Real Hidden Identity-Based Signatures

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

[1] Chinese University of Hong Kong, N.T., Hong Kong
{sherman,zt112}@ie.cuhk.edu.hk
[2] University of Connecticut, C.T., US
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 OA's secret key but also a member database (cf. a public-key repository) in this opening. This "secret members list" put the anonymity of members at risk.
To resolve this "anonymity catch-22" issue, Kiayias and Zhou proposed hidden identity-based signatures (Financial Crypt. 2007), where the opening just takes in the OA's secret key and 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.

1 Introduction

Group signature, introduced by Chaum and van Heyst [1], is a useful tool in applications which expect anonymous authentication, i.e., 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 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 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, 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 can deny an opening request from 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 of this membership list. This list is a very valuable asset attracting any adversary who aims to compromise user anonymity to attack the OA, but may not be as well-protected as the opening trapdoor since it is large in size and secure storage is relatively expensive.

Kiayias and Zhou [2, 3] 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 [2], one needs to solve discrete logarithm problem to get the signer identity. Discrete logarithm problem is an NP problem which 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. Their second scheme [3] 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 Xin and Xu Qiu-liang [4, 5] improved the security of the work of Kiayias and Zhou in terms of anonymity and exculpability, but their construction still requires solving the discrete logarithm problem for opening.

1.1 Our Contributions

We propose a generic construction for HIBS based on standard primitives, i.e., 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 having the membership list hidden, our generic construction is secure even under concurrent joining, such that the GM can interact with multiple users in an arbitrarily interleaving manner. Concurrent joining is more practical than sequential joining for anonymous communication over the Internet (e.g., via Tor) which is the original scenario Kiayias and Zhou [2, 3] brought up to motivate the concept of HIBS.
- We extend our generic construction of HIBS to be linkable, where HIBS signatures generated by the same signer on the same message can be linked without revealing the signer's identity. We call this extension linkable hidden-identity 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.
- Finally, our generic construction and its instantiations are highly compatible with other privacy enhancing features such as (real) traceability [6, 7] and uniqueness [8]. This echoes the work of Galindo, Herranz, and Kiltz [9], which obtains identity-based signature schemes with additional properties from standard signature with the corresponding properties.

1.2 Related Work

Bellare, Micciancio and Warinschi [10] gave security definitions for group signature in the static setting (BMW model) where all members were given their signing keys and provided a trapdoor permutation based construction.

Boyen and Waters [11, 12] proposed group signatures under a weaker model where the adversary attacking anonymity is not given any openings of group signatures [13]. It is also unclear how the opener can efficiently prove in zero-knowledge the correctness of the opening. Furthermore, both schemes are exculpable, i.e., a malicious group manager can frame the users by "signing on behalf" of the group members, since the signing credentials of the scheme do not contain any component which is only known to the members. Finally, Boyen-Waters group signature is based on a composite order bilinear group, making it much less efficient than its counterpart using prime order bilinear groups in general. Although Lewko [14] has proposed a technique to simulate the features of composite order bilinear groups in a prime order group, it is still inefficient because the technique uses a vector of elements of a prime order group to simulate just one element of a composite order bilinear group.

The setting of dynamic groups was formalized by Bellare, Shi and Zhang [15] (BSZ model), accompanied by a construction based on trapdoor permutation. Groth [16] suggested the first constant-size group signature scheme without random oracles in the BSZ model, but the constant is huge. Groth [17] proposed a practical and fully anonymous group signature without random oracles. Full anonymity refers to the availability of opening oracle to the adversary (cf., [11, 12]). Abe *et al.* [18] proposed group signatures with efficient concurrent join by making use of structure-preserving signatures.

Recently, Bootle et al. [19] studied fully dynamic group signatures. To support a fully dynamic group, their construction is taking the idea of having a membership list to the extreme, which simply allows a public database to be updatable whenever there is a new member joining the group.

The notion of linkability has also been studied in the ad hoc (ring signature) settings (*e.g.,* [20, 21]).

