(Hierarchical Identity-Based) Threshold Ring Signatures without Random Oracles

Victor K. Wei and Tsz Hon Yuen

Dept. of Information Engineering, The Chinese Univ. of Hong Kong, Hong Kong
{kwwei,thyuen4}@ie.cuhk.edu.hk

March 3, 2006

Abstract. We construct the first several efficient threshold ring signatures (TRS) without random oracles. Specializing to a threshold of one, they are the first several efficient ring signatures without random oracles after the only earlier instantiation of Chow, Liu, Wei, and Yuen [22]. Further specializing to a ring of just one user, they are the short (ordinary) signatures without random oracles summarized in Wei and Yuen [41].

We also construct the first hierarchical identity-based threshold ring signature without random oracles. The signature size is $O(n\lambda_s)$ bits, where λ_s is the security parameter and n is the number of users in the ring. Specializing to a threshold of one, it is the first hierarchical identity-based ring signature without random oracles. Further specializing to a ring of one user, it is the constant-size hierarchical identity-based signature (HIBS) without random oracles in [44] - the signature size is $O(\lambda_s)$ bits which is independent of the number of levels in the hierarchy.

1 Introduction

Anonymity is one of the most important properties in many cryptographic applications. Practical applications like e-cash or e-voting need to ensure that information about the signer is not revealed. A ring signature scheme specifies a set of possible signers, such that the verifier cannot tell which member actually produced the signature. Therefore a ring signature scheme achieves signer anonymity. In addition, it is not possible to decide whether two signatures have been issued by the same member. The concept of ring signatures was proposed by Cramer et al. [24] and ring signatures were first formalized by Rivest et al. [36]. Many different ring signature schemes are proposed, such as [1], [12], [16], [23], [25], [43] and [46]. Different from a group signature scheme (e.g. [6], [18], [20]), the group formation is spontaneous and there is no group manager or open authority to determine the identity of the signer of a ring signature. Therefore assume users' public keys are readily available, a user can form a group by simply collecting the public keys of all the group members including his own. These group members can be totally unaware of being conscripted into the group. Ring signature schemes can be used for whistle blowing [36], anonymous membership authentication for ad hoc groups [16] and many other applications which do not want complicated group formation stage but require signer anonymity.

[16] extended the notion of ring signature schemes to a threshold setting and proposed the first threshold ring signature scheme. Later on, some other threshold ring signature schemes (e.g. [42], [32], [33], [29]) have been proposed. A θ-out-of-n threshold ring signature scheme is defined as a ring signature scheme of which at least θ corresponding private keys of n public keys are needed to produce a signature. The setup-free and signer anonymity properties of a conventional ring signature scheme are preserved in the threshold setting.

Signatures without random oracles. The random oracle model [7] is a popular technique in provable security. Many signature schemes used rewindings of hashings with observable hashing input and output in their reductionist security proofs, like the Schnorr signature or other schemes using the Fiat-Shamir paradigm. However the result of Barak el al. [3, 4] and Goldwasser and Kalai [28] proved the insecurity of the random oracle model as it is used in the Fiat-Shamir paradigm. Several papers proved that some popular cryptosystems previously proved secure in the random oracle were actually provably insecure when the random oracle was instantiated by any real-world hashing functions [19, 5]. As a result, recently there are many new signature schemes which try to prove their security without random oracles, such as group signatures [2, 15], blind signatures [30], group-oriented signatures [40], undeniable signatures [31, 48], etc.

Wei and Yuen [41] proposed some short signautures without random oracles. The signatures originate from the signature schemes in [10, 45, 17, 14]. They showed how these signatures can be consturcted from new assumptions without random oracles. Our new threshold ring signatures wihout random oracles mainly originate from these signatures.

Most of the existing ring signature (including threshold or non-threshold version) schemes rely on the random oracle assumption. Recently, [8] propose a ring signature scheme for any number of users based on general assumptions, and an efficient construction for two users. Both constructions do not rely on random oracles. [22] proposed the first efficient instantiation for any number of users. However, no existing threshold ring signature schemes is provably secure without random oracles.

Identity-based cryptography. Identity-based cryptography, introduced by Shamir [38], allows the users' public keys to be their identity. Usually a trusted third party computes the private key from an identity (any arbitrary string such as name and email address). Comparing with certificate from certificate authority (CA), the identity based public key can identify a user immediately. Besides, the problem of distribution of public keys is avoided in identity-based cryptography. Hierarchical identity-based cryptography [26] is a generalization of identity-based cryptography that mirrors the hierarchy of organizations. An identity at level ℓ of the hierarchy tree can issue private keys to its descendant identities, but cannot sign/decrypt messages on behalf of any identity which are not his descendant. Identity-based threshold ring signature was proposed in [21]. However there is no existing ring signature using hierarchical identity based key pairs.

Our **Contributions** are

1. We construct new ring signatures and threshold ring signatures without random oracles. The proposed seven different threshold ring signature schemes are the *first* which are provably secure without random oracles in the literature. In particular, except one of the ring signature is proposed in [22], the other six schemes are new ring signature schemes whose reductionist security proofs do not rely on the random oracles.
2. We propose a new security notion and model for hierarchical identity-based threshold ring signature (HIBTRS). In particular, if $\theta = 1$, we have a new security notion and model for hierarchical identity-based ring signature (HIBRS).

Our Intuition. *Outsourcing* is a powerful technique in proving the security of cryptographic schemes. When we prove the security of a scheme, usually the most difficult part is to simulate the signing oracle or the decryption oracle of the gauntlet (challenge) user. *Outsourcing*

means that we use the help from the problem instance to answer those oracle queries. Here we introduce different types of outsourcing techniques and then discuss how they can be applied to construct threshold ring signatures without random oracles. We divide the related intractability assumtpions into two types: interactive and non-interactive.

Interactive intractability assumtpions: An interactive intractability problem instance means that an attacker can adaptively query an external oracle for q times and can get distinct valid tuples from the oracle which satisfy a relation $\mathcal{R}$. Finally he needs to return a new valid tuple which satisfies $\mathcal{R}$. [34] proposed a LRSW assumption with an external oracle. In proving the security of a signature scheme, the simulator simply forwards all signing oracle queries to this external oracle and returns its output to the adversary. Signature schemes like [17] use this type of assumption. The problem of interactive intractability assumptions is that we need to assume that the tuples return by the oracle should not help the attacker to solve the intractability problem. Therefore we need to be extremely careful when formulating interactive intractability assumptions.

Non-interactive intractability assumtpions: A non-interactive intractability problem instance does not have any interactive external oracle as the above type of assumptions. For outsourcing, the non-interactive intractability assumtpions can be further divided into two categories. [35] proposed a CAA (Collusion Attack Algorithm) assumption. In this type of assumption, the problem instance gives q tuples in one time at the beginning, which satisfy a relation $\mathcal{R}$. Then the simulator can use these tuples to handle adaptive signing oracle queries from the adversary for q times. Finally the adversary outputs a new tuple which satisfies $\mathcal{R}$. Schemes like [47] use this type of assumption.

[10] proposed a SDH (Strong Diffie-Hellman) assumption and used it to prove the security of a short signature scheme. In this type of assumption, the problem instance gives a tower of powers like $(g, g^x, \ldots, g^{x^q})$. The simulator can use these values to setup the public parameters and to simulate the signing oracle for q times. Then the simulator uses the adversary's answer to compute some power of x. Assumptions like DHI [35], BDHI [9], BDHE [13] also have similar structure.

We notice that CAA type assumptions or interactive intractability assumptions can be used to prove the security for threshold ring signature schemes. We do not find (threshold) ring signature schemes that can be proven secure using SDH type assumptions. Although [43] claimed to do so, but they do not give rigorous proof. [22] proposed the first ring signature scheme without random oracles by using the CAA type assumption.

In this paper, we proposed seven threshold ring signature schemes without random oracles. Three of those use CAA type assumptions in the security proofs, while the remaining four use interactive intractability assumptions. [41] proved the security of signature scheme B in [17] by a CAA type assumption (while the orignal paper used external oracle type assumption). We use both versions in constructing two threshold ring signature schemes. Schemes of [10] and its variant can be used to construct threshold ring signatures, which can be proven secure using either CAA type assumptions or interactive intractability assumptions. However we notice that some signature schemes like [14] or scheme A of [17] can be transformed to threshold ring signature schemes by using only interactive intractability assumptions, but not the CAA types. For the hierarchical identity-based threshold ring signature, we also use an interactive intractability assumption for the security proof.

Organization
This paper is organized as follow: The next section contains preliminaries about the underlying cryptographic primitive used in this paper. In Section 3, we review the definition of secure threshold ring signature schemes and introduce the definition of secure hierarchical identity based threshold ring signature schemes. In Section 4 we show the constructions of some threshold ring signature schemes and give the security proofs. Then we propose our new hierarchical identity-based threshold ring signature instantiation in Section 5 and give the security proofs. Finally, we conclude the paper in Section 6.

2 Preliminaries

Before presenting our results, we review the definitions of groups equipped with a bilinear pairings and some related assumptions.

2.1 Bilinear Pairings

Here we follow the notation in [14]. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two (multiplicative) cyclic groups of prime order q_1. Let g_1 be a generator of $\mathbb{G}_1$ and g_2 be a generator of $\mathbb{G}_2$. We also let ψ be an isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$, with $\psi(g_2) = g_1$, and $\hat{e}$ be a bilinear map such that $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ with the following properties:

1. *Bilinearity*: For all $u \in \mathbb{G}_1$, $v \in \mathbb{G}_2$ and $a, b \in \mathbb{Z}$, $\hat{e}(u^a, v^b) = \hat{e}(u, v)^{ab}$.
2. *Non-degeneracy*: $\hat{e}(g_1, g_2) \neq 1$.
3. *Computability*: There exists an efficient algorithm to compute $\hat{e}(u, v)$.

2.2 Intractability Assumptions

We review several intractability assumptions for existing signature schemes.

Definition 1. *q-SDH [10]: The q-SDH Problem is given $g_1 \in \mathbb{G}_1$, $g_2^{x^i} \in \mathbb{G}_2$, $0 \leq i \leq n$, output $(c, g_1^{1/(x+c)})$. The q-SDH Assumption is that no PPT algorithm can solve the q-SDH problem with running time T and with probability $\geq \epsilon$, over the random choice of x and the random bits consumed by $\mathcal{A}$.*

Assume $\mathbb{G}_2 = \mathbb{G}_1$. We have the following assumption:

Definition 2. *LRSW [34]: The LRSW Problem is given $g, X = g^x, Y = g^y \in \mathbb{G}_1$, and an oracle $O_{X,Y}(\cdot)$ which, upon input m, returns random a and the tuple $(b = a^y, c = a^{x+mxy})$; output $(m^*, a^*, b^* = (a^*)^y, c^* = (a^*)^{x+m^*xy})$ and m^* has never been queried to $O_{X,Y}(\cdot)$. The LRSW Assumption is that no PPT algorithm can solve the LRSW problem with non-negligible probability.*

3 Security Model

We use textbook security models [27] for ACP-UF of standard signature schemes. Hereafter we review the definition and the security notion of threshold ring signature schemes and introduce the one for hierarchical identity based threshold ring signature schemes.

Notice that for unforgeability, we use the static attacker model here. The attacker is given n public keys and $\theta - 1$ corresponding private keys. All signing oracle queries correspond to these n public keys, and the attacker's final output should be a (n, θ)-threshold ring signature for these n public keys.

3.1 Threshold Ring Signature

Let $\lambda_s \in \mathbb{N}$ be a security parameter and $m \in \{0,1\}^*$ be a message.

Definition 3. *A threshold ring signature scheme is a triple (*Setup, Sign, Verify*) where*

- $(s, P) \leftarrow \mathsf{Setup}(1^{\lambda_s})$ *is a probabilistic polynomial time algorithm (PPT) which takes as input a security parameter λ_s, produces a private key s and a public keys P.*
- $\sigma \leftarrow \mathsf{Sign}(1^{\lambda_s}, \hat{s}, L, m)$ *is a PPT which accepts as inputs a security parameter λ_s, a set of private keys $\hat{s}$, a set of public keys L including those corresponding to the private keys in $\hat{s}$ and a message m, produces a threshold ring signature σ.*
- $1/0 \leftarrow \mathsf{Verify}(1^{\lambda_s}, L, m, \sigma, \theta)$ *is a PPT which accepts as inputs a security parameter λ_s, a set of public keys L, a message m, a signature σ and the number of signers θ, returns 1 or 0 for* accept *or* reject*, respectively.*

For simplicity, we usually omit the input of security parameter in the rest of the paper. L may include public keys based on different security parameters. The security of the signature scheme defined above is set to the smallest one among them. Setup may also be extended to take the description of key types.

The security of a ring signature scheme consists of three requirements, namely *Correctness*, *Anonymity* and *Existential Unforgeability*. They are defined as follows.

Correctness. We require that $\mathsf{Verify}(L, m, \mathsf{Sign}(\hat{s}, L, m), |\hat{s}|) = 1$ for any message m and any set of private keys $\hat{s}$ which are generated by $\mathsf{Setup}(1^{\lambda_s})$ and any set of public keys L including those corresponding to the private keys in $\hat{s}$.

We have the following oracle for the adversary to query in the security game:

- Signing Oracle $\mathcal{SO}(m, L')$: On input any message m, a set of n users $L' \subseteq L_{max}$; returns a ring signature $\sigma \leftarrow \mathsf{Sign}(\hat{s}, L', m)$, such that $\mathsf{Verify}(L', m, \sigma, \theta) = 1$ where $\hat{s}$ is the set of θ private keys that correspond to θ public keys in L'.

