Real Hidden Identity-Based Signatures

Sherman S. M. Chow[1(✉)], Haibin Zhang[2], and Tao Zhang[1]

[1] Chinese University of Hong Kong, Shatin, NT, Hong Kong
{sherman,zt112}@ie.cuhk.edu.hk
[2] University of Connecticut, Mansfield, CT 06269, USA
haibin.zhang@uconn.edu

Abstract. Group signature allows members to issue signatures on behalf of the group anonymously in normal circumstances. When the need arises, an opening authority (OA) can open a signature and reveal its true signer. Yet, many constructions require not only the secret key of the OA but also a member database (cf. a public-key repository) for this opening. This "secret members list" put the anonymity of members at risk as each of them is a potential signer.

To resolve this "anonymity catch-22" issue, Kiayias and Zhou proposed hidden identity-based signatures (Financial Crypt. 2007 and IET Information Security 2009), where the opening just takes in the secret key of the OA and directly outputs the signer identity. The membership list can be hidden from the OA since there is no membership list whatsoever. However, their constructions suffer from efficiency problem.

This paper aims to realize the vision of Kiayias and Zhou for real, that is, an efficient construction which achieves the distinctive feature of hidden identity-based signatures. Moreover, our construction is secure against concurrent attack, and easily extensible with linkability such that any double authentication can be publicly detected. Both features are especially desirable in Internet-based services which allow anonymous authentication with revocation to block any misbehaving user. We believe our work will improve the usability of group signature and its variant.

Keywords: Anonymous authentication · Group signature
Hidden identity-based signature

1 Introduction

Group signature, introduced by Chaum and van Heyst [1], is a useful tool in applications which expect anonymous authentication, where the signers typically remain anonymous, yet some authorities can identify any misbehaving user in case of abuse. To join a group, users first obtain their group signing keys from a group manager (GM). The joining protocol is often interactive. Once this registration is done, they can sign on behalf of the group with (conditional) anonymity using the signing keys. The verifiers only know that someone in the

A. Kiayias (Ed.): FC 2017, LNCS 10322, pp. 21–38, 2017.
https://doi.org/10.1007/978-3-319-70972-7_2

group signed the message, but cannot identify the specific signer. Whenever the GM deems appropriate, it can use a system trapdoor to "open" a group signature and reveal its true signer.

A later refinement by Camenisch and Michels [2] separates the power of opening from the GM, by introducing an opening authority (or opener). GM in this setting is in charge of user registration only, and the opening authority (OA) is in charge of opening signatures. However, to enable anonymity revocation in many realizations of group signature, the OA actually requires some help of the GM, specifically, for the membership database the GM holds. This design comes with some flaws—either the OA holds the member list, or the GM interacts with the OA each time an opening is needed, which means the GM should remains online for answering opening requests and it can possibly deny such a request of the OA. Note that the reason why group signatures are used is that the user wants to protect their anonymity. However, the existence of such secret membership list conflicts with this purpose. The members cannot sign in peace because the OA is too powerful with this membership list. This list is a very valuable asset attracting any adversary who aims to compromise user anonymity to attack the OA. However, since it is not a secret key by definition and secure storage for such a large list is relatively expensive, it may not be as well-protected as the opening trapdoor. We end up with a "no-win" no matters which of the above options to adopt.

Kiayias and Zhou [3,4] observed this inconvenient situation and put forth the notion of hidden identity-based signatures (HIBS). The *hidden feature* of HIBS is that not only the signer identity can be hidden from a regular verifier (like group signature), but the membership list is also hidden from the OA since there is no membership list whatsoever. In particular, anonymity revocation will not require such a list.

Realizing HIBS is not straightforward, even though many group signature schemes exist. In their first concrete construction [3], one needs to solve discrete logarithm problem to get the signer identity. Discrete logarithm problem cannot be efficiently solved by any probabilistic polynomial-time algorithm. This makes the hidden feature of their scheme rather artificial. Some existing group signature schemes before their work can (be extended easily to) support this "hidden-identity" feature if the opening requires solving discrete logarithm problem. In other words, one can consider this scheme not a "*real*" hidden identity-based signature scheme. Indeed, other scheme which opens to a group element embedding the identity as an exponent also exists [5]. Their second scheme [4] does not suffer from this problem, yet the efficiency is not that satisfactory. Specifically, it uses Paillier encryption and thus a more involved zero-knowledge proof. Not only the signature contains more group elements, but also each of those becomes larger since the composite order group should be large enough to withstand the best-known factorization attack. In other words, the price for this hidden-identity feature is the cost of the efficiency of all other algorithms of the signature scheme. Liu and Xu [6,7] proposed pairing-based HIBS schemes in the random oracle model which claimed to achieve concurrent security, CCA-anonymity, and exculpability, but their constructions still require solving the discrete logarithm problem for opening.

1.1 Our Contributions

We propose a generic construction for HIBS based on standard primitives: digital signature, encryption, and non-interactive zero-knowledge (NIZK) (or non-interactive witness-indistinguishable (NIWI)) proof. Though conceptually simple, it has impacts in multiple aspects.

- First, we show that the seemingly difficult goal of constructing HIBS can be *generally* achieved from various cryptographic assumptions in a *modular* manner, leading to efficient instantiations without random oracles.
- Beyond retaining the nice feature of supporting opening without requiring any membership list, our generic construction is secure even under concurrent joining, such that the GM can interact with multiple joining users in an arbitrarily interleaving manner. Concurrent joining is more practical than sequential joining for applications over the Internet such as anonymous communication (say, via Tor), which is the original scenario Kiayias and Zhou [3,4] brought up to motivate the concept of HIBS.
- We extend our generic construction of HIBS with linkability [8], where HIBS signatures generated by the same signer on the same message can be linked without revealing the identity of the signer. We call this extension linkable hidden identity-based signature (LHIBS). This extension disallows double-posting of the same user with respect to the same "call for contributions", may it be two responses to the same thread of discussion or two votes cast in the associated reputation systems. With our modular construction, advanced features such as escrowed linkability can be easily equipped [9].
- Finally, our generic construction and its instantiations are highly compatible with other privacy enhancing features such as (real) traceability [10,11] and uniqueness [12]. This echoes the work of Galindo, Herranz, and Kiltz [13], which obtains identity-based signature schemes with additional properties from standard signature with the corresponding properties. The details are shown in the full version.

1.2 Relation to Existing Notions

Note that a major difference of identity-based signature from the traditional signatures based on public-key infrastructure, is simply the removal of a huge list of public-key certificates. One can simply include a signature from the certificate authority in every signature, to realize an identity-based signature. However, every signature comes with this additional certificate, which also means an additional verification is needed in verifying any given signatures.

In hidden identity-based signatures, this certificate can be considered as hidden via an implicit encryption mechanism. As such, one may not agree that such construction should be named as identity-based. Yet, our notion does not suffer from the loss of efficiency as in the case for "certificate-based" identity-based signatures. This is exactly the purpose of this work to show that such construction of HIBS can be constructed in an efficient (and modular) manner. On the

other hand, we stick with the original naming of Kiayias and Zhou [3]. Indeed, as acknowledged in their work, HIBS is essentially a group signature scheme, but just with a special care on the input requirement of the opening mechanism.

Galindo et al. [13] studied what additional properties of identity-based signatures (such as proxy, blind, undeniable, etc.) can be generically obtained from standard signature schemes with the same properties. Their work is also based on the above generic construction of identity-based signatures from standard signatures. Our modular construction here is also compatible with many additional properties in the world of group signatures [11,12,14].

2 Preliminaries

2.1 Notations

If S is a set, $s \xleftarrow{\$} S$ denotes the operation of selecting an element s from S uniformly at random. $\emptyset$ denotes an empty set. If $\mathcal{A}$ is a randomized algorithm, we write $z \xleftarrow{\$} \mathcal{A}(x, y, \cdots)$ to indicate the operation that runs $\mathcal{A}$ on inputs $x, y, \cdots$ (and uniformly selected internal randomness from an appropriate domain) which outputs z. A function $\epsilon(\lambda)$: $\mathbb{N} \rightarrow \mathbb{R}$ is *negligible* if, for any positive number d, there exists some constant $\lambda_0 \in \mathbb{N}$ such that $\epsilon(\lambda) < (1/\lambda)^d$ for any $\lambda > \lambda_0$.