2 Preliminaries

2.1 Notations

If S is a set, $s \overset{\$}{\leftarrow} S$ 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 $z \overset{\$}{\leftarrow} \mathcal{A}(x, y, \cdots)$ 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 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 a probabilistic polynomial-time algorithm to decide whether $g^c = g^{ab}$ or not.*

Assumption 2 (SXDH) *For a bilinear group $\mathcal{G} = (\mathbb{G},\ \mathbb{H},\ \mathbb{G}_T,\ e,\ p,\ g,\ h)$ 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 a 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 [2, 3], 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*) [15, 2]. An issuer is responsible to enroll members, while an opener is responsible for recovering the identities of signatures signed by the users enrolled, whenever need arises. A *hidden identity-based signature* (HIBS) scheme $\mathcal{HIBS}$ is defined based on a set of nine algorithms (KGen, UKGen, Reg, $\mathsf{RegCheck}$, Sign, Verify, Open, Judge, $\mathsf{Dispute}$).

- $\mathsf{KGen}(1^\lambda) \rightarrow (\mathsf{gpk}, \mathsf{ik}, \mathsf{ok})$: The *group key generation* algorithm takes as input the security parameter λ and outputs the *group public key* gpk, the *issuer key* ik which is provided to the issuer, and the *opening key* ok which is provided to the opener.
- $\mathsf{UKGen}(1^\lambda, \mathsf{ID}) \rightarrow (\mathsf{upk}_\mathsf{ID}, \mathsf{usk}_\mathsf{ID})$: 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* $(\mathsf{upk}_\mathsf{ID}, \mathsf{usk}_\mathsf{ID})$.
- $\mathsf{Reg}(\mathsf{gpk}, \mathsf{ik}, \mathsf{ID}, \mathsf{upk}_\mathsf{ID}) \rightarrow \mathsf{cert}_\mathsf{ID}$: 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 upk_ID to return a *user membership certificate* $\mathsf{cert}_\mathsf{ID}$.
- $\mathsf{RegCheck}(\mathsf{gpk}, \mathsf{ID}, \mathsf{upk}_\mathsf{ID}, \mathsf{cert}_\mathsf{ID}) \rightarrow 0/1$: The *registration checking* algorithm[3] takes as input the group public key gpk, a user identity ID, a user personal public and private key pair $(\mathsf{upk}_\mathsf{ID}, \mathsf{usk}_\mathsf{ID})$, 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 $\mathsf{RegCheck}(\mathsf{gpk}, \mathsf{ID}, \mathsf{upk}_\mathsf{ID}, \mathsf{cert}_\mathsf{ID}) = 1$.
- $\mathsf{Sign}(\mathsf{gpk}, \mathsf{ID}, \mathsf{cert}_\mathsf{ID}, \mathsf{usk}_\mathsf{ID}, m) \rightarrow \sigma$: 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 usk_ID, and a message m to return a signature σ.
- $\mathsf{Verify}(\mathsf{gpk}, m, \sigma) \rightarrow 0/1$: 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 $\mathsf{Verify}(\mathsf{gpk}, m, \sigma) = 1$.
- $\mathsf{Open}(\mathsf{gpk}, \mathsf{ok}, m, \sigma) \rightarrow (\mathsf{ID}, \omega)$: 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 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 user personal public key upk_ID, the user membership certificate $\mathsf{cert}_\mathsf{ID}$, which are both provided by the user, and

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

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 [2, 3], we further equip our HIBS with a judge algorithm Judge() to protect against a fully corrupt opener. Compared to that of [15], the Join()/Issue() algorithm [15] is replaced with Reg() and RegCheck() algorithms for the sake of simplicity.

Relation to Existing Notions. Similar to the idea of Galindo, Herranz, and Kiltz [9], a major difference of identity-based signature, from the traditional signatures based on public-key certificate or 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. 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.

While it may make sense for the original notion of identity-based signature, especially under such an efficiency point of view, this is exactly the purpose of this work to show that such construction can be constructed in a modular and efficient manner. On the other hand, we stick with the original naming of Kiayias and Zhou [2]. 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.

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.

- $\mathsf{Link}(\mathsf{gpk}, m, \sigma_1, \sigma_2) \to 0/1$: 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 Verify()) generated by the same signer, this algorithm outputs 1; otherwise, it outputs 0.

