Efficient Identity Based Ring Signature

Sherman S.M. Chow*, S.M. Yiu, and Lucas C.K. Hui

Department of Computer Science
The University of Hong Kong
Pokfulam, Hong Kong
{smchow,smyiu,hui}@cs.hku.hk

Abstract. Identity-based (ID-based) cryptosystems eliminate the need of validity checking of the certificates and the need of registering for a certificate before getting the public key. These two features are desirable especially for the efficiency and the real spontaneity of ring signature, where a user can anonymously sign a message on behalf of a group of spontaneously conscripted users including the actual signer.
To the best of authors' knowledge, the number of pairing computations of all existing ID-based ring signature schemes from bilinear pairings grows linearly with the group size, which made the efficiency of ID-based schemes over traditional schemes questionable.
In this paper, we construct an efficient ID-based ring signature which only needs two pairing computations for any group size. The proposed scheme is proven to be existential unforgeable against adaptive chosen message-and-identity attack under the random oracle model, using the forking lemma for generic ring signature schemes. Extension to support general access structure is also discussed.

Key words: Identity-based signature, ring signature, bilinear pairings, efficiency, real spontaneity, general access structure, anonymity

1 Introduction

Ring signature is a group-oriented signature with privacy concerns: any user can anonymously signs a message on behalf of a group of spontaneously conscripted users including the actual signer. Any verifier can be convinced that the message has been signed by one of the member in this group, but the actual signer remains unknown. However, the theory of ring signature faced two problems when it comes to reality.

In traditional public key infrastructure (PKI), the public key is usually a "random" string that is unrelated to the identity of the user, so there is a need for a trusted-by-all certificate authority (CA) to assure the relationship between the cryptographic keys and the user. Therefore, any verifier of a signature must obtain a copy of user's certificate and check the validity of the certificate before checking the validity of the signature. In ring signature, not only the verifier must verify all the public keys of the group. The signer must do so as well or his/her anonymity is jeopardized (consider the extreme case that all certificates used are indeed invalid except the signer's one). The communication and the validation of a large number of public keys greatly affect the efficiency of the scheme. Moreover, real spontaneity is not always possible for ring signature under traditional PKI. Any signer can spontaneously conscript users who have already registered for a certificate.

Identity-based (ID-based) ring signature solved these problems: the public key of each user can be easily and publicly computed from a string corresponding his/her identity (for example, an email address). This property avoids the necessity of certificates, and associates an implicit public key to each person over the world.

* corresponding author

Unfortunately, the theory of ID-based ring signature also faced obstacle in real application. ID-based ring signature schemes are usually derived from bilinear pairings, a powerful but computationally expensive cryptographic primitive. The important properties of bilinear pairings and associated intractable problems are recalled in Section 3.

From the review in the next section, we know that the number of pairing computations of all existing ID-based ring signature from bilinear pairings grows linearly with the group size, which made the efficiency of ID-based schemes over traditional schemes questionable. It is fair to say devising an ID-based ring signature using sublinear numbers of pairing computation remains an open question.

We close this open problem in this paper. An efficient ID-based ring signature is proposed in Section 5, which only takes two pairing computations for any group size, and the generation of the signature involves no pairing computations at all. The proposed scheme is proven to be existential unforgeable against adaptive chosen message-and-identity attack under the random oracle model. The framework and the security notion of ID-based ring signature are discussed in Section 4.

In the literature, 1-out-of-n-groups ring signature was also considered, which supports an ad-hoc access structure consisting of groups of different sizes. The verifier can be convinced that the signature is generated from all members of a certain group, but cannot know which group has indeed participated in the signing. We notice that an ID-based ring signature for general access structure can be implemented by an 1-out-of-n-groups ring signature. Extension of the proposed scheme to support this general access structure is shown in Section 6.

2 Related Work

ID-based ring signature was introduced in [18] and a more efficient version was proposed in [12]. Small inconsistencies in [18] and [12] were fixed by [1], together with a new proxy ring signature scheme from the delegation function due to [20]. Another ring signature with formally proven security was proposed in [10], where ID-based ring signature from anonymous subsets (i.e. 1-out-of-n-groups ring signature) was also considered. The scheme in [10] supports parallel pairing operations, which is not possible in schemes like [1, 12, 18].