2.2 Bilinear Map

Bilinear pairing is a powerful tool for cryptographers to construct a diversity of primitives. In a bilinear group $\mathcal{G} = (\mathbb{G}, \mathbb{H}, \mathbb{G}_T, p, e, g, h)$, $\mathbb{G}, \mathbb{H}$, and $\mathbb{G}_T$ are groups of prime order p. g and h are random generators for the groups $\mathbb{G}$ and $\mathbb{H}$ respectively. An efficient bilinear map $e : \mathbb{G} \times \mathbb{H} \rightarrow \mathbb{G}_T$ maps two group elements from $\mathbb{G}$ and $\mathbb{H}$ to one from the target group $\mathbb{G}_T$ with the following property.

- *Bilinearity.* For all $u \in \mathbb{G}$, $v \in \mathbb{H}$, $a, b \in \mathbb{Z}$, $e(u^a, v^b) = e(u, v)^{ab}$.
- *Non-degeneracy.* $e(g, h) \neq 1$.
- *Efficiency.* For all $(u, v) \in \mathbb{G} \times \mathbb{H}$, $e(u, v)$ is efficiently computable.

2.3 Assumptions

Assumption 1 (Decisional Diffie-Hellman (DDH)). *For a group $\mathbb{G}$ with a random generator g, given (g^a, g^b, g^c) where a, b, c are randomly chosen from $\mathbb{Z}_p$, it is hard for any probabilistic polynomial-time algorithm to decide whether $g^c = g^{ab}$ or not.*

Assumption 2 (SXDH). *For a bilinear group $\mathcal{G} = (\mathbb{G}, \mathbb{H}, \mathbb{G}_T, p, e, g, h)$ where $e : \mathbb{G} \times \mathbb{H} \rightarrow \mathbb{G}_T$, DDH assumption holds for both $\mathbb{G}$ and $\mathbb{H}$.*

Symmetric eXternal Diffie-Hellman (SXDH) assumption implies that there does not exist any efficient transformation from $\mathbb{G}$ to $\mathbb{H}$ or from $\mathbb{H}$ to $\mathbb{G}$.

Assumption 3 (Decisional Linear (DLIN)). *For a group $\mathbb{G}$, given the tuple $(g_1, g_2, g_3, g_1^a, g_2^b, g_3^c) \in \mathbb{G}^6$ where $g_1, g_2, g_3 \in \mathbb{G}^*$ and $a, b, c \in \mathbb{Z}_p$, it is hard for any probabilistic polynomial-time algorithm to decide whether $g_3^c = g_3^{a+b}$ or not.*

3 Hidden Identity-Based Signatures

We present the syntax and notions of security for HIBS. The contents of this section are strengthening and extending those proposed by Kiayias and Zhou [3,4], adding useful functionalities, and establishing stronger notions of security.

3.1 Syntax of HIBS

We consider HIBS with separated *issuer* (or *group/identity manager*) and *opener* (or *opening authority*) [3,15]. An issuer is responsible for member enrollment, while an opener is responsible for recovering the identities hidden in the signatures given by the enrolled users, whenever need arises.

A *hidden identity-based signature* (HIBS) scheme $\mathcal{HIBS}$ is a set of nine algorithms (KGen, UKGen, Reg, $\mathsf{RegCheck}$, Sign, Verify, Open, Judge, $\mathsf{Dispute}$):

- $\mathsf{KGen}(1^\lambda) \to (\mathsf{gpk}, \mathsf{ik}, \mathsf{ok})$: The *group key generation*[1] algorithm takes as input the security parameter λ and outputs the *group public key* gpk, the *issuer key* ik (for the issuer) and the *opening key* ok (for the opener).
- $\mathsf{UKGen}(1^\lambda, \mathsf{ID}) \to (\mathsf{upk}_{\mathsf{ID}}, \mathsf{usk}_{\mathsf{ID}})$: The *user private key generation* algorithm takes as input the security parameter λ and a user identity ID, and outputs the *user personal public and private key pair* $(\mathsf{upk}_{\mathsf{ID}}, \mathsf{usk}_{\mathsf{ID}})$.
- $\mathsf{Reg}(\mathsf{gpk}, \mathsf{ik}, \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}) \to \mathsf{cert}_{\mathsf{ID}}$: The *registration* algorithm takes as input the group public key gpk, the issuer key ik, a user identity ID, and a user personal public key $\mathsf{upk}_{\mathsf{ID}}$ to return a *user membership certificate* $\mathsf{cert}_{\mathsf{ID}}$.
- $\mathsf{RegCheck}(\mathsf{gpk}, \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}}) \to 0/1$: The *registration checking* algorithm[2] takes as input the group public key gpk, a user identity ID, a user personal public key $\mathsf{upk}_{\mathsf{ID}}$, and a user membership certificate $\mathsf{cert}_{\mathsf{ID}}$ to return a single bit b. We say $\mathsf{cert}_{\mathsf{ID}}$ is a *valid* user membership certificate with respect to ID if $\mathsf{RegCheck}(\mathsf{gpk}, \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}}) = 1$.
- $\mathsf{Sign}(\mathsf{gpk}, \mathsf{ID}, \mathsf{cert}_{\mathsf{ID}}, \mathsf{usk}_{\mathsf{ID}}, m) \to \sigma$: The *HIBS signing* algorithm takes as input the group public key gpk, a user identity ID, the corresponding user membership certificate $\mathsf{cert}_{\mathsf{ID}}$, the user private key $\mathsf{usk}_{\mathsf{ID}}$, and a message m to return a signature σ.
- $\mathsf{Verify}(\mathsf{gpk}, m, \sigma) \to 0/1$: The *HIBS verification* algorithm takes as input the group public key gpk, a message m, a signature σ on m, and returns a single bit b. We say that σ is a *valid* signature of m if $\mathsf{Verify}(\mathsf{gpk}, m, \sigma) = 1$.

[1] We put issuing key generation and opening key generation together for brevity. It is easy to separate them in our schemes such that the respective private keys of the issuer and the opener are generated independently except according to the same security parameter, and the corresponding public keys will be put together in gpk.

[2] This algorithm may be optional for some application scenarios.

- $\mathsf{Open}(\mathsf{gpk}, \mathsf{ok}, m, \sigma) \rightarrow (\mathsf{ID}, \omega)$: The opener takes as input the group public key gpk, its opening key ok, a message m, and a valid signature σ for m, and outputs (ID, ω), where ω is a *proof* to support its claim that user ID indeed signed the message. It is possible that $(\mathsf{ID}, \omega) = \perp$ for a valid signature, in which case the opening procedure is foiled.
- $\mathsf{Judge}(\mathsf{gpk}, (\mathsf{ID}, \omega), (m, \sigma)) \rightarrow 0/1$: The *judge* algorithm takes as input the group public key gpk, the opening (ID, ω), a message m, and a valid signature σ of m to verify that the opening of σ to ID is indeed correct. We say that the opening is *correct* if $\mathsf{Judge}(\mathsf{gpk}, (\mathsf{ID}, \omega), (m, \sigma)) = 1$.
- $\mathsf{Dispute}(\mathsf{gpk}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}}, (\mathsf{ID}, \omega)) \rightarrow 0/1$: The *dispute* algorithm is triggered if a registered user ID refuses to admit guilt after an opening (ID, ω) is published. It takes as input the group public key gpk, the user personal public key $\mathsf{upk}_{\mathsf{ID}}$, the user membership certificate $\mathsf{cert}_{\mathsf{ID}}$, which are both provided by the user, and the opening result (ID, ω) published by the opener, and returns a single bit b. The issuer is *guilty* with respect to ID if $\mathsf{Dispute}(\mathsf{gpk}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}}, (\mathsf{ID}, \omega)) = 1$.