Anonymity. For a (n, θ)-threshold ring signature scheme of θ signers with n public keys, the anonymity is defined as the following game between a simulator and an adversary $\mathcal{A}$:

1. The simulator runs algorithm Setup. Let $L_{max} = \{P_1, \cdots, P_{n_{max}}\}$ be the set of $n_{max} \geq n$ public keys in which each key is generated as $(s_i, P_i) \leftarrow \mathsf{Setup}(1^{\lambda_{s_i}})$ for some $\lambda_{s_i} \in \mathbb{N}$. Let $\lambda_s = \min(\lambda_{s_1}, \cdots, \lambda_{s_{n_{max}}})$. $\mathcal{A}$ is given L_{max}, s_1, …, $s_{n_{max}}$ and the public parameters.
2. $\mathcal{A}$ queries $\mathcal{SO}$ q_S times in arbitrary interleaf.
3. $\mathcal{A}$ randomly selects a message m^*, two distinct sets of θ users L_0, L_1 and a ring $L^* \subseteq L_{max}$ for which $L_0, L_1 \subset L^*$ and sends to the simulator. The simulator randomly picks a bit b and returns $\sigma \leftarrow \mathsf{Sign}(\hat{s}_b, L^*, m^*)$ to $\mathcal{A}$, where $\hat{s}_b$ is the set of secret keys of L_b.
4. Finally $\mathcal{A}$ outputs a bit b'.

$\mathcal{A}$ wins if $b = b'$. Denote $\mathsf{Adv}_{\mathcal{A}}$ be the probability that $\mathcal{A}$ wins in the above game over $1/2$, taken over the coin flips of $\mathcal{A}$ and the simulator.

Definition 4. *A threshold ring signature scheme is anonymous if no PPT adversary $\mathcal{A}$ win the anonymity game with non-negligible* $\mathsf{Adv}_{\mathcal{A}}$.

It means that even all the private keys are known, it remains uncertain that which $|\hat{s}|$ signers out of n possible signers actually generates a threshold ring signature.

Existential Unforgeability. For threshold ring signature, we would like to consider the security model for existential unforgeability. It models the adaptive chosen message attack. For a (n, θ)-threshold ring signature scheme of θ signers with n public keys, the existential unforgeability is defined as the following game between a simulator and an adversary $\mathcal{A}$:

1. The simulator runs algorithm Setup. Let $L_{max} = \{P_1, \cdots, P_{n_{max}}\}$ be the set of $n_{max} \geq n$ public keys in which each key is generated as $(s_i, P_i) \leftarrow \mathsf{Setup}(1^{\lambda_{s_i}})$ for some $\lambda_{s_i} \in \mathbb{N}$. Let $\lambda_s = \min(\lambda_{s_1}, \cdots, \lambda_{s_{n_{max}}})$. $\mathcal{A}$ is given L, a set of $\theta - 1$ private keys $\hat{s}$ and the public parameters.
2. $\mathcal{A}$ queries $\mathcal{SO}$ q_S times in arbitrary interleaf.
3. Finally $\mathcal{A}$ outputs a tuple (L^*, m^*, σ^*).

$\mathcal{A}$ wins if $\mathsf{Verify}(L^*, m^*, \sigma^*, \theta) = 1$, $L^* \subseteq L_{max}$ containing the public keys of $\hat{s}$, $|L^*| = n$ and (m^*, L^*) has never been queried to $\mathcal{SO}$. Denote $\mathsf{Adv}_{\mathcal{A}}$ be the probability that $\mathcal{A}$ wins in the above game, taken over the coin flips of $\mathcal{A}$ and the simulator.

Definition 5. *A threshold ring signature scheme is ACP-UF if no PPT adversary $\mathcal{A}$ has non-negligible $\mathsf{Adv}_{\mathcal{A}}$.*

Note that our security model is similar to the "Unforgeability against chosen-subring attacks" as in [8].

We say that a threshold ring signature scheme is *secure* if it satisfies *Correctness*, *Anonymity* and *Existential Unforgeability*.

3.2 Hierarchical Identity-Based Threshold Ring Signature

Let $\lambda_s \in \mathbb{N}$ be a security parameter and $m \in \{0,1\}^*$ be a message.

Definition 6. *A hierarchical identity-based threshold ring signature scheme is a triple (*Setup, Der, Sign, Verify*) where*

- $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Setup}(1^{\lambda_s})$ *is a PPT which takes as input a security parameter λ_s, produces the hierarchical manager's secret key sk and public key pk.*
- $(\mathsf{sk}_{\mathsf{id}.r}) \leftarrow \mathsf{Der}(\mathsf{id}, \mathsf{sk}_{\mathsf{id}}, r)$ *produces a private keys $\mathsf{sk}_{\mathsf{id}.r}$ for identity $\mathsf{id}.r$ using his parent's secret key $\mathsf{sk}_{\mathsf{id}}$.*
- $\sigma \leftarrow \mathsf{Sign}(1^{\lambda_s}, \hat{s}, L, m)$ *is a PPT which accepts as inputs a security parameter λ_s, a set of private keys $\hat{s}$, a set of public keys L including those corresponding to the private keys in $\hat{s}$ and a message m, produces a hierarchical identity-based threshold ring signature σ.*
- $1/0 \leftarrow \mathsf{Verify}(1^{\lambda_s}, L, m, \sigma, \theta)$ *is a PPT which accepts as inputs a security parameter λ_s, a set of public keys L, a message m, a signature σ and the number of signers θ, returns 1 or 0 for accept or reject, respectively.*

For simplicity, we usually omit the input of security parameter in the rest of the paper. The security of a hierarchical identity-based threshold ring signature scheme consists of three requirements, namely *Correctness*, *Anonymity* and *Existential Unforgeability*. They are defined

as follows.

Correctness. We require that $\mathsf{Verify}(L, m, \mathsf{Sign}(\hat{s}, L, m), |\hat{s}|) = 1$ for any message m and any set of private keys $\hat{s}$ which are generated by $\mathsf{Setup}(1^{\lambda_s})$ and any set of public keys L including those corresponds to the private keys in $\hat{s}$.

We have the following oracles for the adversary to query in the security game:

- Signing Oracle $\mathcal{SO}(m, L')$: On input any message m, a set of n users $L' \subseteq L_{max}$; returns a ring signature $\sigma \leftarrow \mathsf{Sign}(\hat{s}, L', m)$, such that $\mathsf{Verify}(L', m, \sigma, \theta) = 1$ where $\hat{s}$ is the set of θ private keys that correspond to θ public keys in L'.
- Key Extraction Oracle $\mathcal{KEO}(\mathsf{id})$: On input any identity id, return its corresponding secret key $\mathsf{sk}_{\mathsf{id}}$.

Anonymity. For a (n, θ)-threshold ring signature scheme of θ signers with n public keys, the anonymity is defined as the following game between a simulator and an adversary $\mathcal{A}$:

1. The simulator runs algorithm Setup. Let $L_{max} = \{P_1, \cdots, P_{n_{max}}\}$ be the set of $n_{max} \geq n$ public keys in which each key is generated as $(s_i, P_i) \leftarrow \mathsf{Setup}(1^{\lambda_{s_i}})$ for some $\lambda_{s_i} \in \mathbb{N}$. Let $\lambda_s = \min(\lambda_{s_1}, \cdots, \lambda_{s_{n_{max}}})$. $\mathcal{A}$ is given L, s_1, …, $s_{n_{max}}$ and the public parameters.
2. $\mathcal{A}$ queries $\mathcal{SO}$ q_S times in arbitrary interleaf.
3. $\mathcal{A}$ randomly selects a message m^*, two distinct sets of θ users L_0, L_1 and a ring $L^* \subseteq L_{max}$ for which $L_0, L_1 \subset L^*$ and sends to the simulator. The simulator randomly picks a bit b and returns $\sigma \leftarrow \mathsf{Sign}(\hat{s}_b, L^*, m^*)$ to $\mathcal{A}$, where $\hat{s}_b$ is the set of secret keys of $\hat{P}_b$.
4. Finally $\mathcal{A}$ outputs a bit b'.

$\mathcal{A}$ wins if $b = b'$. Denote $\mathsf{Adv}_{\mathcal{A}}$ be the probability that $\mathcal{A}$ wins in the above game over $1/2$, taken over the coin flips of $\mathcal{A}$ and the simulator.

Definition 7. *A threshold ring signature scheme is anonymous if no PPT adversary $\mathcal{A}$ win the anonymity game with non-negligible $\mathsf{Adv}_{\mathcal{A}}$.*

Existential Unforgeability. We would like to consider the security model for existential unforgeability. It models the adaptive chosen message attack. For a (n, θ, ℓ)-hierarchical identity-based threshold ring signature scheme of θ signers with n public keys (identities with level at most ℓ), the existential unforgeability is defined as the following game between a simulator and an adversary $\mathcal{A}$:

1. The simulator runs algorithm Setup. Let $L_{max} = \{\mathsf{id}_1, \cdots, \mathsf{id}_{n_{max}}\}$ be the set of n_{max} identities and the corresponding secret key generated by Der are $\mathsf{sk}_{\mathsf{id}_i}$ for $1 \leq i \leq n_{max}$. The maximum level of hierarchy for each identity is ℓ. $\mathcal{A}$ is given L_{max}, a set of $\theta - 1$ private keys $\hat{s} \subset \{\mathsf{sk}_{\mathsf{id}_1}, \ldots, \mathsf{sk}_{\mathsf{id}_{n_{max}}}\}$ and the public parameters.
2. $\mathcal{A}$ queries $\mathcal{SO}$ q_S times and $\mathcal{KEO}$ q_K times in arbitrary interleaf.
3. Finally $\mathcal{A}$ outputs a tuple (L^*, m^*, σ^*).

$\mathcal{A}$ wins if $\mathsf{Verify}(L^*, m^*, \sigma^*, \theta) = 1$, $L^* \subseteq L_{max}$ containing the identities of $\hat{s}$, $|L^*| = n$, m^* has never been queried to $\mathcal{SO}$ and no identity in L_{max} or its prefixes have been queried to $\mathcal{KEO}$. Denote $\mathsf{Adv}_{\mathcal{A}}$ be the probability that $\mathcal{A}$ wins in the above game, taken over the coin flips of $\mathcal{A}$ and the simulator.

threshold (n, θ) ring signature	sk $1 \le i \le n$	pk $1 \le i \le n$, $0 \le j < \theta$	signature and verification, $1 \le i \le n$, $0 \le j < \theta$
SDH	x_i, y_i	$h_j, g, g^{x_i}, g^{y_i}, \mathcal{H}_i(\cdot)$	(σ_i, R_i): $\prod_i \sigma_i^{i^j(x_i+\mathcal{H}_i(m)+R_i y_i)} = h_j$
PSDH	x_i, y_i	$h_j, g, g^{x_i}, g^{y_i}, g^{z_i y_i}, \mathcal{H}(\cdot)$	(σ_i, m_1): $\prod_i \sigma_i^{i^j(x_i+m_1)(y_i+m_2)} = h_j$ $\mathcal{H}(m) = m_1 \oplus m_2$
HaCL04B-wh	x_i, y_i, z_i	$h_j, g, g^{x_i}, g^{y_i}, g^{z_i}$, $g^{x_i y_i}, g^{y_i z_i}, g^{x_i y_i z_i}, \mathcal{H}_i(\cdot)$	$(R_i, a_i, A_i, b_i, B_i, c_i)$: $A_i = a_i^{z_i}$ $\wedge\ b_i = a_i^{y_i}\ \wedge\ B_i = A_i^{y_i}$ $\wedge\ c_i = (a_i b_i^{\mathcal{H}_i(m)} B_i^{R_i})^{x_i}$ for all i $\wedge\ h_j = \prod_{i=1}^n (a_i)^{i^j}$.
SDH*	x_i	$h_j, g, g^{x_i}, \mathcal{H}_i(\cdot)$	(σ_i): $\prod_i \sigma_i^{i^j(x_i+\mathcal{H}_i(m))} = h_j$
BLS	x_i	$g, g^{x_i}, \mathcal{H}_j(\cdot)$	(σ_i, h_i): $\prod_i h_i^{i^j} = \mathcal{H}_j(\mathsf{pk}, m)$, $h_i^{x_i} = \sigma_i$ for all i
CL04A	x_i, y_i	$h_j, g, g^{x_i}, g^{y_i}, g^{x_i y_i}$	(a_i, b_i, c_i): $h_j = \prod_i a_i^{i^j}$, $b_i = a_i^{y_i}$, $c_i = a_i^{x_i + m x_i y_i}$ for all i
CL04B	x_i, y_i, z_i	$h_j, g, g^{x_i}, g^{y_i}, g^{z_i}$, $g^{x_i y_i}, g^{y_i z_i}, g^{x_i y_i z_i}$	$(a_i, A_i, b_i, B_i, c_i)$: $A_i = a_i^{z_i}$ $\wedge\ b_i = a_i^{y_i}\ \wedge\ B_i = A_i^{y_i}$ $\wedge\ c_i = (a_i b_i^{m_1} B_i^{m_2})^{x_i}$ for all i $\wedge\ h_j = \prod_{i=1}^n (a_i)^{i^j}$ $\wedge\ m = (m_1, m_2)$.

Table 1. Threshold ring signatures without random oracles.

Definition 8. *A hierarchical identity-based threshold ring signature scheme is ACP-UF if no PPT adversary $\mathcal{A}$ has non-negligible* $\mathsf{Adv}_{\mathcal{A}}$.

We also define a weaker version of unforgeability, namely "Selective-ID, ACP-UF" (sID-ACP-UF). The difference with ACP-UF is that the adversary $\mathcal{A}'$ gives the identity that he will forge at the beginning of the game. Then during the game, the adversary is not allowed to query $\mathcal{KEO}$ and $\mathcal{SO}$ for this identity or its prefix. Denote $\mathsf{Adv}_{\mathcal{A}'}$ be the probability that $\mathcal{A}'$ wins in the above game, taken over the coin flips of $\mathcal{A}'$ and the simulator.

Definition 9. *A hierarchical identity-based threshold ring signature scheme is sID-ACP-UF if no PPT adversary $\mathcal{A}'$ has non-negligible* $\mathsf{Adv}'_{\mathcal{A}}$.

We say that a hierarchical identity-based threshold ring signature scheme is *secure* if it satisfies *Correctness*, *Anonymity* and *Existential Unforgeability*.

