Identity-Committable Signatures and Their Extension to Group-Oriented Ring Signatures

Cheng-Kang Chu and Wen-Guey Tzeng
Department of Computer Science, National Chiao Tung University,
Hsinchu, Taiwan 30050
Email:{ckchu,wgtzeng}@cs.nctu.edu.tw

Abstract

The identity of "Deep Throat", a pseudonym of the information source in the Watergate scandal, remained mysterious for more than three decades. In 2005, an ex-FBI official claimed that he was the anonymous source. Nevertheless, some are still inconvinced.

In this paper, we introduce a new notion of identity-committable signatures (ICS) to ensure the anonymity of "Deep Throat" inside a group. A member of an organization can sign a message on behalf of himself (regular signature) or the organization (identity-committed signature). In the latter case, the signer's identity is hidden from anyone, and can be opened by himself only. We describe the requirements of ICS and give the formal definition of it. Then we extend the notion of ICS to *group-oriented ring signatures* (GRS) which further allow the signer to hide his identity behind multiple groups. We believe a GRS scheme is more efficient and practical than a ring signature scheme for leaking secrets. Finally, we provide concrete constructions of ICS and GRS with *information-theoretic* anonymity, that is, the identity of the signer is fully-protected.

Keywords: group signatures, ring signatures, anonymous signatures

1 Introduction

In the early of 1970s, Woodward and Bernstein, two reporters of Washington Post, broke many stories that eventually led to the resignation of President Richard M. Nixon. This is the famous Watergate scandal in the history of the United States. The information source, assumed the pseudonym "Deep Throat", remained confidential for more than three decades. Woodward and Bernstein guaranteed that they would not reveal Deep Throat's identity unless he is willing to or he died. It is not till 2005 that, Felt, the ex-FBI No. 2, claimed that he was the anonymous source for Watergate affairs.

From this story, we learn some characteristics of being a "Deep Throat":

- Full-Anonymity. Keeping identity anonymous is the most important thing for Deep Throat. Even the president can not trace the information source. Felt is fortunate that the reporters are dependable. If they were threatened or bribed, the identity of Deep Throat may be exposed much early.
- Group Authenticity. Although we can not learn the identity of Deep Throat, we should be able to verify that the information comes from a specific organization for these inside stories. The two reporters described above knew that the information from Felt is trustworthy because Felt was working in FBI at that time.
- Self-Identifiability. After the event, in order to benefit from the identity or witness in the court, Deep Throat should be able to prove that he is the information source. In fact, although the Washington Post confirmed that Felt was Deep Throat, some people still question that.

Based on these characteristics, we try to construct a signature scheme in the following scenario.

> *David, an employee of a government organization, owns a personal signing key issued by the organization. He uses this key to sign official documents. One day, he discovers a startling scandal inside the organization. He decides to be a "Deep Throat", i.e. anonymously expose it to people. So he uses his signing key to generate a signature on a report of the scandal on behalf of the organization rather than his personal identity, and sends it to a journalist. The journalist first verifies that the information indeed comes from someone inside the organization, and then publishes it. No one, including the chief of the organization who owns the master secret key, can determine the identity of Deep Throat. After that, David continues his work in that organization as usual. Someday, if David wishes to, he can exhibit a witness identifying himself as Deep Throat.*

Consider the existent signature schemes which may achieve this objective. For group signatures, there is a group manager with identifiability. David will be afraid to expose the scandal. For ring signatures, David needs to collect all public keys (or identities) of the staff in the organization to form the ring. The computation and communication costs are too large to be practical. Besides, in some secret agency, the identities of its staff are classified. David may not be able to get the public keys of other secret agents.

In this paper, we propose a new notion of identity-committable signatures (ICS) which fits for the above scenario. A member of an organization can sign a message on behalf of himself (regular signature) or the organization (identity-committed signature). In the latter case, the signer's identity is hidden from anyone, and can be opened by himself only. We describe the requirements of ICS and give the formal definition of it. Then we extend the

notion of ICS to *group-oriented ring signatures* (GRS) which further allow the signer to hide his identity behind multiple groups. Deep Throat who works in FBI can sign secrets on behalf of numerous related organizations such as FBI, CIA, NSA, etc. The size of the signature is only linear to the number of included organizations. Since the signer can include the whole members of a group at a time, a GRS scheme is more efficient and practical than general ring signature schemes.

Related Works. In fact, ICS are intermediate between group signatures and ring signatures. We consider some concrete constructions of these two signature schemes:

- Group signatures: The notion of group signatures was introduced by Chaum and Van Heyst [17]. Since then, many other schemes were proposed [18, 15, 12, 13, 3, 6, 4, 9, 25, 11]. Some works mentioned separability [26, 14], where the identifying ability can be designated to a revocation manager. It is possible to use such separable group signature to construct ICS, but we try to find more direct and more efficient solutions. Some group signature schemes with traceability [24, 31] give the signer self-identifiability, but there is still a group manager identifying the signer.

- Ring signatures: Rivest, Shamir, and Tauman [33, 34] first introduced the notion of ring signatures. Subsequently, many constructions were proposed under various settings of signing keys [36, 1, 21, 20, 8]. Some works also mentioned the self-identifiability [33, 29]. But in their constructions, this property either needs to store witnesses with size linear to the number of non-signers in the ring, or only guarantees the computational anonymity. Linkable ring signatures [35, 27, 28] stress the ability of checking whether two ring signatures are signed by the same signer. There are some ID-based constructions [36, 22, 19, 30, 5] and constant-size constructions [20, 30, 5]. All these schemes need a private key generator (PKG) with a master secret. In fact, we can regard signers under the same PKG as the members of a group. So signing on behalf of the whole group is a better idea than signing on behalf of a list of group members. Even for constant-size schemes, the computation cost of the signing and verifying procedures are linear to the number of ring members.

2 Definition of ICS

In this section we give the formal definition of identity-committable signatures.

2.1 Components

An identity-committable signature scheme consists of the following algorithms.

- **Setup**(1^λ): For the security parameter in unary, 1^λ, the algorithm chooses a master secret key K and outputs the corresponding public parameter μ.

- **Extract**(μ, ID, K): Output the private key SK for the identity ID.
- **Sign**(μ, m, SK): Output the regular signature σ on message m.
- **Verify**(μ, ID, m, σ): If σ is signed by ID's private key on m, output 'accept'; otherwise, output 'reject'.
- **IC-Sign**(μ, m, SK): Output an identity-committed signature σ_{IC} on message m and a witness ω for identifying.
- **IC-Verify**(μ, m, σ_{IC}): If σ_{IC} is signed by a private key of the organization on m, output 'accept'; otherwise output 'reject'.
- **Identify**$(\mu, ID, \omega, \sigma_{IC})$: If σ_{IC} is a valid identity-committed signature and ω opens σ_{IC} to ID, output 'valid'; otherwise output 'invalid'.

Let PKG be the private key generator of an organization. PKG first runs **Setup**, and publishes the public parameters. Then it issues the private key for each organization member by performing **Extract**. Each member uses **Sign** and **Verify** algorithms for regular signing and verification. When a member tries to anonymously sign a message, he performs **IC-Sign** to get the identity-committed signature and a witness. He outputs the signature to the verifier such that the verifier can verify it via the **IC-Verify** algorithm. The signer holds the witness secretly for later revealing his identity if he wants. Someday, he can execute **Identify** by using the witness to prove that he is the original signer.

2.2 Security Definition

Bellare et al. [7] characterize the fundamental properties of group signatures in terms of two crucial security requirements. But the two requirements are not sufficient for ICS. Informally speaking, an identity-committable signature scheme should satisfy the following properties.

1. Completeness: With the private key issued by the PKG of an organization, one can sign messages on behalf of himself or the organization. In the latter case, he can prove that he is the original signer.
2. Unforgeability: The scheme should be secure against existential forgery of regular signature under adaptively chosen message and identity attack.
3. ICS-Unforgeability: For someone outside the organization, the scheme should be secure against existential forgery of identity-committed signature under adaptively chosen message attack.

4. ICS-Anonymity: No one but the signer himself can identify the signer of an identity-committed signature.

5. ICS-Binding: The identity-committed signature can only be opened to the original signer.

Formally, we have the following definition for an identity-committable signature scheme.

