want to keep our focus on how a KGC can decrypt the message using the master secret key. Thus, we only show the essential components in the master public key mpk, the master secret key msk, the ciphertext, and the variable that can be computed (without using any

Table 1. Concise Review of IBE Schemes for $\mathcal{ACI}-\mathcal{KGC}$ Analysis. Elements in $\mathbb{G}, \mathbb{Z}_p, \mathbb{G}_T$: capital letters, small letters, small letters with hat respectively. Generators of $\mathbb{G}$ and $\mathbb{G}_T$: P and $\hat{g} = e(P,P)$ resp. Ephemeral randomness employed in encryption: r, r'. $Q_{\mathsf{ID}} = H_0(\mathsf{ID})$, where $H_0(\cdot) : \{0,1\}^n \to \mathbb{G}$. Hierarchical identity: $(\mathsf{ID}_1, \mathsf{ID}_2, \cdots)$.

Schemes	mpk	msk	Ciphertext	$\mathcal{K}$
FDH-IBE [12,45]	P^s	s	P^r	$e({Q_{\mathsf{ID}}}^r, P^s)$
GS-HIBE [29]	P^s	s	$P^r, Q_{\mathsf{ID}_2}^r, \cdots$	$e({Q_{\mathsf{ID}_1}}^r, P^s)$
BSS-MIBE [4]	P^s, Q	s	P^r	$e(Q, P^s)^r$
BB-EIIBE [8]	$\hat{g}, V = P^s$	s	V^r	$\hat{g}^r$
BB-(H)IBE [8]	$e(P,S)$	S	P^r	$e(P,S)^r$
BW-IBE [15]	$\hat{v} = \hat{g}^{s_1 s_2 s_3}, V_1 = P^{s_1}, V_2 = P^{s_2}$	s_1, s_2, s_3	$V_1^{r-r'}, V_2^{r'}$	$\hat{v}^r$
KV-IBE [38]	$\hat{g}, \hat{v}_1 = \hat{g}^{s_1}, \hat{v}_2 = \hat{g}^{s_2}$	s_1, s_2	$\hat{g}^r, t$	$(\hat{v}_1^t \hat{v}_2)^r$

secret key) from the ciphertext (t in KV-IBE), which are sufficient for the KGC to do the decryption. We use $\mathcal{K}$ to denote the random session key created by the implicit KEM, which is a crucial piece of data to decrypt the ciphertext.

4.1 Schemes That Are Not $\mathcal{OW}-\mathcal{KGC}$-Secure

The session key $\mathcal{K}$ in BSS-MIBE can be computed by $e(Q, P^r)^s$. For BB-EIIBE, $\mathcal{K}$ can be computed by $e(P, V^r)^{1/s}$. For BB-(H)IBE, $e(P^r, S) = \mathcal{K}$. For BW-IBE, it can be computed by $e((V_2^{r'})^{1/s_2}(V_1^{r-r'})^{1/s_1}, P)^{s_1 s_2 s_3} = e(P^{r'} P^{r-r'}, P^{s_1 s_2 s_3}) = \hat{v}^r$. For KV-IBE, $(\hat{g}^r)^{s_1 t + s_2} = \mathcal{K}$. Hence, they are not $\mathcal{OW}-\mathcal{KGC}$-secure. BBAIBE [31] is not exactly covered by the above analysis, however, it can be easily shown that it is not $\mathcal{OW}-\mathcal{KGC}$-secure. Note that all of the above computations use the master secret key as-is, instead of exploiting the knowledge of any discrete logarithm between some group elements in the system parameters.

4.2 Schemes That Are $\mathcal{ACI}-\mathcal{KGC}$-Secure

We consider FDH-IBE [12,45] – when $\mathcal{K} = e({Q_{\mathsf{ID}}}^r, P^s)$ is used to encrypt the message $m \in \mathbb{G}_T$ by $m\mathcal{K}$, this gives a CPA-secure IBE scheme. To prove its $\mathcal{ACI}-\mathcal{KGC}$-security, we assume the parameters for the hash functions are setup by an honest party, which means the random oracles are not controlled by the adversary in the security proof.

Theorem 3. *If DBP is hard, FDH-IBE is $\mathcal{ACI}-\mathcal{KGC}$ secure.*

Due to the lack of space, we give an informal argument to get some intuition on why is it so. Given any pair of messages (m_0^*, m_1^*) and an encryption of one of them, there is always a pair of identities $(\mathsf{ID}_0, \mathsf{ID}_1)$ such that the decryption of the ciphertext using session key $e({Q_{\mathsf{ID}_0}}^r, P^s)$ gives m_0^* and decryption using $e({Q_{\mathsf{ID}_1}}^r, P^s)$ gives m_1^*. If the challenge identity is chosen from a uniform distribution with high entropy, any adversary simply has no clue to distinguish, and hence the scheme is $\mathcal{ACI}-\mathcal{KGC}$-secure. Note that the above argument remains valid even if the adversary can compute r from P^r.

For the CCA2-secure BF-IBE [12], we can prove it is $\mathcal{ACI}-\mathcal{KGC}$ secure by considering the computational bilinear problem (CBP), the computational variant of DBP (i.e., to compute $e(g,g)^{ab}$ instead of distinguishing it from random). The simulation is similar to that in Theorem 3, but $e(g,g)^{ab}$ will be "trapped" by the random oracle if the adversary has non-negligible in winning the game.