4 Threshold ring signatures without random oracles

We introduce the first threshold ring signature schemes without random oracles. For threshold ring signature schemes, a group of θ signers can form a ring of size n and sign on behalf of the ring. Notice that $\theta = 1$ specializes threshold ring signatures to ring signatures, and if further $n = 1$ then ring signatures specialize to ordinary signatures.

In this section, we introduce threshold ring signature schemes which originate from the standard signatures in [41, 10, 14, 17]. We first introduce three schemes $\mathsf{TRS}_{\mathsf{SDH}}$, $\mathsf{TRS}_{\mathsf{PSDH}}$ and $\mathsf{TRS}_{\mathsf{HaCL04B\text{-}wh}}$, and then introduce four other schemes whose intractability assumptions include external oracles. The intractability assumptions for all schemes can be found in table 2.

scheme	intractability assumption	intractability problem
SDH	(q,n,θ) -DsjSDH	Given $\{h_j : 0 \le j < \theta\}$, g, $\{x_i : 1 \le i \le \theta-1\}$, $\{g^{x_k} : \theta \le k \le n\}$, collision resistant hash function $\mathcal{H}_1$, …, $\mathcal{H}_n$, $\{(m_{i,\tau}, \sigma_{i,\tau}) : 1 \le i \le n, 1 \le \tau \le q\}$ such that $\prod_{i=1}^{n} \sigma_{i,\tau}^{i^j(x_i+\mathcal{H}_i(m_{i,\tau}))} = h_j$ for $\forall \tau, j$, all m_τ's are distinct. Then compute $\{m^*, (\sigma_i^*, \gamma_i) : 1 \le i \le n\}$, such that $h_j = \prod_{i=1}^{n} \sigma_i^{*\,i^j(x_i+\mathcal{H}_i(m^*)+\gamma_i)}$ $\forall j$, $0 \le j < \theta$, and for all τ, $\mathcal{H}_i(m^*) + \gamma_i \ne \mathcal{H}_i(m_\tau)$ with some i.
PSDH	(q,n,θ) -DsjSDH'	Given $\{h_j : 0 \le j < \theta\}$, g, $\{x_i : 1 \le i \le \theta-1\}$, $\{g^{x_k} : \theta \le k \le n\}$, $\{(m_{i,\tau}, \sigma_{i,\tau}) : 1 \le i \le n, 1 \le \tau \le q\}$ such that $\prod_{i=1}^{n} \sigma_{i,\tau}^{i^j(x_i+m_{i,\tau})} = h_j$ for $\forall \tau, j$, all m_τ's are distinct. Then compute $\{m^*, \sigma_1^*, \ldots, \sigma_n^*\}$, such that $h_j = \prod_{i=1}^{n} \sigma_i^{*\,i^j(x_i+m^*)}$ $\forall j$, $0 \le j < \theta$, and for all τ, $m^* \ne m_\tau$ with some i.
	$(\mathcal{H}, q)$ -SSPI	Given $\mathcal{H}$, distinct nonzero $a_1, \ldots, a_q$, output b and (i,j), $1 \le i < j \le q$, satisfying $\mathcal{H}(b) = a_i \oplus a_j$.
HaCL04B-wh	(q,n,θ) -whLRSW	Given g, $\{x_i, y_i : 1 \le i \le \theta-1\}$, $\{g^{x_k}, g^{y_k}, g^{x_k y_k} : \theta \le k \le n\}$, $\{h_j : 0 \le j < \theta\}$, collision resistant hash function $\mathcal{H}_1$, …, $\mathcal{H}_n$, $\{(\hat{m}_\tau, \hat{a}_{i,\tau}, \hat{b}_{i,\tau}, \hat{c}_{i,\tau}) : 1 \le \tau \le q, 1 \le i \le n\}$ such that: $\hat{b}_{i,\tau} = \hat{a}_{i,\tau}^{y_i}$, $\hat{c}_{i,\tau} = \hat{a}_{i,\tau}^{x_i + x_i y_i \mathcal{H}_i(\hat{m}_\tau)}$, $h_j = \prod_{i=1}^{n} (\hat{a}_i)^{i^j}$ for all j, and all $\hat{m}_\tau$'s are distinct; to output $\{m^*, (a_i^*, b_i^*, c_i^*, \gamma_i) : 1 \le i \le n\}$, such that $b_i^* = a_i^{*y_i}$, $c_i^* = a_i^{*x_i + x_i y_i \mathcal{H}_i(m^*) + x_i \gamma_i}$, $h_j = \prod_{i=1}^{n} (a_i^*)^{i^j}$ for all j; and for all τ, $\mathcal{H}_i(m^*) + \gamma_i \ne \mathcal{H}_i(\hat{m}_\tau)$ with some i.
SDH*	(q,n,θ) -ODsjSDH*	Given $\{h_j : 0 \le j < \theta\}$, g, x_i for $1 \le i \le \theta-1$, g^{x_k} for $\theta \le k \le n$, collision resistant hash function $\mathcal{H}_1$, …, $\mathcal{H}_n$, and an oracle $O(\cdot)$ which upon input m_τ returns $(\sigma_{1,\tau}, \ldots, \sigma_{n,\tau})$ such that $h_j = \prod_{i=1}^{n} \sigma_{i,\tau}^{(x_i + \mathcal{H}_i(m_\tau))i^j}$ $\forall j$, sequentially for $1 \le \tau \le q$; to output $(m^*, \sigma_1^*, \ldots, \sigma_n^*)$ such that $h_j = \prod_{i=1}^{n} \sigma_i^{*(x_i + \mathcal{H}_i(m^*))i^j}$ $\forall j$ and $m^* \ne m_\tau$ $\forall \tau$.
BLS	(q, n, θ) -ODsjBLS	Given g, x_1, …, $x_{\theta-1}$, g^{x_i}, $\theta \le i \le n$, collision resistant hash function $\mathcal{H}_0$, …, $\mathcal{H}_{\theta-1}$ and an oracle $O(\cdot)$ which upon input m_τ returns $(\sigma_{1,\tau}, h_{1,\tau}, \ldots, \sigma_{n,\tau}, h_{n,\tau})$ such that $\sigma_{i,\tau} = h_{i,\tau}^{x_i}$, $\mathcal{H}_j(m_\tau) = \prod_{i=1}^{n} (h_{i,\tau})^{i^j}$ $\forall j$, sequentially for $1 \le \tau \le q$; to output $(\sigma_1^*, h_1^*, \ldots, \sigma_n^*, h_n^*)$ such that $\sigma_i^* = h_i^{*x_i}$, $\mathcal{H}_j(m^*) = \prod_{i=1}^{n} (h_i^*)^{i^j}$ $\forall j$.
CL04A, CL04B	(q, n, θ) -ODsjLRSW	Given g,$\{x_i, y_i : 1 \le i \le \theta-1\}$, $\{g^{x_k}, g^{y_k}, g^{x_k y_k} : \theta \le k \le n\}$, $\{h_j : 0 \le j < \theta\}$, and an oracle $O(\cdot)$ which upon input m_τ and returns $(a_{i,\tau}, b_{i,\tau}, c_{i,\tau})$ for $1 \le i \le n$ such that $b_i = a_i^{y_i}$, $c_i = a_i^{x_i + x_i y_i m}$, $h_j = \prod_{i=1}^{n} (a_{i,\tau})^{i^j}$ $\forall j$, sequentially for $1 \le \tau \le q$; to output $\{m^*, (a_i^*, b_i^*, c_i^*, \gamma_i) : 1 \le i \le n\}$, such that $b_i^* = a_i^{*y_i}$, $c_i^* = a_i^{*x_i + x_i y_i \mathcal{H}_i(m^*)}$, $h_j = \prod_{i=1}^{n} (a_i^*)^{i^j}$ $\forall j$ and $m^* \ne m_\tau$ $\forall \tau$.

Table 2. Threshold ring signatures' intractability assumptions.

4.1 Threshold ring signature $\mathsf{TRS}_{\mathsf{SDH}}(n, \theta)$

We introduce the threshold ring signature scheme which originates from the second signature scheme in [10]. The ring signature of this scheme is introduced in [22]. The threshold ring signature scheme is as follows:

1. Setup: User i's sk-pk pair is $((x_i, y_i), (g^{x_i}, g^{y_i}))$, for $1 \le i \le n$. The ring signature's public keys includes all user public keys plus h_j, $0 \le j < \theta$ and collision resistant hashing functions $\mathcal{H}_i$.
2. Sign: The users' public keys are $(g^{x_1}, g^{y_1}, \ldots, g^{x_n}, g^{x_n})$. WLOG, suppose the signers are $(g^{x_1}, g^{y_1}), \ldots, (g^{x_\theta}, g^{y_\theta})$, having secret keys $(x_1, y_1), \ldots, (x_\theta, y_\theta)$ respectively.
   (a) For $i \in \{\theta+1, \ldots, n\}$, the signers pick $r_i, R_i \in_R \mathbb{Z}_p^*$ and set $\sigma_i = g^{r_i}$, $W_i = g^{r_i(x_i + H_i(m) + R_i y_i)}$.

(b) Then they solve for $W_1, \ldots W_\theta$ such that:

$$\prod_{i=1}^{n} W_i^{i^j} = h_j \quad \text{for all} \quad j \in \{0, \ldots, \theta - 1\}.$$

(c) For each user $j \in \{1, \ldots, \theta\}$, he picks $R_i \in_R \mathbb{Z}_p^*$ and computes $\sigma_j = W_j^{1/(x_j + \mathcal{H}_j(m) + R_j y_j)}$ using his own secret key x_j, y_j.
(d) The threshold ring signature is:

$$\sigma = ((\sigma_1, R_1), \cdots, (\sigma_n, R_n))$$

3. Verify: The verification is

$$\hat{\mathbf{e}}(h_j, g) = \prod_{i=1}^{n} \hat{\mathbf{e}}(\sigma_i, g^{(x_i + \mathcal{H}_i(m) + R_i y_i) i^j}), \text{ for every } j, 0 \leq j < \theta \tag{1}$$

Theorem 1. *The threshold ring signature* $\mathsf{TRS}_{\mathsf{SDH}}{-}(n, \theta)$ *is secure provided the* (q_S, n, θ)*-DsjSDH Assumption holds and* $\mathcal{H}_i$ *are collision-resistant hashing functions.*

Corollary 1. *The* $\mathsf{TRS}_{\mathsf{SDH}}(n, 1)$ *is secure provided the* $(q_S, n, 1)$*-DsjSDH Assumption holds and* $\mathcal{H}_i$ *are collision-resistant hashing functions.*

Corollary 2. *The* $\mathsf{TRS}_{\mathsf{SDH}}(1, 1)$ *is secure provided the* $(q_S, 1, 1)$*-DsjSDH Assumption holds and* $\mathcal{H}_i$ *are collision-resistant hashing functions.*

Proof Sketch: The proof of correctness of the scheme is straightforward and hence is omitted.

Then we prove the anonymity below. For $i \in \{\theta + 1, \ldots, n\}$, σ_i's are random since r_i's are randomly picked. For $j \in \{1, \ldots, \theta\}$, σ_j's can be considered as in the form of g^{r_j} as g is the generator and hence such r_j always exists. They are determined by σ_i's by the equations, so σ_j's is also uniformly distributed. Also the $R_1, \ldots, R_n$ are also randomly picked. To conclude, the distribution of the components of the signature generated by our scheme is independent of what is the group of participating signers, for any message m and any set of signers associated to the ring signature. Therefore the adversary $\mathcal{A}$ has no advantage in winning the anonymity game.

We prove the unforgeabiltiy below. **Setup**: Simulator $\mathcal{S}$ receives a (q_S, n, θ)-DsjSDH Problem instance: Given h_0, …, $h_{\theta-1}$, $\mathcal{H}_1$, …, $\mathcal{H}_n$, g, g^z, distinct z_1, …, $z_{\theta-1}$, $\{a_i : \theta \leq i \leq n\}$, $\{\hat{m}_\tau : 1 \leq \tau \leq q_S\}$, $\{\hat{\sigma}_{i,\tau} : 1 \leq i \leq n, 1 \leq \tau \leq q_S\}$ such that:

$$\prod_{i=1}^{\theta-1} \hat{\sigma}_{i,\tau}^{(z_i + \mathcal{H}_i(\hat{m}_\tau)) i^j} \prod_{i=\theta}^{n} \hat{\sigma}_{i,\tau}^{(z a_i + \mathcal{H}_i(\hat{m}_\tau)) i^j} = h_j \quad \text{for} \quad \forall j \in \{0, \ldots, \theta - 1\}, \tau \in \{1, \ldots, q_S\}$$

For simplicity, denote $z a_i = z_i$ for $\theta \leq i \leq n$. $\mathcal{S}$ randomly picks z_{n+1}, …, $z_{n_{max}}$. $\mathcal{S}$ flips a fair coin c_{mode} and sets up as follows:

1. If $c_{mode} = 1$, $\mathcal{S}$ randomly picks y_i, sets $\mathsf{pk}_i = (g^{z_i}, g^{y_i})$, $1 \leq i \leq n_{max}$.
2. If $c_{mode} = 2$, $\mathcal{S}$ randomly picks x_i, sets $\mathsf{pk}_i = (g^{x_i}, g^{z_i})$, $1 \leq i \leq n_{max}$.

(*Remark:* For simplicity we do not shuffle the index of users here.)
Simulating $\mathcal{SO}$: If $c_{mode} = 1$, upon the τ-th $\mathcal{SO}$ query input (m_τ, L_τ), $1 \leq \tau \leq q_S$:

– If $L_\tau \neq (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$, then $\mathcal{S}$ knows at least θ secret keys and hence can compute the threshold ring signature.
– If $L_\tau = (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$, then do the followings. If $m_\tau = \hat{m}_\tau$, $\mathcal{S}$ aborts the simulation. Otherwise, $\mathcal{S}$ sets $m_{i,\tau} = \mathcal{H}_i(m_\tau)$ and computes $R_{i,\tau}$ satisfying $\mathcal{H}_i(\hat{m}_\tau) = m_{i,\tau} + R_{i,\tau} y_i$. Output the ring signature $(\sigma_{i,\tau}, R_{i,\tau})$, with $\sigma_{i,\tau} = \hat{\sigma}_{i,\tau}$. Note $\prod_{i=1}^{n} \sigma_{i,\tau}^{(x_i + m_{i,\tau} + R_{i,\tau} y_i) i^j} = h_j$.

