ID-Based Ring Signature Scheme secure in the Standard Model

Man Ho Au[1], Joseph K. Liu[2], Y. H. Yuen[3], and Duncan S. Wong[4]

[1] Centre for Information Security Research
School of Information Technology and Computer Science
University of Wollongong
Wollongong 2522, Australia
mhaa456@uow.edu.au
[2] Department of Computer Science
University of Bristol
Bristol, BS8 1UB, UK
liu@cs.bris.ac.uk
[3] Department of Information Engineering
The Chinese University of Hong Kong
Shatin, N.T., Hong Kong
thyuen4@ie.cuhk.edu.hk
[4] Department of Computer Science
City University of Hong Kong
Kowloon, Hong Kong
duncan@cityu.edu.hk

Abstract. The only known construction of ID-based ring signature schemes which maybe secure in the standard model is to attach certificates to non-ID-based ring signatures. This method leads to schemes that are somewhat inefficient and it is an open problem to find more efficient and direct constructions. In this paper, we propose two such constructions. Our first scheme, with signature size linear in the cardinality of the ring, is secure in the standard model under the computational Diffie-Hellman assumption. The second scheme, achieving constant signature size, is secure in a weaker attack model (the selective ID and weak chosen message model), under the Diffie-Hellman Inversion assumption.

1 Introduction

Identity-based (ID-based) cryptosystem, introduced by Shamir [17], eliminated the need for checking the validity of the certificates. In an ID-based cryptosystem, public key of each user is easily computable from a string corresponding to this user's identity (e.g. an email address, a telephone number, etc.). A private key generator (PKG) then computes the private keys from a master secret for the users. This property avoids the necessity of certificates and associates an implicit public key (user identity) to each user within the system.

Ring signature is a group-oriented signature with privacy concerns. A user can sign anonymously on behalf of a group on his own choice, while group members can be totally unaware of being conscripted in the group. Any verifier can

be convinced that a message has been signed by one of the members in this group, but the actual identity of the signer is hidden.

ID-based ring signature combines the property of ring signature and ID-based signature. The first construction is in [21]. Since then, several construction have been proposed [12,3,22,13,10]. The above scheme are all based on pairings with signature size linear in the cardinality of the ring. Non-pairing-based approach can be found in [2]. The first constant-size construction appears in [11]. Independent work was given in [15]. Both of them use accumulator. Later [20] point out a flaw in [15] and outline a patch. All existing constructions are only secure in the random oracle model.

There are only a few number of ring signature scheme secure in the standard model. One is a generic scheme based on standard signature, public-key encryption and ZAP proof system; and a second, more efficient ring signature scheme but supporting only 2 users[4]. Another one is an independent work by Chow *et. al.* without utilizing encryption and ZAP but rely on a new assumption [9]. Recently, independent of our work, Wei and Yuen have proposed a Hierarchical Identity-Based Threshold Ring Signature scheme in the standard model [19].

Our Contribution. We give two direction construction for ID-Based ring signature scheme. Signature size of the first scheme is linear with the cardinality of the ring. We prove that it is secure under the computational Diffie-Hellman assumption. Signature size of the second scheme is constant. We prove that the second scheme is secure under the Diffie-Hellman Inversion assumption in the selective-ID weak chosen message attack model. In terms of signature size and computational cost, our schemes outperform schemes constructed indirectly following the generic approach described above.

2 Security Model

2.1 Algorithm Definition

An ID-Based $(1, n)$ Ring Signature scheme is a tuple of probabilistic polynomial-time (PPT) algorithms below:

- **Setup**. On input an unary string 1^λ where λ is a security parameter, the algorithm outputs a master secret key s and a list of system parameters param that includes λ and the descriptions of a user secret key space $\mathcal{D}$, a message space $\mathcal{M}$ as well as a signature space Ψ.
- **Extract**. On input a list param of system parameters, an identity $ID_i \in \{0,1\}^*$ for a user and the master secret key s, the algorithm outputs the user's secret key $d_i \in \mathcal{D}$. When we say identity ID_i corresponds to user secret key d_i or vice versa, we mean the pair (ID_i, d_i) is an input-output pair of **Extract** with respect to param and s.
- **Sign**. On input a list param of system parameters, a group size n of length polynomial in λ, a set $\{ID_i \in \{0,1\}^* | i \in [1,n]\}$ of n user identities, a message $m \in \mathcal{M}$, and a secret key $\{d_j \in \mathcal{D} | j \in [1,n]\}$, the algorithm outputs an ID-based $(1, n)$ ring signature $\sigma \in \Psi$.

– **Verify**. On input a list param of system parameters, a group size n of length polynomial in λ, a set $\{ID_i \in \{0,1\}^* | i \in [1,n]\}$ of n user identities, a message $m \in \mathcal{M}$, a signature $\sigma \in \Psi$, it outputs either valid or $\mathsf{invalid}$.

Correctness. An ID-Based $(1,n)$ Ring Signature scheme should satisfy the *verification correctness* – signatures signed by honest signers are verified to be invalid with negligible probability.

2.2 Security Requirement

A secure ID-Based $(1,n)$ Ring Signature scheme should be *unforgeable* and *anonymous* which will be defined in a similar way to that of a traditional ring signature scheme.

Unforgeability. It should not be possible for an adversary to forge any signature just from the identities of the group members. We specify a security model which mainly captures the following two attacks:

1. Adaptive chosen message attack
2. Adaptive chosen identity attack

Adaptive chosen message attack allows an adversary to obtain message-signature pairs on demand during the forging attack. Adaptive chosen identity attack allows the adversary to forge a signature with respect to a group chosen by the adversary. To support adaptive chosen message attack, we provide the adversary the following oracle queries.

– **Extraction oracle** ($\mathcal{EO}$)**:** On input ID_i, $d_i \leftarrow$ **Extract**(param, ID_i) is returned . The oracle is stateful, meaning that if $ID_i = ID_j$, then $d_i = d_j$.
– **Signing oracle** ($\mathcal{SO}$)**:** $\mathcal{A}$ chooses a group of n identities $\{ID_i\}_{i\in[1,n]}$ and a message m, the oracle outputs a valid ID-based $(1,n)$ ring signature denoted by $\sigma \leftarrow$ **Sign**$(\mathsf{param}, n, \{ID_i | i \in [1,n]\}, m)$. The signing oracle may query the extraction oracle during its operation.

Let $\mathcal{U} = \{ID_1, \cdots, ID_N\}$ be a set of identities. An adversary $\mathcal{A}$ with oracles $\mathcal{EO}$ and $\mathcal{SO}$ *succeeds* if it outputs $(L, m, \sigma) \leftarrow \mathcal{A}^{\mathcal{SO},\mathcal{EO}}(\mathcal{U})$, such that it satisfies **Verify**$(\mathsf{param}, L, m, \sigma) = \mathsf{valid}$, where $L \subseteq \mathcal{U}$ and $|L| = n$ with restriction that (L, m) should not be in the set of oracle queries and replies between $\mathcal{A}$ and $\mathcal{SO}$, and $\mathcal{A}$ is not allowed to make an Extraction query on any identity $ID \in L$.

The advantage of an adversary $\mathcal{A}$ is defined to be

$$\mathbf{Adv}_{\mathcal{A}} = \Pr[\mathcal{A} \text{ succeeds }]$$

Definition 1 (Unforgeability). *An adversary $\mathcal{A}$ is said to be an (ϵ, t, q_e, q_s)-forger of an ID-based $(1,n)$ ring signature scheme if $\mathcal{A}$ has advantage at least ϵ, runs in time at most t, and makes at most q_e and q_s extraction and signing oracles queries respectively. A scheme is said to be (ϵ, t, q_e, q_s)-unforgeable if no (ϵ, t, q_e, q_s)-forger exists.*

Note that it cannot achieve the unforteability in the stronger sense that the adversary produces a different signature on the same message and the same list of identities, as described in [1,14] since our proposed scheme does not enjoy this level of stronger security.