Lemma 3. *If CBP is hard, BF-IBE is $\mathcal{ACI}-\mathcal{KGC}$ secure.*

Thus, we can still enjoy the usual CCA2-security against the user (outsider adversary) with the extra $\mathcal{ACI}-\mathcal{KGC}$ protection. A similar argument applies to Gentry-Silverberg HIBE and Yao *et al.*'s HIBE [51]. Extra elements in the challenge ciphertext only contain more information about r and the identities at the lower level, which cannot help the adversary to determine the first-level identity or distinguish the ciphertext. They can also be easily simulated by manipulating the random oracle. This gives an interesting result that even when the ciphertext is not "strictly" user-anonymous, it is still possible to get $\mathcal{ACI}-\mathcal{KGC}$-security.

5 "Escrow-Free" IBE in the Standard Model

BF-IBE is $\mathcal{ACI}-\mathcal{KGC}$-secure but its CCA2-security is only proven in the random oracle model. Below we review Gentry-IBE [28], an IBE with CCA2-security proven in the standard model, under the original four-algorithm IBE framework.

Setup: The KGC selects g, h_1, h_2, h_3 randomly from $\mathbb{G}$, randomly chooses an exponent $\alpha \in_R \mathbb{Z}_p$, sets $g_1 = g^\alpha \in \mathbb{G}$, and chooses a hash function $H : \{0,1\}^n \rightarrow \mathbb{Z}_p$ from a family of universal one-way hash functions. The public parameters and the master secret key are given by $mpk = (g, g_1, h_1, h_2, h_3, H)$, $msk = \alpha$.

KeyDer: To generate a private key for identity $\mathsf{ID} \in \mathbb{Z}_p$, the KGC picks $\tau_{\mathsf{ID},i} \in_R \mathbb{Z}_p$ and computes $h_{\mathsf{ID},i} = \left(h_i g^{-\tau_{\mathsf{ID},i}}\right)^{\frac{1}{\alpha-\mathsf{ID}}}$ for $i \in \{1,2,3\}$, outputs $\{\tau_{\mathsf{ID},i}, h_{\mathsf{ID},i}\}_{i\in\{1,2,3\}}$. The KGC must always use the same random value $\tau_{\mathsf{ID},i}$ for ID. This can be accomplished by using a pseudorandom function (PRF) or an internal log [28].

Enc: To encrypt $m \in \mathbb{G}_T$ for identity $\mathsf{ID} \in \mathbb{Z}_p$, the sender picks $r \in_R \mathbb{Z}_p$, computes $\mathfrak{C} = (u, v, w, y) = \Big((g_1 g^{-\mathsf{ID}})^r,\ e(g,g)^r,\ m/e(g,h_1)^r,\ e(g,h_2)^r e(g,h_3)^{r\cdot H(u,v,w)} \Big)$.

Dec: To decrypt the ciphertext $\mathfrak{C}$ with a private key $\{\tau_{\mathsf{ID},i}, h_{\mathsf{ID},i}\}_{i\in\{1,2,3\}}$, first check $\mathfrak{C}$'s validity by testing if $y = e(u, h_{\mathsf{ID},2} h_{\mathsf{ID},3}{}^{\beta}) v^{\tau_{\mathsf{ID},2}+\tau_{\mathsf{ID},3}\beta}$ where $\beta = H(u, v, w)$. In case of inequality, $\perp$ is outputted. Otherwise, return $m = w \cdot e(u, h_{\mathsf{ID},1}) v^{\tau_{\mathsf{ID},1}}$.

5.1 Modification

To get $\mathcal{ACI}-\mathcal{KGC}$, instead of letting the KGC to select g, h_1, h_2, h_3 randomly from $\mathbb{G}$, we require that the discrete logarithm of one with respect to another be unknown to the KGC, or $\mathcal{OW}-\mathcal{KGC}$ can be easily broken. This requirement was not stated in [28]. In practice, this can be achieved by using a common

public seed to generate these parameters with a cryptographic hash function. Specifically, we separate the master key generation from the Setup as follows.

Setup: The trusted initializer chooses the group $\mathbb{G}$ according to the security parameter, and selects g, h_1, h_2, h_3 randomly from $\mathbb{G}$. It also chooses a hash function $H : \{0,1\}^n \to \mathbb{Z}_p$ from a family of universal one-way hash functions. The public parameter *param* is given by (g, h_1, h_2, h_3, H).

MKeyGen: The KGC chooses an exponent $\alpha \in_R \mathbb{Z}_p$. It sets $g_1 = g^\alpha \in \mathbb{G}$. The master public/private key pair is given by $(mpk = g_1,\ msk = \alpha)$.

Note that the above change does not affect the original security guarantees of Gentry-IBE against users attack, i.e. CCA2-security and user anonymity.

5.2 Security

With Lemma 2, the below theorem shows that the above IBE is $\mathcal{ACI} - \mathcal{KGC}$ secure without extra number-theoretic assumptions other than what has been assumed in the original proof for indistinguishability against users' attack [28].