Threshold ring signature is the t-out-of-n threshold version of ring signature, where t or more entities can jointly generate a valid signature but $t-1$ or fewer entities cannot. These schemes are applied in pervasive computing applications and mobile ad-hoc networks, where ad-hoc groups are very common. The first ID-based threshold ring signature was proposed in [6]. It is robust. Moreover, it supports trusted authority compatibility, which enables the signer to conscript non-participating signers under different trusted authorities. The scheme's time and space complexity are up to the state-of-the-art of existing pairing-based ring signature and threshold ring signature, if not better than. Actually, the scheme in [6] was the most efficient (in terms of number of pairing operations required) ID-based ring signature scheme (when $t = 1$).

Taken into account the total computational costs for signature generation and verification, existing solutions [1, 6, 10, 12, 18] need a number of pairing computations ranging from $n + 1$ to $4n - 1$ where n is the group size of the ring signature. Since pairing computation is usually the most expensive one among others in ID-based cryptosystems, this linear dependence with the group size is undesirable.

We remark that there are non-ID-based ring signature schemes from bilinear pairings, for examples, [2, 13, 16, 17, 19, 20].

Indeed, the real spontaneity of ID-based ring signature also relies on the assumption that the trusted authority (the private key generator) will not reveal any information about who has requested for his/her private key and who has not. In [9], an separable and anonymous ID-based key issuing protocol was proposed such that any eavesdropper cannot learn what is the identity associated with the private key being issued even though the key is not transmitted via a secure channel.

Ring signature scheme can be used to derive other primitives as well. It had been utilized to construct non-interactive deniable ring authentication [14], perfect concurrent signature [15] and multi-designated verifiers signature [4, 11].

3 Preliminaries

Before presenting our results, we review the definitions of bilinear pairing and related complexity assumptions. The definition of generic ring signature and the forking lemma for such class of ring signature will be discussed as well.

3.1 Bilinear Pairings

Bilinear pairing is an important primitive for many cryptographic schemes [1–20]. Here, we describe some of its key properties.

Let $(\mathbb{G}_1, +)$ and $(\mathbb{G}_2, \cdot)$ be two cyclic groups of prime order q. The bilinear pairing is given as $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, which satisfies the following properties:

1. *Bilinearity*: For all $P, Q, R \in \mathbb{G}_1$, $\hat{e}(P + Q, R) = \hat{e}(P, R)\hat{e}(Q, R)$, and $\hat{e}(P, Q + R) = \hat{e}(P, Q)\hat{e}(P, R)$.
2. *Non-degeneracy*: There exists $P, Q \in \mathbb{G}_1$ such that $\hat{e}(P, Q) \neq 1$.
3. *Computability*: There exists an efficient algorithm to compute $\hat{e}(P, Q)$ $\forall P, Q \in \mathbb{G}_1$.

3.2 Complexity Assumptions

Definition 1. *Given a generator P of a group $\mathbb{G}$ and a 3-tuple (aP, bP, cP), the Decisional Diffie-Hellman problem (DDHP) is to decide whether $c = ab$.*

Definition 2. *Given a generator P of a group $\mathbb{G}$, (P, aP, bP, cP) is defined as a valid Diffie-Hellman tuple if $c = ab$.*

Definition 3. *Given a generator P of a group $\mathbb{G}$ and a 2-tuple (aP, bP), the Computational Diffie-Hellman problem (CDHP) is to compute abP.*

Definition 4. *If $\mathbb{G}$ is a group such that DDHP can be solved in polynomial time but no probabilistic algorithm can solve CDHP with non-negligible advantage within polynomial time, then we call $\mathbb{G}$ a Gap Diffie-Hellman (GDH) group.*

We assume the existence of a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ that one can solve Decisional Diffie-Hellman Problem in polynomial time.

3.3 Forking Lemma for Ring Signature Schemes

The unforgeability of (ID-based) ring signature schemes can be proven with the help of the forking lemma for generic ring signature scheme [10]. Here we review the required conditions for a ring signature scheme to be considered as *generic*. Denote $H(\cdot)$ be a cryptographic hash function that outputs k bits, where k is the security parameter. Consider a group L of n members ($L = \{ID_1, ID_2, \cdots, ID_n\}$) and a message m, a generic ring signature scheme will produce ring signatures in the form of $\{L, m, R_1, R_2, \cdots, R_n, h_1, h_2, \cdots, h_n, \sigma\}$ where for $i \in \{1, 2, \cdots, n\}$, R_is are distinct and no R_i can appear in a signature with probability greater than $2/2^k$; $h_i = H(L, m, R_i)$ and σ is dependent on all of $\{R_i\}$, $\{h_i\}$ and m.