Anonymity. It should not be possible for an adversary to tell the identity of the signer with a probability larger than $1/n$, where n is the cardinality of the ring, even assuming that the adversary has unlimited computing resources.

Definition 2 (Anonymity). *An ID-based $(1, n)$ ring signature scheme is unconditional anonymous if for any group of n users with identity $\{ID_1, \cdots, ID_n\}$, any message m and signature $\sigma \leftarrow \textbf{\textit{Sign}}(\mathsf{param}, n, \{ID_i | i \in [1, n]\}, m)$, any adversary $\mathcal{A}$, even with unbounded computational power, cannot identify the actual signer with probability better than random guessing. That is, $\mathcal{A}$ can only output the identity of the actual signer with probability no better than $1/n$.*

3 The Proposed Scheme

Our proposed ID-based ring signature scheme is motivated from the signature scheme in [16,7] and the encryption scheme in [18].

3.1 Construction

Let $H_u : \{0,1\}^* \rightarrow \{0,1\}^{n_u}$ and $H_m : \{0,1\}^* \rightarrow \{0,1\}^{n_m}$ be two collision-resistant hash functions for some $n_u, n_m \in \mathbb{Z}$. They are used to create identities and messages of the desired length respectively. The proposed scheme is defined by the following algorithms.

Setup. Select a pairing $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ where the order of $\mathbb{G}_1$ is p. Let g be a generator of $\mathbb{G}_1$. Randomly select $\alpha \in_R \mathbb{Z}_p$, $g_2 \in_R \mathbb{G}_1$ and compute $g_1 = g^\alpha$. Also select randomly the following elements:

- $u', m' \in_R \mathbb{G}_1$
- $\hat{u}_i \in_R \mathbb{G}_1$ for $i = 1, \ldots, n_u$. Let $\hat{U} = \{\hat{u}_i\}$.
- $\hat{m}_i \in_R \mathbb{G}_1$ for $i = 1, \ldots, n_m$. Let $\hat{M} = \{\hat{m}_i\}$.

The public parameters param are $(e, \mathbb{G}_1, \mathbb{G}_2, g, g_1, g_2, u', \hat{U}, m', \hat{M})$ and the master secret key is g_2^α.

Extract. Let $\mathtt{u}_j = H_u(ID_j)$ for user j with identity ID_j, where $j \in \mathbb{Z}$. Let $\mathtt{u}_j[i]$ be the i-th bit of $\mathtt{u}_j$. Define $\mathcal{U}_j \subset \{1, \ldots, n_u\}$ to be the set of indicies such that $\mathtt{u}_j[i] = 1$.

To construct the private key, d_j, of identity ID_j, randomly selects $r_{u_j} \in_R \mathbb{Z}_p$ and compute

$$d_j = \left(g_2^\alpha \left(U_j\right)^{r_{u_j}}, g^{r_{u_j}} \right) = (D_j^{(1)}, D_j^{(2)})$$

where $U_j = u' \prod_{i \in \mathcal{U}_j} \hat{u}_i$.

Sign. Let $L = \{ID_1, \ldots, ID_n\}$ be the list of n identities to be included in the ring signature, including the one of the actual signer. To sign a message $m \in \{0,1\}^*$, compute $\mathfrak{m} = H_m(m, L)$. Let $\mathfrak{m}[i]$ be the i-th bit of $\mathfrak{m}$ and $\mathcal{M} \subset \{1, \ldots, n_m\}$ be the set of indicies i such that $\mathfrak{m}[i] = 1$.

Let the signer be indexed π, where $\pi \in [1, n]$, with private key $d_\pi = (D_\pi^{(1)}, D_\pi^{(2)})$. Randomly select $r_1, \ldots, r_n, r_{\mathfrak{m}} \in_R \mathbb{Z}_p$, compute $U_j = u' \prod_{i \in \mathcal{U}_j} \hat{u}_i$ for $j = 1, \ldots, n$ and

$$\begin{aligned}\sigma = &\left(D_\pi^{(1)} \Big(\prod_{j=1}^{n} (U_j)^{r_j} \Big) \Big(m' \prod_{i \in \mathcal{M}} \hat{m}_i \Big)^{r_{\mathfrak{m}}} \ , \ g^{r_1} \ , \ \ldots \ , \ g^{r_{\pi-1}} \ , \ D_\pi^{(2)} g^{r_\pi} \ , \ g^{r_{\pi+1}} \ , \right. \\ &\left. \ldots \ , \ g^{r_n} \ , \ g^{r_{\mathfrak{m}}} \right) \\ = &(V, R_1, \ldots, R_n, R_{\mathfrak{m}})\end{aligned}$$

Verify. Given a signature $\sigma = (V, R_1, \ldots, R_n, R_{\mathfrak{m}})$ for a list of identities L on a message m, a verifier first computes $\mathfrak{m} = H_m(m, L)$, $U_j = u' \prod_{i \in \mathcal{U}_j} \hat{u}_i$ for $j = 1, \ldots, n$ and checks whether

$$e(V, g) \stackrel{?}{=} e(g_2, g_1) \ \big(\prod_{j=1}^{n} e(U_j, R_j) \big) \ e(m' \prod_{i \in \mathcal{M}} \hat{m}_i, R_{\mathfrak{m}})$$

Output valid if the equality holds. Otherwise output invalid.

Correctness It is easy to see that the signature scheme is correct, as shown in following:

$$\begin{aligned}e(V, g) &= e\Big(g_2^{\alpha} \big(U_\pi\big)^{r_{u_\pi}} \big(U_1\big)^{r_1} \ldots \big(U_n\big)^{r_n} \big(m' \prod_{i \in \mathcal{M}} \hat{m}_i\big)^{r_{\mathfrak{m}}}, g \Big) \\ e(V, g) &= e\Big(g_2^{\alpha} \big(U_1\big)^{r_1} \ldots \big(U_\pi\big)^{r_{u_\pi} + r_\pi} \ldots \big(U_n\big)^{r_n} \big(m' \prod_{i \in \mathcal{M}} \hat{m}_i\big)^{r_{\mathfrak{m}}}, g \Big) \\ &= e(g_2, g)^{\alpha} e\big(U_1, g\big)^{r_1} \ldots e\big(U_\pi, g\big)^{r_{u_\pi} + r_\pi} \ldots e\big(U_n, g\big)^{r_n} e\big(m' \prod_{i \in \mathcal{M}} \hat{m}_i, g\big)^{r_{\mathfrak{m}}} \\ &= e(g_2, g_1) e\big(U_1, R_1\big) \ldots e\big(U_n, R_n\big) e\big(m' \prod_{i \in \mathcal{M}} \hat{m}_i, R_{\mathfrak{m}}\big)\end{aligned}$$

3.2 Security Analysis

We will prove that our proposed scheme is unconditional anonymous and existentially unforgeable under a chosen message and identity attack, in the standard model.