Theorem 4. *If MDBP is hard, the above IBE is $\mathcal{ACI} - \mathcal{KGC}$ secure.*

Proof. Let $\mathcal{A}$ be an adversary that breaks $\mathcal{ACI} - \mathcal{KGC}$ of the IBE system described above. We construct an algorithm, $\mathcal{S}$, that solves a MDBP instance $(g, g^r, g^{s^{-1}}, e(g,g)^s, \hat{t})$ as follows.

$\mathcal{S}$ randomly chooses two exponents $\gamma_2, \gamma_3 \in_R \mathbb{Z}_p$ and a hash function $H : \{0,1\}^n \to \mathbb{Z}_p$ from a family of universal one-way hash functions. The system parameter *param* is set as (g, h_1, h_2, h_3, H) where $h_1 = g^r$, $h_2 = g^{\gamma_2}$ and $h_3 = g^{\gamma_3}$. $\mathcal{A}$ then returns $g_1 = g^\alpha \in \mathbb{G}$ as the master public key, $\alpha \in \mathbb{Z}_p$ is not given to $\mathcal{S}$ and $\mathcal{S}$ never uses α in the simulation. $\mathcal{S}$ also picks a random element $c \in_R \mathbb{Z}_p$.

To simulate the embedded-identity encryption oracle with message m_i as input (for $i \in \{1, \cdots, q_E\}$), $\mathcal{S}$ selects a random element $d_i \in_R \mathbb{Z}_p$ and returns

$$(u_i, v_i, w_i, y_i) = \left((g^{s^{-1}})^{cd_i}, e(g,g)^{d_i}, m_i / e(g,h_1)^{d_i}, e(g,g)^{d_i(\gamma_2 + \gamma_3 \cdot H(u_i, v_i, w_i))}\right).$$

Let $\hat{s} = e(g,g)^s$. When $\mathcal{A}$ outputs two equal length messages (m_0^*, m_1^*), $\mathcal{S}$ randomly generates a bit b, the challenge ciphertext is given by $\mathfrak{C} = (u, v, w, y) = \left(g^c, \hat{s}, m_b^* / \hat{t}, \hat{s}^{\gamma_2 + \gamma_3 \cdot \beta}\right)$, where $\beta = H(u, v, w)$. From the structure of the ciphertext, the intended recipient's identity ID^* is implicitly defined by $c = s(\alpha - \mathsf{ID}^*)$.

Since $s^{-1}c = s^{-1}s(\alpha - \mathsf{ID}^*) = \alpha - \mathsf{ID}^*$, the ciphertexts returned by the embedded-identity encryption oracle are valid ciphertexts encrypted for ID^*.

After $\mathcal{A}$ receives $\mathfrak{C}$, it outputs b' with probability ϵ at the end of the guess stage. If $b = b'$, $\mathcal{S}$ outputs 0 (meaning $\hat{t} = e(g,g)^{rs}$); otherwise, it outputs 1.

If $\hat{t} = e(g,g)^{rs}$, (u, v, w, y) is a valid, appropriately-distributed challenge to $\mathcal{A}$. If $\hat{t} \neq e(g,g)^{rs}$, since $\hat{t}$ is uniformly random and independent from $\mathcal{A}$'s view (other than the challenge ciphertext), (u, v, w, y) imparts no information regarding the bit b, so we have the success probability equal to

$$\Pr[\hat{t} = e(g,g)^{rs}] \cdot \Pr[\mathcal{A} \text{ succeeds}] + \Pr[\hat{t} \neq e(g,g)^{rs}] \cdot \Pr[b \neq b']$$
$$= (\frac{1}{2})(\frac{1}{2} + \epsilon) + (\frac{1}{2})(\frac{1}{2}) = \frac{1}{2} + \frac{\epsilon}{2}$$ □

Using a similar argument, SK-IBE [44] can be proven $\mathcal{ACI} - \mathcal{KGC}$-secure.

5.3 $\mathcal{ACI} - \mathcal{KGC}$-Security without User-Anonymity

Now we modify the scheme presented in §5.1 to give a contrived construction in the standard model. The modification just introduces the term g^{ID} to the ciphertext. An immediate consequence is that the modified scheme no longer provides user-anonymity, To revise the $\mathcal{ACI} - \mathcal{KGC}$ proof, the extra term in the challenge ciphertext (and this term appears in all ciphertexts returned by the embedded-identity encryption oracle as well) can be simulated by $g^{\alpha}/(g^{s^{-1}})^{c}$.

5.4 Comparisons with Accountability, Anonymity with Respect to the KGC, and ID-Based Non-malleability

The above scheme can be made to be accountable [30], but other accountable IBE schemes [31,40] are not $\mathcal{ACI} - \mathcal{KGC}$-secure, which shows that accountability is orthogonal to $\mathcal{ACI} - \mathcal{KGC}$-security. For KwrtA-anonymous IBE, [34] showed that BF-IBE [12] is KwrtA but not ID-based non-malleable, a variant of SK-IBE [44] is both KwrtA and ID-based non-malleable, while BB-IBE [8], AHIBE [15] and Gentry-IBE [28] are *not* KwrtA but are ID-based non-malleable. Together with our analysis in §4, it is clear that the notions of KGC-anonymity, ID-based non-malleability and $\mathcal{ACI} - \mathcal{KGC}$-security are independent of each other.