Definition 1 (Identity-Committable Signatures) *Define the following oracles which can be queried adaptively by any probabilistic polynomial-time algorithm (PPTA) $\mathcal{A}$ against the challenger $\mathcal{C}$.*

- *$Extract^{\mathcal{A}}(ID)$: $\mathcal{C}$ returns the private key for identity ID.*
- *$Sign^{\mathcal{A}}(ID, m)$: $\mathcal{C}$ returns a regular signature of identity ID on message m.*
- *$IC\text{-}Sign^{\mathcal{A}}(ID, m)$: $\mathcal{C}$ returns an identity-committed signature on m along with a witness which identifies ID as the signer.*

An identity-committable signature scheme is secure if it meets the following requirements.

- ***Completeness.*** *For any m and ID, it holds that*

$$\Pr[\textbf{\textit{Verify}}(\mu, ID, m, \sigma) = accept : \sigma \leftarrow \textbf{\textit{Sign}}(\mu, m, SK); \\ SK \leftarrow \textbf{\textit{Extract}}(\mu, ID, K); (\mu, K) \leftarrow \textbf{\textit{Setup}}(1^{\lambda})] = 1$$

  and

$$\Pr[\textbf{\textit{IC-Verify}}(\mu, m, \sigma_{IC}) = accept, \textbf{\textit{Identify}}(\mu, ID, \omega, \sigma_{IC}) = valid : \\ (\sigma_{IC}, \omega) \leftarrow \textbf{\textit{IC-Sign}}(\mu, m, SK); SK \leftarrow \textbf{\textit{Extract}}(\mu, ID, K); \\ (\mu, K) \leftarrow \textbf{\textit{Setup}}(1^{\lambda})] = 1.$$

- ***Unforgeability.*** *Given the public parameters and access of all oracles, no PPTA $\mathcal{A}$ can output a valid regular signature (ID, m, σ) with non-negligible probability if $Extract^{\mathcal{A}}(ID)$ and $Sign^{\mathcal{A}}(ID, m)$ are never queried.*
- ***ICS-Unforgeability.*** *Given the public parameters and access of Sign and IC-Sign oracles, no PPTA $\mathcal{A}$ can output a valid identity-committed signature (m, σ_{IC}) with non-negligible probability if $Sign^{\mathcal{A}}(ID^*, m)$ and $IC\text{-}Sign^{\mathcal{A}}(ID^*, m)$ are never queried for any ID^*.*
- ***ICS-Anonymity.*** *Given the public parameters and access of all oracles, no PPTA $\mathcal{A}$ has a non-negligible advantage against a challenger $\mathcal{C}$ in the following game:*

1. *$\mathcal{A}$ chooses two identities ID_0, ID_1 and a message m, and sends them to $\mathcal{C}$.*
2. *$\mathcal{C}$ chooses $b \in_R \{0,1\}$, and computes an identity-committed signature σ_{IC} on m by ID_b's private key. Then $\mathcal{C}$ sends σ_{IC} to $\mathcal{A}$.*
3. *$\mathcal{A}$ outputs the guess b'. If $b' = b$, $\mathcal{A}$ wins the game.*

- ***ICS-Binding.*** *Given the public parameters and access of all oracles, no PPTA $\mathcal{A}$ can output a valid identity-committed signature (m, σ_{IC}) and two witnesses (ID, ω) and (ID', ω') with non-negligible probability.*

3 Definition of GRS

In this section we give the formal definition of group-oriented ring signatures.

3.1 Components

A group-oriented ring signature scheme consists of the following algorithms.

- **Setup**(1^λ): For the security parameter 1^λ, the algorithm chooses a master secret key K and outputs the corresponding public parameter μ.
- **Extract**(μ, ID, K): Output the private key SK for the identity ID.
- **GR-Sign**(L, m, SK): For the list L of public parameters of all groups, output a group-oriented ring signature σ_{GR} on message m.
- **GR-Verify**(L, m, σ_{GR}): If σ_{GR} is signed by a private key of a group in the list L, output 'accept'; otherwise output 'reject'.

Each PKG of groups first performs **Setup**, and publish the public parameters. It also issues the private key for each group member by performing **Extract**. When a signer wants to sign messages on behalf of some groups, he takes the public parameters of these groups to form the list L. Then the signer executes **GR-Sign** to generate the group-oriented ring signature. The verifier also takes the list L, and executes **GR-Verify** to confirm that σ_{GR} is signed by a member of one group in L.

3.2 Security Definition

We have the following definition for a group-oriented ring signature scheme.

Definition 2 (Group-Oriented Ring Signatures) *Define the following oracles which can be queried adaptively by any PPTA $\mathcal{A}$ against the challenger $\mathcal{C}$ with a list L of public parameters.*

- *$Extract^{\mathcal{A}}(i, ID)$: $\mathcal{C}$ returns the private key for identity ID of the i-th group in L.*
- *$GR\text{-}Sign^{\mathcal{A}}(i, L', ID, m)$: $\mathcal{C}$ returns a group-oriented ring signature, signed by identity ID of the i-th group in L, on m for the list L'. Note that L' must contain the i-th parameter of L, but the other parameters of L' need not be in the list L.*

A group-oriented ring signature scheme is secure if it meets the following requirements.

- ***Completeness.*** *For any m, ID and L, it holds that*

$$\Pr[\textbf{\textit{GR-Verify}}(L, m, \sigma_{GR}) = accept : \sigma_{GR} \leftarrow \textbf{\textit{GR-Sign}}(L, m, SK); \\ SK \leftarrow \textbf{\textit{Extract}}(\mu, ID, K); (\mu, K) \leftarrow \textbf{\textit{Setup}}(1^{\lambda}); \mu \in L] = 1.$$

- ***Unforgeability.*** *Given a list of public parameters $L = (\mu_1, \ldots, \mu_l)$ and access of all oracles, let C be the set of $\mu_i \in L$ where $Extract^{\mathcal{A}}(i, ID^*)$ is queried for any ID^*. No PPTA $\mathcal{A}$ can output a valid group-oriented ring signature (L^*, m, σ_{GR}) with non-negligible probability if $L^* \subseteq L \backslash C$ and $GR\text{-}Sign^{\mathcal{A}}(i^*, L^*, ID^*, m)$ is never queried for any i^* and ID^*.*
- ***Anonymity.*** *Given a list of public parameters $L = (\mu_1, \ldots, \mu_l)$ and access of all oracles, no PPTA $\mathcal{A}$ has a non-negligible advantage against a challenger $\mathcal{C}$ in the following game:*
  1. *$\mathcal{A}$ chooses two identities $(i_0, ID_0), (i_1, ID_1)$, a list L^* and a message m, where $\mu_{i_0}, \mu_{i_1} \in L^*$, and sends them to $\mathcal{C}$.*
  2. *$\mathcal{C}$ chooses $b \in_R \{0, 1\}$, and computes a group-oriented ring signature σ_{GR} on m for L^* by the private key of ID_b of the i_b-th group in L. Then $\mathcal{C}$ sends σ_{GR} to $\mathcal{A}$.*
  3. *$\mathcal{A}$ outputs the guess b'. If $b' = b$, $\mathcal{A}$ wins the game.*

4 Concrete Constructions

In this section we first think of a generic construction of ICS and then propose specific constructions of ICS and GRS.

4.1 Generic ICS Construction

We first provide a generic ICS scheme from an ID-based signature scheme and a commitment scheme. The signature scheme $\Sigma = (\mathsf{Setup}_\Sigma, \mathsf{Extract}_\Sigma, \mathsf{Sign}_\Sigma, \mathsf{Verify}_\Sigma)$ is defined as the regular signature part of ICS components (Section 2.1). The commitment scheme $\Gamma = (\mathsf{Commit}_\Gamma, \mathsf{Reveal}_\Gamma)$ is defined as follows.

- $\mathsf{Commit}_\Gamma(\sigma)$: For a secret σ, output a committed value γ and a witness ω.
- $\mathsf{Reveal}_\Gamma(\gamma, \omega)$: If γ is the commitment of σ, and ω is the corresponding witness, output the secret σ.

There are two requirements for a secure commitment scheme:

1. Hiding: Before reveal step, the receiver does not learn anything about the committed value.
2. Binding: The sender cannot change the committed value after the commit step.

The organization first designates a special ID_G as the group identity, and issues the corresponding private key SK_G along with personal private keys to all members. When a member wants to generate an identity-committed signature, he uses the key SK_G to sign the message and commits his regular signature on that message. In the **Identify** process, the signer reveals the regular signature from the commitment. The detail is given as follows.