If $c_{mode} = 2$, upon the τ-th $\mathcal{SO}$ query input (m_τ, L_τ), $1 \leq \tau \leq q_S$:

– If $L_\tau \neq (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$, then $\mathcal{S}$ knows at least θ secret keys and hence can compute the threshold ring signature.
– If $L_\tau = (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$, then do the followings. If $m_\tau = \hat{m}_\tau$, $\mathcal{S}$ aborts the simulation. Otherwise, $\mathcal{S}$ sets $m_{i,\tau} = \mathcal{H}_i(m_\tau)$, compute $R_{i,\tau} = (x_i + m_{i,\tau})/\mathcal{H}_i(\hat{m}_\tau)$. Output the ring signature $(\sigma_{i,\tau}, R_{i,\tau})$, with $\sigma_{i,\tau} = \hat{\sigma}_{i,\tau}^{1/R_{i,\tau}}$. Note $\prod_{i=1}^{n} \sigma_{i,\tau}^{(x_i + m_{i,\tau} + R_{i,\tau} y_i) i^j} = h$.

Simulation Deviation: It can be shown that any pairwise statistical distance among (1) Real World, (2) Ideal World-1 where $c_{mode} = 1$, and (3) Ideal-World-2 where $c_{mode} = 2$, is negligible. The proof is tedious but mechanical. We omit it.

Extractions: With probability ϵ, attacker $\mathcal{A}$ eventually delivers a forgery message-signature pair $(L^*, m^*, (\sigma_i^*, R_i^*))$, $m^* \neq m_\tau$, $\forall \tau$. If $L^* \neq (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$, $\mathcal{S}$ declares failure and exits. Otherwise $L^* = (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$ and there are two cases:

With $c_{mode} = 1$, and $x_i = z_i$: Conditioned on the above event, let $\epsilon_{1,1}$ denote the conditional probability of $\mathcal{A}$'s delivered ring signature satisfying $\mathcal{H}_i(m^*) + R_i^* y_i \neq \mathcal{H}_i(\hat{m}_\tau)$ $\exists i$ for every τ. $\mathcal{S}$ outputs $(m^*, (\sigma_i^*, R_i^* y_i) : 1 \leq i \leq n)$ and the (q_S, n, θ)-DsjSDH Problem is solved.

With $c_{mode} = 2$, and $y_i = z_i$: Conditioned on the above event, let $\epsilon_{2,2}$ denote the conditional probability of $\mathcal{A}$'s delivered ring signature satisfying $\mathcal{H}_i(m^*) + R_i^* y_i = \mathcal{H}_i(\hat{m}_\tau)$ for all i, for some τ. Note $\mathcal{H}_i(m^*) + R_i^* y_i = \mathcal{H}_i(m_\tau) + R_{i,\tau} y_i$ and $m^* \neq m_\tau$. We obtain $y_i = (R_{i,\tau} - R_i^*)^{-1}$ $(\mathcal{H}_i(m^*) - \mathcal{H}_i(m_\tau))$. The DLP for $y_i = z a_i$ is solved, and consequently the (q_S, n, θ)-DsjSDH Problem at hand is solved.

□

4.2 Threshold ring signature $\mathsf{TRS}_{\mathsf{PSDH}}(n, \theta)$

We introduce the threshold ring signature scheme which originates from the signature scheme in [41]. The threshold ring signature scheme is as follows:

1. Setup: User i's sk-pk pair is $((x_i, y_i), (g^{x_i}, g^{y_i}, g^{x_i y_i}))$ for $1 \leq i \leq n$. The ring signature's public keys include all user public keys plus h_j, $0 \leq j < \theta$ and collision resistant hashing functions $\mathcal{H}$.
2. Sign: The users' public keys are $(g^{x_1}, g^{y_1}, g^{x_1 y_1}, \ldots, g^{x_n}, g^{x_n}, g^{x_n y_n})$. WLOG, suppose the signers have secret keys $(x_1, y_1), \ldots, (x_\theta, y_\theta)$.
   (a) The signers randomly pick m_1 and compute $m_2 = \mathcal{H}(m) \oplus m_1$.
   (b) For $i \in \{\theta+1, \ldots, n\}$, the signers pick $r_i \in_R \mathbb{Z}_p^*$ and sets $\sigma_i = g^{r_i}$, $W_i = g^{r_i (x_i + m_1)(y_i + m_2)}$.
   (c) Then they solve for $W_1, \ldots W_\theta$ such that:

$$\prod_{i=1}^{n} W_i^{i^j} = h_j \quad \text{for all} \quad j \in \{0, \ldots, \theta - 1\}.$$

   (d) For each user $j \in \{1, \ldots, \theta\}$, he picks $R_i \in_R \mathbb{Z}_p^*$ and computes $\sigma_j = W_j^{1/(x_j + m_1)(y_j + m_2)}$ using his own secret key x_j, y_j.

(e) The threshold ring signature is:

$$\sigma = (\sigma_1, \cdots, \sigma_n, m_1)$$

3. Verify: The verification is

$$\hat{\mathbf{e}}(h_j, g) = \prod_{i=1}^{n} \hat{\mathbf{e}}(\sigma_i, g^{(x_i+m_1)(y_i+m_2)i^j}), \text{ for every } j, 0 \le j < \theta \tag{2}$$

where $\mathcal{H}(m) = m_1 \oplus m_2$.

Theorem 2. *The threshold ring signature $\mathsf{TRS}_{\mathsf{PSDH}}(n, \theta)$ is secure provided the (q_S, n, θ)-DsjSDH' Assumption holds and $\mathcal{H}$ is a collision-resistant, SSPIR(Sum Second Pre-Image Resistant) hashing function.*

Corollary 3. *The $\mathsf{TRS}_{\mathsf{PSDH}}(n, 1)$ is secure provided the $(q_S, n, 1)$-DsjSDH' Assumption holds and $\mathcal{H}$ is a collision-resistant, SSPIR hashing function.*

Corollary 4. *The $\mathsf{TRS}_{\mathsf{PSDH}}(1, 1)$ is secure provided the $(q_S, 1, 1)$-DsjSDH Assumption holds and $\mathcal{H}$ is a collision-resistant, SSPIR hashing function.*

Proof Sketch: The proof of correctness and the anonymity of the scheme are straightforward and hence are omitted. We prove the unforgeabiltiy below.

Setup: Simulator $\mathcal{S}$ receives a (q_S, n, θ)-DsjSDH' Problem instance: Given h_0, ..., $h_{\theta-1}$, g, g^z, distinct z_1, ..., $z_{\theta-1}$, $\{a_i : \theta \le i \le n\}$, $\{\hat{m}_\tau : 1 \le \tau \le q_S\}$, $\{\hat{\sigma}_{i,\tau} : 1 \le i \le n, 1 \le \tau \le q_S\}$ such that:

$$\prod_{i=1}^{\theta-1} \hat{\sigma}_{i,\tau}^{(z_i+\hat{m}_\tau)i^j} \prod_{i=\theta}^{n} \hat{\sigma}_{i,\tau}^{(za_i+\hat{m}_\tau)i^j} = h_j \quad \text{for} \quad \forall j \in \{0, \ldots, \theta-1\}, \tau \in \{1, \ldots, q_S\}$$

For simplicity, denote $za_i = z_i$ for $\theta \le i \le n$. $\mathcal{S}$ randomly picks z_{n+1}, ..., $z_{n_{max}}$. $\mathcal{S}$ flips a fair coin c_{mode} and sets up as follows:

1. If $c_{mode} = 1$, $\mathcal{S}$ randomly picks y_i, sets $\mathsf{pk}_i = (g^{z_i}, g^{y_i})$, $1 \le i \le n_{max}$.
2. If $c_{mode} = 2$, $\mathcal{S}$ randomly picks x_i, sets $\mathsf{pk}_i = (g^{x_i}, g^{z_i})$, $1 \le i \le n_{max}$.

(*Remark:* For simplicity we do not shuffle the index of users here.)

Simulating $\mathcal{SO}$: If $c_{mode} = 1$, upon the τ-th $\mathcal{SO}$ query input (m_τ, L_τ), $1 \le \tau \le q_S$:

- If $L_\tau \ne (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$, then $\mathcal{S}$ knows at least θ secret keys and hence can compute the threshold ring signature.
- If $L_\tau = (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$, then do the followings. If $\mathcal{H}(m_\tau) = \hat{m}_\tau$, $\mathcal{S}$ declares failure and exits. Otherwise, set $m_{1,\tau} = \hat{m}_\tau$ and compute $m_{2,\tau} = \mathcal{H}(m_\tau) \oplus m_{1,\tau}$. Output the ring signature $(\sigma_{i,\tau}, m_{1,\tau})$, with $\sigma_{i,\tau} = \hat{\sigma}_{i,\tau}^{1/(y_i+m_{2,\tau})}$. Note $\prod_{i=1}^{n} \sigma_{i,\tau}^{(za_i+\hat{m}_\tau)(y_i+m_{2,\tau})i^j} = h_j$.

If $c_{mode} = 2$, upon the τ-th $\mathcal{SO}$ query input (m_τ, L_τ), $1 \le \tau \le q_S$:

- If $L_\tau \ne (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$, then $\mathcal{S}$ knows at least θ secret keys and hence can compute the threshold ring signature.
- If $L_\tau = (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$, then do the followings. If $\mathcal{H}(m_\tau) = \hat{m}_\tau$, $\mathcal{S}$ declares failure and exits. Otherwise, set $m_{2,\tau} = \hat{m}_\tau$ and compute $m_{1,\tau} = \mathcal{H}(m_\tau) \oplus m_{2,\tau}$. Output the ring signature $(\sigma_{i,\tau}, m_{2,\tau})$, with $\sigma_{i,\tau} = \hat{\sigma}_{i,\tau}^{1/(x_i+m_{1,\tau})}$. Note $\prod_{i=1}^{n} \sigma_{i,\tau}^{(x_i+m_{1,\tau})(za_i+\hat{m}_\tau)i^j} = h_j$.

Simulation Deviation: It can be shown that any pairwise statistical distance among (1) Real World, (2) Ideal World-1 where $c_{mode} = 1$, and (3) Ideal-World-2 where $c_{mode} = 2$, is negligible. The proof is tedious but mechanical. We omit it.

Extractions: With probability ϵ, attacker $\mathcal{A}$ eventually delivers a forgery message-signature pair $(L^*, m^*, m_1^*, \sigma_i^*)$, $m^* \neq m_\tau, \forall \tau$. If $L^* \neq (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$, $\mathcal{S}$ declares failure and exits. Otherwise $L^* = (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$ and then $\mathcal{S}$ computes $m_2^* = H(m^*) \oplus m_1^*$. When the pair is valid, one of the following events must happen:

- Event A1: $m_1^* \neq m_{1,\tau}$, for any τ. If also $c_{mode} = 1$, then the DsjSDH' problem instance is solved by the tuple $(m_1^*, \sigma_i^{*(y_i + m_2^*)})$.
- Event A2: $m_2^* \neq m_{2,\tau}$, for any τ. If also $c_{mode} = 2$, then the DsjSDH' Problem instance is solved by the tuple $(m_2^*, \sigma_i^{*(x_i + m_1^*)})$.
- Event B: $m_1^* = m_{1,\tau}$ and $m_2^* = m_{2,\tau'}$ for some $\tau \neq \tau'$. The $(\mathcal{H}, q_S)$-SSPI Problem is solved by (m^*, τ, τ') where $\mathcal{H}(m^*) = m_{1,\tau} \oplus m_{2,\tau'}$.
- Event C: $m_1^* = m_{1,\tau}$ and $m_2^* = m_{2,\tau}$. Then we have $m^* \neq m_\tau$ and $\mathcal{H}(m^*) = \mathcal{H}(m_\tau)$. Then $\mathcal{H}$ is not collision-resistant.

Remarks: For the threshold ring signature using the product SDH type assumptions, we can also have a variant that $m_{1,i} \oplus m_{2,i} = \mathcal{H}_i(m)$, where each $m_{1,i}, m_{2,i}$ are distinct for different i. The scheme and proofs are similar and hence are omitted.