Theorem 1 (Anonymity). *The scheme proposed in Section 3 is unconditional anonymous.*

Proof. In the signature $\sigma = (V, R_1, \ldots, R_n, R_{\mathfrak{m}})$, $\{R_i\}, i \in [1, n] \setminus \pi$ and $R_{\mathfrak{m}}$ are randomly generated which provide no information on the actual signer. $R_\pi = g^{r_{u_\pi}} g^{r_\pi}$. r_π is randomly generated by the actual signer. r_{u_π} is randomly generated by the master which is independent to any user. Thus R_π is also randomly distributed. V is in the form of $g_2^\alpha \big(U_1\big)^{r_1} \ldots \big(U_\pi\big)^{r_{u_\pi}+r_\pi} \ldots \big(U_n\big)^{r_n} \big(m' \prod_{i \in \mathcal{M}} \hat{m}_i\big)^{r_{\mathfrak{m}}}$. Using the same argument, $r_1, \ldots, r_{u_\pi} + r_\pi, \ldots, r_n, r_{\mathfrak{m}}$ are random numbers while α is the master's secret key. All of them provide no information on the actual signer. It is no better for the adversary to do a wild guess. Our proposed scheme is unconditional anonymous. □

For unforgeability, our scheme relies on the hardness of CDH problem, which is stated as below:

Definition 3 (Computational Diffie-Hellman (CDH) problem). *Given a group G of prime order p with generator g and elements $g^a, g^b \in G$ where a, b are selected uniformly at random from $\mathbb{Z}_p^*$, the CDH problem in G is to compute g^{ab}.*

We say that the (ϵ, t)-CDH assumption holds in a group G if no algorithm running in time at most t can solve the CDH problem in G with probability at least ϵ.

Theorem 2 (Existential Unforgeability). *The 1-out-of-n ID-based ring signature scheme proposed in Section 3 is (ϵ, t, q_e, q_s)-unforgeable, assuming that the (ϵ', t')-CDH assumption holds in $\mathbb{G}_1$, where*

$$\epsilon' \geq \frac{\epsilon}{2^{n+3}(q_e + q_s)^n (n_u + 1)^n q_s (n_m + 1)}$$
$$t' = t + O\Big(\big(q_e n_u + q_s(n n_u + n_m)\big)\rho + (q_e + n q_s)\tau\Big)$$

and ρ and τ are the time for a multiplication and an exponentiation in $\mathbb{G}_1$ respectively.

Proof. Assume there is a (ϵ, t, q_e, q_s)-adversary $\mathcal{A}$ exists. We are going to construct another PPT $\mathcal{B}$ that makes use of $\mathcal{A}$ to solve the CDH problem with probability at least ϵ' and in time at most t'.

$\mathcal{B}$ is given a problem instance as follow: Given a group $\mathbb{G}_1$, a generator $g \in \mathbb{G}_1$, two elements $g^a, g^b \in \mathbb{G}_1$. It is asked to output another element $g^{ab} \in \mathbb{G}_1$. In order to use $\mathcal{A}$ to solve for the problem, $\mathcal{B}$ needs to simulates a challenger and the oracles (the extraction oracle and the signing oracle) for $\mathcal{A}$. $\mathcal{B}$ does it in the following way.

Setup. Let $l_u = 2(q_e + q_s)$ and $l_m = 2q_s$. $\mathcal{B}$ randomly selects two integers k_u and k_m such that $0 \leq k_u \leq n_u$ and $0 \leq k_m \leq n_m$. Also assume that $l_u(n_u + 1) < p$ and $l_m(n_m + 1) < p$ for the given values of q_e, q_s, n_u and n_m. It randomly selects the following integers:

- $x' \in_R \mathbb{Z}_{l_u}$; $z' \in_R \mathbb{Z}_{l_m}$; $y', w' \in_R \mathbb{Z}_p$

- $\hat{x}_i \in_R \mathbb{Z}_{l_u}$, for $i = 1, \ldots, n_u$. Let $\hat{X} = \{\hat{x}_i\}$.
- $\hat{z}_i \in_R \mathbb{Z}_{l_m}$, for $i = 1, \ldots, n_m$. Let $\hat{Z} = \{\hat{z}_i\}$.
- $\hat{y}_i \in_R \mathbb{Z}_p$, for $i = 1, \ldots, n_u$. Let $\hat{Y} = \{\hat{y}_i\}$.
- $\hat{w}_i \in_R \mathbb{Z}_p$, for $i = 1, \ldots, n_m$. Let $\hat{W} = \{\hat{w}_i\}$.

We further define the following functions for binary strings $\mathfrak{u}_j$ and $\mathfrak{m}$ where $\mathfrak{u}_j = H_u(ID_j)$ for an identity ID_j, $j \in \mathbb{Z}$ and $\mathfrak{m} = H_m(m, L)$ for a message m and a list of identities L, as follow:

$$F(\mathfrak{u}_j) = x' + \sum_{i \in \mathcal{U}_j} \hat{x}_i - l_u k_u \qquad \text{and} \qquad J(\mathfrak{u}_j) = y' + \sum_{i \in \mathcal{U}_j} \hat{y}_i$$

$$K(\mathfrak{m}) = z' + \sum_{i \in \mathcal{M}} \hat{z}_i - l_m k_m \qquad \text{and} \qquad L(\mathfrak{m}) = w' + \sum_{i \in \mathcal{M}} \hat{w}_i$$

$\mathcal{B}$ constructs a set of public parameters as follow:

$$\begin{aligned} g_1 &= g^a, \qquad g_2 = g^b \\ u' &= g_2^{-l_u k_u + x'} g^{y'}, \qquad \hat{u}_i = g_2^{\hat{x}_i} g^{\hat{y}_i} \quad \text{for} \quad 1 \le i \le n_u \\ m' &= g_2^{-l_m k_m + z'} g^{w'}, \qquad \hat{m}_i = g_2^{\hat{z}_i} g^{\hat{w}_i} \quad \text{for} \quad 1 \le i \le n_m \end{aligned}$$

Note that the master secret will be $g_2^\alpha = g_2^a = g^{ab}$ and we have the following equations:

$$U_j = u' \prod_{i \in \mathcal{U}_j} \hat{u}_i = g_2^{F(\mathfrak{u}_j)} g^{J(\mathfrak{u}_j)} \qquad \text{and} \qquad m' \prod_{i \in \mathcal{M}} \hat{m}_i = g_2^{K(\mathfrak{m})} g^{L(\mathfrak{m})}$$

All public parameters are passed to $\mathcal{A}$.

Oracles Simulation. $\mathcal{B}$ simulates the extraction and signing oracles as follow:

(*Extraction oracle.*) Upon receiving a query for a private key of an identity ID_j, B compute $\mathfrak{u} = H_u(ID_j)$. Although $\mathcal{B}$ does not know the master secret, it can still construct the private key by assuming $F(\mathfrak{u}_j) \neq 0 \bmod p$. It randomly chooses $r_{u_j} \in_R \mathbb{Z}_p$ and computes the private key as

$$d_{u_j} = (D_j^{(1)}, D_j^{(2)}) = \left(g_1^{-\frac{J(\mathfrak{u}_j)}{F(\mathfrak{u}_j)}} \left(U_j\right)^{r_{u_j}}, g_1^{-\frac{1}{F(\mathfrak{u}_j)}} g^{r_{u_j}} \right)$$