- **Setup**(1^λ): Perform $\mathsf{Setup}_\Sigma(1^\lambda)$ to get the public parameters μ and master secret key K. Define a group identity ID_G which differs from all members. Output (μ, ID_G, K).
- **Extract**(μ, ID, K): Perform $\mathsf{Extract}_\Sigma(\mu, ID_G, K)$ and $\mathsf{Extract}_\Sigma(\mu, ID, K)$ to get SK_G and SK_{ID}, respectively. Output (SK_G, SK_{ID}) as the private key for identity ID.
- **Sign**(μ, m, SK_{ID}): Output the regular signature $\sigma = \mathsf{Sign}_\Sigma(\mu, m, SK_{ID})$.
- **Verify**(μ, ID, m, σ): Output the result of $\mathsf{Verify}_\Sigma(\mu, ID, m, \sigma)$.
- **IC-Sign**(μ, m, SK_G, SK_{ID}): Perform $\mathsf{Commit}_\Gamma(\sigma)$ to get a committed value γ and a witness ω, where $\sigma = \mathsf{Sign}_\Sigma(\mu, m, SK_{ID})$. Then compute $\sigma_G = \mathsf{Sign}_\Sigma(\mu, m||\gamma, SK_G)$. Output the identity-committed signature $\sigma_{IC} = (\sigma_G, \gamma)$ and the witness ω.
- **IC-Verify**(μ, m, σ_{IC}): Parse the identity-committed signature σ_{IC} as (σ_G, γ). Output the result of $\mathsf{Verify}_\Sigma(\mu, ID_G, m||\gamma, \sigma_G)$.
- **Identify**$(\mu, ID, \omega, \sigma_{IC})$: If $\sigma_{IC} = (\sigma_G, \gamma)$ is a valid identity-committed signature on m, then output the result of $\mathsf{Verify}_\Sigma(\mu, ID, m, \sigma)$, where $\sigma = \mathsf{Reveal}_\Gamma(\gamma, \omega)$.

Security. Completeness can be checked straightforwardly. Since the scheme makes use of Σ to generate regular signatures, unforgeability can be directly obtained from that of Σ.

Theorem 1 (Unforgeability) *If there is an algorithm $\mathcal{A}$ that forges a regular signature of our scheme under adaptively chosen message and identity attack with advantage ϵ in time t, then there is an algorithm $\mathcal{B}$ which can forge a signature of Σ under the same attack with the same advantage in time $O(t)$.*

Proof. On input the public parameters of Σ, $\mathcal{B}$ gives $\mathcal{A}$ the same public parameters along with a reserved identity ID_G. Then $\mathcal{B}$ simulates oracles queries in the following ways:

- $Extract^{\mathcal{A}}(ID)$: Send ID and ID_G to the oracle $Extract^{\mathcal{B}}$ of Σ, and return the results SK_{ID} and SK_G to $\mathcal{A}$.
- $Sign^{\mathcal{A}}(ID, m)$: Pass (ID, m) to the oracle $Sign^{\mathcal{B}}$ of Σ, and return the result signature σ to $\mathcal{A}$.
- $IC\text{-}Sign^{\mathcal{A}}(ID, m)$: Send (ID, m) to the oracle $Sign^{\mathcal{B}}$ to get σ, compute the commitment γ as the real scheme, and send the query $IC\text{-}Sign^{\mathcal{B}}(ID_G, m||\gamma)$ to get σ_G. Then return (σ_G, γ) to $\mathcal{A}$.

When $\mathcal{A}$ succeeds in forging a regular signature, $\mathcal{B}$ can output it as the forgery of Σ.[1] □

For ICS-unforgeability, the problem is reduced from forging an ID_G's signature of Σ.

Theorem 2 (ICS-Unforgeability) *If there is an algorithm $\mathcal{A}$ that forges an identity-committed signature of the above scheme under adaptively chosen message attack with advantage ϵ in time t, then there is an algorithm $\mathcal{B}$ which can forge a signature of Σ under the same attack with the same advantage in time $O(t)$.*

Proof. On input the public parameters of Σ, $\mathcal{B}$ simulates the scheme like the proof of unforgeability, except that $\mathcal{A}$ does not have the access of $Extract^{\mathcal{A}}$. When $\mathcal{A}$ outputs an identity-committed signature, $\mathcal{B}$ can output it as the forgery of Σ under identity ID_G. □

The ICS-Anonymity requirement follows the hiding property of Γ.

Theorem 3 (ICS-Anonymity) *If there is an algorithm $\mathcal{A}$ that breaks ICS-Anonymity requirement with advantage ϵ in time t, then there is an algorithm $\mathcal{B}$ which can break the binding property of Γ with the same advantage in time $O(t)$.*

Proof. The algorithm $\mathcal{B}$ plays the ICS-Anonymity game with $\mathcal{A}$ and simulates oracle access as the real scheme. When $\mathcal{A}$ sends two identities and a message, $\mathcal{B}$ computes the corresponding signatures to get the challenge committed value γ, and computes σ_{IC} as the real scheme. Finally, $\mathcal{B}$ outputs the guess of $\mathcal{A}$. We can see that $\mathcal{B}$ succeeds in distinguishing the committed values of two secrets with the same advantage. Moreover, if Γ has *perfect hiding* property, the scheme is information-theoretically anonymous. □

The ICS-Binding requirement follows the binding property of Γ.

Theorem 4 (ICS-Binding) *If there is an algorithm $\mathcal{A}$ that breaks ICS-Binding requirement with advantage ϵ in time t, then there is an algorithm $\mathcal{B}$ which can break the binding property of Γ with the same advantage in time $O(t)$.*

[1] Note that $\mathcal{A}$ will not output an ID_G's signature as the forgery because it is treated as the identity-committed signature in this scheme.

Proof. The algorithm $\mathcal{B}$ generates public parameters and simulates oracle access as the real scheme. If $\mathcal{A}$ outputs an identity-committed signature (σ_G, γ) and two witnesses $(ID, \omega), (ID', \omega')$, then $\mathcal{B}$ can use ω and ω' to open γ to different σ's. This violates the binding property. □

Although the generic scheme meets the security requirements of ICS, it is weak in some scenario while all group members use the same private key to generate identity-committed signatures. For example, if Alice signs a personal message in the private communication with Bob, Bob may use Alice's signature to generate an identity-committed signature, and then frame Alice as Deep Throat. Moreover, the generic scheme loses some additional properties such as *chosen-linkability* and *private-communicability* introduced later.

4.2 The ICS Scheme Based on Pairings

Let $\mathbb{G}$ and $\mathbb{G}_1$ be two cyclic groups of prime order p. We write $\mathbb{G}$ additively and $\mathbb{G}_1$ multiplicatively. Let $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$ is a map with the following properties:

- Bilinear: for all $P, Q \in \mathbb{G}$ and $a, b \in \mathbb{Z}$, $e(aP, bQ) = e(P, Q)^{ab}$.
- Non-degenerate: for some $P \in \mathbb{G}$, $e(P, P) \neq 1$.

We say that $\mathbb{G}$ is a bilinear group [23] if the group operations in $\mathbb{G}$ and $\mathbb{G}_1$, and the bilinear map are efficiently computable.

Our scheme needs three following complexity assumptions. The first two are the discrete logarithm problem and the computational Diffie-Hellman problem in bilinear group $\mathbb{G}$. The third one is the Diffie-Hellman problem with chosen bases.

Discrete Logarithm Problem (DLP). The discrete logarithm problem in an (additive) cyclic group $\mathbb{G}$ is, given $P, aP \in \mathbb{G}$, to output $a \in \mathbb{Z}_p$. We say that a PPTA algorithm $\mathcal{A}$ has advantage ϵ in solving DLP in $\mathbb{G}$ if

$$\Pr[\mathcal{A}(P, aP) = a : P, aP \in_R \mathbb{G}] \geq \epsilon.$$

The DL assumption in $\mathbb{G}$ holds if no PPTA $\mathcal{A}$ has non-negligible advantage ϵ in solving DL problem in $\mathbb{G}$.

Computational Diffie-Hellman Problem (CDHP). The computational Diffie-Hellman problem in an (additive) cyclic group $\mathbb{G}$ is, given $P, aP, bP \in \mathbb{G}$, to output $abP \in \mathbb{G}$. We say that a PPTA algorithm $\mathcal{A}$ has advantage ϵ in solving CDHP in $\mathbb{G}$ if

$$\Pr[\mathcal{A}(P, aP, bP) = abP : P, aP, bP \in_R \mathbb{G}] \geq \epsilon.$$

The CDH assumption in $\mathbb{G}$ holds if no PPTA $\mathcal{A}$ has non-negligible advantage ϵ in solving CDH problem in $\mathbb{G}$.