This linking feature can be used to identify double-posting without opening the signer's identity.

We now briefly consider the correctness notions for HIBS. Correctness includes *registration correctness* (with respect to Reg() and RegCheck() algorithms), *signing correctness* (with respect to Sign() and Verify() algorithms), *opening correctness* (with respect to Open() and Judge() algorithms), and *dispute correctness*. The first three can be easily adapted from those of [2, 15], while the last one requires the $\mathsf{Dispute}()$ algorithm to function correctly when a suspected user was indeed framed.

3.3 Security Notions for HIBS

We strengthen the notions due to Kiayias and Zhou [2, 3], and consider the "strongest" achievable notions (following [15]): anonymity, traceability, and non-frameability. The security notions in [2, 3], namely, security against misidentification forgery and exculpability attacks (formally given in [3]), has been shown to be implied by traceability and non-frameability [19].

Similar to the study of Kiayias and Zhou [2, 3], 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 be given 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 $\mathsf{cert}_{\mathsf{ID}} \leftarrow \mathsf{Reg}(\mathsf{gpk}, \mathsf{ik}, \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}})$, sets $\mathtt{MSG}_{\mathsf{ID}} \leftarrow \emptyset$, and sets $\mathtt{HU} \leftarrow \mathtt{HU} \cup \{\mathsf{ID}\}$.
- $\mathsf{SignO}(\mathsf{ID}, \mathsf{cert}_{\mathsf{ID}}, m)$: 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 $\mathsf{Reg}()$, 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 $\mathtt{HU} \leftarrow \mathtt{HU}/\{\mathsf{ID}\}$, and returns $(\mathsf{usk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}})$.
- $\mathsf{OpenO}(m, \sigma)$: 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 $\mathbf{Exp}^{\text{cca-anon}}_{\mathcal{HIBS}}(\mathcal{A})$
    $(\mathsf{gpk}, \mathsf{ik}, \mathsf{ok}) \xleftarrow{\$} \mathsf{KGen}(1^\lambda)$; $\mathtt{CU} \leftarrow \emptyset$; $\mathtt{HU} \leftarrow \emptyset$;
    $(\mathsf{ID}_0, \mathsf{ID}_1, m, \mathsf{s}) \xleftarrow{\$} \mathcal{A}^{\mathsf{CorruptO}(\cdot), \mathsf{RegO}(\cdot), \mathsf{OpenO}(\cdot,\cdot)}(\text{'}\mathsf{find}\text{'}, \mathsf{gpk}, \mathsf{ik})$
    $b \xleftarrow{\$} \{0, 1\}$; $\sigma \xleftarrow{\$} \mathsf{Sign}(\mathsf{gpk}, \mathsf{ID}_b, \mathsf{cert}_{\mathsf{ID}_b}, \mathsf{usk}_{\mathsf{ID}_b}, m)$
    $b' \xleftarrow{\$} \mathcal{A}^{\mathsf{CorruptO}(\cdot,\cdot), \mathsf{RegO}(\cdot), \mathsf{OpenO}(\cdot,\cdot)}(\text{'}\mathsf{guess}\text{'}, \sigma, \mathsf{s})$
    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