By letting $\tilde{r}_{u_j} = r_{u_j} - \frac{a}{F(\mathfrak{u}_j)}$, it can be verifier that d_{u_j} is a valid private key, shown as follow:

$$\begin{aligned} D_j^{(1)} &= g_1^{-\frac{J(\mathfrak{u}_j)}{F(\mathfrak{u}_j)}} \left(U_j\right)^{r_{u_j}} \\ &= g_1^{-\frac{J(\mathfrak{u}_j)}{F(\mathfrak{u}_j)}} (g_2^{F(\mathfrak{u}_j)} g^{J(\mathfrak{u}_j)})^{r_{u_j}} \\ &= g^{-\frac{aJ(\mathfrak{u}_j)}{F(\mathfrak{u}_j)}} (g_2^{F(\mathfrak{u}_j)} g^{J(\mathfrak{u}_j)})^{r_{u_j}} \end{aligned}$$

$$
\begin{aligned}
&= g^{-\frac{aJ(\mathfrak{u}_j)}{F(\mathfrak{u}_j)}} (g_2^{F(\mathfrak{u}_j)} g^{J(\mathfrak{u}_j)})^{\frac{a}{F(\mathfrak{u}_j)}} (g_2^{F(\mathfrak{u}_j)} g^{J(\mathfrak{u}_j)})^{-\frac{a}{F(\mathfrak{u}_j)}} (g_2^{F(\mathfrak{u}_j)} g^{J(\mathfrak{u}_j)})^{r_{u_j}} \\
&= g^{-\frac{aJ(\mathfrak{u}_j)}{F(\mathfrak{u}_j)}} g^{ab} g^{\frac{aJ(\mathfrak{u}_j)}{F(\mathfrak{u}_j)}} (g_2^{F(\mathfrak{u}_j)} g^{J(\mathfrak{u}_j)})^{\tilde{r}_{u_j}} \\
&= g^{ab} (g_2^{F(\mathfrak{u}_j)} g^{J(\mathfrak{u}_j)})^{\tilde{r}_{u_j}} \\
&= g_2^a (g_2^{F(\mathfrak{u}_j)} g^{J(\mathfrak{u}_j)})^{\tilde{r}_{u_j}} \\
&= g_2^a (U_j)^{\tilde{r}_{u_j}}
\end{aligned}
$$

and

$$D_j^{(2)} = g_1^{-\frac{1}{F(\mathfrak{u}_j)}} g^{r_{u_j}} = g^{r_{u_j} - \frac{a}{F(\mathfrak{u}_j)}} = g^{\tilde{r}_{u_j}}$$

To the adversary, all private keys given by $\mathcal{B}$ are indistinguishable from the keys generated by the true challenger.

If $F(\mathfrak{u}_j) = 0 \bmod p$, since the above computation cannot be performed (division by 0), the simulator aborts. To make it simple, the simulator will abort if $F(\mathfrak{u}_j) = 0 \bmod l_u$. The equivalency can be observed as follow. From the assumption $l_u(n_u + 1) < p$, it implies $0 \leq l_u k_u < p$ and $0 \leq x' + \sum_{i \in \mathcal{U}_j} \hat{x}_i < p$ ($\because x' < l_u, \hat{x}_i < l_u, |\mathcal{U}_j| \leq n_u$). We have $-p < F(\mathfrak{u}_j) < p$ which implies if $F(\mathfrak{u}_j) = 0 \bmod p$ then $F(\mathfrak{u}_j) \bmod l_u$. Hence, $F(\mathfrak{u}_j) \neq 0 \bmod l_u$ implies $F(\mathfrak{u}_j) \neq 0 \bmod p$. Thus the former condition will be sufficient to ensure that a private key can be computed without aborting.

(*Signing oracle.*) For a given query of a signature on the list of identities $L = \{ID_1, \ldots, ID_n\}$ and a message m [5], $\mathcal{B}$ first computes $\mathfrak{u}_j = H_u(ID_j)$ and $\mathfrak{m} = H_m(m, L)$.

If $F(\mathfrak{u}_j) \neq 0 \bmod l_u$ for some $j \in [1, n]$, $\mathcal{B}$ randomly selects $\pi \in_R \mathcal{J}$ where $\mathcal{J}$ is the set of integers j such that $F(\mathfrak{u}_j) \neq 0 \bmod l_u$. $\mathcal{B}$ just constructs a private key for π as in the extraction oracle query, then use the **Sign** algorithm described in the proposed scheme to create a signature on L and m.

If $F(\mathfrak{u}_j) = 0 \bmod l_u$ for *all* $j \in [1, n]$, $\mathcal{B}$ tries to construct the signature in a similar way to the construction of private key in an extraction oracle query. Assume $K(\mathfrak{m}) \neq 0 \bmod l_m$. Using the aforementioned argument, it implies $K(\mathfrak{m}) \neq 0 \bmod p$ provided that $l_m(n_m + 1) < p$. The signature can be constructed by first randomly selecting $r_1, \ldots, r_n, r_{\mathfrak{m}} \in_R \mathbb{Z}_p$ and computing

$$
\begin{aligned}
\sigma &= \left(\left(\prod_{j=1}^{n} (U_j)^{r_j} \right) g_1^{-\frac{L(\mathfrak{m})}{K(\mathfrak{m})}} \left(m' \prod_{i \in \mathcal{M}} \hat{m}_i \right)^{r_{\mathfrak{m}}} , g^{r_1} , \ldots , g^{r_n} , g_1^{-\frac{1}{K(\mathfrak{m})}} g^{r_{\mathfrak{m}}} \right) \\
&= \left(g_2^a \left(\prod_{j=1}^{n} (U_j)^{r_j} \right) \left(m' \prod_{i \in \mathcal{M}} \hat{m}_i \right)^{\tilde{r}_m} , g^{r_1} , \ldots , g^{r_n} , g^{\tilde{r}_m} \right)
\end{aligned}
$$

where $\tilde{r}_m = r_{\mathfrak{m}} - \frac{a}{K(\mathfrak{m})}$. If $K(\mathfrak{m}) = 0 \bmod l_m$, the simulator aborts.

[5] Note that $\mathcal{A}$ is not allowed to make any extraction oracle query on any ID_j, where $ID_j \in L$

Output Calculation. If $\mathcal{B}$ does not abort, $\mathcal{A}$ will return a list of identities $L^* = \{ID_1^*, \ldots, ID_n^*\}$ and a message m^* with a forged signature $\sigma^* = (V, R_1, \ldots, R_n, R_{\mathfrak{m}})$ on L^* and m^* with probability at least ϵ. $\mathcal{B}$ checks whether the following conditions are fulfilled:

1. $F(\mathfrak{u}_j^*) = 0 \bmod p$ for *all* $j \in [1, n]$, where $\mathfrak{u}_j^* = H_u(ID_j^*)$.
2. $K(\mathfrak{m}^*) = 0 \bmod p$, where $\mathfrak{m}^* = H_m(m^*, L^*)$.

If not all the above conditions are fulfilled, $\mathcal{B}$ aborts. Otherwise $\mathcal{B}$ computes and outputs

$$\begin{aligned}
\frac{V}{R_1^{J(\mathfrak{u}_1^*)} \ldots R_n^{J(\mathfrak{u}_n^*)} R_{\mathfrak{m}}^{L(\mathfrak{m}^*)}} &= \frac{g_2^a (U_1)^{r_1} \ldots (U_n)^{r_n} \left(m' \prod_{i \in \mathcal{M}} \hat{m}_i\right)^{r_{\mathfrak{m}}}}{g^{J(\mathfrak{u}_1^*) r_1} \ldots g^{J(\mathfrak{u}_n^*) r_n} g^{L(\mathfrak{m}^*) r_{\mathfrak{m}}}} \\
&= \frac{g_2^a \left(g_2^{F(\mathfrak{u}_1^*)} g^{J(\mathfrak{u}_1^*)}\right)^{r_1} \ldots \left(g_2^{F(\mathfrak{u}_n^*)} g^{J(\mathfrak{u}_n^*)}\right)^{r_n} \left(g_2^{K(\mathfrak{m}^*)} g^{L(\mathfrak{m}^*)}\right)^{r_{\mathfrak{m}}}}{g^{J(\mathfrak{u}_1^*) r_1} \ldots g^{J(\mathfrak{u}_n^*) r_n} g^{L(\mathfrak{m}^*) r_{\mathfrak{m}}}} \\
&= g_2^a \\
&= g^{ab}
\end{aligned}$$

which is the solution to the CDH problem instance.