We note that the hidden-identity nature just applies on the opener. Obviously, the group manager is governing who can join the group, and hence it can store such a list after every Reg invocation. However, it is natural to assume that the group manager is not motivated to put its member at risk.

Following [15] and different from [3,4], we further equip our HIBS with a judge algorithm $\mathsf{Judge}()$ to protect against a fully corrupt opener. Compared to that of [15], the $\mathsf{Join}()/\mathsf{Issue}()$ algorithm [15] is replaced with $\mathsf{Reg}()$ and $\mathsf{RegCheck}()$ algorithms for the sake of simplicity.

We now briefly consider the correctness notions for HIBS. Correctness includes *registration correctness* (with respect to $\mathsf{Reg}()$ and $\mathsf{RegCheck}()$ algorithms), *signing correctness* (with respect to $\mathsf{Sign}()$ and $\mathsf{Verify}()$ algorithms), *opening correctness* (with respect to $\mathsf{Open}()$ and $\mathsf{Judge}()$ algorithms), and *dispute correctness*. The first three can be easily adapted from those of [3,15], while the last one requires the $\mathsf{Dispute}()$ algorithm to function correctly when a suspected user was indeed framed.

3.2 Syntax of Linkable HIBS

We extend hidden identity-based signatures to the notion of linkable HIBS (LHIBS) which supports linking the signatures on the same message by the same (hidden) signer. This feature is implemented by the algorithm below.

- $\mathsf{Link}(\mathsf{gpk}, m, \sigma_1, \sigma_2) \rightarrow 0/1$: This algorithm takes in the group public key and two signatures on the same message m. If σ_1 and σ_2 are two valid signatures (resulting in 1 from $\mathsf{Verify}()$) generated by the same signer, this algorithm outputs 1; otherwise, it outputs 0.

This linking feature can identify double-posting without opening the identity of any signer.

3.3 Security Notions for HIBS

We strengthen the notions due to Kiayias and Zhou [3,4], and consider the "strongest" achievable notions (following [15]): anonymity, traceability, and non-frameability. The security notions in [3,4], namely, security against misidentification forgery and exculpability attacks (formally given in [4]), have been shown to be implied by traceability and non-frameability [16].

Similar to the study of Kiayias and Zhou [3,4], we do not have an explicit security definition to model the hidden identity nature of the scheme. It is more a functionality requirement that the opener does not need such a list for the proper operation. In principle, such opener can collect all signatures in the system, open each of them, with the goal of recovering the whole membership list. Hence, by the correct functionality of the scheme, we cannot afford to have a security definition which prevents an adversary with the opening secret key from outputting the identity of any member.

Notation. We use $\mathtt{HU}$ and $\mathtt{CU}$ (both initially empty) to denote a set of honest and corrupted users respectively, and use $\mathtt{MSG}_{\mathsf{ID}}$ (initially empty) to denote the set of messages queried by the adversary to SignO oracle for ID. An adversary may have access of the following oracles in the security games to be described.

- $\mathsf{RegO}(\mathsf{ID})$: The adversary queries this oracle with a user identity ID. If $\mathsf{ID} \in \mathtt{CU} \cup \mathtt{HU}$, returns $\perp$. Otherwise, this oracle runs $(\mathsf{upk}_{\mathsf{ID}}, \mathsf{usk}_{\mathsf{ID}}) \leftarrow \mathsf{UKGen}(1^\lambda, \mathsf{ID})$ and $\mathsf{cert}_{\mathsf{ID}} \leftarrow \mathsf{Reg}(\mathsf{gpk}, \mathsf{ik}, \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}})$, sets $\mathtt{MSG}_{\mathsf{ID}} \leftarrow \emptyset$, and sets $\mathtt{HU} \leftarrow \mathtt{HU} \cup \{\mathsf{ID}\}$ and stores $(\mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{usk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}})$ internally.
- $\mathsf{SignO}(\mathsf{ID}, \mathsf{cert}_{\mathsf{ID}}, m)$: This oracle takes in an identity ID and a message m from the adversary, runs $\sigma \leftarrow \mathsf{Sign}(\mathsf{gpk}, \mathsf{ID}, \mathsf{cert}_{\mathsf{ID}}, \mathsf{usk}_{\mathsf{ID}}, m)$ where $\mathsf{cert}_{\mathsf{ID}}$ is the certificate on ID generated by RegO, sets $\mathtt{MSG}_{\mathsf{ID}} \leftarrow \mathtt{MSG}_{\mathsf{ID}} \cup \{m\}$, and returns σ.
- $\mathsf{CorruptO}(\mathsf{ID})$: This oracle takes in an identity ID, sets $\mathtt{CU} \leftarrow \mathtt{CU} \cup \{\mathsf{ID}\}$ and $\mathtt{HU} \leftarrow \mathtt{HU} \setminus \{\mathsf{ID}\}$, and returns $(\mathsf{upk}_{\mathsf{ID}}, \mathsf{usk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}})$.
- $\mathsf{OpenO}(m, \sigma)$: If $\mathsf{Verify}()$ outputs 1 on (m, σ), this oracle returns $(\mathsf{ID}, \omega) \leftarrow \mathsf{Open}(\mathsf{gpk}, \mathsf{ok}, m, \sigma)$. Otherwise, outputs $\perp$.

Definition 1 (CCA-Anonymity). *An HIBS scheme $\mathcal{HIBS}$ is CCA-anonymous, if in the following experiment, $\mathbf{Adv}^{anon}_{\mathcal{HIBS}}(\mathcal{A})$ is negligible.*

Experiment $\mathbf{Exp}^{\text{cca-anon}}_{\mathcal{HIBS}}(\mathcal{A})$

$(\mathsf{gpk}, \mathsf{ik}, \mathsf{ok}) \xleftarrow{\$} \mathsf{KGen}(1^\lambda)$; $\mathtt{CU} \leftarrow \emptyset$; $\mathtt{HU} \leftarrow \emptyset$;

$(\mathsf{ID}_0, \mathsf{ID}_1, m, \mathsf{s}) \xleftarrow{\$} \mathcal{A}^{\mathsf{CorruptO}(\cdot), \mathsf{RegO}(\cdot), \mathsf{OpenO}(\cdot,\cdot)}(\text{'find'}, \mathsf{gpk}, \mathsf{ik})$

$b \xleftarrow{\$} \{0,1\}; \sigma \xleftarrow{\$} \mathsf{Sign}(\mathsf{gpk}, \mathsf{ID}_b, \mathsf{cert}_{\mathsf{ID}_b}, \mathsf{usk}_{\mathsf{ID}_b}, m)$

$b' \xleftarrow{\$} \mathcal{A}^{\mathsf{CorruptO}(\cdot,\cdot), \mathsf{RegO}(\cdot), \mathsf{OpenO}(\cdot,\cdot)}(\text{'guess'}, \sigma, \mathsf{s})$

if $b' \neq b$ **then return** 0

return 1

where the adversary $\mathcal{A}$ must not have queried $\mathsf{OpenO}(\cdot,\cdot)$ with m and σ in guess phase. We define the advantage of $\mathcal{A}$ in the above experiment by

$$\mathbf{Adv}^{\text{anon}}_{\mathcal{HIBS}}(\mathcal{A}) = \Pr[\mathbf{Exp}^{\text{anon}}_{\mathcal{HIBS}}(\mathcal{A}) = 1] - 1/2.$$

The opening of a group signature corresponds to the chosen ciphertext attack (CCA) which features a decryption oracle to the adversary of public-key encryption. Naturally, one can also consider a variant anonymity notion, chosen-plaintext attack (CPA) anonymity, where the adversary is never given access to the opening oracle. It is known as CPA-anonymity.

Our anonymity notion *strengthens* that of Kiayias and Zhou [4] in the sense the adversary is given access to two more oracles $\mathsf{CorruptO}(\cdot,\cdot)$ and $\mathsf{RegO}(\cdot)$.

We also consider a weak CCA-anonymity for our extension with linkability. The definition is stated below.