Theorem 1 *Consider a generic ring signature scheme with security parameter k. Let $\mathcal{A}$ be a probabilistic polynomial time algorithm which takes as the identity of each members in the group of L and the public parameters that can ask for at most Q queries to the random oracle; if $\mathcal{A}$ can produce a valid ring signature $\{L, m, R_1, \cdots, R_n, h_1, \cdots, h_n\, \sigma\}$, for some $L^* \subset L$ of n users within time bound T and with non-negligible probability of success $\epsilon \geq \frac{7C_n^Q}{2^k}$ Then, within a time period of $2T$ and with probability greater than $\frac{\epsilon^2}{66C_n^Q}$, we can use $\mathcal{A}$ to obtain two valid ring signatures $\{L, m, R_1, \cdots, R_n, h_1, \cdots, h_n\, \sigma\}$ and $\{L, m, R_1, \cdots, R_n, h'_1, \cdots, h'_n\, \sigma'\}$ such that $h_j \neq h'_j$, for some $j \in \{1, \cdots, n\}$ and $h_i = h'_i$ for all $i \in \{1, \cdots, n\} \backslash \{j\}$.*

In the practical implementation, we usually omit $\{h_i\}$ in the ring signature as they can be correctly recovered during the verification process.

4 Framework and Security Notions of ID-based Ring Signature Schemes

Hereafter the definition and the security notion of ID-based ring signature schemes are reviewed.

4.1 ID-based Ring Signature

Framework An ID-based ring signature scheme consists of four algorithms: `Setup`, `KeyGen`, `Sign`, and `Verify`.

- `Setup`: On an unary string input 1^k where k is a security parameter, it produces the master secret key s and the common public parameters *params*, which include a description of a finite signature space and a description of a finite message space.
- `KeyGen`: On an input of signer's identity $ID \in \{0, 1\}^*$ and the master secret key s, it outputs the signer's secret signing key S_{ID}. (The corresponding public verification key Q_{ID} can be computed easily by everyone.)
- `Sign`: On input of a message m, a group of n users' identities $\{ID_i\}$, where $1 \leq i \leq n$, and the secret keys of one members S_{ID_s}, where $1 \leq s \leq n$; it outputs an ID-based ring signature σ on the message m.
- `Verify`: On a ring signature σ, a message m and the group of signers' identities $\{ID_i\}$ as the input, it outputs $\top$ for "true" or $\perp$ for "false", depending on whether σ is a valid signature signed by a certain member in the group $\{ID_i\}$ on a message m.

These algorithms must satisfy the standard consistency constraint of ID-based ring signature scheme, i.e. if $\sigma = \texttt{Sign}(m, \{ID_i\}, S_{ID_s})$, we must have $\texttt{Verify}(\sigma, \{ID_i\}, m) = \top$.

For an ID-based ring signature scheme to be considered as secure, we need to consider its unforgeability and signer ambiguity.

Security Notions The following EUF-IDRS-CMIA2 game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ formally defines the *existential unforgeability of ID-based ring signature under adaptive chosen-message-and-identity attack*.

EUF-IDRS-CMIA2 Game:

Setup: The challenger $\mathcal{C}$ takes a security parameter k and runs the `Setup` to generate common public parameters *params* and also the master secret key s. $\mathcal{C}$ sends *params* to $\mathcal{A}$.

Attack: The adversary $\mathcal{A}$ can perform a polynomially bounded number of queries in an adaptive manner (that is, each query may depend on the responses to the previous queries). The types of queries allowed are described below.

– Hash functions queries: $\mathcal{A}$ can ask for the values of the hash functions (e.g. $H(\cdot)$ and $H_0(\cdot)$ in our proposed scheme) for any input.
– `KeyGen`: $\mathcal{A}$ chooses an identity ID. $\mathcal{C}$ computes $\texttt{KeyGen}(ID) = S_{ID}$ and sends the result to $\mathcal{A}$.
– `Sign`: $\mathcal{A}$ chooses a group of n users' identities $\{ID_i\}$ where $1 \leq i \leq n$, and any message m. $\mathcal{C}$ outputs an ID-based ring signature σ.