Probability Analysis. For the simulation to complete without aborting, we require the following conditions fulfilled:

1. Extraction queries on an identity ID have $F(\mathfrak{u}) \neq 0 \bmod l_u$, where $\mathfrak{u} = H_u(ID)$.
2. Sign queries (L, m) will either have $F(\mathfrak{u}_j) \neq 0 \bmod l_u$, for some $j \in [1, n]$ where $ID_j \in L$, or $K(\mathfrak{m}) \neq 0 \bmod l_m$ where $\mathfrak{m} = H_m(m, L)$.
3. $F(\mathfrak{u}_j^*) = 0 \bmod l_u$ for all $j \in [1, n]$ where $ID_j^* \in L^*$ and $K(\mathfrak{m}^*) = 0 \bmod l_m$.

For ease of analysis, we will bound the probability of a subcase of this event.

Let $\mathfrak{u}_1, \ldots, \mathfrak{u}_{q_I}$ be the output of the hash function H_u appearing in either extract queries or in sign queries not involving any of the challenge identity included in L^*, and let $\mathfrak{m}_1, \ldots, \mathfrak{m}_{q_M}$ be the output of the hash function H_m in the sign queries involving the challenge list of identities L^*. We have $q_I \leq q_e + q_s$ and $q_M \leq q_s$. We also define the events A_i, A^*, B_ℓ, B^* as follow:

$$\begin{aligned}
&A_i : F(\mathfrak{u}_i) \neq 0 \bmod l_u && \text{where } i = 1, \ldots, q_I \\
&A^* : F(\mathfrak{u}_j^*) = 0 \bmod p && \text{for all } j \in [1, n] \text{ where } ID_j^* \in L^* \\
&B_\ell : K(\mathfrak{m}_\ell) \neq 0 \bmod l_m && \text{where } \ell = 1, \ldots, q_M \\
&B^* : K(\mathfrak{m}^*) = 0 \bmod p
\end{aligned}$$

The probability of $\mathcal{B}$ not aborting is

$$\Pr[\mathsf{not\ abort}] \geq \Pr\left[\left(\bigwedge_{i=1}^{q_I} A_i \wedge A^*\right) \wedge \left(\bigwedge_{\ell=1}^{q_M} B_\ell \wedge B^*\right)\right]$$

Note that the events $\left(\bigwedge_{i=1}^{q_I} A_i \wedge A^*\right)$ and $\left(\bigwedge_{\ell=1}^{q_M} B_\ell \wedge B^*\right)$ are independent.

The assumption $l_u(n_u+1) < p$ implies if $F(\mathfrak{u}) = 0 \bmod p$ then $F(\mathfrak{u}) = 0 \bmod l_u$. Since k_u, x' and $\hat{X}$ are randomly chosen,

$$\begin{aligned}\Pr[A^*] &= \prod_{j=1}^{n} \Pr[F(\mathfrak{u}_j^*) = 0 \bmod p \wedge F(\mathfrak{u}_j^*) = 0 \bmod l_u] \\ &= \prod_{j=1}^{n} \Pr[F(\mathfrak{u}_j^*) = 0 \bmod l_u] \Pr[F(\mathfrak{u}_j^*) = 0 \bmod p \mid F(\mathfrak{u}_j^*) = 0 \bmod l_u] \\ &= \Big(\frac{1}{l_u}\frac{1}{n_u+1}\Big)^n\end{aligned}$$

On the other hand, we have

$$\begin{aligned}\Pr\left[\bigwedge_{i=1}^{q_I} A_i | A^*\right] &= 1 - \Pr\left[\bigvee_{i=1}^{q_I} \overline{A_i} \mid A^*\right] \\ &\geq 1 - \sum_{i=1}^{q_I} \Pr[\overline{A_i} \mid A^*]\end{aligned}$$

where $\overline{A_i}$ denote the event $F(\mathfrak{u}_i) = 0 \bmod l_u$.

Also note that the events $F(\mathfrak{u}_{i_1}) = 0 \bmod l_u$ and $F(\mathfrak{u}_{i_2}) = 0 \bmod l_u$ are independent, where $i_1 \neq i_2$, since the outputs of $F(\mathfrak{u}_{i_1})$ and $F(\mathfrak{u}_{i_2})$ will differ in at least one randomly chosen value. Also since the events A_i and A^* are independent for any i, we have $\Pr[\overline{A_i}|A^*] = 1/l_u$ and

$$\begin{aligned}\Pr\left[\bigwedge_{i=1}^{q_I} A_i \wedge A^*\right] &= \Pr[A^*] \Pr\left[\bigwedge_{i=1}^{q_I} A_i | A^*\right] \\ &= \left(\frac{1}{l_u(n_u+1)}\right)^n \left(1 - \frac{q_I}{l_u}\right) \\ &\geq \left(\frac{1}{l_u(n_u+1)}\right)^n \left(1 - \frac{q_e+q_s}{l_u}\right) \\ &= \left(\frac{1}{2(q_e+q_s)(n_u+1)}\right)^n \left(1 - \frac{1}{2}\right) \\ &\quad (\text{ by setting } l_u = 2(q_e+q_s) \ ) \\ &= \frac{1}{2^{n+1}(q_e+q_S)^n(n_u+1)}\end{aligned}$$

Using similar analysis technique for signing queries we can have

$$\Pr\left[\bigwedge_{\ell=1}^{q_M} B_\ell \wedge B^*\right] \geq \frac{1}{4q_s(n_m+1)}$$

By combining the above result, we have

$$\Pr[\mathsf{not\ abort}] \geq \Pr\left[\left(\bigwedge_{i=1}^{q_I} A_i \wedge A^*\right) \wedge \left(\bigwedge_{\ell=1}^{q_M} B_\ell \wedge B^*\right)\right]$$
$$\geq \frac{1}{2^{n+3}(q_e+q_s)^n(n_u+1)^n q_s(n_m+1)}$$

If the simulation does not abort, $\mathcal{A}$ will produce a forged signature with probability at least ϵ. Thus $\mathcal{B}$ can solve for the CDH problem instance with probability

$$\epsilon' \geq \frac{\epsilon}{2^{n+3}(q_e+q_s)^n(n_u+1)^n q_s(n_m+1)}$$

Remark: We note that since n is included as the exponent of the denominator, we suggest that n may not be too large in order to claim its security.

Time Complexity Analysis. The time complexity of $\mathcal{B}$ is dominated by the exponentiation and multiplication operations for large values of n_u and n_m performed in the extraction and signing queries.

There are $O(n_u)$ and $O(nn_u + n_m)$ multiplications and O(1) and O(n) exponentiations in the extraction and singing stage respectively. The time complexity of $\mathcal{B}$ is

$$t + O\Big(\big(q_e n_u + q_s(nn_u + n_m)\big)\rho + (q_e + nq_s)\tau\Big)$$

□

4 Constant-size Identity Based Ring Signature

We propose a constant-size identity based ring signature without random oracles. The size of the signature is independent of the size of the ring. However, this scheme has a restriction on the maximum number of signers of the ring when the private key is extracted from the identity. Furthermore, the scheme is provably secure in a weak model for unforgeability, namely selective-identity, weak chosen message attack. The security model of weak chosen message attack can be found in [5], and the model of selective-identity can be found in [8]. Their difference from standard model is that the adversary gives the challenge message and challenge identity at the beginning of the unforgeability game.