Definition 2 (Weak CCA-Anonymity). *An HIBS scheme $\mathcal{HIBS}$ is weak CCA-anonymous, if in the following experiment, $\mathbf{Adv}^{anon}_{\mathcal{HIBS}}(\mathcal{A})$ is negligible.*

Experiment $\mathbf{Exp}^{\text{weak-anon}}_{\mathcal{HIBS}}(\mathcal{A})$

$(\mathsf{gpk}, \mathsf{ik}, \mathsf{ok}) \xleftarrow{\$} \mathsf{KGen}(1^\lambda)$; $\mathtt{CU} \leftarrow \emptyset$; $\mathtt{HU} \leftarrow \emptyset$;

$(\mathsf{ID}_0, \mathsf{ID}_1, m, \mathsf{s}) \xleftarrow{\$} \mathcal{A}^{\mathsf{CorruptO}(\cdot),\mathsf{RegO}(\cdot),\mathsf{OpenO}(\cdot,\cdot)}(\text{'find'}, \mathsf{gpk}, \mathsf{ik})$

if $m \in \mathtt{MSG}_{\mathsf{ID}_0}$ **or** $m \in \mathtt{MSG}_{\mathsf{ID}_1}$ **then abort**

$b \xleftarrow{\$} \{0,1\}; \sigma \xleftarrow{\$} \mathsf{Sign}(\mathsf{gpk}, \mathsf{ID}_b, \mathsf{cert}_{\mathsf{ID}_b}, \mathsf{usk}_{\mathsf{ID}_b}, m)$

$b' \xleftarrow{\$} \mathcal{A}^{\mathsf{CorruptO}(\cdot,\cdot),\mathsf{RegO}(\cdot),\mathsf{OpenO}(\cdot,\cdot)}(\text{'guess'}, \sigma, \mathsf{s})$

if $b' \neq b$ **then return** 0

return 1

where the adversary $\mathcal{A}$ must not have queried $\mathsf{OpenO}(\cdot,\cdot)$ with m and σ in guess phase. We define the advantage of $\mathcal{A}$ in the above experiment by

$$\mathbf{Adv}^{\text{anon}}_{\mathcal{HIBS}}(\mathcal{A}) = \Pr[\mathbf{Exp}^{\text{anon}}_{\mathcal{HIBS}}(\mathcal{A}) = 1] - 1/2.$$

One can formulate a CPA counterpart for this definition. For the linkable HIBS, the linking token is deterministic, and is decided by the combination of identity and message to be signed. Hence, in the weak CCA-anonymity game, the adversary is not allowed to submit challenge identity-message pairs which have appeared in the signing queries. Otherwise, the adversary will obtain a linking token on the challenge identity-message pair, and break anonymity of HIBS trivially.

Next, we present traceability and non-frameability, which together imply (and in fact stronger than) the security against misidentification forgery and exculpability attacks [4].

Definition 3 (Traceability). *An HIBS scheme $\mathcal{HIBS}$ is traceable, if in the following experiment, $\mathbf{Adv}^{trace}_{\mathcal{HIBS}}(\mathcal{A})$ is negligible.*

Experiment $\mathbf{Exp}^{\text{trace}}_{\mathcal{HIBS}}(\mathcal{A})$

$(\mathsf{gpk}, \mathsf{ik}, \mathsf{ok}) \xleftarrow{\$} \mathsf{KGen}(1^\lambda)$; $\mathtt{CU} \leftarrow \emptyset$; $\mathtt{HU} \leftarrow \emptyset$;

$(m, \sigma) \xleftarrow{\$} \mathcal{A}^{\mathsf{CorruptO}(\cdot),\mathsf{RegO}(\cdot,\cdot)}(\mathsf{gpk}, \mathsf{ok})$

if $\mathsf{Verify}(\mathsf{gpk}, m, \sigma) = 0$

then return 0

$(\mathsf{ID}, \omega) \leftarrow \mathsf{Open}(\mathsf{gpk}, \mathsf{ok}, m, \sigma)$

if $(\mathsf{ID}, \omega) = \perp$ **or** $\mathsf{Judge}(\mathsf{gpk}, \mathsf{ID}, \omega, m, \sigma) = 0$

then return 1

return 0

The advantage of $\mathcal{A}$ in the above experiment is defined by

$$\mathbf{Adv}^{\text{trace}}_{\mathcal{HIBS}}(\mathcal{A}) = \Pr[\mathbf{Exp}^{\text{trace}}_{\mathcal{HIBS}}(\mathcal{A}) = 1].$$

Definition 4 (Non-frameability). *The definition of non-frameability consists of two aspects:* ***signer-non-frameability*** *and* ***issuer-non-frameability****.*

– An HIBS scheme $\mathcal{HIBS}$ is signer-non-frameable, if in the following experiment, $\mathbf{Adv}^{\text{signer-nf}}_{\mathcal{HIBS}}(\mathcal{A})$ is negligible.

Experiment $\mathbf{Exp}^{\text{signer-nf}}_{\mathcal{HIBS}}(\mathcal{A})$

$(\mathsf{gpk}, \mathsf{ik}, \mathsf{ok}) \xleftarrow{\$} \mathsf{KGen}(1^\lambda)$; $\mathtt{CU} \leftarrow \emptyset$; $\mathtt{HU} \leftarrow \emptyset$;

$(m, \sigma, \mathsf{ID}, \omega) \xleftarrow{\$} \mathcal{A}^{\mathsf{CorruptO}(\cdot),\mathsf{SignO}(\cdot,\cdot),\mathsf{RegO}(\cdot)}(\mathsf{gpk}, \mathsf{ik}, \mathsf{ok})$

if $\mathsf{Verify}(\mathsf{gpk}, m, \sigma) = 0$

then return 0

if $\mathsf{ID} \in \mathtt{HU}$ **and** $m \notin \mathtt{MSG}_{\mathsf{ID}}$ **and**

$\mathsf{Judge}(\mathsf{gpk}, \mathsf{ID}, \omega, m, \sigma) = 1$ **and**

$\mathsf{Dispute}(\mathsf{gpk}, \mathsf{cert}_{\mathsf{ID}}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{ID}, \omega) = 0$

then return 1

return 0

We define the advantage of $\mathcal{A}$ in the above experiment by

$$\mathbf{Adv}^{\text{signer-nf}}_{\mathcal{HIBS}}(\mathcal{A}) = \Pr[\mathbf{Exp}^{\text{signer-nf}}_{\mathcal{HIBS}}(\mathcal{A}) = 1].$$

– An HIBS scheme $\mathcal{HIBS}$ is issuer-non-frameable, if in the following experiment, $\mathbf{Adv}^{\text{issuer-nf}}_{\mathcal{HIBS}}(\mathcal{A})$ is negligible.

Experiment $\mathbf{Exp}^{\text{issuer-nf}}_{\mathcal{HIBS}}(\mathcal{A})$

$(\mathsf{gpk}, \mathsf{ik}, \mathsf{ok}) \xleftarrow{\$} \mathsf{KGen}(1^\lambda)$; $\mathtt{CU} \leftarrow \emptyset$; $\mathtt{HU} \leftarrow \emptyset$;

$(m, \sigma, \mathsf{ID}, \omega) \xleftarrow{\$} \mathcal{A}^{\mathsf{CorruptO}(\cdot),\mathsf{SignO}(\cdot,\cdot),\mathsf{RegO}(\cdot)}(\mathsf{gpk}, \mathsf{ok})$

if $\mathsf{Verify}(\mathsf{gpk}, m, \sigma) = 0$

then return 0

if $\mathsf{Judge}(\mathsf{gpk}, \mathsf{ID}, \omega, m, \sigma) = 1$ **and**

$\mathsf{Dispute}(\mathsf{gpk}, \mathsf{cert}_{\mathsf{ID}}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{ID}, \omega) = 1$

then return 1

return 0

We define the advantage of $\mathcal{A}$ in the above experiment by

$$\mathbf{Adv}^{\text{issuer-nf}}_{\mathcal{HIBS}}(\mathcal{A}) = \Pr[\mathbf{Exp}^{\text{issuer-nf}}_{\mathcal{HIBS}}(\mathcal{A}) = 1].$$

In the signer-non-frameability game, the issuer is considered honest, and any other parties, including the signers, are not guaranteed to be honest. This security game models the scenario that an adversary creates an HIBS forgery on an identity of an honest signer without the consent of the issuer.