Forgery: The adversary $\mathcal{A}$ outputs an ID-based ring signature σ and a group of n users' identities $\{ID_i\}$ where $1 \leq i \leq n$. The only restriction is that $(m, \{ID_i\})$ does not appear in the set of previous `Sign` queries and each of the secret keys in $\{S_{ID_i}\}$ is never returned by any `KeyGen` query. i.e. no private keys in $\{S_{ID_i}\})$ is known. It wins the game if $\texttt{Verify}(\sigma, \{ID_i\})$ is equal to $\top$. The advantage of $\mathcal{A}$ is defined as the probability that it wins.

Definition 5. *An ID-based ring signature scheme is said to have the existential unforgeability against adaptive chosen-message-and-identity attacks property (EUF-IDRS-CMIA2 secure) if no adversary has a non-negligible advantage in the EUF-IDRS-CMIA2 game.*

Definition 6. *An ID-based ring signature scheme is said to have the unconditional signer ambiguity if for any group of n users' identities $\{ID_i\}$ where $1 \leq i \leq n$, any message m and any signature σ, where $\sigma = \texttt{Sign}(m, \{ID_i\})$; any verifier $\mathcal{A}$ even with unbounded computing resources, cannot identify the actual signer with probability better than a random guess. That is, $\mathcal{A}$ can only output the actual signer indexed by s with probability no better than $\frac{1}{n}$.*

4.2 ID-Based Ring Signature for General Access Structure

Framework An ID-based ring signature scheme for general access structure consists of four algorithms: `Setup`, `KeyGen`, `Sign`, and `Verify`.

– `Setup`: On an unary string input 1^k where k is a security parameter, it produces the master secret key s and the common public parameters *params*, which include a description of a finite signature space and a description of a finite message space.
– `KeyGen`: On an input of signer's identity $ID \in \{0,1\}^*$ and the master secret key s, it outputs the signer's secret signing key S_{ID}. (The corresponding public verification key Q_{ID} can be computed easily by everyone.)
– `Sign`: On input of a message m, n group of users' identities $\{\mathcal{U}_i\}$, where $1 \leq i \leq n$ and $\mathcal{U}_i = \{ID_{i_j}\}$, and the secret keys $\{S_{ID_{s_j}}\}$ of all members of one of the group $\mathcal{U}_s$, where $1 \leq s \leq n$; it outputs an ID-based ring signature for general access structure σ on the message m.

– `Verify`: On input of a ring signature σ, a message m and n group of users' identities $\{\mathcal{U}_i\}$, where $1 \leq i \leq n$ and $\mathcal{U}_i = \{ID_{i_j}\}$, it outputs $\top$ for "true" or $\perp$ for "false", depending on whether σ is a valid signature signed by all members of a certain group in the $\{\mathcal{U}_i\}$ on a message m.

These algorithms must satisfy the standard consistency constraint of ID-based ring signature scheme for general access structure, i.e. if $\sigma = \texttt{Sign}(m, \{\mathcal{U}_i\}, S_{ID_{s_j}})$, we must get "true" from the verification algorithm taking the signature, the message and the groups of identities as the input, i.e. $\texttt{Verify}(\sigma, \{\mathcal{U}_i\}, m) = \top$.

For an ID-based ring signature scheme for general access structure to be considered as secure, we need to consider its unforgeability and signer ambiguity.

Security Notions The following EUF-IDRSG-CMIA2 game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ formally defines the *existential unforgeability of ID-based ring signature under adaptive chosen-message-and-identity attack*.

EUF-IDRSG-CMIA2 Game:

Setup: The challenger $\mathcal{C}$ takes a security parameter k and runs the `Setup` to generate common public parameters *params* and also the master secret key s. $\mathcal{C}$ sends *params* to $\mathcal{A}$.

Attack: The adversary $\mathcal{A}$ can perform a polynomially bounded number of queries in an adaptive manner (that is, each query may depend on the responses to the previous queries). The types of queries allowed are described below.

– Hash functions queries: $\mathcal{A}$ can ask for the values of the hash functions (e.g. $H(\cdot)$ and $H_0(\cdot)$ in our proposed scheme) for any input.
– `KeyGen`: $\mathcal{A}$ chooses an identity ID. $\mathcal{C}$ computes $\texttt{KeyGen}(ID) = S_{ID}$ and sends the result to $\mathcal{A}$.
– `Sign`: $\mathcal{A}$ chooses n group of users' identities $\{\mathcal{U}_i\}$, where $1 \leq i \leq n$ and $\mathcal{U}_i = \{ID_{i_j}\}$, and any message m. $\mathcal{C}$ outputs an ID-based ring signature for general access structure σ.