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

This notion is called CCA since the opening of a group signature just corresponds to the chosen ciphertext attack which features a decryption oracle to the adversary of public-key encryption. Naturally, one can also consider the variant of 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 [3] 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 $\mathbf{Exp}^{\text{weak-anon}}_{\mathcal{HIBS}}(\mathcal{A})$
    $(\mathsf{gpk}, \mathsf{ik}, \mathsf{ok}) \xleftarrow{\$} \mathsf{KGen}(1^\lambda)$; $\mathtt{CU} \leftarrow \emptyset$; $\mathtt{HU} \leftarrow \emptyset$;
    $(\mathsf{ID}_0, \mathsf{ID}_1, m, \mathsf{s}) \xleftarrow{\$} \mathcal{A}^{\mathsf{CorruptO}(\cdot),\mathsf{RegO}(\cdot),\mathsf{OpenO}(\cdot,\cdot)}(\text{‘}\mathsf{find}\text{’}, \mathsf{gpk}, \mathsf{ik})$
    if $m \in \mathtt{MSG}_{\mathsf{ID}_0} \vee m \in \mathtt{MSG}_{\mathsf{ID}_1}$ then abort
    $b \xleftarrow{\$} \{0,1\}; \sigma \xleftarrow{\$} \mathsf{Sign}(\mathsf{gpk}, \mathsf{ID}_b, \mathsf{cert}_{\mathsf{ID}_b}, \mathsf{usk}_{\mathsf{ID}_b}, m)$
    $b' \xleftarrow{\$} \mathcal{A}^{\mathsf{CorruptO}(\cdot,\cdot),\mathsf{RegO}(\cdot),\mathsf{OpenO}(\cdot,\cdot)}(\text{‘}\mathsf{guess}\text{’}, \sigma, \mathsf{s})$
    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 [3].

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 issuer's consent. 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 $\mathbf{Exp}^{\text{link}}_{\mathcal{LHIBS}}(\mathcal{A})$
    $(\mathsf{gpk}, \mathsf{ik}, \mathsf{ok}) \xleftarrow{\$} \mathsf{KGen}(1^\lambda)$; $\mathtt{CU} \leftarrow \emptyset$; $\mathtt{HU} \leftarrow \emptyset$;
    $(m, \mathsf{ID}, \sigma_0, \sigma_1) \xleftarrow{\$} \mathcal{A}^{\mathsf{CorruptO}(\cdot),\mathsf{SignO}(\cdot,\cdot),\mathsf{RegO}(\cdot)}(\mathsf{gpk}, \mathsf{ik}, \mathsf{ok})$
    if $\exists i \in \{0,1\}$, s.t. $\mathsf{Verify}(\mathsf{gpk}, m, \sigma_i) = 0$
        then return 0
    if $\mathsf{Link}(\mathsf{gpk}, m, \sigma_0, \sigma_1)$
        then return 1
    return 0
```

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

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

```
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 $\omega$ 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 $(m, \sigma)$
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 $(\mathsf{ID}, \omega)$
Alg $\mathsf{Dispute}(\mathsf{gpk}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}}, (\mathsf{ID}, \omega))$
  parse $\omega$ 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 $\mathcal{HIBS}$ = (KGen, UKGen, Reg, RegCheck, Sign, Verify, Open, Judge, Dispute): R is the common reference string for the underlying proof system (P, V).

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 [22] and formally proven secure by Bellare, Neven, and Namprempre [23]. To construct our generic HIBS, we "hide" the whole signing process with an encryption and prove so in an NIZK (or NIWI) sense.[4]

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

```
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 $(\mathsf{sk}, \mathsf{sk}_F)$
  $T \leftarrow \mathsf{FEval}(\mathsf{sk}_F, (\mathsf{ID}, m))$
  $\sigma' \leftarrow \mathsf{sig}(\mathsf{sk}, m)$
  $C \leftarrow \mathsf{Enc}(\mathsf{ek}, r, (\sigma', \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}}))$
  $\pi \xleftarrow{\$} P(R, (m, \mathsf{VK}, \mathsf{ek}, C, T),$
        $(r, \sigma', \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}}, \mathsf{sk}_F))$
  $\sigma \leftarrow (C, \pi, T)$
  return $(m, \sigma)$

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

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 $\sigma_i$ as $(C_i, \pi_i, T_i)$
  if $T_1 = T_2$ then return $1$;
  else return $0$
```

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

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 generates a signature on the signer's identity and public key with the GM's signing key, 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 signer's identity.

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 $\mathcal{E} = (\mathsf{EKGen}, \mathsf{Enc}, \mathsf{Dec})$ be a public key encryption scheme. Let (P, V) be an NIZK (or NIWI) proof system. We define an HIBS scheme $\mathcal{HIBS}$ in Figure 1.

In particular, the underlying language for the proof system (P, V) is defined as

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

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 Figure 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, $\mathcal{E}$ is IND-CCA-secure (IND-CPA-secure), and the proof system (P, V) is adaptively sound, adaptively zero-knowledge, and one-time simulation-sound.*

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.