4.1 Construction

Our scheme is motivated from the encryption scheme in [6]. Let $H_u : \{0,1\}^* \to \mathbb{Z}_p^*$ and $H_m : \{0,1\}^* \to \mathbb{Z}_p^*$ be two collision-resistant hash functions. They are used to create identities and messages of the desired length respectively. The proposed scheme is defined by the following algorithms.

Setup. Select a pairing $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ where the order of $\mathbb{G}_1$ is p. Let g be a generator of $\mathbb{G}_1$. Randomly select $\alpha \in_R \mathbb{Z}_p$, $g_2 \in_R \mathbb{G}_1$ and compute $g_1 = g^\alpha$. Also select randomly the following elements:

– $u', m' \in_R \mathbb{G}_1$
– $\hat{u}_i \in_R \mathbb{G}_1$ for $i = 1, \ldots, n+1$. Let $\hat{U} = \{\hat{u}_i\}$.

The public parameters param are $(e, \mathbb{G}_1, \mathbb{G}_2, g, g_1, g_2, u', \hat{U})$ and the master secret key is g_2^α.

Extract. To generate a private key for ID, let $\mathsf{id} = H_u(ID)$. For $1 \leq i \leq n+1$, the algorithm picks a random $r_i \in \mathbb{Z}_p^*$ and computes:

$$\begin{aligned} SK_{ID,i} &= \Big(g_2^\alpha (u' \hat{u}_i^{\mathsf{id}})^{r_i},\ \ g^{r_i},\ \ \hat{u}_1^{r_i},\ \ \ldots,\ \ \hat{u}_{i-1}^{r_i},\ \ \hat{u}_{i+1}^{r_i},\ \ \ldots,\ \ \hat{u}_{n+1}^{r_i}\Big) \\ &= (a_i,\ b_i,\ c_{i,1},\ \ldots,\ c_{i,i-1},\ c_{i,i+1},\ \ldots,\ c_{i,n+1}) \end{aligned}$$

Sign. Let $L = \{ID_1, \ldots, ID_{n'}\}$ be the list of $n' < n$ identities to be included in the ring signature, including the one of the actual signer at index π. Let $\mathsf{id}_i = H_u(ID_i)$ for $i = 1, \ldots, n'$. To sign a message $M \in \{0,1\}^*$, let $\mathsf{m} = H_m(M, L)$. The signer picks random $t \in \mathbb{Z}_p$, and uses $SK_{ID,\pi}$ to compute:

$$\begin{aligned} V &= a_\pi \cdot \Big(\prod_{j=1, j\neq\pi}^{n'} c_{\pi,j}^{\mathsf{id}_j}\Big) \cdot c_{\pi,n'+1}^{\mathsf{m}} \cdot (\hat{u}_1^{\mathsf{id}_1} \cdots \hat{u}_{n'}^{\mathsf{id}_{n'}} \cdot \hat{u}_{n'+1}^{\mathsf{m}} \cdot u')^t \\ R &= b_\pi \cdot g^t \end{aligned}$$

The signature σ is (V, R).

Verify. Given a signature $\sigma = (V, R)$ for a list of identities $L = \{ID_1, \ldots, ID_{n'}\}$ on a message M, a verifier first computes $\mathsf{m} = H_m(M, L)$ and $\mathsf{id}_i = H_u(ID_i)$ for $i = 1, \ldots, n'$ and then checks whether

$$\hat{e}(g, V) \stackrel{?}{=} \hat{e}(g_1, g_2) \cdot \hat{e}(R, \hat{u}_1^{\mathsf{id}_1} \cdots \hat{u}_{n'}^{\mathsf{id}_{n'}} \cdot \hat{u}_{n'+1}^{\mathsf{m}} \cdot u')$$

Output valid if the equality holds. Otherwise output $\mathsf{invalid}$.

Correctness. The scheme is correct as shown in the following:

$$\begin{aligned} \hat{e}(g, V) &= \hat{e}(g, a_\pi \cdot \Big(\prod_{j=1, j\neq\pi}^{n'} c_{\pi,j}^{\mathsf{id}_j}\Big) \cdot c_{\pi,n'+1}^{\mathsf{m}} \cdot (\hat{u}_1^{\mathsf{id}_1} \cdots \hat{u}_{n'}^{\mathsf{id}_{n'}} \cdot \hat{u}_{n'+1}^{\mathsf{m}} \cdot u')^t) \\ &= \hat{e}(g, g_2^\alpha \cdot (\hat{u}_1^{\mathsf{id}_1} \cdots \hat{u}_{n'}^{\mathsf{id}_{n'}} \cdot \hat{u}_{n'+1}^{\mathsf{m}} \cdot u')^{r_\pi + t}) \\ &= \hat{e}(g_1, g_2) \cdot \hat{e}(R, \hat{u}_1^{\mathsf{id}_1} \cdots \hat{u}_{n'}^{\mathsf{id}_{n'}} \cdot \hat{u}_{n'+1}^{\mathsf{m}} \cdot u') \end{aligned}$$

4.2 Security Analysis

Theorem 3 (Anonymity). *The scheme proposed in Section 4 is unconditional anonymous.*

Proof. In the signature $\sigma = (V, R)$, $R = g^{r_\pi} g^t$. t is randomly generated by the actual signer. r_π is randomly generated by the master which is independent to any user. Thus R is a random number. V is in the form of $g_2^\alpha \big(\hat{u}_1^{\mathsf{id}_1} \cdots \hat{u}_{n'}^{\mathsf{id}_{n'}}\big)^{r_\pi + t}$.

Using the same argument, $r_\pi + t$ is a random number while α is the master's secret key. All of them provide no information on the actual signer. It is no better for the adversary to do a wild guess. Our proposed scheme is unconditional anonymous. □

We prove the security for unforgeability in the selective-ID attack model [6].

Definition 4. *(n-DHI problem) The n-Diffie-Hellman Inversion problem is that, given* g, g^α, g^{α^2}, …, $g^{\alpha^n} \in \mathbb{G}$, *for unknown* $\alpha \in \mathbb{Z}_p^*$, *to compute* $g^{1/\alpha}$.

Definition 5. *(n-DHI* problem) The n-Diffie-Hellman Inversion* problem is that, given* g, g^α, g^{α^2}, …, $g^{\alpha^n} \in \mathbb{G}$, *for unknown* $\alpha \in \mathbb{Z}_p^*$, *to compute* $g^{\alpha^{n+1}}$.

The n-DHI problem and n-DHI* problem are proven equivalent in [23]. We say that the (ϵ, t, n)-DHI* assumption holds if no algorithm running in polynomial time t can solve a random instance of the n-DHI* problem with non-negligible probability ϵ.

Theorem 4. *The 1-out-of-*$(n-1)$ *ID-based ring signature scheme proposed in section 4 is* (ϵ, t, q_e, q_s)*-unforgeable under the selective-ID attack model, assuming that the* (ϵ', t', n)*-DHI* assumption holds in* $\mathbb{G}_1$ *and* H_u, H_m *are collision resistant hash functions, where*

$$\epsilon' \geq \epsilon\Big(1 - \frac{1}{p}\Big)^{q_e}\Big(1 - \frac{1}{p^2}\Big)^{q_s}$$
$$t' = t + O\Big((q_e + q_s)n\rho\Big) + O\Big((q_e + q_s)n\tau\Big)$$

and ρ *and* τ *are the time for a multiplication and an exponentiation in* $\mathbb{G}_1$ *respectively.*

Proof. Assume there is a (ϵ, t, q_e, q_s)-adversary $\mathcal{A}$ exists. We are going to construct another PPT $\mathcal{B}$ that makes use of $\mathcal{A}$ to solve the n-DHI* problem with probability at least ϵ' and in time at most t'.