Chosen-Base CDH Problem (CB-CDHP). The chosen-base CDH problem in an (additive) cyclic group $\mathbb{G}$ is, given $P, aP, bP \in \mathbb{G}$, to output $Q, abQ \in \mathbb{G}\backslash\{e_{\mathbb{G}}\}$, where $e_{\mathbb{G}}$ is the identity of $\mathbb{G}$. We say that a PPTA algorithm $\mathcal{A}$ has advantage ϵ in solving CB-CDHP in $\mathbb{G}$ if

$$\Pr[\mathcal{A}(P, aP, bP) = (Q, abQ), Q \in \mathbb{G}\backslash\{e_{\mathbb{G}}\} : P, aP, bP \in_R \mathbb{G}] \geq \epsilon.$$

The CB-CDH assumption in $\mathbb{G}$ holds if no PPTA $\mathcal{A}$ has non-negligible advantage ϵ in solving CB-CDH problem in $\mathbb{G}$.

The Scheme. The algorithms of our construction are described as follows. The construction is based on the ID-based signature scheme proposed by Cha and Cheon [16], which can be proved secure in the random oracle model.

- **Setup**(1^λ): On input security parameter 1^λ, randomly choose two groups $\mathbb{G}$ and $\mathbb{G}_1$, a bilinear map e and a generator P defined above. Choose two random values $x, y \in \mathbb{Z}_p$, compute

  $$P_X = xP \qquad \text{and} \qquad P_Y = yP.$$

  Choose three cryptographically secure hash functions $H_1 : \{0,1\}^* \to \mathbb{G}$ and $H_2 : \{0,1\}^* \times \mathbb{G} \to \mathbb{Z}_p$. $H_2' : \{0,1\}^* \times \mathbb{G} \times \mathbb{G} \to \mathbb{Z}_p$. Output (x, y) as the master secret key and $\mu = (\mathbb{G}, \mathbb{G}_1, e, P, P_X, P_Y, H_1, H_2, H_2')$ as the public parameters.

- **Extract**(μ, ID, x, y): Let $Q_{ID} = H_1(ID)$, compute

  $$Q'_{ID} = xQ_{ID} \qquad \text{and} \qquad S_{ID} = xyQ_{ID}.$$

  Output (Q'_{ID}, S_{ID}) as the private key for identity ID.

- **Sign**$(\mu, m, Q_{ID}, Q'_{ID}, S_{ID})$: Compute

  $$U = rQ'_{ID} \qquad \text{and} \qquad V = (r + h)S_{ID},$$

  where $r \in_R \mathbb{Z}_p$ and $h = H_2(m, U)$. Output the regular signature $\sigma = (Q'_{ID}, U, V)$.

- **Verify**(μ, ID, m, σ): Parse the regular signature σ as (Q'_{ID}, U, V). Compute $Q_{ID} = H_1(ID)$ and $h = H_2(m, U)$. Check that

  $$e(Q_{ID}, P_X) \stackrel{?}{=} e(Q'_{ID}, P) \quad \text{and} \quad e(U, P_Y) \stackrel{?}{=} e(V, P)e(Q'_{ID}, -P_Y)^h.$$

  If both equations hold, output 'accept'; otherwise output 'reject'.

- **IC-Sign**$(\mu, m, Q'_{ID}, S_{ID})$: Randomly choose a value $w \in \mathbb{Z}_p^* \backslash \{1\}$, compute

$$Q = wQ_{ID}, \quad Q' = wQ'_{ID}, \quad U = rQ' \quad \text{and} \quad V = (r+h)S,$$

where $S = wS_{ID}, r \in_R \mathbb{Z}_p$ and $h = H'_2(m, Q, U)$. Output the identity-committed signature $\sigma_{IC} = (Q, Q', U, V)$ and the witness w.

- **IC-Verify**(μ, m, σ_{IC}): Parse the identity-committed signature σ_{IC} as (Q, Q', U, V). Compute $h = H'_2(m, Q, U)$. Check that

$$e(Q, P_X) \stackrel{?}{=} e(Q', P) \quad \text{and} \quad e(U, P_Y) \stackrel{?}{=} e(V, P)e(Q', -P_Y)^h.$$

If both equations hold, output 'accept'; otherwise output 'reject'.

- **Identify**$(\mu, ID, w, \sigma_{IC})$: Compute $Q_{ID} = H_1(ID)$. If $\sigma_{IC} = (Q, Q', U, V)$ is a valid identity-committed signature and $Q_{ID} = w^{-1}Q$, output 'valid'; otherwise output 'invalid'.

Note that we cannot verify whether $w = 1$ in the **IC-Verify** algorithm. One may directly use a standard signature for some ID as an identity-committed signature. However, this is reasonable because ICS is designed for exposing messages. If someone already signed a message m, then the identity-committed signature for the same m is meaningless.

The security argument of this construction can be found in Appendix A.

Additional Properties. In addition to the properties of ICS we defined, our construction provides two characteristics.

- Chosen-Linkability. The signer can decide the linkability of his identity-committed signatures. If a signer wants to show that some identity-committed signatures are signed by him, he can use the same witness w to mask his identity. The verifier knows that the signatures with the same Q come from the same signer.

- Private-Communicability. One can privately communicate with the signer of an identity-committed signature without revealing the signer's identity. For an identity-committed signature (Q, Q', U, V), one can treat Q as the public key of the signer, and encrypt messages using Boneh and Franklin's IBE scheme [10] (let Q be the hashed value of H_1). The ciphertext can be posted onto some bulletin board, and only the original signer[2] can decrypt the message.

[2]The PKG also can decrypt the message, but we can use the certificateless encryption scheme [2] to eliminate the trust of PKG.

4.3 Group-Oriented Ring Signatures

Abe et al. [1] proposed a ring signature scheme that allows mixed use of different flavors of keys at the same time. All participants can choose their keys with different parameter domains. By applying their construction to our ICS scheme, we get an efficient GRS scheme. A signer can sign messages on behalf of the organization which he belongs to, and then take the public parameters of other organizations to form a ring signature. These groups have their own public parameters, respectively.

First, we slightly modify **IC-Sign** and **IC-Verify** of our ICS scheme to be a three-move type signature scheme.

- **IC-Sign'**$(\mu, m, Q'_{ID}, S_{ID})$: Randomly choose a value $w \in \mathbb{Z}_p^* \backslash \{1\}$, compute

$$Q = wQ_{ID}, \quad Q' = wQ'_{ID}, \quad U = rQ' \quad \text{and} \quad V = (r+h)S,$$

  where $S = wS_{ID}$, $r \in_R \mathbb{Z}_p$ and $h = H'_2(m, Q, e(U, P_Y))$. Output the identity-committed signature $\sigma_{IC} = (Q, Q', h, V)$ and the witness w.

- **IC-Verify'**(μ, m, σ_{IC}): Parse the identity-committed signature σ_{IC} as (Q, Q', h, V). Compute $U' = e(V, P)e(Q', -P_Y)^h$. Check that

$$e(Q, P_X) \stackrel{?}{=} e(Q', P) \quad \text{and} \quad h \stackrel{?}{=} H'_2(m, Q, U').$$

  If both equations hold, output 'accept'; otherwise output 'reject'.

It is easy to see that the modification does not affect the security proof of the original scheme.

Let $L = \{\mu^{(i)} = (\mathbb{G}^{(i)}, \mathbb{G}_1^{(i)}, e^{(i)}, P^{(i)}, P_X^{(i)}, P_Y^{(i)}, H_1^{(i)}, H_2^{(i)}, H_2'^{(i)}) | 1 \le i \le n\}$ be the list of public parameters of the n groups that the signer wants to form the ring. Assume that the signer belongs to the s-th group. The GRS scheme is as follows.

- **Setup** and **Extract**: The same as the algorithms of the ICS scheme.

- **GR-Sign**(L, m, Q'_{ID}, S_{ID})
  - For $i = s$: Randomly choose a value $w \in \mathbb{Z}_p^* \backslash \{1\}$, compute

$$Q^{(s)} = wQ_{ID}, \quad Q'^{(s)} = wQ'_{ID} \quad \text{and} \quad U'^{(s)} = e(rQ'^{(s)}, P_Y^{(s)})$$

    where $r \in_R \mathbb{Z}_p$.
  - For $i = s+1, \ldots, n, 1, \ldots, s-1$: Randomly choose $z^{(i)} \in \mathbb{Z}$ and $V^{(i)} \in \mathbb{G}^{(i)}$. Compute

$$Q^{(i)} = z^{(i)}P^{(i)}, \quad Q'^{(i)} = z^{(i)}P_X^{(i)} \quad \text{and} \quad h^{(i)} = H_2'^{(i)}(L, m, Q^{(i)}, U'^{(i-1)})$$

    and set $U'^{(i)} = e^{(i)}(V^{(i)}, P^{(i)})e^{(i)}(Q'^{(i)}, -P_Y^{(i)})^{h^{(i)}}$.