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

$$\begin{aligned}\mathcal{L} :=\{&(m, \mathsf{VK}, \mathsf{ek}, C, T)|\exists(r, \sigma, \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}}, h^{x_1}, h^{x_2}, h^{\frac{1}{y}})\\ &[\mathsf{VFY}(\mathsf{VK}, (\mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}), \mathsf{cert}_{\mathsf{ID}}) = 1 \wedge \mathsf{vfy}(vk_{\mathsf{ID}}, m, \sigma) = 1\\ &\wedge C = \mathsf{Enc}(\mathsf{ek}, r, (\sigma, \mathsf{ID}, \mathsf{upk}_{\mathsf{ID}}, \mathsf{cert}_{\mathsf{ID}}))\\ &\wedge T = \mathsf{FEval}(\mathsf{sk}_{\mathsf{ID}}, (\mathsf{ID}, m))]\}.\end{aligned}$$

Theorem 2. *$\mathcal{LHIBS}$ in Figure 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, $\mathcal{E}$ 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 [24]. 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 [18] as the first-level signature (i.e., $\mathcal{DS}_1$) to sign the second-level signature (i.e., $\mathcal{DS}_2$) 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 [25] as the second-level scheme (for $\mathcal{DS}_2$), while the third instantiation uses a signature scheme by Yuen *et al.* [26] 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 verified 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 [3], our two instantiations of HIBS in our stronger model (i.e., Inst1 and Inst2), and the most efficient group signature scheme (as a baseline) that provides concurrent security, CCA-anonymity, and non-frameability [27]. The size in kilobytes (KB) of the group elements are measured on "MNT159" [28] curve.

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.* [27] 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 [29], which fits with the SXDH setting.

The resulting CPA-anonymous HIBS Inst1 consists of 43 group elements and 1 scalar value (in $\mathbb{Z}_q$). Following the existing approach [17], the proposed instantiation Inst1 can achieve CCA-anonymity with extra 15 group elements. Thus, the resulting CCA-anonymous HIBS Inst1 consists of 58 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 standard model. The first level signature $\mathcal{DS}_1$ can be proven secure basing on static assumptions in 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 [30].

We select the signature scheme from [30] 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 [31], 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. The CCA-anonymous HIBS Inst2 obtained therefore consists of 174 group elements and 1 scalar value.

5.3 Instantiation 3

Our third HIBS instantiation Inst3 replaces the second level signature, BB signature, with a dual form exponent inversion signature scheme proposed by Yuen *et al.* [26]. 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 [30] 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

Scheme	RO	Hidden-ID	Non-frame.	Anon.	Concur.	Assumption	Sig. Size	Length
KZ [3]	yes	yes	yes	CCA	no	DCR; S-RSA	$\approx 3^{[N]} + 16^{[n]}$	7.33KB
AHO [27]	no	no	yes	CCA	yes	q-SFP	$55 + 1^{[q]}$	1.09KB
Inst1	no	yes	yes	CCA	yes	q-SFP; q-SDH	$58 + 1^{[q]}$	1.15KB
Inst2	no	yes	yes	CCA	yes	DLIN; q-SDH	$174 + 1^{[q]}$	3.41KB
Inst3	no	yes	yes	CCA	yes	DLIN	$489 + 1^{[q]}$	9.58KB

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)