6 Anonymous Private Key Issuing

In anonymous key issuing (AKI), we need to achieve two somewhat contradictory requirements simultaneously. On one hand, the identity of a user should not be leaked, but a user must be authenticated to obtain the corresponding private key. We propose a new system architecture to realize such an AKI protocol, by employing non-colluding identity-certifying authority (ICA) and KGC.

From a high level, the ICA is responsible for issuing each user a certificate on the purported identity after authentication. This certificate is generated using the master certifying key sk_{cert}. The certificate alone would not enable the user to decrypt. The user should contact the KGC who issues a private key based on the certificate presented, but the KGC never gets to know the identity involved in the certificate. The user private key is still generated with the help of the master secret key, that is owned by the KGC and kept secret from the ICA. Figure 1 depicts the certification and the key issuing process. Since the ICA keeps the identities list of the system's users, we make the trust assumption that the ICA does not collude with the KGC (or the KGC can get the identities list easily).

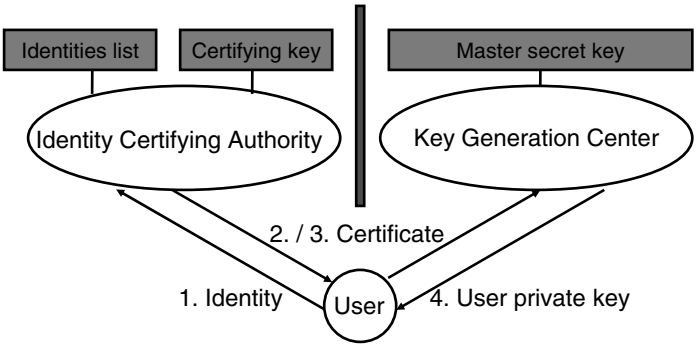

Fig. 1. Our System Architecture

As in PKI, we also assume that the ICA would not impersonate any user. Our solution requires a user to contact two parties before getting a key. Nevertheless, it may be cost-prohibitive to have a globally available KGC to authenticate users and issue keys to users via secure channels in a typical ID-based cryptosystem.

6.1 General Framework

An anonymous key issuing protocol for an IBE scheme consists of four polynomial-time algorithms in additional to the Setup and MKeyGen algorithms from the IBE. For brevity, the public parameter *param* output by Setup is omitted below.

1. via $(pk_{cert}, sk_{cert}) \xleftarrow{\$} \mathsf{IKeyGen}()$ the ICA probabilistically outputs the public/private key pair for certification pk_{cert}, sk_{cert};
2. via $(cert, aux) \xleftarrow{\$} \mathsf{SigCert}(sk_{cert}, \mathsf{ID})$ the ICA probabilistically outputs a certificate for identity ID and some auxiliary information aux;
3. $\mathsf{ObtainKey}(mpk, \mathsf{ID}, cert, aux) \leftrightarrow \mathsf{IssueKey}(sk, cert)$ are two interactive algorithms which execute a user secret key issuing protocol between a user and the KGC. The user takes as input the master public key mpk, an identity ID, and the corresponding certificate $cert$ with auxiliary information aux, and gets a user secret key $usk[\mathsf{ID}]$ as output. The KGC gets the master secret key msk and the certificate $cert$ as input and gets nothing as output.

Here we give a general design framework of such a protocol. We do not claim that any design based on the primitives mentioned here must be secure, but we will analyze the security of our proposed protocol, which is based on the standard argument in anonymous credential literature [5,16].

The first step of our AKI protocol is to get a certificate on an identity from the ICA, which just utilizes a signature scheme. However, the user needs to show this signature to the KGC without leaking the identity (being signed). So the ICA signs on a hiding commitment of the identity instead. This also requires the ability to prove that the contents of a commitment have been signed.

For the KGC side, considering that a user secret key in IBE is essentially a signature on an identity given by the master secret key, obtaining a user secret key without leaking the identity to the KGC boils down to obtaining something similar to a blind signature from the KGC (not to be confused with the signature by the ICA). The blinding step can make a commitment to the identity, the key issuing protocol becomes one for obtaining a signature on a committed value. A crucial difference between our protocol and a blind signature or anonymous credential is manifest at the final stage of our protocol. We require that the user can transform the response from the KGC to a normal signature which directly signs on the value being committed, such that it can be used as the private decryption key of the IBE scheme. In particular, if the final signature just includes a non-interactive proof for proving that the contents of a commitment has been signed, it does not seem to work with any of the existing IBE schemes.

6.2 Security Requirements

One can view $(cert, aux)$ as a signature and $\mathsf{SigCert}$ as the signing algorithm of a signature scheme. For security we require existential unforgeability against adaptive chosen message attack. We omit this standard definition. Our framework assumes $\mathsf{SigCert}$ is used to sign on the (perfectly binding and strongly computationally hiding) commitment of an identity, which is included in *cert*.

Regarding $\mathsf{ObtainKey}$ and $\mathsf{IssueKey}$, we require that malicious users can only get the user private key for the identity "embedded" in the ICA's certificate from the interaction with the KGC, but nothing else. For security protection of the users, we require that the KGC cannot learn anything from the certificate about the real identity of the user. Below is a formalization of the above intuition, which is adopted from some of the security properties of the P-signature [5], a suite of protocols for obtaining signature in a privacy-preserving way.