4.3 Threshold ring signature $\mathsf{TRS}_{\mathsf{HaCL04B\text{-}wh}}(n, \theta)$

In [41], they introduce a signature scheme without random oracles which originates from the signature scheme B in [17]. We introduce the threshold ring signature scheme version for it. The scheme is as follows:

1. Setup: User i's sk-pk pair is $((x_i, y_i, z_i), (g^{x_i}, g^{y_i}, g^{z_i}, g^{x_i y_i}, g^{y_i z_i}, g^{x_i y_i z_i}))$ for $1 \leq i \leq n$. The ring signature's public keys include all user public keys, $h_0, \ldots, h_{\theta-1}$, and collision resistant hashing functions $\mathcal{H}_1$, ..., $\mathcal{H}_n$.
2. Sign: WLOG, suppose the signers have secret keys x_j, y_j for $1 \leq j \leq \theta$.
   (a) For $i \in \{\theta + 1, \ldots, n\}$, the signers pick $r_i, R_i \in_R \mathbb{Z}_p^*$ and set $a_i = g^{r_i}$, $A_i = g^{z_i r_i}$, $b_i = g^{y_i r_i}$, $B_i = g^{y_i z_i r_i}$, $c_i = g^{x_i r_i} g^{x_i y_i r_i m_1} g^{x_i y_i z_i r_i m_2}$.
   (b) The signers compute a_1, ..., a_θ such that $h_j = \prod_{i=1}^{n} (a_i)^{i^j}$ for $0 \leq j < \theta$.
   (c) Each signer t computes $A_t = a_t^{z_t}$, $b_t = a_t^{y_t}$, $B_t = a_t^{y_t z_t}$, $c_t = (a_t b_t^{\mathcal{H}_{i(m)}} B_t^{R_t})^{x_t}$ using his secret keys (x_t, y_t, z_t).
   (d) The threshold ring signature is

$$\sigma = ((R_1, a_1, A_1, b_1, B_1, c_1), \cdots, (R_n, a_n, A_n, b_n, B_n, c_n))$$

3. Verify: The verification is

$$\begin{aligned} & \hat{\mathbf{e}}(A_i, g) = \hat{\mathbf{e}}(a_i, g^{z_i}) \ \wedge \ \hat{\mathbf{e}}(b_i, g) = \hat{\mathbf{e}}(a_i, g^{y_i}) \ \wedge \ \hat{\mathbf{e}}(B_i, g) = \hat{\mathbf{e}}(A_i, g^{y_i}) \\ \wedge \ & \hat{\mathbf{e}}(B_i, g) = \hat{\mathbf{e}}(b_i, g^{z_i}) \ \wedge \ \hat{\mathbf{e}}(c_i, g) = \hat{\mathbf{e}}(a_i b_i^{\mathcal{H}_{i(m)}} B_i^{R_i}, g^{x_i}) \text{ for all } i \\ \wedge \ & h_j = \prod_{i=1}^{n} (a_i)^{i^j} \quad \text{for all} \quad j \end{aligned} \tag{3}$$

Theorem 3. *The threshold ring signature* $\mathsf{TRS}_{\mathsf{HaCL04B\text{-}wh}}(n,\theta)$ *is secure provided the* $(q_S,$ $n,\theta)$*-whLRSW Assumption holds and* $\mathcal{H}_1, \ldots, \mathcal{H}_n$ *are collision-resistant hashing functions.*

Corollary 5. *The* $\mathsf{TRS}_{\mathsf{HaCL04B\text{-}wh}}(n,1)$ *is secure provided the* $(q,n,1)$*-whLRSW Assumption holds and* $\mathcal{H}_1, \ldots, \mathcal{H}_n$ *are collision-resistant hashing functions.*

Corollary 6. *The* $\mathsf{TRS}_{\mathsf{HaCL04B\text{-}wh}}(1,1)$ *is secure provided the* $(q,1,1)$*-whLRSW Assumption holds and* $\mathcal{H}_1, \ldots, \mathcal{H}_n$ *are collision-resistant hashing functions.*

Proof Sketch: The proof of correctness and the anonymity of the scheme are straightforward and hence are omitted. We prove the unforgeabiltiy below.

Setup: Simulator $\mathcal{S}$ receives, simultaneously, the following problem instances:

1. a (q,n,θ)-whLRSW problem instance: g, $\{(u_j,v_j) : 1 \le j \le \theta-1\}$, $\{(g^{u_k}, g^{v_k}) : \theta \le k \le n\}$, $\mathcal{H}_1, \ldots, \mathcal{H}_n$, $(\hat{m}_\tau, \hat{a}_{i,\tau}, \hat{b}_{i,\tau}, \hat{c}_{i,\tau})$, for $1 \le \tau \le q_S$, $1 \le i \le n$ such that:

$$\hat{\mathbf{e}}(\hat{b}_{i,\tau}, g) = \hat{\mathbf{e}}(\hat{a}_{i,\tau}, g^{v_i}) \ \wedge \ \hat{\mathbf{e}}(\hat{c}_{i,\tau}, g) = \hat{\mathbf{e}}(\hat{a}_{i,\tau}\hat{b}_{i,\tau}^{\mathcal{H}_i(\hat{m}_\tau)}, g^{u_i}) \ \wedge \ h_j = \prod_{i=1}^{n} (\hat{a}_i)^{i^j} \quad \text{for all} \quad j$$

2. a DL (discrete logarithm) problem instance: g, g^w.

$\mathcal{S}$ flips a fair coin c_{mode} and sets up as follows:

1. If $c_{mode} = 1$, $\mathcal{S}$ randomly picks z_i for $1 \le i \le n_{max}$, u_j, v_j for $n+1 \le j \le n_{max}$, sets $\mathsf{pk} = (g^{u_i}, g^{v_i}, g^{z_i})$.
2. If $c_{mode} = 2$, $\mathcal{S}$ randomly picks x_i, y_i, z_i for $1 \le i \le n_{max}$, except for random index $t \in \{1, \ldots, n_{max}\}$, $\mathcal{S}$ sets $z_t = w$. $\mathcal{S}$ then sets $\mathsf{pk} = (g^{x_i}, g^{y_i}, g^{z_i})$.

(*Remark:* For simplicity we do not shuffle the index of users here.)

Simulating $\mathcal{SO}$: If $c_{mode} = 1$, upon the τ-th $\mathcal{SO}$ query input (m_τ, L_τ), $1 \le \tau \le q_S$:

- If $L_\tau \ne (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$, then $\mathcal{S}$ knows at least θ secret keys and hence can compute the threshold ring signature.
- If $L_\tau = (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$, then do the followings. If $\hat{m}_\tau = m_\tau$, $\mathcal{S}$ declares failure and exits. Otherwise, solve for $R_{i,\tau}$ such that $\mathcal{H}_i(\hat{m}_\tau) = \mathcal{H}_i(m_\tau) + R_{i,\tau} z_i$ for $1 \le i \le n$. Output the signature $(R_{i,\tau}, a_{i,\tau} = \hat{a}_{i,\tau}, A_{i,\tau} = a_{i,\tau}^{z_i}, b_{i,\tau} = \hat{b}_{i,\tau}, B_{i,\tau} = b_{i,\tau}^{z_i}, c_{i,\tau} = \hat{c}_\tau)$.

If $c_{mode} = 2$, for the τ-th $\mathcal{SO}$ query input (m_τ, L_τ), $1 \le \tau \le q_S$, then $\mathcal{S}$ knows at least θ secret keys and hence can compute the threshold ring signature.

Simulation deviation: It can be shown that the pairwise simulation deviation between any two of the following worlds are negligible: (1) Real World, (2) Ideal World-1 where $c_{mode} = 1$, and (3) Ideal-World-2 where $c_{mode} = 2$. The proof is tedious but mechanical. We omit it.

Extraction: With probability ϵ, attacker $\mathcal{A}$ eventually delivers a valid message-signature pair $(L^*, m^*, (R_i^*, a_i^*, A_i^*, b_i^*, B_i^*, c_i^*))$, for $1 \le i \le n$, $m^* \ne m_\tau$ for all τ. If $L^* \ne (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$, $\mathcal{S}$ declares failure and exits. Otherwise $L^* = (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$ and then there are two events:

- Event A: For each τ, $\mathcal{H}_i(m^*) + R_i^* z_i \ne \mathcal{H}_i(\hat{m}_\tau)$ for some $1 \le i \le n$.
- Event B: For some τ, $\mathcal{H}_i(m^*) + R_i^* z_i = \mathcal{H}_i(\hat{m}_\tau)$ for all $1 \le i \le n$.

For $i = 1, 2$, let $\epsilon_{i,A}$ (resp. $\epsilon_{c_{mode},B}$) denotes the probability that $c_{mode} = i$ and Event A (resp. Event B). The negligibility of simulation deviations implies that $\epsilon_{1,A} = \epsilon_{2,A} = \epsilon_A$ and $\epsilon_{1,B} = \epsilon_{2,B} = \epsilon_B$. Note $\epsilon = \epsilon_A + \epsilon_B$. In Event A, the tuple $(m^*, \gamma_i = R_i^* z_i, a_i^*, b_i^*, c_i^*)$ solves the (q_S, n, θ)-ODsjLRSW Problem instance at hand. In Event B, we have $\mathcal{H}_i(m^*) + R_i^* z_i = \mathcal{H}_i(\hat{m}_\tau) = \mathcal{H}_i(m_\tau) + R_{i,\tau} z_i$, for all i, $m^* \neq m_\tau$. Therefore we can solve $w = z_t = (\mathcal{H}_t(m^*) - \mathcal{H}_t(m_\tau))^{(R_{t,\tau} - R_t^*)^{-1}}$. Combining the result of both simulation forks, we obtain:

1. The probability of Event A and $c_{mode} = 1$ is $\epsilon_A/2$. With this probability, we solve the (q_S, n, θ)-whLRSW Problem instance at hand.
2. The probability of Event B and $c_{mode} = 1$ is $\epsilon_B/2$. With this probability, we solve the DL Problem instance.

4.4 Threshold ring signature $\mathsf{TRS}_{\mathsf{SDH}^*}(n, \theta)$

We introduce the threshold ring signature scheme which originates from the first signature scheme in [10]. The scheme is as follows:

1. Setup: User i's sk-pk pair is (x_i, g^{x_i}) for $1 \leq i \leq n$. The ring signature's public keys include all user public keys plus h_j, $0 \leq j < \theta$ and collision resistant hashing functions $\mathcal{H}_i$.
2. Sign: The users' public keys are $(g^{x_1}, \ldots, g^{x_n})$. WLOG, suppose the signers are $g^{x_1}, \ldots, g^{x_\theta}$, having secret keys $x_1, \ldots, x_\theta$ respectively.
   (a) For $i \in \{\theta + 1, \ldots, n\}$, the signers pick $r_i \in_R \mathbb{Z}_p^*$ and set $\sigma_i = g^{r_i}$, $W_i = g^{r_i(x_i + H_i(m))}$.
   (b) Then they solve for $W_1, \ldots W_\theta$ such that:

$$\prod_{i=1}^{n} {W_i}^{i^j} = h_j \quad \text{for all} \quad j \in \{0, \ldots, \theta - 1\}.$$

   (c) For each user $j \in \{1, \ldots, \theta\}$, he computes $\sigma_j = W_j^{1/(x_j + \mathcal{H}_j(m))}$ using his own secret key x_j.
   (d) The threshold ring signature is:

$$\sigma = (\sigma_1, \cdots, \sigma_n)$$

3. Verify: The verification is

$$\hat{\mathbf{e}}(h_j, g) = \prod_{i=1}^{n} \hat{\mathbf{e}}(\sigma_i, g^{(x_i + \mathcal{H}_{i(m))} i^j}), \text{ for every } j, 0 \leq j < \theta \tag{4}$$

Theorem 4. *The threshold ring signature $\mathsf{TRS}_{\mathsf{SDH}^*}(n, \theta)$ is secure provided the (q_S, n, θ)-ODsjSDH* Assumption holds and $\mathcal{H}_i$ are collision-resistant hashing functions.*

Corollary 7. *The $\mathsf{TRS}_{\mathsf{SDH}^*}(n, 1)$ is secure provided the $(q_S, n, 1)$-ODsjSDH* Assumption holds and $\mathcal{H}_i$ are collision-resistant hashing functions.*

Corollary 8. *The $\mathsf{TRS}_{\mathsf{SDH}^*}(1, 1)$ is secure provided the $(q_S, 1, 1)$-ODsjSDH* Assumption holds and $\mathcal{H}_i$ are collision-resistant hashing functions.*

Proof Sketch: The proof of correctness and the anonymity of the scheme are straightforward and hence are omitted. We prove the unforgeabiltiy below.

Setup: Simulator $\mathcal{S}$ receives a (q_S, n, θ)-ODsjSDH* Problem instance: g, $\mathcal{H}_i$, x_i for $1 \leq i \leq \theta - 1$, g^{x_k} for $\theta \leq k \leq n$. $\mathcal{S}$ also gets an oracle $O(\cdot)$ from the problem instance. $\mathcal{S}$ randomly picks x_k for $n+1 \leq k \leq n_{max}$. He gives the public parameters and also g^{x_i} for $1 \leq i \leq n_{max}$ to $\mathcal{A}$.

Simulating $\mathcal{SO}$: For query with (L_τ, m_τ),

- If $L_\tau \neq (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$, then $\mathcal{S}$ knows at least θ secret keys and hence can compute the threshold ring signature.
- If $L_\tau = (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$, then $\mathcal{S}$ queries $O(m_\tau)$ and forwards the answer to $\mathcal{A}$.

Simulation Deviation: It can be shown that the statistical distance among the Real World and the Ideal World is negligible.

Extraction: $\mathcal{A}$ outputs $(\sigma_1^*, \ldots, \sigma_n^*)$ for L^*, message $m^* \neq m_\tau$ for all $1 \leq \tau \leq n$. If $L^* \neq (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$, $\mathcal{S}$ declares failure and exits. Otherwise $L^* = (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$ and then $\mathcal{S}$ uses the signature to answer the problem instance.

4.5 Threshold Ring signature $\mathsf{TRS}_{\mathsf{BLS}}(n, \theta)$

We introduce the threshold ring signature scheme which originates from the signature scheme in [14]. The scheme is as follows:

1. Setup:User i's sk-pk pair is (x_i, g^{x_i}) for $1 \leq i \leq n$. The ring signature's public keys include all user public keys plus collision resistant hashing functions $\mathcal{H}_0$, ..., $\mathcal{H}_{\theta-1}$.
2. Sign: The users' public keys are $(g^{x_1}, \ldots, g^{x_n})$. WLOG, suppose the signers have secret keys x_1, ..., x_θ.
   (a) For $i \in \{\theta+1, \ldots, n\}$, the signers pick $r_i \in_R \mathbb{Z}_p^*$ and set $h_i = g^{r_i}$, $\sigma_i = g^{x_i r_i}$.
   (b) They compute $h_1, \ldots, h_\theta$ such that $\mathcal{H}_j(m) = \prod_{i=1}^{n} (h_i)^{i^j}$ where $0 \leq j < \theta$.
   (c) Each signer t computes $\sigma_t = h_t^{x_t}$ using his own secret key x_t.
   (d) The threshold ring signature is

$$\sigma = ((\sigma_1, h_1), \cdots, (\sigma_n, h_n))$$

3. Verify: The verification is

$$\mathcal{H}_j(m) = \prod_{i=1}^{n} (h_i)^{i^j} \text{ for all } j \ \wedge \ \hat{\mathbf{e}}(\sigma_i, g) = \hat{\mathbf{e}}(h_i, g^{x_i}) \text{ for all } i$$

Theorem 5. *The threshold ring signature* $\mathsf{TRS}_{\mathsf{BLS}}(n, \theta)$ *is secure provided the* (q_S, n, θ)*-ODsjBLS Assumption holds and* $\mathcal{H}_0, \ldots, \mathcal{H}_{\theta-1}$ *are collision-resistant hashing functions.*

Corollary 9. *The* $\mathsf{TRS}_{\mathsf{BLS}}(n, 1)$ *is secure provided the* $(q_S, n, 1)$*-ODsjBLS Assumption holds and* $\mathcal{H}_0, \ldots, \mathcal{H}_{\theta-1}$ *are collision-resistant hashing functions*

Corollary 10. *The* $\mathsf{TRS}_{\mathsf{BLS}}(1, 1)$ *is secure provided the* $(q_S, 1, 1)$*-ODsjBLS Assumption holds and* $\mathcal{H}_0, \ldots, \mathcal{H}_{\theta-1}$ *are collision-resistant hashing functions*

Proof Sketch: The proof of correctness and the anonymity of the scheme are straightforward and hence are omitted. We prove the unforgeabiltiy below.