Forgery: The adversary $\mathcal{A}$ outputs an ID-based ring signature σ and n group of users' identities $\{\mathcal{U}_i\}$, where $1 \leq i \leq n$ and $\mathcal{U}_i = \{ID_{i_j}\}$. The only restriction is that $(m, \{\mathcal{U}_i\})$ does not appear in the set of previous `Sign` queries and for each group of identities $\{\mathcal{U}_i\}$, at least one secret key in $\{S_{ID_{i_j}}\}$ is never returned by any `KeyGen` query. It wins the game if $\texttt{Verify}(\sigma, \{\mathcal{U}_i\})$ is equal to $\top$. The advantage of $\mathcal{A}$ is defined as the probability that it wins.

Definition 7. *An ID-based ring signature scheme for general access structure is said to have the existential unforgeability against adaptive chosen-message-and-identity attacks property (EUF-IDRSG-CMIA2 secure) if no adversary has a non-negligible advantage in the EUF-IDRSG-CMIA2 game.*

Definition 8. *An ID-based ring signature scheme for general access structure is said to have the unconditional group of signers ambiguity if for any n group of users' identities $\{\mathcal{U}_i\}$, where $1 \leq i \leq n$ and $\mathcal{U}_i = \{ID_{i_j}\}$, any message m and any signature σ, where $\sigma = \texttt{Sign}(m, \{\mathcal{U}_i\})$; any verifier $\mathcal{A}$ not from the actual signer group, even with unbounded computing resources, cannot identify the actual group of signers with probability better than a random guess. That is, $\mathcal{A}$ can only output the actual signers group indexed by s with probability no better than $\frac{1}{n}$.*

5 Efficient ID-based Ring Signature

5.1 Construction

Define $\mathbb{G}_1, \mathbb{G}_2$, and $\hat{e}(\cdot,\cdot)$ as in the Section 3 where $\mathbb{G}_1$ is a GDH group. $H(\cdot)$ and $H_0(\cdot)$ are two cryptographic hash functions where $H : \{0,1\}^* \rightarrow \mathbb{G}_1$ and $H_0 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$.

`Setup`: The trusted authority (TA) randomly chooses $x \in_R \mathbb{Z}_q^*$, keeps it as the master secret key and computes the corresponding public key $P_{pub} = xP$. The system parameters are:

$$params = \{\mathbb{G}_1, \mathbb{G}_2, \hat{e}(\cdot,\cdot), q, P, P_{pub}, H(\cdot), H_0(\cdot)\}.$$

`KeyGen`: The signer with identity $ID \in \{0,1\}^*$ submits ID to TA. TA sets the signer's public key Q_{ID} to be $H(ID) \in \mathbb{G}_1$, computes the signer's private signing key S_{ID} by $S_{ID} = xQ_{ID}$. Then TA sends the private signing key to the signer via a secure channel, or using the secure and anonymous protocol proposed in [9].

`Sign`: Let $L = \{ID_1, ID_2, \cdots, ID_n\}$ be the set of all identities of n users. The actual signer, indexed by s (i.e. his/her public key is $Q_{ID_s} = H(ID_s)$), carries out the following steps to give an ID-based ring signature on behalf of the group L.

1. Choose $r_i \in_R \mathbb{Z}_q^*$, compute $U_i = r_i Q_{ID_i}$ and $h_i = H_0(m||L||U_i)$ $\forall i \in \{1,2,\cdots,n\}\backslash\{s\}$.
2. Choose $r'_s \in_R \mathbb{Z}_q^*$, compute $U_s = r'_s Q_{ID_s} - \sum_{i \neq s}\{(r_i + h_i)Q_{ID_i}\}$.
3. Compute $h_s = H_0(m||L||U_s)$ and $V = (h_s + r'_s)S_{ID_s}$.
4. Output the signature for m and L as $\sigma = \{\cup_{i=1}^n \{U_i\}, V\}$.

`Verify`: A verifier can check the validity of a signature $\sigma = \{\cup_{i=1}^n \{U_i\}, V\}$ for the message m and a set of identities L as follows.

1. Compute $h_i = H_0(m||L||U_i)$ $\forall i \in \{1,2,\cdots,n\}$.
2. Checking whether $\hat{e}(P_{pub}, \sum_{i=1}^n (U_i + h_i Q_{ID_i})) = \hat{e}(P, V)$.
3. Accept the signature if it is true, reject otherwise.