Definition 9. *An AKI protocol satisfies* issuer privacy *if there exists a simulator* $\mathsf{SimIssue}$ *such that for all PPT adversaries* $(\mathcal{A}_1, \mathcal{A}_2)$*,*

$$
\begin{aligned}
&|\Pr[\, param \xleftarrow{\$} \mathsf{Setup}(1^\lambda); (mpk, msk) \xleftarrow{\$} \mathsf{MKeyGen}(param);\\
&\qquad (\mathsf{ID}, aux, st) \xleftarrow{\$} \mathcal{A}_1(param, mpk, msk); com \leftarrow \mathsf{Commit}(param, \mathsf{ID}, aux);\\
&\qquad b \xleftarrow{\$} \mathcal{A}_2(st) \leftrightarrow \mathsf{IssueKey}(param, msk, com) : b = 1]\\
&- \Pr[\, param \xleftarrow{\$} \mathsf{Setup}(1^\lambda); (mpk, msk) \xleftarrow{\$} \mathsf{MKeyGen}(param);\\
&\qquad (\mathsf{ID}, aux, st) \xleftarrow{\$} \mathcal{A}_1(param, mpk, msk); com \leftarrow \mathsf{Commit}(param, \mathsf{ID}, aux);\\
&\qquad b \xleftarrow{\$} \mathcal{A}_2(st) \leftrightarrow \mathsf{SimIssue}(param, \mathsf{KeyDer}(msk, \mathsf{ID}), com) : b = 1]| < \mathsf{negl}(\lambda).
\end{aligned}
$$

Intuitively, this captures the requirement that the protocol itself reveals no information to the adversary (in particular, msk) other than a user secret key.

In our definition, both $\mathsf{SimIssue}$ and $\mathsf{IssueKey}$ get an honestly generated commitment, for adversarially chosen identity ID and opening aux. Since we assume the commitment is perfectly binding, this automatically guarantees that the

identity associated with the commitment is well defined, and only a user secret key corresponding to that particular identity is obtained by the adversary.

For a cleaner definition, SigCert is not involved. Whether SimIssue and IssueKey receives a signature on a commitment of ID or ID itself is just about how their interfaces take ID as the input. We allow SimIssue to rewind the adversary and it can extract the hidden ID from the commitment.

The above definition assumes the adversary knows msk even its purpose is for the protection of the secrecy of msk. This is adopted from the security definition of secure two-party computation protocols, which models the situation that even the adversary is given some partial information of msk (e.g. through our IBE scheme), it is still unable to distinguish whether it is interacting with a simulator or the real key issuing protocol. Together with the security of the underlying IBE scheme (e.g. CCA2 with access to a user secret key oracle), our definition guarantees that the AKI protocol can be used with the IBE scheme.

Definition 10. *An AKI protocol satisfies* user privacy *if there exists a simulator* SimObtain *such that for all PPT adversaries* $(\mathcal{A}_1, \mathcal{A}_2)$,

$$
\begin{aligned}
&|\Pr[\, param \xleftarrow{\$} \mathsf{Setup}(1^\lambda), (mpk, \mathsf{ID}, aux, st) \xleftarrow{\$} \mathcal{A}_1(param);\\
&\qquad com \leftarrow \mathsf{Commit}(param, \mathsf{ID}, aux);\\
&\qquad b \xleftarrow{\$} \mathcal{A}_2(st) \leftrightarrow \mathsf{ObtainKey}(param, mpk, \mathsf{ID}, com, aux) : b = 1]\\
&-\Pr[\, param \xleftarrow{\$} \mathsf{Setup}(1^\lambda), (mpk, \mathsf{ID}, aux, st) \xleftarrow{\$} \mathcal{A}_1(param);\\
&\qquad com \leftarrow \mathsf{Commit}(param, \mathsf{ID}, aux);\\
&\qquad b \xleftarrow{\$} \mathcal{A}_2(st) \leftrightarrow \mathsf{SimObtain}(param, mpk, com) : b = 1]| < \mathsf{negl}(\lambda).
\end{aligned}
$$

This models that the protocol reveals no information about the identity ID to the malicious KGC which interacts with the user. Both privacy notions are defined based on a single interaction, but a simple hybrid argument can be used to show that these definitions imply privacy over many sequential instances.

6.3 AKI Protocol for Modified Gentry-IBE

Our protocol extends the interactive protocol for obtaining a signature on a committed value of the first P-signature scheme in [5][4]. We change the signature structure of their scheme so that it fits with the user secret key produced in the modified Gentry-IBE. There are three components sharing the same structure in the key. For brevity, we just show how to build the first component.

Setup: This algorithm executes Setup of modified Gentry-IBE, setups the perfectly binding, strongly computationally hiding commitment and the signature.

IKeyGen: The ICA generates a key pair (pk_{cert}, sk_{cert}) for the signature scheme.

[4] While the signature of the second construction in [5] shares similarity with the user secret key of BB-IBE [8], its second component r cannot be recovered.

$\mathsf{SigCert}$: For $\mathsf{ID} \in \{0,1\}^n$, the ICA creates the certificate $cert = (sig, com, aux)$ by randomly picking[5] aux from the decommitment-string space; and generating a signature sig on $com = \mathsf{Commit}(\mathsf{ID}, aux)$ by running the signing algorithm.