Finally, compute

$$h^{(s)} = H_2'^{(s)}(L, m, Q^{(s)}, U'^{(s-1)}) \quad \text{and} \quad V^{(s)} = (r + h^{(s)})S_{ID}.$$

Output $\sigma_{GR} = (h^{(1)}, (Q^{(1)}, Q'^{(1)}, V^{(1)}), \ldots, (Q^{(n)}, Q'^{(n)}, V^{(n)}))$.

- **GR-Verify**(L, m, σ_{GR})
  For $i = 1, \ldots, n$, compute

$$U'^{(i)} = e^{(i)}(V^{(i)}, P^{(i)})e^{(i)}(Q'^{(i)}, -P_Y^{(i)})^{h^{(i)}},$$

  where $h^{(i)} = H_2'^{(i)}(L, m, Q^{(i)}, U'^{(i-1)})$ if $i \neq 1$. Check that

$$e^{(i)}(Q^{(i)}, P_X^{(i)}) \stackrel{?}{=} e^{(i)}(Q'^{(i)}, P^{(i)}) \quad \text{and} \quad h^{(1)} \stackrel{?}{=} H_2'^{(1)}(L, m, Q^{(1)}, U'^{(n)}).$$

  If both equations hold, output 'accept'; otherwise output 'reject'.

Certainly, the signer can also add some single persons to the list of the ring. By the generic construction of [1], these individual public keys can be "three-move type" or "trapdoor-one-way type". Therefore, this extension improves the efficiency of ring signatures without loss of generality.

We provide security proofs in Appendix B.

5 Conclusions

In this paper we introduce the new notion of identity-committable signatures that allow the signer to "commit" his identity on the signature generated on behalf of the signer's group. Later, the signer can open the identity and prove that he is the original signer. Furthermore, we also introduce the extension of ICS, group-oriented ring signatures, which can be regarded as a very efficient and practical ring signature scheme. We give the definitions of ICS and GRS schemes. Finally, we provide the implementations providing unconditional anonymity, chosen-linkability and private-communicability.

Acknowledgement

We first thank anonymous reviewers for giving us many useful suggestions. Also, we are grateful to Sherman S.M. Chow for pointing out some security flaws in our manuscript.

References

[1] Masayuki Abe, Miyako Ohkubo, and Koutarou Suzuki. 1-out-of-n signatures from a variety of keys. In *Proceedings of Advances in Cryptology - ASIACRYPT '02*, volume 2501 of *LNCS*, pages 415–432. Springer, 2002.

[2] Sattam S. Al-Riyami and Kenneth G. Paterson. Certificateless public key cryptography. In *Proceedings of Advances on Cryptology - ASIACRYPT '03*, volume 2894 of *LNCS*, pages 452–473. Springer, 2003.

[3] Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik. A practical and provably secure coalition-resistant group signature scheme. In *Proceedings of Advances in Cryptology - CRYPTO '00*, volume 1880 of *LNCS*, pages 255–270. Springer, 2000.

[4] Giuseppe Ateniese and Breno de Medeiros. Efficient group signatures without trapdoors. In *Proceedings of Advances on Cryptology - ASIACRYPT '03*, volume 2894 of *LNCS*, pages 246–268. Springer, 2003.

[5] Man Ho Au, Joseph K. Liu, Y. H. Yuen, and Duncan S. Wong. Id-based ring signature scheme secure in the standard model. Cryptology ePrint Archive, Report 2006/205, 2006.

[6] Olivier Baudron and Jacques Stern. Non-interactive private auctions. In *Proceedings of Financial Cryptography (FC '01)*, volume 2339 of *LNCS*, pages 364–378. Springer-Verlag, 2001.

[7] Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In *Proceedings of Advances in Cryptology - EUROCRYPT '03*, volume 2656 of *LNCS*, pages 614–629. Springer, 2003.

[8] Adam Bender, Jonathan Katz, and Ruggero Morselli. Ring signatures: Stronger definitions, and constructions without random oracles. In *Proceedings of the 3rd Theory of Cryptography Conference (TCC '06)*, volume 3876 of *LNCS*, pages 60–79. Springer, 2006.

[9] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In *Proceedings of Advances in Cryptology - CRYPTO '04*, volume 3152 of *LNCS*, pages 41–55. Springer, 2004.

[10] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. In *Proceedings of Advances in Cryptology - CRYPTO '01*, volume 2139 of *LNCS*, pages 213–229. Springer-Verlag, 2001.

[11] Xavier Boyen and Brent Waters. Compact group signatures without random oracles. In *Proceedings of Advances in Cryptology - EUROCRYPT '06*, volume 4004 of *LNCS*, pages 427–444. Springer, 2006.

[12] Jan Camenisch. Efficient and generalized group signatures. In *Proceedings of Advances in Cryptology - EUROCRYPT '97*, volume 1233 of *LNCS*, pages 465–479. Springer, 1997.

[13] Jan Camenisch and Markus Michels. A group signature scheme with improved efficiency. In *Proceedings of Advances in Cryptology - ASIACRYPT '98*, volume 1514 of *LNCS*, pages 160–174. Springer, 1998.

[14] Jan Camenisch and Markus Michels. Separability and efficiency for generic group signature schemes. In *Proceedings of Advances in Cryptology - CRYPTO '99*, volume 1666 of *LNCS*, pages 413–430. Springer, 1999.

[15] Jan Camenisch and Markus Stadler. Proof systems for general statements about discrete logarithms. Technical Report 260, Institute for Theoretical Computer Science, ETH Zurich, Mar 1997.

[16] Jae Choon Cha and Jung Hee Cheon. An identity-based signature from gap diffie-hellman groups. In *Proceedings of the Public-Key Cryptography (PKC '03)*, volume 2567 of *LNCS*, pages 18–30. Springer, 2003.

[17] David Chaum and Eugène van Heyst. Group signatures. In *Proceedings of Advances in Cryptology - EUROCRYPT '91*, volume 547 of *LNCS*, pages 257–265. Springer, 1991.

[18] Lidong Chen and Torben P. Pedersen. New group signature schemes. In *Proceedings of Advances in Cryptology - EUROCRYPT '94*, volume 950 of *LNCS*, pages 171–181. Springer, 1994.

[19] Sherman S. M. Chow, Siu-Ming Yiu, and Lucas Chi Kwong Hui. Efficient identity based ring signature. In *Proceedings of Applied Cryptography and Network Security 2005 (ACNS '05)*, volume 3531 of *LNCS*, pages 499–512. Springer, 2005.

[20] Yevgeniy Dodis, Aggelos Kiayias, Antonio Nicolosi, and Victor Shoup. Anonymous identification in ad hoc groups. In *Proceedings of Advances in Cryptology - EUROCRYPT '04*, volume 3027 of *LNCS*, pages 609–626. Springer, 2004.

[21] Javier Herranz and Germán Sáez. Forking lemmas for ring signature schemes. In *Proceedings of Progress in Cryptology - INDOCRYPT '03*, volume 2904 of *LNCS*, pages 266–279. Springer, 2003.

[22] Javier Herranz and Germán Sáez. New identity-based ring signature schemes. In *Proceedings of International Conference on Information and Communication Security (ICICS '04)*, volume 3269 of *LNCS*, pages 27–39. Springer, 2004.

[23] Antoine Joux. A one round protocol for tripartite diffie-hellman. *Journal of Cryptology*, 17(4):263–276, 2004.

[24] Aggelos Kiayias, Yiannis Tsiounis, and Moti Yung. Traceable signatures. In *Proceedings of Advances in Cryptology - EUROCRYPT '04*, volume 3027 of *LNCS*, pages 571–589. Springer, 2004.

[25] Aggelos Kiayias and Moti Yung. Group signatures with efficient concurrent join. In *Proceedings of Advances in Cryptology - EUROCRYPT '05*, volume 3494 of *LNCS*, pages 198–214. Springer, 2005.

[26] Joe Kilian and Erez Petrank. Identity escrow. In *Proceedings of Advances in Cryptology - CRYPTO '98*, volume 1462 of *LNCS*, pages 169–185. Springer, 1998.