Setup: Simulator $\mathcal{S}$ receives a (q_S, n, θ)-ODsjBLS Problem instance: g, x_1, ..., $x_{\theta-1}$, g^{x_i} for $\theta \leq i \leq n$, collision resistant hashing functions $\mathcal{H}_j$ for $0 \leq j < \theta$ and uses these as the public parameters given to $\mathcal{A}$. $\mathcal{S}$ also gets an oracle $O(\cdot)$ from the problem instance. $\mathcal{S}$ randomly picks x_k for $n+1 \leq k \leq n_{max}$ and gives g^{x_k} to $\mathcal{A}$.

Simulating $\mathcal{SO}$: For query with (L_τ, m_τ),

- If $L_\tau \neq (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$, then $\mathcal{S}$ knows at least θ secret keys and hence can compute the threshold ring signature.
- If $L_\tau = (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$, then $\mathcal{S}$ queries $O(m_\tau)$ and forwards the answer to $\mathcal{A}$.

Simulation Deviation: It can be shown that the statistical distance among the Real World and the Ideal World is negligible.

Extraction: $\mathcal{A}$ outputs σ_i^*, h_i^* for $1 \leq i \leq n$ for L^*, message $m^* \neq m_\tau$ for all $1 \leq \tau \leq n$. If $L^* \neq (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$, $\mathcal{S}$ declares failure and exits. Otherwise $L^* = (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$ and then $\mathcal{S}$ uses the signature to answer the problem instance.

4.6 Threshold Ring signature $\mathsf{TRS}_{\mathsf{CL04A}}(n, \theta)$

We introduce the threshold ring signature scheme which originates from the signature scheme A in [17]. The scheme is as follows:

1. Setup: User i's sk-pk pair is $((x_i, y_i), (g^{x_i}, g^{y_i}, g^{x_i y_i}))$ for $1 \leq i \leq n$. The ring signature's public keys include all user public keys, $h_0, \ldots, h_{\theta-1}$.
2. Sign: The users' public keys are $(g^{x_i}, g^{y_i}, g^{x_i y_i})$ for $1 \leq i \leq n$. WLOG, suppose the signers have secret keys x_j, y_j for $1 \leq j \leq \theta$.
   (a) For $i \in \{\theta+1, \ldots, n\}$, the signers pick $r_i \in_R \mathbb{Z}_p^*$ and set $a_i = g^{r_i}$, $b_i = g^{y_i r_i}$, $c_i = g^{x_i r_i} g^{x_i y_i r_i m}$.
   (b) The signers compute a_1, ..., a_θ such that $h_j = \prod_{i=1}^{n} (a_i)^{i^j}$ for $0 \leq j < \theta$.
   (c) Each signer t computes $b_t = a_t^{y_t}$, $c_t = (a_t b_t^m)^{x_t}$ using his secret keys (x_t, y_t).
   (d) The threshold ring signature is

$$\sigma = ((a_1, b_1, c_1), \cdots, (a_n, b_n, c_n))$$

3. Verify: The verification is

$$\hat{\mathbf{e}}(b_i, g) = \hat{\mathbf{e}}(a_i, g^{y_i}) \ \wedge \ \hat{\mathbf{e}}(c_i, g) = \hat{\mathbf{e}}(a_i b_i^m, g^{x_i}) \text{ for all } i$$
$$\wedge \ h_j = \prod_{i=1}^{n} (a_i)^{i^j} \quad \text{for all} \quad j \tag{5}$$

Theorem 6. *The threshold ring signature* $\mathsf{TRS}_{\mathsf{CL04A}}(n, \theta)$ *is secure provided the* (q_S, n, θ)*-ODsjLRSW Assumption holds.*

Corollary 11. *The* $\mathsf{TRS}_{\mathsf{CL04A}}(n, 1)$ *is secure provided the* $(q_S, n, 1)$*-ODsjLRSW Assumption holds.*

Corollary 12. *The* $\mathsf{TRS}_{\mathsf{CL04A}}(1, 1)$ *is secure provided the* $(q_S, 1, 1)$*-ODsjLRSW Assumption holds.*

Proof Sketch: The proof of correctness and the anonymity of the scheme are straightforward and hence are omitted. We prove the unforgeabiltiy below.

Setup: Simulator $\mathcal{S}$ receives a (q_S, n, θ)-ODsjLRSW Problem instance: g, $h_0, \ldots, h_{\theta-1}$, (x_1, y_1), ..., $(x_{\theta-1}, y_{\theta-1})$, $(g^{x_i}, g^{y_i}, g^{x_i y_i})$ for $\theta \leq i \leq n$ and uses these as the public parameters given to $\mathcal{A}$. $\mathcal{S}$ also gets an oracle $O(\cdot)$ from the problem instance. $\mathcal{S}$ randomly picks x_k, y_k for $n+1 \leq k \leq n_{max}$ and gives $(g^{x_k}, g^{y_k}, g^{x_k y_k})$ to $\mathcal{A}$.

Simulating $\mathcal{SO}$: For query with (L_τ, m_τ),

- If $L_\tau \neq (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$, then $\mathcal{S}$ knows at least θ secret keys and hence can compute the threshold ring signature.
- If $L_\tau = (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$, then $\mathcal{S}$ queries $O(m_\tau)$ and forwards the answer to $\mathcal{A}$.

Simulation Deviation: It can be shown that the statistical distance among the Real World and the Ideal World is negligible.

Extraction: $\mathcal{A}$ outputs a_i^*, b_i^*, c_i^* for $1 \leq i \leq n$ for L^*, message $m^* \neq m_\tau$ for all $1 \leq \tau \leq n$. If $L^* \neq (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$, $\mathcal{S}$ declares failure and exits. Otherwise $L^* = (\mathsf{pk}_1, \ldots, \mathsf{pk}_n)$ and then $\mathcal{S}$ uses the signature to answer the problem instance.

4.7 Threshold Ring signature $\mathsf{TRS}_{\mathsf{CL04B}}(n, \theta)$

We introduce the threshold ring signature scheme which originates from the signature scheme B in [17]. The scheme is as follows:

1. Setup: User i's sk-pk pair is $((x_i, y_i, z_i), (g^{x_i}, g^{y_i}, g^{z_i}, g^{x_i y_i}, g^{y_i z_i}, g^{x_i y_i z_i}))$ for $1 \leq i \leq n$. The ring signature's public keys includes all user public keys, and $h_0, \ldots, h_{\theta-1}$.
2. Sign: WLOG, suppose the signers have secret keys x_j, y_j for $1 \leq j \leq \theta$ and the message is $m = (m_1, m_2)$.
   (a) For $i \in \{\theta+1, \ldots, n\}$, the signers pick $r_i, R_i \in_R \mathbb{Z}_p^*$ and set $a_i = g^{r_i}$, $A_i = g^{z_i r_i}$, $b_i = g^{y_i r_i}$, $B_i = g^{y_i z_i r_i}$, $c_i = g^{x_i r_i} g^{x_i y_i r_i m_1} g^{x_i y_i z_i r_i m_2}$.
   (b) The signers compute a_1, ..., a_θ such that $h_j = \prod_{i=1}^{n} (a_i)^{i^j}$ for $0 \leq j < \theta$.
   (c) Each signer t computes $A_t = a_t^{z_t}$, $b_t = a_t^{y_t}$, $B_t = a_t^{y_t z_t}$, $c_t = (a_t b_t^{m_1} B_t^{m_2})^{x_t}$ using his secret keys (x_t, y_t, z_t).
   (d) The threshold ring signature is

$$\sigma = ((a_1, A_1, b_1, B_1, c_1), \cdots, (a_n, A_n, b_n, B_n, c_n))$$

3. Verify: The verification is

$$\begin{aligned} &\hat{\mathbf{e}}(A_i, g) = \hat{\mathbf{e}}(a_i, g^{z_i}) \ \wedge \ \hat{\mathbf{e}}(b_i, g) = \hat{\mathbf{e}}(a_i, g^{y_i}) \ \wedge \ \hat{\mathbf{e}}(B_i, g) = \hat{\mathbf{e}}(A_i, g^{y_i}) \\ \wedge \ &\hat{\mathbf{e}}(B_i, g) = \hat{\mathbf{e}}(b_i, g^{z_i}) \ \wedge \ \hat{\mathbf{e}}(c_i, g) = \hat{\mathbf{e}}(a_i b_i^{m_1} B_i^{m_2}, g^{x_i}) \text{ for all } i \\ \wedge \ &h_j = \prod_{i=1}^{n} (a_i)^{i^j} \quad \text{for all} \quad j \end{aligned} \tag{6}$$

Theorem 7. *The threshold ring signature $\mathsf{TRS}_{\mathsf{CL04B}}(n, \theta)$ is secure provided the (q_S, n, θ)-ODsjLRSW Assumption holds.*

Corollary 13. *The $\mathsf{TRS}_{\mathsf{CL04B}}(n, 1)$ is secure provided the $(q_S, n, 1)$-ODsjLRSW Assumption holds.*

Corollary 14. *The* $\mathsf{TRS}_{\mathsf{CL04B}}(1,1)$ *is secure provided the* $(q_S,1,1)$*-ODsjLRSW Assumption holds.*

Proof Sketch: The proof of correctness and the anonymity of the scheme are straightforward and hence are omitted. We prove the unforgeabiltiy below.

Setup: Simulator $\mathcal{S}$ receives, simultaneously, the following problem instances:

1. a (q_S,n,θ)-ODsjLRSW problem instance: g, $\{(u_j,v_j): 1\le j\le \theta-1\}$, $\{(g^{u_k},g^{v_k}): \theta\le k\le n\}$, h_0, ..., $h_{\theta-1}$ and an oracle $O(\cdot)$.
2. a DL problem instance: g, g^w.

$\mathcal{S}$ flips a fair coin c_{mode} and sets up as follows:

1. If $c_{mode}=1$, $\mathcal{S}$ randomly picks z_i for $1\le i\le n_{max}$, u_j,v_j for $n+1\le j\le n_{max}$, sets $\mathsf{pk}=(g^{u_i},g^{v_i},g^{z_i})$.
2. If $c_{mode}=2$, $\mathcal{S}$ randomly picks x_i,y_i,z_i for $1\le i\le n_{max}$, except for random index $t\in\{1,\ldots,n_{max}\}$, $\mathcal{S}$ sets $z_t=w$. $\mathcal{S}$ then sets $\mathsf{pk}=(g^{x_i},g^{y_i},g^{z_i})$.

(*Remark:* For simplicity we do not shuffle the index of users here.)

Simulating $\mathcal{SO}$: If $c_{mode}=1$, upon the τ-th $\mathcal{SO}$ query input (m_τ,L_τ), $1\le\tau\le q_S$:

- If $L_\tau\neq(\mathsf{pk}_1,\ldots,\mathsf{pk}_n)$, then $\mathcal{S}$ knows at least θ secret keys and hence can compute the threshold ring signature.
- If $L_\tau=(\mathsf{pk}_1,\ldots,\mathsf{pk}_n)$, then do the followings. With message $m_\tau=(m_{1,\tau},m_{2,\tau})$, $\mathcal{S}$ computes $m'_\tau=m_{1,\tau}+m_{2,\tau}z$ and queries $O(m'_\tau)$. $\mathcal{S}$ gets $(a_{i,\tau},b_{i,\tau},c_{i,\tau})$ for $1\le i\le n$. $\mathcal{S}$ forwards the answer $(a_{i,\tau},A_{i,\tau}=a_{i,\tau}^{z_i},b_{i,\tau},B_{i,\tau}=b_{i,\tau}^{z_i},c_{i,\tau})$ to $\mathcal{A}$.

If $c_{mode}=2$, for the τ-th $\mathcal{SO}$ query input (m_τ,L_τ), $1\le\tau\le q_S$, then $\mathcal{S}$ knows at least θ secret keys and hence can compute the threshold ring signature.

Simulation deviation: It can be shown that the pairwise simulation deviation between any two of the following worlds are negligible: (1) Real World, (2) Ideal World-1 where $c_{mode}=1$, and (3) Ideal-World-2 where $c_{mode}=2$. The proof is tedious but mechanical. We omit it.

Extraction: With probability ϵ, attacker $\mathcal{A}$ eventually delivers a valid message-signature pair $(L^*,m^*,(R_i^*,a_i^*,A_i^*,b_i^*,B_i^*,c_i^*))$, for $1\le i\le n$, $m^*\neq m_\tau$ for all τ. If $L^*\neq(\mathsf{pk}_1,\ldots,\mathsf{pk}_n)$, $\mathcal{S}$ declares failure and exits. Otherwise $L^*=(\mathsf{pk}_1,\ldots,\mathsf{pk}_n)$, denote $m^*=(m_1^*,m_2^*)$ and then there are two events:

- Event A: For each τ, $m_1^*+m_2^*z_i\neq m_{1,\tau}+m_{2,\tau}z_i$, for some $1\le i\le n$.
- Event B: For some τ, $m_1^*+m_2^*z_i=m_{1,\tau}+m_{2,\tau}z_i$, for all $1\le i\le n$.