$\mathsf{ObtainKey}(mpk, \mathsf{ID}, cert, aux) \leftrightarrow \mathsf{IssueKey}(msk, cert)$:

1. The user and the KGC engage in a secure two-party computational protocol[6], where the user's private input is (ρ, ID, aux) where $\rho \in_R \mathbb{Z}_p$, and the KGC's private input is α. The KGC then gets a private output which is either $x = (\alpha - \mathsf{ID})\rho$ if $com = \mathsf{Commit}(\mathsf{ID}, aux)$, or $x = \perp$ otherwise.
2. If $x \neq \perp$, the KGC randomly picks[7] $\tau_{\mathsf{ID},1} \in \mathbb{Z}_p$. Then it computes $usk'_{cert} = (usk'_1 = (h_1 g^{-\tau_{\mathsf{ID},1}})^{1/x}, usk'_2 = \tau_{\mathsf{ID},1})$.
3. The user outputs $(usk_1, usk_2) = ((usk'_1)^\rho = (h_1 g^{-\tau_{\mathsf{ID},1}})^{1/(\alpha - \mathsf{ID})}, usk'_2)$.

Analysis. Signer privacy and user privacy follow exactly as in the protocol in [5]. $\mathsf{SimIssue}$ invokes the simulator for the two-party computational (2PC) protocol to extract the adversary's input (ρ, ID, aux), check if $com = \mathsf{Commit}(\mathsf{ID}, aux)$ and sends (usk_1^ρ, usk_2) to the user. $\mathsf{SimObtain}$ also invokes the same simulator to extract the secret key. Then the simulator is given the target output of the computation x, and proceeds to interact with the adversary such that if the adversary completes the protocol, its output is x. In both cases, if the adversary can determine that it is talking with a simulator, it must be the case that the adversary's input to the protocol was incorrect which breaks the security of 2PC.

6.4 Related Work

"Anonymous" private key issuing in ID-based cryptosystems was firstly considered by Sui *et al.* [48], in a system where the duties of authentication and key issuing are separated to local registration authorities (LRAs) and the KGC. Instead of having an LRA to issue a signature, a user supplies a password to the LRA. However, their anonymity guarantee just considers outsider adversaries, and actually an LRA is required to send a list of identities and passwords to the KGC, while our protocol does not require any communication between them.

The "blind" extraction protocols for IBE with leak freeness and selective-failure blindness were proposed in a rigorous manner by Green and Hohenberger [32]. Our notion of issuer privacy is very similar to leak freeness as both are defined in a secure 2PC fashion. A minor difference is that their definition is not coupled with any specific way (e.g. commitment) to hide the identity. Nevertheless, their concrete protocols utilize commitment scheme as well. The motivating

[5] We require that the ICA always use the same aux for a given ID. We can just take aux as the output of a PRF with input ID, for a seed only known to the ICA.

[6] An efficient protocol for securely computing $g'^{1/(sk+m)}$ based on any homomorphic encryption in the standard model [16, §4.3.3] can be used.

[7] If a certificate signing the same commitment is presented later, same $\tau_{\mathsf{ID},1}$ is used.

application in [32] is oblivious transfer, hence the notion of selective-failure blindness considers maliciously generated parameter. Our user privacy is weaker, but it should be fine for our purpose, especially when the KGC is not motivated to induce a selective failure and the user can verify the validity of the key obtained.

As noted in [32], it is non-trivial to come up with an efficient AKI protocol for BF-IBE, another IBE that we showed is $\mathcal{ACI} - \mathcal{KGC}$-secure. However, if one is willing to weaken the security guarantee from 2PC to something like one-more unforgeability of blind signature [6], we conjecture that an efficient AKI protocol for BF-IBE can be constructed similar to the blind signature scheme in [6].

6.5 Applications in Privacy-Preserving Searches on Encrypted Data

Anonymous IBE has attracted attention for the privacy benefits, and as a leverage to construct public key encryption with keyword search [1] as follows. Identity strings are used to represent the keywords. The private key for a particular identity is the trapdoor for testing whether a ciphertext is tagged with a particular keyword. The role of the KGC is now known as the trapdoor generator. To create an encrypted tag, one encrypts a random message using the keyword as the identity in IBE, and appends the message with the tag. To locate the ciphertexts tagged with a keyword, one tries to use a trapdoor to decrypt the tag, and see if the result matches the accompanying message.

Back to our notion, $\mathcal{ACI} - \mathcal{KGC}$ implies that the compromise of the private key does not leak the keyword from an encrypted tag. Our AKI protocol also finds application in privacy-preserving delegated forensic search with authorization, which the government issues a warrant on a keyword to a law enforcing agent (e.g. the police). This warrant is then presented to the encrypted-data owner to indicate that the agent is authorized to ask for a trapdoor for the certified keyword, without revealing what is of forensic interests or (the extreme way of) asking the data owner to surrender the private key. While the idea of privacy-preserving delegated keyword search has been considered, only blind protocols for non-user-anonymous IBE schemes like BB-IBE and Waters-IBE are proposed [32], and without addressing a realistic concern that the hidden keyword should be certified by some authority. We remark that the government can be responsible for the system parameter generation to ensure keyword privacy.