[27] Joseph K. Liu, Victor K. Wei, and Duncan S. Wong. Linkable spontaneous anonymous group signature for ad hoc groups. In *Proceedings of the 9th Australasian Conference on Information Security and Privacy (ACISP '04)*, volume 3108 of *LNCS*, pages 325–335. Springer, 2004.

[28] Joseph K. Liu and Duncan S. Wong. Linkable ring signatures: Security models and new schemes. In *Proceedings of International Conference on Computational Science and Its Applications (ICCSA '05), Part 2*, volume 3481 of *LNCS*, pages 614–623. Springer, 2005.

[29] Jiqiang Lv and Xinmei Wang. Verifiable ring signature. In *Proceedings of The 3rd International Workshop on Cryptology and Network Security (CANS '03, in conjunction with DMS '03)*, pages 663–667, 2003.

[30] Lan Nguyen. Accumulators from bilinear pairings and applications. In *Proceedings of Topics in Cryptology: The Cryptographer's Track at RSA Conference (CT-RSA '05)*, volume 3376 of *LNCS*, pages 275–292. Springer, 2005.

[31] Lan Nguyen and Reihaneh Safavi-Naini. Efficient and provably secure trapdoor-free group signature schemes from bilinear pairings. In *Proceedings of Advances in Cryptology - EUROCRYPT '04*, volume 3027 of *LNCS*, pages 372–386. Springer, 2004.

[32] David Pointcheval and Jacques Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 13(3):361–396, 2000.

[33] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In *Proceedings of Advances in Cryptology - ASIACRYPT '01*, volume 2248 of *LNCS*, pages 552–565. Springer, 2001.

[34] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret: Theory and applications of ring signatures. In *Essays in Memory of Shimon Even*, volume 3895 of *LNCS*, pages 164–186. Springer, 2006.

[35] Patrick P. Tsang, Victor K. Wei, Tony K. Chan, Man Ho Au, Joseph K. Liu, and Duncan S. Wong. Separable linkable threshold ring signatures. In *Proceedings of Progress in Cryptology - INDOCRYPT '04*, volume 3348 of *LNCS*, pages 384–398. Springer, 2004.

[36] Fangguo Zhang and Kwangjo Kim. Id-based blind signature and ring signature from pairings. In *Proceedings of Advances in Cryptology - ASIACRYPT '02*, volume 2501 of *LNCS*, pages 533–547. Springer, 2002.

A Security Proofs of The ICS Scheme

In addition to the three oracles $Extract^{\mathcal{A}}, Sign^{\mathcal{A}}$ and $IC\text{-}Sign^{\mathcal{A}}$ defined in Section 2.2, we provide three hash oracles $H_1^{\mathcal{A}}, H_2^{\mathcal{A}}, H'^{\mathcal{A}}_2$ for adversary $\mathcal{A}$. Without loss of generality, we assume that all adversary algorithms query oracles with the same input at most once, and query $H_1(ID)$ before ID is used as an input of queries to H_2, $Extract$, $Sign$ and $IC\text{-}Sign$. The proof techniques are similar to that of the underlying signature scheme [16]. Since the completeness requirement can be checked straightforward, we provide the other security arguments as follows.

Lemma 1 *[16, Lemma 1] If there is an algorithm $\mathcal{A}$ that forges a regular signature of our scheme under adaptively chosen message and identity attack with advantage ϵ in time t, then there is an algorithm $\mathcal{A}_1$ which can forge a signature under chosen message and given identity attack with advantage $\epsilon_1 \geq \epsilon(1-\frac{1}{p})\frac{1}{q_{H_1}}$ in time $t_1 \leq t$, where q_{H_1} is the maximum number of queries to H_1 made by $\mathcal{A}$.*

Proof. On input ID and system parameters, $\mathcal{A}_1$ performs the following steps:

1. Randomly choose $j \in \{1, 2, \ldots, q_{H_1}\}$. Let ID_i be the i-th query to $H_1^{\mathcal{A}}$ where $i \in \{1, 2, \ldots, q_{H_1}\}$. Define $ID'_i = ID_i$ if $i \neq j$ and $ID'_j = ID$.

2. Execute $\mathcal{A}$ on the given system parameters. When $\mathcal{A}$ queries to $H_1^{\mathcal{A}}(ID_i)$, $Extract^{\mathcal{A}}(ID_i)$, $Sign^{\mathcal{A}}(ID_i, m)$ and $IC\text{-}Sign^{\mathcal{A}}(ID_i, m)$, return $H_1^{\mathcal{A}_1}(ID'_i)$, $Extract^{\mathcal{A}_1}(ID'_i)$, $Sign^{\mathcal{A}_1}(ID'_i, m)$ and $IC\text{-}Sign^{\mathcal{A}_1}(ID'_i, m)$, respectively. Besides, define $H_2^{\mathcal{A}} = H_2^{\mathcal{A}_1}$ and $H'^{\mathcal{A}}_2 = H'^{\mathcal{A}_1}_2$.

3. Finally, $\mathcal{A}$ outputs a forgery (ID_0, m, σ). If $ID_0 = ID$ and (ID_0, m, σ) is a valid signature, then output (ID, m, σ); otherwise output fail.

Since H_1 is modeled as a random oracle, the output distribution of all oracles queried by $\mathcal{A}$ are indistinguishable from the distribution of oracles queried by $\mathcal{A}_1$. By the assumption of $\mathcal{A}$, we have

$$\Pr[(ID_0, m, \sigma) \text{ is valid}] \geq \epsilon.$$

For the same reason, $\mathcal{A}$ outputs a valid signature (ID_0, m, σ) without query to $H_1(ID_0)$ is negligible. That is,

$$\Pr[ID_0 = ID_i, i \in \{1, 2, \ldots, q_{H_1}\} | (ID_0, m, \sigma) \text{ is valid}] \geq 1 - \frac{1}{p}.$$

Moreover, since j is randomly chosen, we have

$$\Pr[ID_0 = ID | ID_0 = ID_i, i \in \{1, 2, \ldots, q_{H_1}\}] \geq \frac{1}{q_{H_1}}.$$

By combining these equations, we have

$$\Pr[\mathcal{A} \text{ outputs a valid signature } (ID, m, \sigma)] \geq \epsilon \cdot (1 - \frac{1}{p}) \cdot \frac{1}{q_{H_1}}.$$

□

Lemma 2 *If there is an algorithm $\mathcal{A}_1$ that forges a regular signature of our scheme under adaptively chosen message and given identity attack with advantage $\epsilon_1 \geq 10(q_S + 1)(q_S + q_{H_2})/p$ in time t_1, then there is an algorithm $\mathcal{B}$ which can solve CDHP with advantage $\epsilon' \geq 1/9$ in time $t' \leq 23 q_{H_2} t_1 / \epsilon_1$, where q_{H_2} and q_S are the maximum number of queries to H_2 and Sign, respectively.*

Proof. Given a CDHP instance (P, aP, bP), $\mathcal{B}$ computes abP by performing the following steps:

1. Choose an identity ID for $\mathcal{A}_1$. Let $P_X = xP$ and $P_Y = aP$, where x is randomly chosen from $\mathbb{Z}_p$. Let q_{H_1} be the maximum number of queries to H_1. Define the oracles queried by $\mathcal{A}_1$ as follows, where i, i_j, i_k, i_l denotes the i-th H_1 query, the j-th $Extract$ query, the k-th $Sign$ query and the l-th $IC\text{-}Sign$ query, respectively.
$H_1^{\mathcal{A}_1}(ID_i) = \begin{cases} bP & \text{if } ID_i = ID; \\ z_i P & \text{otherwise}, z_i \in_R \mathbb{Z}_p \end{cases}, 1 \leq i \leq q_{H_1},$
$Extract^{\mathcal{A}_1}(ID_{i_j}) = (Q'_j, S_j) = (xz_{i_j} P, xz_{i_j}(aP)),$
$Sign^{\mathcal{A}_1}(ID_{i_k}, m_k) = (Q'_k, U_k, V_k)$
$= (xH_1^{\mathcal{A}_1}(ID_{i_k}), v_k P - h_k x H_1^{\mathcal{A}_1}(ID_{i_k}), v_k(aP)),$
where $v_k, h_k \in_R \mathbb{Z}_p, 1 \leq k \leq q_S$.

$$\begin{aligned} IC\text{-}Sign^{\mathcal{A}_1}(ID_{i_l}, m_l) &= (w_l, Q_l, Q'_l, U_l, V_l) \\ &= (w_l, w_l H_1^{\mathcal{A}_1}(ID_{i_l}), x w_l H_1^{\mathcal{A}_1}(ID_{i_l}), \\ &\quad v_l P - h_l x w_l H_1^{\mathcal{A}_1}(ID_{i_l}), v_l(aP)), \\ &\quad \text{where } w_l, v_l, h_l \in_R \mathbb{Z}_p. \end{aligned}$$

Note that h_k and h_l will be stored as the result of the queries to $H_2^{\mathcal{A}_1}(m_k, U_k)$ and $H_2^{\mathcal{A}_1}(m_l, U_l)$, respectively. If a query of $Sign^{\mathcal{A}_1}$ or $IC\text{-}Sign^{\mathcal{A}_1}$ produces a result which is inconsistent with other results of queries to $Sign^{\mathcal{A}_1}$ or $IC\text{-}Sign^{\mathcal{A}_1}$ or $H_2^{\mathcal{A}_1}$, output fail and exit.