Setup. $\mathcal{B}$ is given the n-DHI* tuple $(g, g^x, \ldots, g^{x^n})$. The game begins with $\mathcal{A}$ sends the challenge identity $L^* = \{ID_1^*, \ldots, ID_{n-1}^*\}$ and the challenge message M^* to $\mathcal{B}$. Denote $\mathsf{id}_j^* = H_u(ID_j^*)$ for $1 \leq j \leq n-1$ and $\mathsf{id}_n^* = H_m(M^*, L^*)$. $\mathcal{B}$ picks a random $\gamma \in \mathbb{Z}_p$ and assigns $g_1 = g^x, g_2 = g^{x^n} \cdot g^\gamma$. $\mathcal{B}$ picks random $\gamma_1, \ldots \gamma_{n+1} \in \mathbb{Z}_p$ and sets $\hat{u}_j = g^{\gamma_j} g^{-x^{n-j+1}}$, for $1 \leq j \leq n$. It also picks a random $\delta \in \mathbb{Z}_p$ and computes $u' = g^{\delta + \sum_{j=1}^{n} x^{n-j+1} \mathsf{id}_j^*}$. $\mathcal{B}$ gives $\mathcal{A}$ the public parameters $\mathsf{param} = (g, g_1, g_2, u', \hat{u}_1, \ldots, \hat{u}_n)$. The corresponding (unknown) master secret key is $g_2^x = g^{x(x^n+\gamma)}$.

Oracle Simulation. $\mathcal{B}$ simulates the extraction and signing oracles as follow:

(*Extraction oracle.*) Upon receiving a query for a private key of an identity ID, if $H_u(ID) = H_u(ID_1^*)$, $\mathcal{B}$ declares failure and exits. Otherwise the simulator

[6] Selective-ID model requires the adversary to choose the challenged ID before any oracle queries.

chooses a random $\tilde{r}_1 \in \mathbb{Z}_p$. Denote $\mathsf{id} = H_u(ID)$ and $r_1 = \frac{x}{(\mathsf{id}-\mathsf{id}_1^*)} + \tilde{r}_1$ and compute:

$$a_1 = g^{x\gamma} \cdot Z \cdot g^{x^n \tilde{r}_1(\mathsf{id}_1^* - \mathsf{id})} \quad \text{where} \quad Z = \left(g^{\delta + \mathsf{id}\gamma_1} \cdot \prod_{i=2}^{n} g^{x^{n-i+1}\mathsf{id}_i^*} \right)^{r_1}$$

$$b_1 = g^{r_1} = g^{x/(\mathsf{id}-\mathsf{id}_1^*)} g^{\tilde{r}_1}$$

$$c_{1,2} = \hat{u}_2^{r_1} = g^{(\gamma_2 - x^{n-1})(\frac{x}{(\mathsf{id}-\mathsf{id}_1^*)} + \tilde{r}_1)}$$

$$\vdots$$

$$c_{1,n} = \hat{u}_2^{r_1} = g^{(\gamma_n - x)(\frac{x}{(\mathsf{id}-\mathsf{id}_1^*)} + \tilde{r}_1)}$$

Refer to [6] for the well-formedness of the secret key. The computation for $(a_i, b_i, c_{i,j})$ where $1 \leq i \leq n-1$ are similar and hence are omitted.

(*Signing oracle.*) For input identities $L = (ID_1, \ldots, ID_{n'})$ and message M, denote $\mathsf{id}_j = H_u(ID_j)$ for $1 \leq j \leq n'$ and $\mathsf{id}_{n'+1} = H_m(M, L)$. If $\{\mathsf{id}_1, \ldots, \mathsf{id}_{n'+1}\}$ is the same as $\{\mathsf{id}_1^*, \ldots, \mathsf{id}_n^*\}$ or is a prefix of it, $\mathcal{B}$ declares failure and exits. Otherwise there exists a $k \leq n$ such that $\mathsf{id}_k \neq \mathsf{id}_k^*$. We set k be the smallest such index. To answer the query, $\mathcal{B}$ derives for the secret key of identity id_k as in the extraction oracle, and then computes the signature using the secret key.

Output Calculation. Finally, $\mathcal{A}$ returns a signature σ^* for message M^* and signers L^*. We denote $\sigma^* = (V^*, R^*)$. Therefore we can set $R^* = g^{\bar{r}}$ for some $\bar{r} \in \mathbb{Z}_p$. Then:

$$\begin{aligned} V^* &= g_2^{\alpha}(u' \prod_{i=1}^{n} \hat{u}_i^{\mathsf{id}_i^*})^{\bar{r}} \\ &= g_2^{\alpha}(g^{\delta} \prod_{j=1}^{n} g^{x^{n-j+1}\mathsf{id}_j^*} \prod_{i=1}^{n} (\frac{g^{\gamma_i}}{g^{x^{n-i+1}}})^{\mathsf{id}_i^*})^{\bar{r}} \\ &= g_2^{\alpha}(g^{\delta} \prod_{i=1}^{n} g^{\gamma_i \mathsf{id}_i^*})^{\bar{r}} \\ &= g_2^{\alpha}(g^{\delta + \sum_{i=1}^{n}(\gamma_i \mathsf{id}_i^*)})^{\bar{r}} \end{aligned}$$

Therefore $\mathcal{B}$ returns $g^{x^{\ell+1}} = g_2^{\alpha}/g^{x\gamma} = V^*/(R^{*\delta + \sum_{i=1}^{\ell}(\gamma_i I_i^*)} g^{x\gamma})$ as the solution.

Probability Analysis. For the simulation to complete without aborting, we require the following conditions fulfilled:

1. Extraction queries on an identity ID have $H_u(ID) = H_u(ID_1^*)$.
2. Sign queries for $\{\mathsf{id}_1, \ldots, \mathsf{id}_{n'+1}\}$ is not the same as $\{\mathsf{id}_1^*, \ldots, \mathsf{id}_n^*\}$ or is a prefix of it.

We define the events A_i, B_ℓ as follow:

$$A_i : H_u(ID_i) \neq H_u(ID_1^*) \qquad \text{where } i = 1, \ldots, q_e$$

$$B_\ell : \{\mathsf{id}_{\ell,1}, \ldots, \mathsf{id}_{\ell,n'_\ell+1}\} \neq \{\mathsf{id}_1^*, \ldots, \mathsf{id}_{\bar{n}}^*\} \qquad \text{where } \ell = 1, \ldots, q_s,\ 2 \leq \bar{n} \leq n$$

The probability of $\mathcal{B}$ not aborting is

$$\Pr[\mathsf{not\ abort}] \geq \Pr\left[\Big(\bigwedge_{i=1}^{q_e} A_i\Big) \wedge \Big(\bigwedge_{\ell=1}^{q_s} B_\ell\Big)\right]$$

Note that the events $\left(\bigwedge_{i=1}^{q_e} A_i\right)$ and $\left(\bigwedge_{\ell=1}^{q_s} B_\ell\right)$ are independent.