7 Conclusions

We propose a new notion of anonymous ciphertext indistinguishability against KGC attacks ($\mathcal{ACI} - \mathcal{KGC}$), which is orthogonal to existing notions like user anonymity. We modified Gentry's IBE to get an $\mathcal{ACI} - \mathcal{KGC}$-secure IBE in the standard model. We propose a new system architecture with an anonymous key issuing (AKI) protocol to protect the confidentiality of the users identities. We hope that future IBE proposals will consider $\mathcal{ACI} - \mathcal{KGC}$ as one of the key properties, and IBE with $\mathcal{ACI} - \mathcal{KGC}$ or AKI protocol will find more applications.

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. J. Crypt. 21(3), 350–391
2. Al-Riyami, S.S., Paterson, K.G.: Certificateless Public Key Cryptography. In: Laih, C.-S. (ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 452–473. Springer, Heidelberg (2003)
3. Attrapadung, N., Furukawa, J., Gomi, T., Hanaoka, G., Imai, H., Zhang, R.: Efficient Identity-Based Encryption with Tight Security Reduction. In: Pointcheval, D., Mu, Y., Chen, K. (eds.) CANS 2006. LNCS, vol. 4301, pp. 19–36. Springer, Heidelberg (2006)
4. Baek, J., Safavi-Naini, R., Susilo, W.: Efficient Multi-receiver Identity-Based Encryption and Its Application to Broadcast Encryption. In: Vaudenay, S. (ed.) PKC 2005. LNCS, vol. 3386, pp. 380–397. Springer, Heidelberg (2005)
5. Belenkiy, M., Chase, M., Kohlweiss, M., Lysyanskaya, A.: P-signatures and Noninteractive Anonymous Credentials. In: Canetti, R. (ed.) TCC 2008. LNCS, vol. 4948, pp. 356–374. Springer, Heidelberg (2008)
6. Boldyreva, A.: Threshold Signatures, Multisignatures and Blind Signatures based on the Gap-Diffie-Hellman-Group Signature. In: Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol. 2567, pp. 31–46. Springer, Heidelberg (2002)
7. Boldyreva, A., Goyal, V., Kumar, V.: Identity-Based Encryption with Efficient Revocation. In: CCS 2008, pp. 417–426 (2008)
8. Boneh, D., Boyen, X.: Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004)
9. Boneh, D., Boyen, X.: Secure Identity Based Encryption Without Random Oracles. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 443–459. Springer, Heidelberg (2004)
10. Boneh, D., Boyen, X., Goh, E.-J.: Hierarchical Identity Based Encryption with Constant Size Ciphertext. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 440–456. Springer, Heidelberg (2005)
11. Boneh, D., Boyen, X., Shacham, H.: Short Group Signatures. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004)
12. 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)
13. Boneh, D., Hamburg, M.: Generalized Identity Based and Broadcast Encryption Schemes. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 455–470. springer, Heidelberg (2008)
14. Boneh, D., Waters, B.: Conjunctive, Subset, and Range Queries on Encrypted Data. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 535–554. Springer, Heidelberg (2007)
15. 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)
16. Chase, M.: Efficient Non-Interactive Zero-Knowledge Proofs for Privacy Applications. PhD thesis, Brown University (2008)

17. Chatterjee, S., Sarkar, P.: Generalization of the Selective-ID Security Model for HIBE Protocols. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T.G. (eds.) PKC 2006. LNCS, vol. 3958, pp. 241–256. Springer, Heidelberg (2006)
18. Chatterjee, S., Sarkar, P.: HIBE With Short Public Parameters Without Random Oracle. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 145–160. Springer, Heidelberg (2006)
19. Chatterjee, S., Sarkar, P.: Multi-receiver Identity-Based Key Encapsulation with Shortened Ciphertext. In: Barua, R., Lange, T. (eds.) INDOCRYPT 2006. LNCS, vol. 4329, pp. 394–408. Springer, Heidelberg (2006)
20. Chatterjee, S., Sarkar, P.: New Constructions of Constant Size Ciphertext HIBE Without Random Oracle. In: Rhee, M.S., Lee, B. (eds.) ICISC 2006. LNCS, vol. 4296, pp. 310–327. Springer, Heidelberg (2006)
21. Chatterjee, S., Sarkar, P.: Trading Time for Space: Towards an Efficient IBE Scheme with Short(er) Public Parameters in the Standard Model. In: Park, C.-s., Chee, S. (eds.) ICISC 2004. LNCS, vol. 3506, pp. 424–440. Springer, Heidelberg (2005)
22. Chen, L., Cheng, Z.: Security Proof of Sakai-Kasahara's Identity-Based Encryption Scheme. In: Smart, N.P. (ed.) Cryptography and Coding 2005. LNCS, vol. 3796, pp. 442–459. Springer, Heidelberg (2005)
23. Chow, S.S.M.: Certificateless Encryption. In: Joye, M., Neven, G. (eds.) Identity-Based Cryptography. IOS Press, Amsterdam (2008)
24. Chow, S.S.M., Choo, K.-K.R.: Strongly-Secure Identity-Based Key Agreement and Anonymous Extension. In: Garay, J.A., Lenstra, A.K., Mambo, M., Peralta, R. (eds.) ISC 2007. LNCS, vol. 4779, pp. 203–220. Springer, Heidelberg (2007)
25. Chow, S.S.M., Roth, V., Rieffel, E.: General Certificateless Encryption and Timed-Release Encryption. In: Ostrovsky, R., De Prisco, R., Visconti, I. (eds.) SCN 2008. LNCS, vol. 5229, pp. 126–143. Springer, Heidelberg (2008)
26. Dent, A.W., Libert, B., Paterson, K.G.: Certificateless Encryption Schemes Strongly Secure in the Standard Model. In: Cramer, R. (ed.) PKC 2008. LNCS, vol. 4939, pp. 344–359. Springer, Heidelberg (2008)
27. Galindo, D.: Boneh-Franklin Identity Based Encryption Revisited. In: Caires, L., Italiano, G.F., Monteiro, L., Palamidessi, C., Yung, M. (eds.) ICALP 2005. LNCS, vol. 3580, pp. 791–802. Springer, Heidelberg (2005)
28. Gentry, C.: Practical Identity-Based Encryption Without Random Oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445–464. Springer, Heidelberg (2006)
29. Gentry, C., Silverberg, A.: Hierarchical ID-Based Cryptography. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 548–566. Springer, Heidelberg (2002)
30. Goyal, V.: Reducing Trust in the PKG in Identity Based Cryptosystems. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 430–447. Springer, Heidelberg (2007)
31. Goyal, V., Lu, S., Sahai, A., Waters, B.: Black-Box Accountable Authority Identity-Based Encryption. In: CCS 2008, pp. 427–436 (2008)
32. Green, M., Hohenberger, S.: Blind Identity-Based Encryption and Simulatable Oblivious Transfer. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 265–282. Springer, Heidelberg (2007)
33. Horwitz, J., Lynn, B.: Toward Hierarchical Identity-Based Encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 466–481. Springer, Heidelberg (2002)