On the other hand, the issuer-non-frameability game models the scenario that the adversary chooses an honest signer and creates forgery on behalf of this chosen signer without being caught.

The combination of signer-non-frameability and issuer-non-frameability implies unforgeability. Suppose an adversary can win the game of unforgeability against chosen message attack, it can trivially win both the signer-non-frameability game and the issuer-non-frameability game.

LHIBS and HIBS share the security requirements above, and LHIBS has one more security requirement called linkability.

Definition 5 (Linkability). *An HIBS scheme $\mathcal{LHIBS}$ is linkable, if in the following experiment,* $\mathbf{Adv}^{link}_{\mathcal{HIBS}}(\mathcal{A})$ *is negligible.*

Experiment $\mathbf{Exp}^{\text{link}}_{\mathcal{LHIBS}}(\mathcal{A})$

$(\mathsf{gpk}, \mathsf{ik}, \mathsf{ok}) \xleftarrow{\$} \mathsf{KGen}(1^\lambda)$; $\mathtt{CU} \leftarrow \emptyset$; $\mathtt{HU} \leftarrow \emptyset$;

$(m, \mathsf{ID}, \sigma_0, \sigma_1) \xleftarrow{\$} \mathcal{A}^{\mathsf{CorruptO}(\cdot),\mathsf{SignO}(\cdot,\cdot),\mathsf{RegO}(\cdot)}(\mathsf{gpk}, \mathsf{ik}, \mathsf{ok})$

$\mathsf{ID}_i \leftarrow \mathsf{Open}(\mathsf{gpk}, \mathsf{ok}, m, \sigma_i),\ i \in \{0, 1\}$

if $\exists i \in \{0, 1\}$, s.t. $\mathsf{Verify}(\mathsf{gpk}, m, \sigma_i) = 0$

then return 0

if $\mathsf{ID}_0 = \mathsf{ID}_1$ **and** $\mathsf{Link}(\mathsf{gpk}, m, \sigma_0, \sigma_1) = 0$

then return 1

if $\mathsf{ID}_0 \neq \mathsf{ID}_1$ **and** $\mathsf{Link}(\mathsf{gpk}, m, \sigma_0, \sigma_1) = 1$

then return 1

return 0

We define the advantage of $\mathcal{A}$ in the above experiment by

$$\mathbf{Adv}^{\text{link}}_{\mathcal{LHIBS}}(\mathcal{A}) = \Pr[\mathbf{Exp}^{\text{link}}_{\mathcal{LHIBS}}(\mathcal{A}) = 1].$$

4 Generic Construction

This section presents a generic construction of HIBS built from standard signature schemes and an NIZK (or NIWI) proof system, then extends it to support linkability.

4.1 Generic HIBS

To design a generic construction of HIBS, we start from a generic construction of identity-based signature (IBS) from standard signature schemes—certificate-based approach to IBS, originally brought up by Shamir [17] and formally proven secure by Bellare, Neven, and Namprempre [18]. To construct our generic HIBS, we "hide" the whole signing process with an encryption and prove so in an NIZK (or NIWI) sense.[3]

When a signer joins the system, it generates a public-private key pair of a signature scheme, and sends the public key along with its identity to the GM for a certificate. The GM use its signing key to generate a signature on the identity and public key of the signer, and returns this signature to the signer as a certificate. To create an HIBS, the signer first uses its own signing key to create a signature on the message, then encrypts the certificate, the signature on the message, its identity, and its public key, and finally generates an NIZK proof on the certificate, the signature on the message, and the ciphertext. The ciphertext and the proof are output as the HIBS signature. The proof asserts three statements. First, the certificate is a valid signature generated by the GM. Second, the signature on the message is valid with respect to the public key from the certificate. Third, the identity, the public key, and the certificate encrypted in the ciphertext are the ones used to create the signature. The validity of the first two statements indicates that the signer is authentic. The validity of the third statement enforces the traceability of HIBS. The party with the decryption key can open the signature and obtain the identity of the signer.

Let $\mathcal{DS}_1 = (\mathsf{SKG}, \mathsf{SIG}, \mathsf{VFY})$ and $\mathcal{DS}_2 = (\mathsf{skg}, \mathsf{sig}, \mathsf{vfy})$ be two signature schemes. Let $\mathcal{OTS} = (\mathsf{OKGen}, \mathsf{OSig}, \mathsf{OVerify})$ be a one-time signature scheme. Let $\mathcal{E} = (\mathsf{EKGen}, \mathsf{Enc}, \mathsf{Dec})$ be a public key encryption scheme. Let (P, V) be an NIZK (or NIWI) proof system. We define an HIBS scheme $\mathcal{HIBS}$ in Fig. 1. In particular, the underlying language for the proof system (P, V) is defined as

$$\begin{aligned}\mathcal{L} :=& \{(m, \mathsf{ovk}, \mathsf{VK}, \mathsf{ek}, C, T) | \exists (r, \sigma, \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}}) \\ & [\mathsf{VFY}(\mathsf{VK}, (\mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}), \mathsf{cert}_{\mathsf{ID}}) = 1 \wedge \mathsf{vfy}(vk_{\mathsf{ID}}, (m, \mathsf{ovk}), \sigma) = 1 \\ & \wedge C = \mathsf{Enc}(\mathsf{ek}, r, (\sigma, \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}}))]\}\end{aligned}$$

[3] Or, we could directly use NIZK proof of knowledge (NIZKPoK), being notionally equivalent to CCA encryption.

where we write $\mathsf{Enc}(\mathsf{ek}, r, M)$ for the encryption of a message M under the public key ek using the randomness r.

In the proposed generic construction, when a user joins the system, the communication between the user and the GM just consists of one round (two message flows). Thus, even when multiple users are joining the system at the same time, the issuing process can still be conducted securely. The follow theorem establishes the security of $\mathcal{HIBS}$.

Theorem 1. *The proposed generic construction $\mathcal{HIBS}$ in Fig. 1 is CCA-anonymous (CPA-anonymous), traceable, signer-non-frameable, and issuer-non-frameable, if $\mathcal{DS}_1$ and $\mathcal{DS}_2$ are unforgeable against chosen message attacks, $\mathcal{OTS}$ is a one-time secure signature, $\mathcal{E}$ is IND-CCA-secure (IND-CPA-secure), and the proof system (P, V) is adaptively sound, adaptively zero-knowledge, and one-time simulation-sound.*

Alg $\mathsf{KGen}(1^\lambda)$
$R \xleftarrow{\$} \{0,1\}^{p(\lambda)}$
$(\mathsf{VK}, \mathsf{SK}) \xleftarrow{\$} \mathcal{DS}_1.\mathsf{SKG}(1^\lambda)$
$(\mathsf{ek}, \mathsf{dk}) \xleftarrow{\$} \mathcal{E}.\mathsf{EKGen}(1^\lambda)$
$\mathsf{gpk} \leftarrow (R, \mathsf{ek}, \mathsf{VK})$
$\mathsf{ik} \leftarrow \mathsf{SK}$
$\mathsf{ok} \leftarrow \mathsf{dk}$
return $(\mathsf{gpk}, \mathsf{ik}, \mathsf{ok})$

Alg $\mathsf{UKGen}(1^\lambda, \mathsf{ID})$
$(\mathsf{upk}_{\mathsf{ID}}, \mathsf{usk}_{\mathsf{ID}}) \xleftarrow{\$} \mathcal{DS}_2.\mathsf{skg}(1^\lambda)$
return $(\mathsf{upk}_{\mathsf{ID}}, \mathsf{usk}_{\mathsf{ID}})$