The assumption that H_u and H_m are collision resistant hash functions implies:

$$\Pr[A_i] = 1 - \frac{1}{p}$$
$$\Pr[B_i] = 1 - (\frac{1}{p})^{n_i'+1}$$

By combining the above result, we have

$$\begin{aligned}\Pr[\mathsf{not\ abort}] &\geq \Pr\left[\Big(\bigwedge_{i=1}^{q_e} A_i\Big) \wedge \Big(\bigwedge_{\ell=1}^{q_s} B_\ell\Big)\right] \\ &= \Big(1-\frac{1}{p}\Big)^{q_e} \prod_{i=1}^{q_s}\Big(1-(\frac{1}{p})^{n_i'+1}\Big) \\ &\geq \Big(1-\frac{1}{p}\Big)^{q_e}\Big(1-\frac{1}{p^2}\Big)^{q_s}\end{aligned}$$

If the simulation does not abort, $\mathcal{A}$ will produce a forged signature with probability at least ϵ. Thus $\mathcal{B}$ can solve for the DHI* problem instance with probability

$$\epsilon' \geq \epsilon\Big(1-\frac{1}{p}\Big)^{q_e}\Big(1-\frac{1}{p^2}\Big)^{q_s}$$

Time Complexity Analysis. The time complexity of $\mathcal{B}$ is dominated by the exponentiation and multiplication operations for large values of n_u and n_m performed in the extraction and signing queries.

There are $O(n)$ multiplications and $O(n)$ exponentiations in the both extraction and singing stage. The time complexity of $\mathcal{B}$ is

$$t + O\Big((q_e+q_s)n\rho\Big) + O\Big((q_e+q_s)n\tau\Big)$$

□

Full Unforgeability As shown in many papers with selective-ID security model, we can always turns the proof into adaptive-ID model by hashing the identity prior to using it. However the reduction introduces a 2^d multiplicative security loss factor in the standard model, where d is the length of the output of the hash function.

To turn a signature scheme from secure against weak chosen message attack to secure against adaptive chosen message attack secure, we can make use of one-time signature. Suppose we have a one-time signature scheme (Sign, Verify) which is secure against adaptive chosen message attack. To sign a ring signature for message M, a user needs to generate key pairs (pk, sk) for the one-time signature scheme. Then he uses the ring signature scheme in the previous section to sign on pk to get a ring signature σ_1. After that, he uses sk to sign on the message M to get a signature $\sigma_2 = \mathsf{Sign}(sk, M)$. The final signature is $(\sigma_1, \sigma_2, pk, M)$. To verify the signature, the verifier checks if the ring signature for pk is valid and if $\mathsf{Verify}(pk, M)$ is true.

5 Conclusion

In this paper, we have proposed two new ID-based ring signature schemes which are secure in the standard model. Our first scheme, with signature size linear in the cardinality of the ring, is secure in the standard model under the computational Diffie-Hellman assumption. The second scheme, achieving constant signature size, is secure in a weaker attack model (the selective ID and weak chosen message model), under the Diffie-Hellman Inversion assumption. It also applies certain limitation on the size of the ring in the signature.

It remains an open problem to construct a scheme that is secure in the strongest model with constant size signature while removing all limitations on the size of ring.

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. M. Au, J. K. Liu, P. P. Tsang, and D. S. Wong. A suite of id-based threshold ring signature schemes with different levels of anonymity. Cryptology ePrint Archive, Report 2005/326, 2005. `http://eprint.iacr.org/`.
3. A. K. Awasthi and S. Lal. ID-based Ring Signature and Proxy Ring Signature Schemes from Bilinear Pairings. Cryptology ePrint Archive, Report 2004/184, 2004. `http://eprint.iacr.org/`.
4. A. Bender, J. Katz, and R. Morselli. Ring signatures: Stronger definitions, and constructions without random oracles. In *TCC 2006*, volume 3816 of *Lecture Notes in Computer Science*, pages 60–79. Springer, 2006.
5. D. Boneh and X. Boyen. Short signatures without random oracles. In *Proc. EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 56–73. Springer, 2004.
6. D. Boneh, X. Boyen, and E.-J. Goh. Hierarchical identity based encryption with constant size ciphertext. In *Proc. EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 440–456. Springer, 2005.
7. X. Boyen and B. Waters. Compact group signatures without random oracles. In *Advances in Cryptology—EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 427–444. Springer-Verlag, 2006.

8. R. Canetti, S. Halevi, and J. Katz. A forward-secure public-key encryption scheme. In *Proc. EUROCRYPT 2003*, volume 2656 of *Leture Notes in Computer Science*, pages 255–271. Springer-Verlag, 2003.
9. S. S. M. Chow, J. K. Liu, V. K. Wei, and T. H. Yuen. Ring signatures without random oracles. In *ASIACCS 06*, pages 297–302. ACM, 2006.
10. S. S. M. Chow, S.-M. Yiu, and L. C. K. Hui. Efficient identity based ring signature. In *ACNS 2005*, volume 3531 of *Lecture Notes in Computer Science*, pages 499–512. Springer, 2005.
11. Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup. Anonymous identification in ad hoc groups. In *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 609–626. Springer-Verlag, 2004.
12. J. Herranz and G. Sáez. A provably secure ID-based ring signature scheme. Cryptology ePrint Archive, Report 2003/261, 2003. `http://eprint.iacr.org/`.
13. C.-Y. Lin and T.-C. Wu. An identity-based ring signature scheme from bilinear pairings. Cryptology ePrint Archive, Report 2003/117, 2003. `http://eprint.iacr.org/`.
14. J. K. Liu and D. S. Wong. Linkable ring signatures: Security models and new schemes (extended abstract). In *ICCSA 2005*, volume 3481 of *LNCS*, pages 614–623. Springer-Verlag, 2005.
15. L. Nguyen. Accumulators from Bilinear Pairings and Applications. In *CT-RSA 2005*, volume 3376 of *LNCS*, pages 275–292, 2005.
16. K. Paterson and J. Schuldt. Efficient identity-based signatures secure in the standard model. Cryptology ePrint Archive, Report 2006/080, 2006. `http://eprint.iacr.org/2006/080/`.
17. A. Shamir. Identity-Based Cryptosystems and Signature Schemes. In *CRYPTO 1984*, volume 196 of *LNCS*, pages 47–53, 1984.
18. B. Waters. Efficient identity-based encryption without random oracles. In *Proc. EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 114–127. Springer-Verlag, 2005.
19. V. Wei and Y. H. Yuen. (hierarchical identity-based) threshold ring signatures. http://eprint.iacr.org/2006/193/, 2006.
20. F. Zhang and X. Chen. Cryptanalysis and improvement of an id-based ad-hoc anonymous identification scheme at ct-rsa 05. Cryptology ePrint Archive, Report 2005/103, 2005. `http://eprint.iacr.org/`.
21. F. Zhang and K. Kim. ID-Based Blind Signature and Ring Signature from Pairings. In *ASIACRYPT 2002*, volume 2501 of *LNCS*, pages 533–547. Springer-Verlag, 2002.
22. F. Zhang and K. Kim. Efficient ID-Based Blind Signature and Proxy Signature from Bilinear Pairings. In R. Safavi-Naini and J. Seberry, editors, *Information Security and Privacy, 8th Australasian Conference, ACISP 2003, Wollongong, Australia, July 9-11, 2003, Proceedings*, volume 2727 of *Lecture Notes in Computer Science*, pages 312–323. Springer, 2003.
23. F. Zhang, R. Safavi-Naini, and W. Susilo. An efficient signature scheme from bilinear pairings and its applications. In *PKC 2004*, volume 2947 of *Lecture Notes in Computer Science*, pages 277–290. Springer, 2004.