ensure a signer's well-behavior (or 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. [32] 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: EuroCrypt, Springer (1991) 257–265
2. Kiayias, A., Zhou, H.S.: Hidden identity-based signatures. In: Financial Cryptography, Springer (2007) 134–147
3. Kiayias, A., Zhou, H.: Hidden identity-based signatures. IET Information Security **3**(3) (2009) 119–127
4. Liu, X., Xu, Q.l.: Improved hidden identity-based signature scheme. In: ICIS. (2010)
5. Liu, X., Xu, Q.l.: Practical hidden identity-based signature scheme from bilinear pairings. In: ICCSIT. (2010)
6. Kiayias, A., Yung, M.: Group signatures with efficient concurrent join. In: EuroCrypt, Springer (2005) 198–214
7. Chow, S.S.: Real traceable signatures. In: Selected Areas in Cryptography, Springer (2009) 92–107
8. Franklin, M., Zhang, H.: Unique group signatures. In: ESORICS, Springer (2012) 643–660
9. Galindo, D., Herranz, J., Kiltz, E.: On the generic construction of identity-based signatures with additional properties. In: AsiaCrypt, Springer (2006) 178–193
10. Bellare, M., Micciancio, D., Warinschi, B.: Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In: EuroCrypt, Springer (2003) 614–629
11. Boyen, X., Waters, B.: Compact group signatures without random oracles. In: EuroCrypt, Springer (2006) 427–444
12. Boyen, X., Waters, B.: Full-domain subgroup hiding and constant-size group signatures. In: PKC, Springer (2007) 1–15
13. Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: CRYPTO, Springer (2004) 41–55
14. Lewko, A.: Tools for simulating features of composite order bilinear groups in the prime order setting. In: EuroCrypt, Springer (2012) 318–335
15. Bellare, M., Shi, H., Zhang, C.: Foundations of group signatures: The case of dynamic groups. In: Topics in Cryptology (CT-RSA), Springer (2005) 136–153
16. Groth, J.: Simulation-sound NIZK proofs for a practical language and constant size group signatures. In: AsiaCrypt, Springer (2006) 444–459
17. Groth, J.: Fully anonymous group signatures without random oracles. In: AsiaCrypt, Springer (2007) 164–180
18. Abe, M., Fuchsbauer, G., Groth, J., Haralambiev, K., Ohkubo, M.: Structure-preserving signatures and commitments to group elements. In: CRYPTO, Springer (2010) 209–236
19. Bootle, J., Cerulli, A., Chaidos, P., Ghadafi, E., Groth, J.: Foundations of fully dynamic group signatures. In: Applied Cryptography and Network Security (ACNS). (2016) 117–136
20. Franklin, M., Zhang, H.: Unique ring signatures: A practical construction. In: Financial Cryptography and Data Security 2013. Volume LNCS 7859. (2013) 162–170

21. J.K. Liu, V.W., Wong., D.: Linkable spontaneous anonymous group signature for ad hoc groups. In: ACISP 2004
22. Shamir, A.: Identity-based cryptosystems and signature schemes. In: CRYPTO, Springer (1984) 47–53
23. Bellare, M., Namprempre, C., Neven, G.: Security proofs for identity-based identification and signature schemes. In Cachin, C., Camenisch, J.L., eds.: EuroCrypt, Springer (May 2004) 268–286
24. Groth, J., Sahai, A.: Efficient non-interactive proof systems for bilinear groups. In: EuroCrypt, Springer (2008) 415–432
25. Boneh, D., Boyen, X.: Short signatures without random oracles. In: EuroCrypt, Springer (2004) 56–73
26. Yuen, T.H., Chow, S.S.M., Zhang, C., Yiu, S.M.: Exponent-inversion signatures and IBE under static assumptions. Cryptology ePrint Archive, Report 2014/311 (2014) http://eprint.iacr.org/.
27. Abe, M., Haralambiev, K., Ohkubo, M.: Signing on Elements in Bilinear Groups for Modular Protocol Design. Cryptology ePrint Archive, Report 2010/133 (2010) http://eprint.iacr.org/.
28. Miyaji, A., Nakabayashi, M., Takano, S.: New explicit conditions of elliptic curve traces for FR-reduction. IEICE Trans. Fund. **84**(5) (2001) 1234–1243
29. ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. In: CRYPTO, Springer (1985) 10–18
30. Abe, M., Chase, M., David, B., Kohlweiss, M., Nishimaki, R., Ohkubo, M.: Constant-size structure-preserving signatures: Generic constructions and simple assumptions. In: AsiaCrypt, Springer (2012) 4–24
31. Camenisch, J., Haralambiev, K., Kohlweiss, M., Lapon, J., Naessens, V.: Structure preserving CCA secure encryption and applications. In: AsiaCrypt, Springer (2011) 89–106
32. 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) (2011) 29