For $i=1,2$, let $\epsilon_{i,A}$ (resp. $\epsilon_{c_{mode},B}$) denotes the probability that $c_{mode}=i$ and Event A (resp. Event B). The negligibility of simulation deviations implies that $\epsilon_{1,A}=\epsilon_{2,A}=\epsilon_A$ and $\epsilon_{1,B}=\epsilon_{2,B}=\epsilon_B$. Note $\epsilon=\epsilon_A+\epsilon_B$. In Event A, the tuple $(m_1^*,\gamma_i=m_2^*z_i,a_i^*,b_i^*,c_i^*)$ solves the (q_S,n,θ)-ODsjLRSW Problem instance at hand. In Event B, we have $m_1^*+m_2^*z_i=m_{1,\tau}+m_{2,\tau}z_i$, for all i, $m^*\neq m_\tau$. Therefore we can solve $w=z_t=(m_1^*-m_{1,\tau})^{(m_{2,\tau}-m_2^*)^{-1}}$. Combining the result of both simulation forks, we obtain:

1. The probability of Event A and $c_{mode}=1$ is $\epsilon_A/2$. With this probability, we solve the (q_S,n,θ)-ODsjLRSW Problem instance at hand.
2. The probability of Event B and $c_{mode}=1$ is $\epsilon_B/2$. With this probability, we solve the DL Problem instance.

hierarchical identity-based threshold (n,θ,ℓ) ring signature	sk $1 \le i \le n$	pk $1 \le i \le n$ $1 \le k \le \ell$	signature, $1 \le i \le n$, $0 \le j < \theta$, and verification
HVZK↓ 2	$d_{1,i}, d_{2,i}$	$g, g^\alpha, g_2, g_3, g_4, g_5, h_k, Q_i, \mathcal{H}(\cdot)$	$(D_{1,i}, D_{2,i}, c_i, Z_{1,i}, Z_{2,i}) : \hat{\mathbf{e}}(D_{1,i}, Q_i) = \hat{\mathbf{e}}(g, D_{2,i})$ $\wedge\ \hat{\mathbf{e}}(Z_{1,i}, g)\hat{\mathbf{e}}(g_5, D_{2,i}) = \hat{\mathbf{e}}(g_2, g^\alpha)^{c_i}\hat{\mathbf{e}}(Z_{2,i}, Q_i)\hat{\mathbf{e}}(g_4, D_{1,i})$ $\wedge\ \mathcal{H}(D_{1,1}, D_{2,1}, \cdots, D_{1,n}, D_{2,n}, m, \mathsf{param}) = \sum_{i=1}^{n}(c_i)i^j$

Table 3. Hierarchical identity-based threshold ring signatures without random oracles.

5 Hierarchical Identity-Based Threshold Ring Signature (HIBTRS)

For this scheme, we have a slightly different security model. In the Sign protocol, we assume each user announces two of the above HIBS signatures, which satisfy the relation:

$$S_I = \{(D_1, D_2, c, Z_1, Z_2) : I = \{\mathsf{id}_1, \ldots, \mathsf{id}_\ell\} \ \wedge\ \hat{\mathbf{e}}(D_1, Q) = \hat{\mathbf{e}}(g, D_2)$$
$$\wedge\ \hat{\mathbf{e}}(g, Z_1)\hat{\mathbf{e}}(g_5, D_2) = \hat{\mathbf{e}}(g_1, g_2)^c\hat{\mathbf{e}}(Z_2, Q)\hat{\mathbf{e}}(D_1, g_4)\ \wedge\ Q = g_3\prod_{i=1}^{\ell} h_i^{\mathsf{id}_i}\}$$

For the ACP-UF, we also include a Key Extraction Oracle for the adversary to query the secret keys of some identities which are not the prefix of the ring members given by simulator $\mathcal{S}$. The scheme is as follows:

$\mathsf{HIBTRS}_{\mathsf{HVZK}\downarrow 2}(n, \theta)$

1. **Setup:** To generate system parameters, the algorithm selects a random generator g, g_2, g_3, g_4, g_5, h_1, ..., $h_\ell \in \mathbb{G}$, picks a random $\alpha \in \mathbb{Z}_p$, and sets $g_1 = g^\alpha$. It chooses an collision-resistant hash function $\mathcal{H}$. The system parameters $\mathsf{param} = (g, g_1, g_2, g_3, g_4, g_5, h_1, \ldots, h_\ell)$ and the master key is g_2^α.
2. **Der:** To generate a private key for $\mathsf{ID} = (\mathsf{id}_1, \ldots, \mathsf{id}_k)$. where $k \le \ell$, the algorithm picks a random $r \in \mathbb{Z}_p$ and computes:

$$SK_{\mathsf{ID}} = \left(g_2^\alpha \cdot (h_1^{\mathsf{id}_1} \cdots h_k^{\mathsf{id}_k} \cdot g_3)^r,\quad g^r,\quad h_{k+1}^r, \ldots, h_\ell^r\right) = (a_0, a_1, b_{k+1}, \ldots, b_\ell)$$

   The private key for ID can also be generated by its parent $\mathsf{ID}_{|k-1} = (\mathsf{id}_1, \ldots, \mathsf{id}_{k-1})$. Details refer to [11].
3. Sign: Given $\{I_1, \ldots, I_n\}$ and WLOG suppose the signers have $(\mathsf{sk}_{I_1}, \ldots, \mathsf{sk}_{I_\theta})$.
   (a) For each $i \in \{\theta+1, \cdots, n\}$, assume two distinct tuples from S_{I_i} are available, which denote as $(D'_{1,i}, D'_{2,i}, c'_i, Z'_{1,i}, Z'_{2,i})$ and $(D''_{1,i}, D''_{2,i}, c''_i, Z''_{1,i}, Z''_{2,i})$.
   Denote $g_1 = g^\alpha$ and $D'_{1,i} = g^{t'}$. From the relation S_{I_i}, we can see that $Z'_{1,i} = (g_2^\alpha Q^{r'})^{c'} g_4^{t'}$ and $Z'_{2,i} = g^{r'c'} g_5^{t'}$ for some random t', r'. Similarly, we suppose that $Z''_{1,i} = (g_2^\alpha Q^{r''})^{c''} g_4^{t''}$ and $Z''_{2,i} = g^{r''c''} g_5^{t''}$. We require that $r' = r''$.
   (b) The signers pick random a'_i and a''_i to compute $(D_{1,i}, D_{2,i}, c_i, Z_{1,i}, Z_{2,i}) \in S_{I_i}$ as follows:

$$D_{1,i} = (D'_{1,i})^{a'_i}(D''_{1,i})^{a''_i},\quad D_{2,i} = (D'_{2,i})^{a'_i}(D''_{2,i})^{a''_i},\quad c_i = c'_i a'_i + c''_i a''_i,$$
$$Z_{1,i} = (Z'_{1,i})^{a'_i}(Z''_{1,i})^{a''_i},\quad Z_{2,i} = (Z'_{2,i})^{a'_i}(Z''_{2,i})^{a''_i},$$

   (c) For each $j \in \{1, \cdots, \theta\}$, each signer picks random t_j and computes $D_{1,j} = g^{t_j}$, $D_{2,j} = Q_j^{t_j}$. Then the signers compute $c_1, \ldots, c_\theta$ satisfying

$$\mathcal{H}(k, n, \theta, D_{1,1}, D_{2,1}, \cdots, D_{1,n}, D_{2,n}, m, \mathsf{param}, I_1, \ldots I_n) = \sum_{i=1}^{n}(c_i)^{i^k} \quad \text{for all } 0 \le k < \theta$$

(d) For each signer j with secret key $(d_{1,j}, d_{2,j})$, he picks random Δ, computes $\hat{d}_{1,j} = d_{1,j} Q_j^{\Delta} = g_2^{\alpha} Q_j^{r+\Delta}$ and $\hat{d}_2 = d_{2,j} g^{\Delta} = g^{r+\Delta}$. Then he computes the signature $Z_{1,j} = \hat{d}_{1,j}^{c_j} g_4^{t_j}$ and $Z_{2,j} = \hat{d}_2^{c_j} g_5^{t_j}$.

(e) Output the signature

$$\sigma = (D_{1,1}, D_{2,1}, c_1, Z_{1,1}, Z_{2,1}, \cdots, D_{1,n}, D_{2,n}, c_n, Z_{1,n}, Z_{2,n})$$

4. Verify: Upon receiving a signature σ for message m, verify all below before outputting 1:

$$\mathcal{H}(k, n, \theta, D_{1,1}, D_{2,1}, \cdots, D_{1,n}, D_{2,n}, m, \mathsf{param}, I_1, \ldots I_n) = \sum_{i=1}^{n} (c_i) i^k \quad \text{for all } 0 \le k < \theta$$
$$(D_{1,i}, D_{2,i}, c_i, Z_{1,i}, Z_{2,i}) \in S_{I_i}, \quad \text{for all } 1 \le i \le n$$

Intractability Assumption We propose a new intractability assumption as follows.

Definition 10. *The* OrcYW(n, θ, $\mathcal{H}$) Problem *is that given*

1. $\ell \ge 1$, $\{g^{x^i} : 0 \le i \le \ell\}$, γ, δ, g_4, g_5, γ_1, $\cdots$, γ_ℓ, $n_{\max}$ *identity chains* $\mathbf{I}_1$, $\cdots$, $\mathbf{I}_{n_{\max}}$, *a special identity chain* $\mathbf{I}^*$ *among them, full-domain collision-resistant hash function* $\mathcal{H}$,
2. *an oracle* $O_{n,\theta,\mathcal{H}}$ *which upon input a message* m, *a list of* n *identities (identity-chains)* $\mathbf{I}_{k_1}$, $\cdots$, $\mathbf{I}_{k_n}$, *threshold* θ, *outputs a tuple* ($D_{1,1}$, $D_{2,1}$, c_1, $Z_{1,1}$, $Z_{2,1}$, $\cdots$, $D_{1,n}$, $D_{2,n}$, c_n, $Z_{1,n}$, $Z_{2,n}$) *satisfying:*
   For each i, $1 \le i \le n$, *for some random* t_i, r_i *which differ for each query to* $O_{n,\theta,\mathcal{H}}$,

$$D_{1,i} = g^{t_i}, \quad D_{2,i} = Q_i^{t_i}, \quad Z_{1,i} = a_{0,i}^{c_i} g_4^{t_i}, \quad Z_{2,i} = a_{1,i}^{c_i} g_5^{t_i}$$

where

$$Q_i = g_3 \prod_{j=1}^{\ell} h_j^{I_{k_j}}, \quad h_j = g^{\gamma_j} g^{-x^{\ell-j+1}}, \text{ for } 1 \le j \le \ell$$
$$g_2 = g^{x^\ell + \gamma}, \quad g_3 = g^{\delta + \sum_{j=1}^{\ell} x^{\ell-j+1} I_j^*}, \quad a_{0,i} = g_2^x Q_i^{r_i}, \quad a_{1,i} = g^{r_i},$$
$$\sum_{i=1}^{n} c_i^{i^{j'}} = \mathcal{H}(j', n, \theta, D_{1,1}, D_{2,1}, \cdots, D_{1,n}, D_{2,n}, m, \mathsf{param}, \mathbf{I}_{k_1}, \cdots, \mathbf{I}_{k_n}), 0 \le j' < \theta$$
$$\mathsf{param} = (g, g^x, g_2, g_3, g_4, g_5, h_1, \cdots, h_\ell)$$

to output ($\tilde{m}$, $\tilde{L} = \{\tilde{\mathbf{I}}_1, \cdots, \tilde{\mathbf{I}}_n\}$, $\tilde{D}_{1,1}$, $\tilde{D}_{2,1}$, $\tilde{c}_1$, $\tilde{Z}_{1,1}$, $\tilde{Z}_{2,1}$, $\cdots$, $\tilde{D}_{1,n}$, $\tilde{D}_{2,n}$, $\tilde{c}_n$, $\tilde{Z}_{1,n}$, $\tilde{Z}_{2,n}$) *satisfying for each* i, $1 \le i \le n$,

$$\hat{\mathbf{e}}(g, \tilde{Z}_{1,i}) \cdot \hat{\mathbf{e}}(g_5, \tilde{D}_{2,i}) = \hat{\mathbf{e}}(g_1, g_2)^{\tilde{c}_i} \cdot \hat{\mathbf{e}}(\tilde{D}_{1,i}, g_4) \cdot \hat{\mathbf{e}}(\tilde{Z}_{2,i}, Q)$$
$$\wedge \ \hat{\mathbf{e}}(\tilde{D}_{1,i}, Q) = \hat{\mathbf{e}}(g, \tilde{D}_{2,i}) \ \wedge \ (\tilde{m}, \tilde{L}, \theta) \text{ was not queried to } O_{n,\theta,\mathcal{H}}$$

where $\sum_{i=1}^{n} \tilde{c}_i^{i^{j'}} = \mathcal{H}(j', n, \theta, \tilde{D}_{1,1}, \tilde{D}_{2,1}, \cdots, \tilde{D}_{1,n}, \tilde{D}_{2,n}, \tilde{m}, \mathsf{param}, \tilde{L})$, $0 \le j' < \theta$. *The* OrcYW(n, θ, $\mathcal{H}$) Assumption *is that no PPT algorithm can solve a random instance of the OrcYW(*n, θ, $\mathcal{H}$*) Problem with non-negligible probability.*

Reductionist security proof

Theorem 8. *The scheme* $\mathsf{HIBTRS}_{\mathsf{HVZK}\downarrow 2}(n,\theta)$ *is secure provided the* OrcYW $(n, \theta, \mathcal{H})$ Assumption *holds.*

Corollary 15. *The* $\mathsf{HIBTRS}_{\mathsf{HVZK}\downarrow 2}(n,1)$ *is secure provided the* OrcYW $(n, 1, \mathcal{H})$ Assumption *Assumptions holds.*

Corollary 16. *The* $\mathsf{HIBTRS}_{\mathsf{HVZK}\downarrow 2}(1,1)$ *is secure provided the* OrcYW $(1, 1, \mathcal{H})$ Assumption *Assumptions holds.*

Proof Sketch: The correctness and the anonymity of the scheme are straightforward and hence are omitted. The proof of unforgeability is as follows.