2. Run $\mathcal{A}_1$ with the given parameters and oracles. If $\mathcal{A}_1$ outputs a valid signature (m, ID, Q', U, h, V), replay it with the same random tape, but different choice of H_2 queries such that $\mathcal{A}_1$ outputs another signature (m, ID, Q', U, h', V'), where $h \neq h'$.

3. Compute and output $x^{-1}(h - h')^{-1}(V - V')$ if both outputs are expected ones. Otherwise, output fail.

We can see that the oracles $Extract^{\mathcal{A}_1}$ and $Sign^{\mathcal{A}_1}$ output correct keys and signatures as desired, respectively. Moreover, by the random oracle model, $H_1^{\mathcal{A}_1}$, $H_2^{\mathcal{A}_1}$, $Extract^{\mathcal{A}_1}$ and $Sign^{\mathcal{A}_1}$ output random distribution and are indistinguishable from the results of the original scheme. By the result of Pointcheval and Stern [32, Lemma 4], $\mathcal{B}$ will obtain two valid signatures (m, ID, Q', U, h, V) and (m, ID, Q', U, h', V') such that $h \neq h'$ within time $23 q_{H_2} t_1 / \epsilon_1$ and with probability at least $\frac{1}{9}$.

Since the two signatures (m, ID, Q', U, h, V) and (m, ID, Q', U, h', V') are valid, we have

$$\begin{aligned} x^{-1}(h - h')^{-1}(V - V') &= x^{-1}(h - h')^{-1}((r + h)S_{ID} - (r + h')S_{ID}) \\ &= x^{-1}(h - h')^{-1}((r + h)xabP - (r + h')xabP) \\ &= x^{-1}(h - h')^{-1}(h - h')xabP \\ &= abP. \end{aligned}$$

□

By the above two lemmas, the following theorem holds.

Theorem 5 (Unforgeability) *If there is an algorithm $\mathcal{A}$ that forges a regular signature of our scheme under adaptively chosen message and identity attack with advantage $\epsilon \geq 10(q_S + 1)(q_S + q_{H_2})q_{H_1}/(p - 1)$ in time t, then there is an algorithm $\mathcal{B}$ which can solve CDHP with advantage $\epsilon' \geq 1/9$ in time $t' \leq \frac{23 q_{H_1} q_{H_2} t}{\epsilon(1 - \frac{1}{p})}$, where q_{H_1}, q_{H_2} and q_S are the maximum number of queries to H_1, H_2 and Sign, respectively.*

Theorem 6 (ICS-Unforgeability) *If there is an algorithm $\mathcal{A}$ that forges an identity-committed signature of our scheme under adaptively chosen message attack with advantage $\epsilon \geq 10(q_{S_{IC}} + 1)(q_{S_{IC}} + q_{H'_2})/p$ in time t, then there is an algorithm $\mathcal{B}$ which can solve CB-CDHP with advantage $\epsilon' \geq 1/9$ in time $t' \leq 23 q_{H'_2} t/\epsilon$, where $q_{H'_2}$ and $q_{S_{IC}}$ are the maximum number of queries to H'_2 and IC-Sign, respectively.*

Proof. Given a CB-CDHP instance (P, aP, bP), $\mathcal{B}$ computes abQ for some Q by performing the following steps:

1. Let $P_X = aP$ and $P_Y = bP$. Let q_{H_1} be the maximum number of queries to H_1. Define the oracles queried by $\mathcal{A}$ as follows, where i, i_k, i_l denotes the i-th H_1 query, the k-th $Sign$ query and the l-th $IC\text{-}Sign$ query, respectively.
   $H_1^{\mathcal{A}}(ID_i) = z_i P$, $z_i \in_R \mathbb{Z}_p$, $1 \le i \le q_{H_1}$
   $$\begin{aligned} Sign^{\mathcal{A}}(ID_{i_k}, m_k) &= (Q'_k, U_k, V_k) \\ &= (z_{i_k}(aP), v_k P - h_k z_{i_k}(aP), v_k(bP)), \\ &\quad \text{where } v_k, h_k \in_R \mathbb{Z}_p. \\ IC\text{-}Sign^{\mathcal{A}}(ID_{i_l}, m_l) &= (w_l, Q_l, Q'_l, U_l, V_l) \\ &= (w_l, w_l z_{i_l} P, w_l z_{i_l}(aP), \\ &\quad v_l P - h_l w_l z_{i_l}(aP), v_l(bP)), \\ &\quad \text{where } w_l, v_l, h_l \in_R \mathbb{Z}_p, 1 \le l \le q_{S_{IC}}. \end{aligned}$$
   Note that h_k and h_l will be stored as the result of the query $H_2'^{\mathcal{A}}(m_k, U_k)$ and $H_2'^{\mathcal{A}}(m_l, U_l)$, respectively. If a query of $Sign^{\mathcal{A}}$ or $IC\text{-}Sign^{\mathcal{A}}$ produces a result which is inconsistent with other results of queries to $Sign^{\mathcal{A}}$ or $IC\text{-}Sign^{\mathcal{A}}$ or $H_2'^{\mathcal{A}}$, output fail and exit.

2. Run $\mathcal{A}$ with the given parameters and oracles. When $\mathcal{A}$ outputs a valid signature (m, Q, Q', U, h, V), replay it with the same random tape, but different choice of H_2' queries such that $\mathcal{A}$ outputs another signature (m, Q, Q', U, h', V'), where $h \neq h'$.

3. Compute and output $(h - h')^{-1}(V - V')$ if both outputs are expected ones. Otherwise, output fail.

We can see that the oracles $Sign^{\mathcal{A}}$ and $IC\text{-}Sign^{\mathcal{A}}$ output correct signatures as desired. Moreover, by the random oracle model, $H_1^{\mathcal{A}}$, $H_2'^{\mathcal{A}}$, $Sign^{\mathcal{A}}$ and $IC\text{-}Sign^{\mathcal{A}}$ output random distribution and are indistinguishable from the results of the original scheme. By the result of Pointcheval and Stern [32, Lemma 4], $\mathcal{B}$ will obtain two valid signatures (m, Q, Q', U, h, V) and (m, Q, Q', U, h', V') such that $h \neq h'$ within time $23 q_{H_2'} t/\epsilon$ and with probability at least $\frac{1}{9}$.

Since the two signatures (m, Q, Q', U, h, V) and (m, Q, Q', U, h', V') are valid, we have

$$\begin{aligned} (h - h')^{-1}(V - V') &= (h - h')^{-1}((r + h)S_{ID} - (r + h')S_{ID}) \\ &= (h - h')^{-1}((r + h)abQ - (r + h')abQ) \\ &= (h - h')^{-1}(h - h')abQ \\ &= abQ. \end{aligned}$$

□

Theorem 7 (ICS-Anonymity) *Our scheme has the information-theoretic ICS-Anonymity property.*

Proof. For a valid identity-committed signature $\sigma_{IC} = (Q, Q', U, V)$, it can be opened to any identity ID^* because there is a w^* such that

$$Q = w^* Q_{ID^*},$$

where $Q_{ID^*} = H_1(ID^*)$. Therefore, the signature has information-theoretic ICS-Anonymity. □

Theorem 8 (ICS-Binding) *If there is an algorithm $\mathcal{A}$ that breaks ICS-Binding property with advantage ϵ in time t, then there is an algorithm $\mathcal{B}$ which can solve DLP with advantage $\epsilon' \geq \epsilon(1 - \frac{1}{p^2})\frac{1}{q_{H_1}^2}$ in time $t' = O(t)$, where q_{H_1} is the maximum number of queries to H_1.*

Proof. On input $(\tilde{P}, a\tilde{P})$, $\mathcal{B}$ computes a as follows.