Alg $\mathsf{Reg}(\mathsf{gpk}, \mathsf{ik}, \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}})$
$\mathsf{cert}_{\mathsf{ID}} \xleftarrow{\$} \mathsf{SIG}(\mathsf{SK}, (\mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}))$
return $\mathsf{cert}_{\mathsf{ID}}$

Alg $\mathsf{RegCheck}(\mathsf{gpk}, \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}})$
return $\mathsf{VFY}(\mathsf{VK}, (\mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}), \mathsf{cert}_{\mathsf{ID}})$

Alg $\mathsf{Judge}(\mathsf{gpk}, (\mathsf{ID}, \omega), (m, \sigma))$
parse ω **as** $(\sigma', \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}})$
return $\mathsf{VFY}(\mathsf{VK}, (\mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}), \mathsf{cert}_{\mathsf{ID}}) \wedge \mathsf{vfy}(\mathsf{upk}_{\mathsf{ID}}, m, \sigma')$

Alg $\mathsf{Sign}(\mathsf{gpk}, \mathsf{ID}, \mathsf{cert}_{\mathsf{ID}}, \mathsf{usk}_{\mathsf{ID}}, m)$
$\sigma' \leftarrow \mathsf{sig}(\mathsf{usk}_{\mathsf{ID}}, m)$
$C \leftarrow \mathsf{Enc}(\mathsf{ek}, r, (\sigma', \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}}))$
$\pi \xleftarrow{\$} P(R, (m, \mathsf{VK}, \mathsf{ek}, C), (r, \sigma', \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}}))$
$\sigma \leftarrow (C, \pi)$
return (m, σ)

Alg $\mathsf{Verify}(\mathsf{gpk}, m, \sigma)$
return $V(R, (m, \mathsf{VK}, \mathsf{ek}, C), \pi)$

Alg $\mathsf{Open}(\mathsf{gpk}, \mathsf{ok}, m, \sigma)$
if $V(R, (m, \mathsf{VK}, \mathsf{ek}, \tau, C, \pi)) = 0$
return $\perp$
$(\sigma', \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}}) \leftarrow \mathsf{Dec}(\mathsf{dk}, C)$
$\omega \leftarrow (\sigma', \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}})$
return (ID, ω)

Alg $\mathsf{Dispute}(\mathsf{gpk}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}}, (\mathsf{ID}, \omega))$
parse ω **as** $(\sigma', \mathsf{upk}'_{\mathsf{ID}}, \mathsf{cert}'_{\mathsf{ID}})$
if $\mathsf{VFY}(\mathsf{VK}, (\mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}), \mathsf{cert}_{\mathsf{ID}}) = 0$
then return $\perp$
if $\mathsf{VFY}(\mathsf{VK}, (\mathsf{ID}, \mathsf{upk}'_{\mathsf{ID}}), \mathsf{cert}'_{\mathsf{ID}}) = 1$ **and** $\mathsf{upk}'_{\mathsf{ID}} \neq \mathsf{upk}_{\mathsf{ID}}$
then return 1
return 0

Fig. 1. A generic construction for hidden identity-based signature $\mathcal{HIBS} = (\mathsf{KGen}, \mathsf{UKGen}, \mathsf{Reg}, \mathsf{RegCheck}, \mathsf{Sign}, \mathsf{Verify}, \mathsf{Open}, \mathsf{Judge}, \mathsf{Dispute})$: R is the common reference string for the underlying proof system (P, V).

4.2 Extension with Linkability

Figure 2 shows how we extend the generic construction $\mathcal{HIBS} = (\mathsf{KGen}, \mathsf{UKGen}, \mathsf{Reg}, \mathsf{RegCheck}, \mathsf{Sign}, \mathsf{Verify}, \mathsf{Open}, \mathsf{Judge}, \mathsf{Dispute})$ to a linkable HIBS (LHIBS) scheme.

Alg $\mathsf{KGen}(1^\lambda)$
$(\mathsf{gpk}, \mathsf{ik}, \mathsf{ok}) \leftarrow \mathcal{HIBS}.\mathsf{KGen}(1^\lambda)$
return $(\mathsf{gpk}, \mathsf{ik}, \mathsf{ok})$

Alg $\mathsf{UKGen}(1^\lambda, \mathsf{ID})$
$(\mathsf{vk}, \mathsf{sk}) \xleftarrow{\$} \mathcal{HIBS}.\mathsf{UKGen}(1^\lambda, \mathsf{ID})$
$(\mathsf{pk}_F, \mathsf{sk}_F) \leftarrow \mathsf{FGen}(1^\lambda)$
$\mathsf{upk}_{\mathsf{ID}} \leftarrow (\mathsf{vk}, \mathsf{pk}_F)$
$\mathsf{usk}_{\mathsf{ID}} \leftarrow (\mathsf{sk}, \mathsf{sk}_F)$
return $(\mathsf{upk}_{\mathsf{ID}}, \mathsf{usk}_{\mathsf{ID}})$

Alg $\mathsf{Reg}(\mathsf{gpk}, \mathsf{ik}, \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}})$
$\mathsf{cert}_{\mathsf{ID}} \xleftarrow{\$} \mathcal{HIBS}.\mathsf{Reg}(\mathsf{gpk}, \mathsf{ik}, \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}})$
return $\mathsf{cert}_{\mathsf{ID}}$

Alg $\mathsf{RegCheck}(\mathsf{gpk}, \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}})$
return $\mathcal{HIBS}.\mathsf{RegCheck}(\mathsf{gpk}, \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}})$

Alg $\mathsf{Open}(\mathsf{gpk}, \mathsf{ok}, m, \sigma)$
return $\mathcal{HIBS}.\mathsf{Open}(\mathsf{gpk}, \mathsf{ok}, m, \sigma)$

Alg $\mathsf{Judge}(\mathsf{gpk}, (\mathsf{ID}, \omega), (m, \sigma))$
return $\mathcal{HIBS}.\mathsf{Judge}(\mathsf{gpk}, (\mathsf{ID}, \omega), (m, \sigma))$

Alg $\mathsf{Sign}(\mathsf{gpk}, \mathsf{ID}, \mathsf{cert}_{\mathsf{ID}}, \mathsf{usk}_{\mathsf{ID}}, m)$
parse $\mathsf{usk}_{\mathsf{ID}}$ **as** $(\mathsf{sk}, \mathsf{sk}_F)$
$(T, \pi_F) \leftarrow \mathsf{FProve}(\mathsf{sk}_F, (\mathsf{ID}, m))$
$\sigma' \leftarrow \mathsf{sig}(\mathsf{sk}, m)$
$C \leftarrow \mathsf{Enc}(\mathsf{ek}, r, (\sigma', \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}}))$
$\pi \xleftarrow{\$} P(R, (m, \mathsf{VK}, \mathsf{ek}, C, T), (r, \sigma', \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}}, \pi_F))$
$\sigma \leftarrow (C, \pi, T)$
return (m, σ)

Alg $\mathsf{Verify}(\mathsf{gpk}, m, \sigma)$
return $V(R, (m, \mathsf{VK}, \mathsf{ek}, C, T), \pi)$

Alg $\mathsf{Dispute}(\mathsf{gpk}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}}, (\mathsf{ID}, \omega))$
return $\mathcal{HIBS}.\mathsf{Dispute}(\mathsf{gpk}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}}, (\mathsf{ID}, \omega))$

Alg $\mathsf{Link}(\mathsf{gpk}, m, \sigma_1, \sigma_2)$
if $\mathsf{Verify}(\mathsf{gpk}, m, \sigma_1) = 0$
or $\mathsf{Verify}(\mathsf{gpk}, m, \sigma_2) = 0$
then return $\perp$
parse σ_i **as** (C_i, π_i, T_i)
if $T_1 = T_2$ **then return** 1;
else return 0

Fig. 2. A generic construction for linkable hidden identity-based signature $\mathcal{LHIBS} = (\mathsf{KGen}, \mathsf{UKGen}, \mathsf{Reg}, \mathsf{RegCheck}, \mathsf{Sign}, \mathsf{Verify}, \mathsf{Open}, \mathsf{Judge}, \mathsf{Dispute}, \mathsf{Link})$