Setup: Simulator $\mathcal{S}$ received a OrcYW$(n,\theta,\mathcal{H})$ Problem instance: $\{g^{x^i} : 0 \leq i \leq \ell\}$,$\gamma$, δ, g_4, g_5, $\gamma_1, \cdots, \gamma_\ell$, $n_{\max}$ identity chains $\mathbf{I}_1, \cdots, \mathbf{I}_{n_{\max}}$, a special identity chain $\mathbf{I}^*$ among them, a full-domain collision-resistant hash function $\mathcal{H}$ and an oracle $O_{n,\theta,\mathcal{H}}$.

$\mathcal{S}$ computes $g_1 = g^x$, $g_2 = g^{x^\ell+\gamma}$, $g_3 = g^{\delta+\sum_{j=1}^{\ell} x^{\ell-j+1} I_j^*}$ and $h_j = g^{\gamma_j} g^{-x^{\ell-j+1}}$, for $1 \leq j \leq \ell$. $\mathcal{S}$ randomly selects $\theta - 1$ identities from $\mathbf{I}_i$ and computes their secret keys using the method in the paragraph **Simulating** $\mathcal{KEO}$ below. $\mathcal{S}$ gives the public parameters $\mathsf{param} = (g, g_1, g_2, g_3, g_4, g_5, h_1, \ldots, h_\ell)$, $n_{\max}$ identity chains, and $\theta - 1$ private keys to $\mathcal{A}$.

Simulating $\mathcal{SO}$: For query with (L_τ, m_τ), $\mathcal{S}$ queries $O_{n,\theta,\mathcal{H}}(L_\tau, m_\tau)$ and forwards the answer to $\mathcal{A}$.

Simulating $\mathcal{KEO}$**:** Simulate as in [11]. For input identity $\mathsf{ID} = (\mathsf{id}_1, \ldots, \mathsf{id}_u)$, if ID is $\mathbf{I}^*$ or a prefix of it, the simulator declares failure and exits. Otherwise there exists a $k \leq u$ such that $\mathsf{id}_k \neq I_k^*$. We set k be the smallest such index. To answer the query, the simulator derives a secret key for the identity $(\mathsf{id}_1, \ldots, \mathsf{id}_k)$ from which it then constructs a private key for $\mathsf{ID} = (\mathsf{id}_1, \ldots, \mathsf{id}_k, \ldots, \mathsf{id}_u)$.

To generate the secret key for the identity $(\mathsf{id}_1, \ldots, \mathsf{id}_k)$, the simulator chooses a random $\tilde{r} \in \mathbb{Z}_p$. Denote $r = \frac{x^k}{(\mathsf{id}_k - I_k^*)} + \tilde{r}$ and compute:

$$a_0 = y_1^\gamma \cdot Z \cdot g^{x^{\ell-k+1}\tilde{r}(I_k^* - \mathsf{id}_k)} \quad \text{where} \quad Z = \left(g^{\delta+\sum_{i=1}^{k} \mathsf{id}_i \gamma_i} \cdot \prod_{i=k+1}^{\ell} g^{x^{\ell-i+1} I_i^*} \right)^r$$

$$a_1 = g^r = g^{x^k/(\mathsf{id}_k - I_k^*)} g^{\tilde{r}}$$

Refer to [11] for the well-formedness of the secret key. The remaining $h_{k+1}^r, \ldots, h_\ell^r$ can be computed by the simulator since they do not involve a $g^{x^{\ell+1}}$ term.

Simulation Deviation: It can be shown that the statistical distance among the Real World and the Ideal World is negligible.

Extraction: $\mathcal{A}$ outputs $(D_{1,i}^*, D_{2,i}^*, c_i, Z_{1,i}^*, Z_{2,i}^*)$ for $1 \leq i \leq n$ for L^*, message $m^* \neq m_\tau$ for all $1 \leq \tau \leq q_S$. Then $\mathcal{S}$ uses the signature to answer the problem instance.

6 Discussions and Conclusions

The combination of Schnorr [37]'s *ROS (Randomized Oversampled System)* and Wagner [39]'s *generalized birthday attack* may apply to our (threshold) ring signatures, resulting in sub-exponential-time forgery algorithms. However, that does not violate the security models.

In this paper, we propose seven new threshold ring signature schemes without random oracles. We also introduce the notion of hierarchical identity-based threshold ring signature, propose an efficient instantiation and prove its security without random oracles.

References

1. M. Abe, M. Ohkubo, and K. Suzuki. 1-out-of-n signatures from a variety of keys. In *Proc. ASIACRYPT 2002*, pages 415–432. Springer-Verlag, 2002. Lecture Notes in Computer Science No. 2501.
2. G. Ateniese, J. Camenisch, S. Hohenberger, and B. de Medeiros. Practical group signatures without random oracles. Cryptology ePrint Archive, Report 2005/385, 2005. http://eprint.iacr.org/.
3. B. Barak. How to go beyond the black-box simulation barrier. In *FOCS 2001*, pages 106–115. IEEE Computer Soceity, 2001.
4. B. Barak, Y. Lindell, and S. P. Vadhan. Lower bounds for non-black-box zero knowledge. In *FOCS 2003*, pages 384–393. IEEE Computer Soceity, 2003.
5. M. Bellare, A. Boldyreva, and A. Palacio. An uninstantiable random-oracle-model scheme for a hybrid-encryption problem. In *EUROCRYPT 2004*, pages 171–188. Springer-Verlag, 2004. Lecture Notes in Computer Science No. 3027.
6. M. Bellare, D. Micciancio, and B. Warinschi. Foundations of group signatures: formal definitions, simplified requirements and a construction based on general assumptions. In *EUROCRYPT'03*, volume 2656 of *LNCS*. Springer-Verlag, 2003.
7. M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proc. 1st ACM Conference on Computer and Communications Security*, pages 62–73. ACM Press, 1993.
8. A. Bender, J. Katz, and R. Morselli. Ring signatures: Stronger definitions, and constructions without random oracles. To appear in TCC 06. Cryptology ePrint Archive, Report 2005/304, 2005.
9. D. Boneh and X. Boyen. Efficient selective-ID secure identity based encryption without random oracles. In *Proc. EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 223–238. Springer-Verlag, 2004.
10. D. Boneh and X. Boyen. Short signatures without random oracles. In *Proc. EUROCRYPT 2004*, pages 56–73. Springer-Verlag, 2004. Lecture Notes in Computer Science No. 3027.
11. D. Boneh, X. Boyen, and E.-J. Goh. Hierarchical identity based encryption with constant size ciphertext. In *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 440–456. Springer, 2005.
12. D. Boneh, C. Gentry, B. Lynn, and H. Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. In *Proc. EUROCRYPT 2003*, pages 416–432. Springer-Verlag, 2003. Lecture Notes in Computer Science No. 2656.
13. D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In *Proc. CRYPTO 2005*, pages 258–275. Springer-Verlag, 2005. Lecture Notes in Computer Science No. 3621.
14. D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. In *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 514–532. Springer-Verlag, 2001.
15. X. Boyen and B. Waters. Compact group signatures without random oracles. Cryptology ePrint Archive, Report 2005/381, 2005. http://eprint.iacr.org/.
16. E. Bresson, J. Stern, and M. Szydlo. Threshold ring signatures and applications to ad-hoc groups. In *Proc. CRYPTO 2002*, pages 465–480. Springer-Verlag, 2002. Lecture Notes in Computer Science No. 2442.
17. J. Camenisch and A. Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In *Proc. CRYPTO 2004*. Springer-Verlag, 2004. Lecture Notes in Computer Science No. 3152.
18. J. Camenisch and M. Stadler. Efficient group signature schemes for large groups (extended abstract). In *CRYPTO'97*, pages 410–424. Springer-Verlag, 1997.
19. R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology, revisited. In *Proc. 13th ACM Symp. on Theory of Computing*, pages 209–128. ACM Press, 1998.
20. D. Chaum and E. van Heyst. Group signatures. In *EUROCRYPT'91*, volume 547 of *LNCS*, pages 257–265. Springer-Verlag, 1991.
21. S. S. Chow, L. C. Hui, and S. Yiu. Identity based threshold ring signature. In *Proc. ICISC 2004*, pages 218–232. Springer-Verlag, 2005. Lecture Notes in Computer Science No. 3506.
22. S. S. Chow, J. K. Liu, V. K. Wei, and T. H. Yuen. Ring signature without random oracles. To appear in ASIACCS06. Cryptology ePrint Archive, Report 2005/317, 2005. http://eprint.iacr.org/.
23. S. S. Chow, S. Yiu, and L. C. Hui. Efficient identity based ring signature. In *Applied Cryptography and Network Security (ACNS 2005)*, pages 499–512. Springer-Verlag, 2005. Lecture Notes in Computer Science No. 3531.
24. R. Cramer, I. Damgård, and B. Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In *Proc. CRYPTO 94*, pages 174–187. Springer-Verlag, 1994. Lecture Notes in Computer Science No. 839.
25. Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup. Anonymous identification in ad hoc groups. In *Proc. EUROCRYPT 2004*, pages 609–626. Springer-Verlag, 2004. Lecture Notes in Computer Science No. 3027.

26. C. Gentry and A. Silverberg. Hierarchical ID-based cryptography. In *Proc. ASIACRYPT 2002*, pages 548–566. Springer-Verlag, 2002. Lecture Notes in Computer Science No. 2501.
27. O. Goldreich. *Foundations of Cryptography*, volume 1 and 2. Cambridge Univesity Press, 2001 and 2005.
28. S. Goldwasser and Y. T. Kalai. On the (in)security of the Fiat-Shamir paradigm. In *FOCS 2003*, pages 102–113. IEEE Computer Soceity, 2003.
29. T. Isshiki and K. Tanaka. An (n-t)-out-of-n threshold ring signature scheme. In *ACISP 2005*, pages 406–416. Springer-Verlag, 2005. Lecture Notes in Computer Science No. 3574.
30. A. Kiayias and H. Zhou. Two-round concurrent blind signatures without random oracles. Cryptology ePrint Archive, Report 2005/435, 2005. http://eprint.iacr.org/.
31. F. Laguillaumie and D. Vergnaud. Short undeniable signatures without random oracles: The missing link. In *Proc. INDOCRYPT 2005*, LNCS No. 3797, pages 283–296. Springer-Verlag, 2005.
32. J. K. Liu, V. K. Wei, and D. S. Wong. A separable threshold ring signature scheme. In *Proc. ICISC 2003*, pages 12–26. Springer-Verlag, 2003. Lecture Notes in Computer Science No. 2971.
33. J. K. Liu and D. S. Wong. On the security models of (threshold) ring signature schemes. In *Proc. ICISC 2004*, pages 204–217. Springer-Verlag, 2005. Lecture Notes in Computer Science No. 3506.
34. A. Lysyanskaya, R. Rivest, A. Sahai, and S. Wolf. Pseudonym systems. In *Selected Areas in Cryptography (SAC) 1999*, volume 1758 of *LNCS*, pages 184–199. Springer-Verlag, 1999.
35. S. Mitsunari, R. Sakai, and M. Kasahara. A new traitor tracing. *IEICE Trans. Fundamentals*, E85-A(2):481–484, 2002.
36. R. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In *Proc. ASIACRYPT 2001*, pages 552–565. Springer-Verlag, 2001. Lecture Notes in Computer Science No. 2248.
37. C. P. Schnorr. Security of blind discrete log signatures against interactive attacks. In *ICICS 2001*, volume 2229, pages 1–12. Springer–Verlag, 2001. LNCS.
38. A. Shamir. Identity-based cryptosystems and signature schemes. In *Proc. CRYPTO 84*, pages 47–53. Springer-Verlag, 1984. Lecture Notes in Computer Science No. 196.
39. D. Wagner. A generalized birthday problem. In *Proc. CRYPTO 2002*, pages 288–303. Springer-Verlag, 2002. Lecture Notes in Computer Science No. 2442.
40. H. Wang, Y. Zhang, and D. Feng. Short threshold signature schemes without random oracles. In *Proc. INDOCRYPT 2005*, Lecture Notes in Computer Science No. 3797, pages 297–310. Springer-Verlag, 2005.
41. V. K. Wei and T. H. Yuen. More short signatures without random oracles. To appear in IJNS. Cryptology ePrint Archive, Report 2005/463, 2005. http://eprint.iacr.org/.
42. D. S. Wong, K. Fung, J. K. Liu, and V. K. Wei. On the RS-Code construction of ring signature schemes and a threshold setting of RST. In *Proc. ICICS 2003*, pages 34–46. Springer-Verlag, 2003. Lecture Notes in Computer Science No. 2836.
43. J. Xu, Z. Zhang, and D. Feng. A ring signature scheme using bilinear pairings. In *WISA 2004*, Lecture Notes in Computer Science No. 3325, pages 163–172. Springer-Verlag, 2005.
44. T. H. Yuen and V. K. Wei. Constant-size hierarchical identity-based signature/signcryption without random oracles. Cryptology ePrint Archive, Report 2005/412, 2005. http://eprint.iacr.org/.
45. F. Zhang, X. Chen, W. Susilo, and Y. Mu. A new short signature scheme without random oracles from bilinear pairings. Cryptology ePrint Archive, Report 2005/386, 2005. http://eprint.iacr.org/.
46. F. Zhang and K. Kim. ID-Based blind signature and ring signature from pairings. In *Proc. ASIACRYPT 2002*, pages 533–547. Springer-Verlag, 2002. Lecture Notes in Computer Science No. 2501.
47. F. Zhang, R. Safavi-Naini, and W. Susilo. An efficient signature scheme from bilinear pairings and its applications. In *Proc. PKC'2004*, pages 277–290. Springer-Verlag, 2004. Lecture Notes in Computer Science No. 2947.
48. R. Zhang, J. Furukawa, and H. Imai. Short signature and universal designated verifier signature without random oracles. In *Proc. ACNS 2005*, Lecture Notes in Computer Science No. 3531, pages 483–498. Springer-Verlag, 2005.