34. Izabachène, M., Pointcheval, D.: New Anonymity Notions for Identity-Based Encryption. In: Ostrovsky, R., De Prisco, R., Visconti, I. (eds.) SCN 2008. LNCS, vol. 5229, pp. 375–391. Springer, Heidelberg (2008)
35. Katz, J., Sahai, A., Waters, B.: Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products. J. Crypt. (to appear)
36. Kiltz, E.: From Selective-ID to Full Security: The Case of the Inversion-Based Boneh-Boyen IBE Scheme. Cryptology ePrint Archive, 07/033
37. Kiltz, E., Galindo, D.: Chosen-Ciphertext Secure Threshold Identity-Based Key Encapsulation Without Random Oracles. In: De Prisco, R., Yung, M. (eds.) SCN 2006. LNCS, vol. 4116, pp. 173–185. Springer, Heidelberg (2006)
38. Kiltz, E., Vahlis, Y.: CCA2 Secure IBE: Standard Model Efficiency through Authenticated Symmetric Encryption. In: Malkin, T.G. (ed.) CT-RSA 2008. LNCS, vol. 4964, pp. 221–238. Springer, Heidelberg (2008)
39. Libert, B., Quisquater, J.-J.: Identity Based Encryption Without Redundancy. In: Ioannidis, J., Keromytis, A.D., Yung, M. (eds.) ACNS 2005. LNCS, vol. 3531, pp. 285–300. Springer, Heidelberg (2005)
40. Libert, B., Vergnaud, D.: Towards Black-Box Accountable Authority IBE with Short Ciphertexts and Private Keys. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 235–255. Springer, Heidelberg (2009)
41. Naccache, D.: Secure and practical Identity-based Encryption. Inf. Sec. 1(2), 59–64
42. Phan, D.H., Pointcheval, D.: Chosen-Ciphertext Security without Redundancy. In: Laih, C.-S. (ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 1–18. Springer, Heidelberg (2003)
43. Sahai, A., Waters, B.: Fuzzy Identity-Based Encryption. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 457–473. Springer, Heidelberg (2003)
44. Sakai, R., Kasahara, M.: ID based Cryptosystems with Pairing on Elliptic Curve. Cryptology ePrint Archive, 03/054
45. Sakai, R., Ohgishi, K., Kasahara, M.: Cryptosystems based on Pairing over Elliptic Curve (in Japanese). In: SCIS 2001 (2001)
46. Seo, J.H., Kobayashi, T., Ohkubo, M., Suzuki, K.: Anonymous Hierarchical Identity-Based Encryption with Constant Size Ciphertexts. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 215–234. Springer, Heidelberg (2009)
47. 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)
48. Sui, A.F., Chow, S.S.M., Hui, L.C.K., Yiu, S.-M., Chow, K.P., Tsang, W.W., Chong, C.F., Pun, K.K.H., Chan, H.W.: Separable and Anonymous Identity-Based Key Issuing. In: ICPADS 2005, pp. 275–279 (2005)
49. Waters, B.: Efficient Identity-Based Encryption Without Random Oracles. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 114–127. Springer, Heidelberg (2003)
50. Weng, J., Liu, S., Chen, K., Ma, C.: Identity-based Parallel Key-Insulated Encryption without Random Oracles. In: Barua, R., Lange, T. (eds.) INDOCRYPT 2006. LNCS, vol. 4329, pp. 409–423. Springer, Heidelberg (2006)
51. Yao, D., Fazio, N., Dodis, Y., Lysyanskaya, A.: ID-based Encryption for Complex Hierarchies with Applications to Forward Security and Broadcast Encryption. In: CCS 2004, pp. 354–363 (2004)