In this extension, $F = (\mathsf{FGen}, \mathsf{FProve}, \mathsf{FVerify})$ is a pseudorandom function. The verification of computation correctness of $\mathsf{FVerify}()$ is compatible with Groth-Sahai proof. The underlying language for the proof system (P, V) is defined as

$$\begin{aligned}\mathcal{L} :=\{(m, \mathsf{VK}, \mathsf{ek}, C, T) | \exists (r, \sigma, \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}}, \pi_F) \\ [\mathsf{VFY}(\mathsf{VK}, (\mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}), \mathsf{cert}_{\mathsf{ID}}) = 1 \wedge \mathsf{vfy}(vk_{\mathsf{ID}}, m, \sigma) = 1 \\ \wedge\ C = \mathsf{Enc}(\mathsf{ek}, r, (\sigma, \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}})) \\ \wedge\ \mathsf{FProve}(\mathsf{pk}_F, (\mathsf{ID}, m), T, \pi_F) = 1]\}.\end{aligned}$$

Theorem 2. *$\mathcal{LHIBS}$ in Fig. 2 is traceable, linkable, weak CCA-anonymous (weak CPA-anonymous), signer-non-frameable, and issuer-non-frameable, if $\mathcal{DS}_1$ and $\mathcal{DS}_2$ are unforgeable against chosen message attacks, $\mathcal{OTS}$ is a one-time secure signature, $\mathcal{E}$ is IND-CCA-secure (IND-CPA-secure), the proof system (P, V) is adaptively sound, adaptively zero-knowledge, and one-time simulation-sound, and F is a PRF.*

5 Efficient Instantiations

To instantiate our general paradigm without resorting to random oracles, we use Groth-Sahai proof [19]. To this end, we use the group elements representation

for user identities such that they are compatible with Groth-Sahai proof system. In particular, we select a structure-preserving signature [20] as the first-level signature ($\mathcal{DS}_1$) to sign the second-level signature ($\mathcal{DS}_2$) public key and user identity, both of which are group elements. Moreover, the identities, being group elements, can be fully extracted from the Groth-Sahai commitments. This makes the Open algorithm to be purely based on identity, in particular, does not require any archived membership information obtained when the user joins the systems and gets the credential.

We present three instantiations here. All the proposed instantiations use Groth-Sahai proof system as the underlying proof system. The first two instantiations use the full Boneh and Boyen (BB) signature [21] as the second-level scheme (for $\mathcal{DS}_2$), while the third instantiation uses a signature scheme by Yuen et al. [22] which is based on a static assumption. The public-key of BB signature consists of 2 group elements $upk_{\mathsf{ID}} = (y_1, y_2) \in \mathbb{G}^2$. A signature for message $m \in \mathbb{Z}_q$ is of the form $(s, t) \in \mathbb{G} \times \mathbb{Z}_q^*$ which is verifiable by $e(s, y_1 g^m y_2^t) = e(g, g)$. We do not mention the above common designs and only describe the different part in the following instantiations.

Table 1 summarizes the previous HIBS construction (with exculpability) due to Kiayias and Zhou [4], our two instantiations of HIBS in our stronger model, Inst1 and Inst2, and the most efficient group signature scheme (as a baseline) that provides concurrent security, CCA-anonymity, and non-frameability [23]. The size in kilobytes (KB) of the group elements are measured on "MNT159" [24] curve.

Table 1. Summary of the properties among the Kiayias-Zhou HIBS construction (with exculpability), the most efficient group signatures that provides CCA-anonymity and non-frameability (as a baseline), and our two instantiations of HIBS in our stronger model: $[N]$, $[n]$, and $[q]$ respectively denote the size of an element in $\mathbb{Z}_N^*$, $\mathbb{Z}_n^*$, and $\mathbb{Z}_q$ (assuming that the group elements and scalars can be represented in a similar bit-size)

Scheme	RO	Hidden-ID	Non-frame.	Anon.	Concur.	Assumption	Sig. size	Length
KZ [4]	Yes	Yes	Yes	CCA	No	DCR; S-RSA	$\approx 3^{[N]} + 16^{[n]}$	7.33 KB
AHO [23]	No	No	Yes	CCA	Yes	q-SFP	$55 + 1^{[q]}$	1.09 KB
Inst1	No	Yes	Yes	CCA	Yes	q-SFP; q-SDH	$60 + 1^{[q]}$	1.15 KB
Inst2	No	Yes	Yes	CCA	Yes	DLIN; q-SDH	$176 + 1^{[q]}$	3.41 KB
Inst3	No	Yes	Yes	CCA	Yes	DLIN	$494 + 1^{[q]}$	9.58 KB

5.1 Instantiation 1

In our first instantiation Inst1, we select Groth-Sahai proof system instantiated basing on SXDH assumption as the underlying proof system (P, V). As we have discussed previously, this setting is suitable for ElGamal encryption. Furthermore, SXDH setting is the most efficient instantiation of Groth-Sahai proof system, and Type III bilinear group operates with higher efficiency than the other two types do.

This instantiation uses the signature scheme proposed by Abe et al. [23] to implement the first-level structure-preserving signature $\mathcal{DS}_1$. It consists of 7 group elements, 4 of which can be perfectly randomized. The message signed by the first-level signature consists of 3 group elements, including the user identity which is one group element. A proof for the first-level signature consists of 4 elements (since the corresponding two pairing product equations are linear) and a proof for the second-level signature takes 4 group elements. For the underlying encryption scheme $\mathcal{E}$, we selected DDH-based ElGamal [25], which fits with the SXDH setting. $\mathcal{OTS}$ can be instantiated with a weak BB signature [21] which is not one-time. Its public key consists of 1 group element, and its signature consists of 1 group element.

The resulting CPA-anonymous HIBS Inst1 consists of 45 group elements and 1 scalar value (in $\mathbb{Z}_q$). Following the existing approach [26], the proposed instantiation Inst1 can achieve CCA-anonymity with extra 15 group elements. Thus, the resulting CCA-anonymous HIBS Inst1 consists of 60 group elements and 1 scalar value (in $\mathbb{Z}_q$).

5.2 Instantiation 2

Our second HIBS instantiation Inst2 is proven secure basing on simple assumptions in the standard model. The first level signature $\mathcal{DS}_1$ can be proven secure basing on static assumptions in the standard model. If we replace the second level signature, BB signature, with another scheme basing on a static assumption, then the HIBS scheme is basing on static assumption which is more desirable than basing on a q-type assumption as Inst1. This instantiation raises the security level in the cost of losing efficiency.

The DLIN-based Groth-Sahai proof is chosen as the proof system. This DLIN setting is compatible with Camenisch et al.'s encryption scheme [27].

We select the signature scheme from [27] to instantiate $\mathcal{DS}_1$. It consists of 17 group elements, only 2 of which can be perfectly randomized. The proof (for two signatures) includes 10 pairing product equations (none of them are linear) and thus consists of 90 group elements.

Since we select a CCA-secure structure-preserving encryption scheme [28], there is no extra overhead (e.g., addition of the extra 15 group elements in Inst1) to achieve CCA-anonymity. However, it is instantiated with a Type I bilinear group which is not as efficient as a Type III bilinear group. $\mathcal{OTS}$ is instantiated with weaker BB signature. The CCA-anonymous HIBS Inst2 obtained therefore consists of 176 group elements and 1 scalar value.

5.3 Instantiation 3

Our third HIBS instantiation Inst3 replaces the second level signature, and the one-time signature with a dual form exponent inversion signature scheme proposed by Yuen et al. [22]. This signature is based on static assumptions, making the whole scheme constructed upon static assumptions.

The DLIN-based Groth-Sahai proof is chosen as the proof system.