5.2 Consistency

The consistency of our scheme can be easily verified by the following equations.

$$\begin{aligned}
\hat{e}(P_{pub}, \sum_{i=1}^{n} (U_i + h_i Q_i)) &= \hat{e}(P_{pub}, U_s + h_s Q_{ID_s} + \sum_{i \neq s} (U_i + h_i Q_{ID_i})) \\
&= \hat{e}(P_{pub}, h_s Q_{ID_s} + r'_s Q_{ID_s} - \sum_{i \neq s} \{(r_i + h_i) Q_{ID_i}\} + \sum_{i \neq s} (U_i + h_i Q_{ID_i})) \\
&= \hat{e}(P_{pub}, h_s Q_{ID_s} + r'_s Q_{ID_s} - \sum_{i \neq s} (U_i + h_i Q_{ID_i}) + \sum_{i \neq s} (U_i + h_i Q_{ID_i})) \\
&= \hat{e}(P_{pub}, h_s Q_{ID_s} + r'_s Q_{ID_s}) \\
&= \hat{e}(xP, (h_s + r'_s) Q_{ID_s}) \\
&= \hat{e}(P, (h_s + r'_s) x Q_{ID_s}) \\
&= \hat{e}(P, (h_s + r'_s) S_{ID_s})
\end{aligned}$$

5.3 Efficiency

We consider the costly operations which include point addition on $\mathbb{G}_1$ ($\mathbb{G}_1$ Add), point scalar multiplication on $\mathbb{G}_1$ ($\mathbb{G}_1$ Mul), multiplication in $\mathbb{G}_2$ or $\mathbb{Z}_q$ ($\mathbb{G}_2/\mathbb{Z}_q$ Mul), hashing into the group (Hash) and pairing operation (Pairing). We use the `MapToPoint` hash operation in BLS short signature scheme [3]. Before our proposal, the scheme that requires the least number of pairing operations is [6] (named S-IDTRS). Table 1 shows a summary of the efficiency of our proposed scheme (named S-IDRS). Taken into account the total cost of signature generation and verification, we can see that our proposed scheme is the only scheme using a constant number of pairing operations, and with the least total amount of other operations. Moreover, our scheme supports parallel operations for the computation about non-participating signers' parts like [6] and [10], which is not possible in schemes like [1, 12, 18].

Schemes	Efficiency					
	G_1 Add	G_1 Mul	G_2/Z_q Mul	Hash	Pairing	Parallelism
Zhang-Kim [18]	1	2n	2n-1	2n	4n-1	×
Lin-Wu [12]	2n-1	2n	3n	0	2n+1	×
Herranz-Sáez [10]	3n-1	2n	n	0	n+3	✓
Awasthi-Lai [1]	2n-1	2n+1	2n-1	0	4n-1	×
S-IDTRS [6]	2n	4n	n-1	0	n+1	✓
Proposed S-IDRS	3n-2	3n	0	0	2	✓

Table 1. Efficiency of ID-based Ring Signature from Bilinear Pairings

Considering the signature size, we share the same order of space complexities as all other schemes we considered [1, 6, 10, 12, 18], we are not sacrificing the signature size for lowering time complexity.

5.4 Existential Unforgeability and Signer Ambiguity

The security of our proposed scheme is summarized in the following two theorems.

Theorem 2 *In the random oracle model (the hash functions are modeled as random oracles), if there is an algorithm $\mathcal{A}$ that can win the EUF-IDRS-CMIA2 game with non-negligible probability by making a valid ring signature with group size n', in polynomial time with probability $\epsilon_{\mathcal{A}}$, asking at most q_S sign queries, q_H H_1 queries (including those implicitly asked by q_S queries), q_E key generation queries and q_I identity hashing queries, then CDHP can be solved with non-negligible probability in polynomial time.*

Proof. Suppose the challenger $\mathcal{C}$ receives a random instance (P, aP, bP) of the CDHP and has to compute the value of abP. $\mathcal{C}$ will run $\mathcal{A}$ as a subroutine and act as $\mathcal{A}$'s challenger in the EUF-IDRS-CMIA2 game. During the game, $\mathcal{A}$ will consult $\mathcal{C}$ for answers to the random oracles H and H_0. Roughly speaking, these answers are randomly generated, but to maintain the consistency and to avoid collision, $\mathcal{C}$ keeps three lists to store the answers used. We assume $\mathcal{A}$ will ask for $H(ID)$ before ID is used in any other queries.