1. Run **Setup** and execute $\mathcal{A}$ on the output system parameters.
2. Answer the oracle queries as the real scheme except that when $\mathcal{A}$ queries $H_1^{\mathcal{A}}(ID_j)$ and $H_1^{\mathcal{A}}(ID_{j'})$ for two randomly chosen $j, j' \in \{1, 2, \ldots, q_{H_1}\}$, return $\tilde{P}$ and $a\tilde{P}$ respectively.
3. $\mathcal{A}$ outputs an identity-committed signature (Q, Q', U, V) on m, and two witnesses (w, ID) and (w', ID'). If $ID \neq ID_j$ or $ID' \neq ID_{j'}$, output fail and abort. Otherwise, output $a = w/w'$.

We can see that since $Q = wQ_{ID} = w\tilde{P}$ and $Q = w'Q_{ID'} = w'a\tilde{P}$, the value a is properly computed. Moreover, since H_1 is modeled as a random oracle, the output distribution of all oracles queried by $\mathcal{A}$ are indistinguishable from the distribution of the real scheme. By the assumption of $\mathcal{A}$, we have

$$\Pr[w \text{ and } w' \text{ are witnesses for } ID \text{ and } ID'] \geq \epsilon.$$

For the same reason, the probability that $\mathcal{A}$ outputs valid witnesses (w, ID) and (w', ID') without queries to $H_1(ID)$ and $H_1(ID')$ is negligible. That is,

$$\Pr[ID = ID_i, ID' = ID_{i'}, i, i' \in \{1, 2, \ldots, q_{H_1}\} | \\ w \text{ and } w' \text{ are witnesses for } ID \text{ and } ID'] \geq 1 - \frac{1}{p^2}.$$

Moreover, since j and j' are randomly chosen, we have

$$\Pr[ID = ID_j = \tilde{P}, ID' = ID_{j'} = a\tilde{P} | \\ ID = ID_i, ID' = ID_{i'} i, i' \in \{1, 2, \ldots, q_{H_1}\}] \geq \frac{1}{q_{H_1}^2}.$$

By combining these equations, we have

$$\Pr[\mathcal{B} \text{ outputs the correct answer } a \text{ for DLP }] \geq \epsilon \cdot (1 - \frac{1}{p^2}) \cdot \frac{1}{q_{H_1}^2}.$$

□

B Security Proofs of The GRS Scheme

Theorem 9 (Unforgeability) *For a public parameter list L of size n, if there is an algorithm $\mathcal{A}$ that forges a group-oriented ring signature of our scheme under adaptively chosen message attack with advantage $\epsilon \geq 10(q_{S_{GR}} + 1)(q_{S_{GR}} + q_{H_2'})/p$ in time t, then there is an algorithm $\mathcal{B}$ which can solve CB-CDHP with advantage $\epsilon' \geq 1/9$ in time $t' \leq 23q_{H_2'}tn/\epsilon$, where $q_{H_2'}$ and $q_{S_{GR}}$ are the maximum number of queries to H_2' and GR-Sign, respectively.*

Proof. Given a CB-CDHP instance (P, aP, bP), $\mathcal{B}$ computes abQ for some Q by performing the following steps:

1. Randomly choose an index $\hat{i} \in \{1, 2, \ldots, n\}$. Perform **Setup** as usual to generate public parameters $\mu^{(i)}$ for all $i \in \{1, \ldots, n\}\backslash\{\hat{i}\}$. Let $P^{(\hat{i})} = P, P_X^{(\hat{i})} = aP$ and $P_Y^{(\hat{i})} = bP$. Let q_{H_1} be the maximum number of queries to $H_1^{(\hat{i})}$. Define the oracles queried by $\mathcal{A}$ as follows, where j, j_k denotes the j-th $H_1^{(\hat{i})}$ query and the k-th *GR-Sign* query, respectively.

   - For the queries to group $i \in \{1, \ldots, n\}\backslash\{\hat{i}\}$, since the master secret keys are known, compute the answer as the real scheme.
   - $Extract^{\mathcal{A}}(\hat{i}, ID)$: output fail and exit for any ID.
   - $H_1^{(\hat{i})\mathcal{A}}(ID_j) = z_j P$, $z_j \in_R \mathbb{Z}_p$, $1 \leq j \leq q_{H_1}$
   - $GR\text{-}Sign^{\mathcal{A}}(\hat{i}, L', ID_{j_k}, m_k) = (h_k^{(1)}, (Q_k^{(1)}, Q_k'^{(1)}, V_k^{(1)}), \ldots, (Q_k^{(n')}, Q_k'^{(n')}, V_k^{(n')}))$, where
     - $(Q_k^{(\hat{i})}, Q_k'^{(\hat{i})}, V_k^{(\hat{i})}) = (z_{j_k}P, z_{j_k}(aP), v_k(bP)); v_k \in_R \mathbb{Z}_p, 1 \leq k \leq q_{S_{GR}}$,
     - $U'^{(\hat{i})} = e(v_k P - h_k^{(\hat{i})} z_{j_k}(aP), bP)$ is computed implicitly; $h_k^{(\hat{i})} \in_R \mathbb{Z}_p, 1 \leq k \leq q_{S_{GR}}$, and
     - $(Q_k^{(i)}, Q_k'^{(i)}, V_k^{(i)})$, $i \in \{1, \ldots, n\}\backslash\{\hat{i}\}$ are computed as the real scheme (in the case $i \neq s$).

   Note that $h_k^{(\hat{i})}$ will be randomly chosen first, and stored as the result of the query $H_2'^{\mathcal{A}}(L, m_k, Q_k^{(\hat{i})}, U_k^{(\hat{i}-1)})$.

2. Run $\mathcal{A}$ with the given parameters and oracles until it outputs a valid signature $(L^*, h^{(1)}, (Q^{(1)}, Q'^{(1)}, V^{(1)}), \ldots, (Q^{(n^*)}, Q'^{(n^*)}, V^{(n^*)}))$, where $L^* = (\mu^{*(1)}, \ldots, \mu^{*(n^*)})$. If $\mu^{(\hat{i})} \notin L^*$, output fail and abort. Otherwise, replay it with the same random tape, but different choices of $H_2'^{\mathcal{A}}$ queries such that $\mathcal{A}$ outputs another valid signature $(L^*, h'^{(1)}, (Q^{(1)}, Q'^{(1)}, V'^{(1)}), \ldots, (Q^{(n^*)}, Q'^{(n^*)}, V'^{(n^*)}))$, where $h^{(1)} \neq h'^{(1)}$ and $V^{(i)} \neq V'^{(i)}$ for all $i \in \{1, \ldots, n^*\}$.

3. Suppose that $\mu^{*(i^*)} = \mu^{(\hat{i})}$. Compute and output $(h^{(i^*)} - (h'^{(i^*)})^{-1}(V^{(i^*)} - V'^{(i^*)})$ if both outputs are expected ones. Otherwise, output fail.

We can see that the oracles output correct keys and signatures as desired. Moreover, by the random oracle model, $H_1^{\mathcal{A}}$, $H_2'^{\mathcal{A}}$, $Extract^{\mathcal{A}}$ and $GR\text{-}Sign^{\mathcal{A}}$ output random distribution and are indistinguishable from the results of the original scheme. By the result of Pointcheval and Stern [32, Lemma 4], $\mathcal{B}$ will obtain two valid signatures within time $23q_{H_2'}tn/\epsilon$ and with probability at least $\frac{1}{9}$. Since the two signatures are valid, we can compute $abQ^{(i^*)}$ as in Theorem 6. □

Theorem 10 (Anonymity) *Our GRS scheme has the information-theoretic Anonymity property.*

Proof. Consider a valid signature $(L^*, h^{(1)}, (Q^{(1)}, Q'^{(1)}, V^{(1)}), \ldots, (Q^{(n^*)}, Q'^{(n^*)}, V^{(n^*)}))$. Since all $(Q^{(i)}, Q'^{(i)}, V^{(i)})$ are equally distributed for $1 \leq i \leq n$, the adversary cannot identify the group that the signer belongs to. The remaining value $h^{(1)}$ is uniquely determined from (L^*, m) and $(Q^{(i)}, V^{(i)})$'s. Moreover, by Theorem 7, we know that the signature of a single group is also information-theoretic anonymous. □