Again, we use the signature scheme from [27] as $\mathcal{DS}_1$. It consists of 17 group elements, only 2 of which can be perfectly randomized. The proof for the first-level signature includes 9 pairing product equations (none of them are linear) and thus consists of 81 group elements. Although the proof for the second-level signature only include 1 pairing product equation, this scheme requires more elements in the prime order group since it is converted from a dual form signature constructed originally in composite order group. Suppose an n-dimensional space is used to simulate the composite order group in prime order setting. We need n elements in the prime order group to represent one composite order group element, and need n^2 target group elements to represent a target group element in the composite order setting. In this signature scheme, $n = 6$, hence, there are totally 405 elements in this proof. The CCA-anonymous HIBS Inst3, instantiated with a Type I bilinear group, consists of 489 group elements and 1 scalar value.

6 Concluding Remarks

The motivation of group signature is to protect the member's anonymity in issuing signatures on behalf of the group, with an opening mechanism to indirectly ensure well-behavior of signers (or supports anonymity revocation especially when the signing key is compromised by an adversary). Yet, many existing realizations require the existence of a member list for opening to work. The existence of such list simply put the anonymity of the members in danger. A refinement of the group signature without such a list is called *hidden identity-based signatures* (HIBS) in the literature, such that the identity of a real signer is hidden in normal circumstance (just like group signature), yet can be revealed directly via the opening procedure (which does not require any input such as membership database apart from the opening secret key). Moreover, until recent advance in Groth-Sahai proof and structure-preserving signatures (SPS), group signature does not support concurrent member joining efficiently, which makes it impractical for settings with many users joining everyday such as Internet-based applications. In this paper, we propose efficient realization of HIBS which supports concurrent join.

Group signature is a fundamental primitive in supporting anonymous online communication, and we have already witnessed many extensions of group signatures. With our generic design of HIBS based on SPS, we show how various extended notion of group signatures can be realized.

A future direction is to remove the opening authority altogether, as in blacklistable anonymous credential without trusted third party (TTP). However, the newer schemes (e.g. [29] and its follow-up works) often require the verifier to be the issuer itself, and the user credential is updated after each authentication for the efficiency of the whole system. In other words, the concurrency issue in granting the credential becomes even more prominent. Proposing such a system with concurrent security and acceptable efficiency is another interesting question.

Acknowledgment. Sherman Chow is supported in part by the Early Career Scheme and the Early Career Award (CUHK 439713), and General Research Funds (CUHK 14201914) of the Research Grants Council, University Grant Committee of Hong Kong. Haibin acknowledges NSF grant CNS 1330599 and CNS 1413996, as well as the Office of Naval Research grant N00014-13-1-0048.

References

1. Chaum, D., van Heyst, E.: Group signatures. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 257–265. Springer, Heidelberg (1991). https://doi.org/10.1007/3-540-46416-6_22
2. Camenisch, J., Michels, M.: Separability and efficiency for generic group signature schemes. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 413–430. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48405-1_27
3. Kiayias, A., Zhou, H.-S.: Hidden identity-based signatures. In: Dietrich, S., Dhamija, R. (eds.) FC 2007. LNCS, vol. 4886, pp. 134–147. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-77366-5_14
4. Kiayias, A., Zhou, H.: Hidden identity-based signatures. IET Inf. Secur. **3**(3), 119–127 (2009)
5. Boyen, X., Waters, B.: Full-domain subgroup hiding and constant-size group signatures. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 1–15. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-71677-8_1.
6. Liu, X., Xu, Q.-L.: Improved hidden identity-based signature scheme. In: International Conference on Intelligent Computing and Intelligent Systems (ICIS) (2010)
7. Liu, X., Xu, Q.-L.: Practical hidden identity-based signature scheme from bilinear pairings. In: 3rd International Conference on Computer Science and Information Technology (ICCSIT) (2010)
8. Liu, J.K., Wei, V.K., Wong, D.S.: Linkable spontaneous anonymous group signature for ad hoc groups. In: Wang, H., Pieprzyk, J., Varadharajan, V. (eds.) ACISP 2004. LNCS, vol. 3108, pp. 325–335. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-27800-9_28
9. Chow, S.S.M., Susilo, W., Yuen, T.H.: Escrowed linkability of ring signatures and its applications. In: Nguyen, P.Q. (ed.) VIETCRYPT 2006. LNCS, vol. 4341, pp. 175–192. Springer, Heidelberg (2006). https://doi.org/10.1007/11958239_12
10. Kiayias, A., Yung, M.: Group signatures with efficient concurrent join. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 198–214. Springer, Heidelberg (2005). https://doi.org/10.1007/11426639_12
11. Chow, S.S.M.: Real traceable signatures. In: Jacobson, M.J., Rijmen, V., Safavi-Naini, R. (eds.) SAC 2009. LNCS, vol. 5867, pp. 92–107. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-05445-7_6
12. Franklin, M., Zhang, H.: Unique group signatures. In: Foresti, S., Yung, M., Martinelli, F. (eds.) ESORICS 2012. LNCS, vol. 7459, pp. 643–660. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-33167-1_37
13. Galindo, D., Herranz, J., Kiltz, E.: On the generic construction of identity-based signatures with additional properties. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 178–193. Springer, Heidelberg (2006). https://doi.org/10.1007/11935230_12
14. Abe, M., Chow, S.S.M., Haralambiev, K., Ohkubo, M.: Double-trapdoor anonymous tags for traceable signatures. Int. J. Inf. Secur. **12**(1), 19–31 (2013)

15. Bellare, M., Shi, H., Zhang, C.: Foundations of group signatures: the case of dynamic groups. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 136–153. Springer, Heidelberg (2005). https://doi.org/10.1007/978-3-540-30574-3_11
16. Bootle, J., Cerulli, A., Chaidos, P., Ghadafi, E., Groth, J.: Foundations of fully dynamic group signatures. In: Manulis, M., Sadeghi, A.-R., Schneider, S. (eds.) ACNS 2016. LNCS, vol. 9696, pp. 117–136. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-39555-5_7
17. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39568-7_5
18. Bellare, M., Namprempre, C., Neven, G.: Security proofs for identity-based identification and signature schemes. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 268–286. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24676-3_17
19. Groth, J., Sahai, A.: Efficient noninteractive proof systems for bilinear groups. SIAM J. Comput. **41**(5), 1193–1232 (2012)
20. Abe, M., Fuchsbauer, G., Groth, J., Haralambiev, K., Ohkubo, M.: Structure-preserving signatures and commitments to group elements. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 209–236. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14623-7_12
21. Boneh, D., Boyen, X.: Short signatures without random oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 56–73. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24676-3_4
22. Yuen, T.H., Chow, S.S.M., Zhang, C., Yiu, S.: Exponent-inversion signatures and IBE under static assumptions. IACR Cryptology ePrint Archive, Report 2014/311 (2014)
23. Abe, M., Haralambiev, K., Ohkubo, M.: Signing on elements in bilinear groups for modular protocol design. IACR Cryptology ePrint Archive, Report 2010/133 (2010). http://eprint.iacr.org/2010/133
24. Miyaji, A., Nakabayashi, M., Takano, S.: New explicit conditions of elliptic curve traces for FR-reduction. IEICE Trans. Fund. **84**(5), 1234–1243 (2001)
25. ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 10–18. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39568-7_2
26. Groth, J.: Fully anonymous group signatures without random oracles. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 164–180. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-76900-2_10
27. Abe, M., Chase, M., David, B., Kohlweiss, M., Nishimaki, R., Ohkubo, M.: Constant-size structure-preserving signatures: generic constructions and simple assumptions. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 4–24. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34961-4_3
28. Camenisch, J., Haralambiev, K., Kohlweiss, M., Lapon, J., Naessens, V.: Structure preserving CCA secure encryption and applications. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 89–106. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25385-0_5
29. Au, M.H., Tsang, P.P., Kapadia, A.: PEREA: practical TTP-free revocation of repeatedly misbehaving anonymous users. ACM Trans. Inf. Syst. Secur. **14**(4), 29 (2011)

http://www.springer.com/978-3-319-70971-0

Financial Cryptography and Data Security
21st International Conference, FC 2017, Sliema, Malta, April 3-7, 2017, Revised Selected Papers
Kiayias, A. (Ed.)
2017, XIV, 650 p. 132 illus., Softcover
ISBN: 978-3-319-70971-0