$\mathcal{C}$ gives $\mathcal{A}$ the system parameters with $P_{pub} = bP$. Note that b is unknown to $\mathcal{C}$. This value simulates the master key value for the TA in the game.

H requests: We embed part of the challenge aP in the answer of many H queries. When $\mathcal{A}$ asks queries on the hash value of identity ID, $\mathcal{C}$ picks $y_i \in_R \mathbb{Z}_q^*$ and repeats the process until y_i is not in the list L_1. $\mathcal{C}$ then flips a coin $W \in \{0,1\}$ that yields 0 with probability ζ and 1 with probability $1-\zeta$. (ζ will be determined later.) If $W = 0$ then the hash value $H(ID)$ is defined as y_iP; else if $W = 1$ then returns $H(ID) = y_i(aP)$. In either case, $\mathcal{C}$ stores (ID, y_i, W) in the list L.

Note that when $W = 0$, the associated private key is $y_i(bP)$ which $\mathcal{C}$ knows how to compute. But when $W = 1$, since both a and b are unknown to $\mathcal{C}$, a `KeyGen` request on this identity will make $\mathcal{C}$ fails.

H_0 requests: When $\mathcal{A}$ asks queries on these hash values, $\mathcal{C}$ checks the corresponding list L_2. If an entry for the query is found, the same answer will be given to $\mathcal{A}$; otherwise, a randomly generated value will be used as an answer to $\mathcal{A}$, the query and the answer will then be stored in the list.

`Sign` requests: $\mathcal{A}$ chooses a group of n users' identities $L = \{ID_i\}$ where $1 \le i \le n$, and any message m. On input of (L, m), $\mathcal{C}$ outputs an ID-based ring signature σ as follows.

1. Choose an index $s \in_R \{1, 2, \cdots, n\}$.
2. Choose $r_i \in_R \mathbb{Z}_q^*$, compute $U_i = r_i Q_{ID_i}$ and $h_i = H_0(m||L||U_i)$ $\forall i \in \{1, 2, \cdots, n\} \backslash \{s\}$.
3. Choose $h'_s \in_R \mathbb{Z}_q^*$ and $z \in_R \mathbb{Z}_q^*$, compute $U_s = zP - h'_s Q_{ID_s} - \sum_{i \ne s} \{(r_i + h_i) Q_{ID_i}\}$.
4. Store the relationship $h_s = H_0(m||L||U_s)$ to the list L_2 and compute $V = z(bP)$, repeat Step 3 in case collision occurs.
5. Output the signature for m and L as $\sigma = \{\cup_{i=1}^n \{U_i\}, V\}$.

Finally, $\mathcal{A}$ outputs a forged signature $\sigma = \{\cup_{i=1}^n \{U_i\}, V\}$ that is signed by a certain member in the group $\{ID_i\}$ where $Q_{ID_i} = H(ID_i) = y_i(aP) \forall i \in \{1, 2, \cdots, n\}$, i.e. $\mathcal{A}$ has not requested for any one of the private keys of members in the group.

Now we determine the value of ζ. The probability that $\mathcal{C}$ does not fail in all the q_E private key extraction queries is ζ^{q_E}, and the probability that $\mathcal{A}$ forged a signature that $\mathcal{C}$ does not know all the corresponding private keys involved in the signature is $(1-\zeta)^{n'}$. So the combined probability is $\zeta^{q_E}(1-\zeta)^{n'}$. By simple differentiation, we find the value of ζ that maximize this probability is $\frac{q_E}{q_E+n'}$ and the maximized probability is $(1 - \frac{n'}{q_E+n'})^{q_E+n'}(\frac{n'}{q_E})^{n'}$.

The probability for $\mathcal{C}$ not to fail in all the q_S sign queries is $(1 - q_H \frac{2}{2^k})^{q_S}$, which is greater than $(1 - \frac{q_S q_H}{2^{k-1}})$. For very large q_E, the probability for $\mathcal{C}$ to success is $\epsilon_{\mathcal{C}} = \epsilon_{\mathcal{A}} (\frac{n'}{eQ_E})^{n'} (1 - \frac{q_S q_H}{2^{k-1}})$.

It follows from the forking lemma for generic ring signature schemes [10] that if $\epsilon_{\mathcal{C}} \ge 7C_{n'}^{Q_H}/2^k$, and $\mathcal{A}$ can give a valid forged signature within time $T_{\mathcal{A}}$ in the above interaction, then we can construct a Las Vegas machine $\mathcal{A}'$ that outputs two signed messages $\sigma = \{\cup_{i=1}^n \{U_i\}, V\}$ and $\sigma' = \{\cup_{i=1}^n \{U_i\}, V'\}$ within time $2T_{\mathcal{A}}$ and with at least $\epsilon_{\mathcal{C}}{}^2/66C_{n'}^{q_H}$ probability. Suppose $h_i = H_0(m||L||U_i)$ and $h'_i = H_0(m||L||U_i)$ for all $i \in \{1, 2, \cdots, n\}$, we have $h_i = h'_i$ for all $i \in \{1, 2, \cdots, n\} \backslash \{s\}$. Given the machine $\mathcal{A}'$ derived from $\mathcal{A}$, we can solve the CDHP by computing $abP = {y_s}^{-1}(h_s - h'_s)^{-1}(V - V')$, where y_s can be found by looking for ID_s in the list L.

□

Theorem 3 *Our ID-based ring signature scheme satisfies the unconditional signer ambiguity property.*

Proof. Since $\cup_{i \neq s}\{r_i\}$ and also r'_s are randomly generated, hence $\cup_{i=1}^{n}\{U_i\}$ are also uniformly distributed.

It remains to consider whether $V = (h_s + r'_s)S_{ID_s}$ leaks information about the actual signer. Since h_s is publicly computable, we focus on the value of $V - h_s S_{ID_s} = r'_s S_{ID_s}$. Obviously, $r'_s S_{ID_s}$ is related to U_s. Any one can compute the value of $r'_s Q_{ID_s}$ by $U_s + \sum_{i \neq s}(U_i + h_i Q_{ID_i})$. Together with the fact that the bilinearity can relate $r'_s S_{ID_s}$ and $r'_s Q_{ID_s}$ by checking whether $\hat{e}(r'_s Q_{ID_s}, P) = \hat{e}(r'_s S_{ID_s}, P_{pub})$, one may be tempted to see if ID_j is the actual signer by checking whether the following equality holds.

$$\hat{e}(U_j + \sum_{i \neq j}(U_i + h_i Q_{ID_i}), P_{pub}) = \hat{e}(V, P)/\hat{e}(h_j Q_{ID_j}, P_{pub})$$

However, we claim that this method is of no use, as the above equality not only holds when $j = s$, but also $\forall j \in \{1, 2, \cdots, n\}\backslash\{s\}$. i.e. the signature is symmetric.

$$\begin{aligned}
\hat{e}(U_j + \sum_{i \neq j}(U_i + h_i Q_{ID_i}), P_{pub}) &= \hat{e}(\sum U_i + \sum_{i \neq j} h_i Q_{ID_i}, P_{pub}) \\
&= \hat{e}(\sum_{i \neq s} U_i + U_s + \sum_{i \neq j} h_i Q_{ID_i}, P_{pub}) \\
&= \hat{e}(\sum_{i \neq s} U_i + r'_s Q_{ID_s} - \sum_{i \neq s}\{(r_i + h_i)Q_{ID_i}\} + \sum_{i \neq j} h_i Q_{ID_i}, P_{pub}) \\
&= \hat{e}(\sum_{i \neq s} U_i + r'_s Q_{ID_s} - \sum_{i \neq s}(U_i + h_i Q_{ID_i}) + \sum_{i \neq j} h_i Q_{ID_i}, P_{pub}) \\
&= \hat{e}(r'_s Q_{ID_s} - \sum_{i \neq s} h_i Q_{ID_i} + \sum_{i \neq j} h_i Q_{ID_i}, P_{pub}) \\
&= \hat{e}(r'_s Q_{ID_s} + h_s Q_{ID_s} - h_j Q_{ID_j}, P_{pub}) \\
&= \hat{e}(r'_s Q_{ID_s} + h_s Q_{ID_s} - h_j Q_{ID_j}, xP) \\
&= \hat{e}(r'_s S_{ID_s} + h_s S_{ID_s} - h_j S_{ID_j}, P) \\
&= \hat{e}(V - h_j S_{ID_j}, P) \\
&= \hat{e}(V, P)/\hat{e}(h_j S_{ID_j}, P) \\
&= \hat{e}(V, P)/\hat{e}(h_j Q_{ID_j}, xP) \\
&= \hat{e}(V, P)/\hat{e}(h_j Q_{ID_j}, P_{pub})
\end{aligned}$$

Indeed, the above equality is just the same as the equality to be checked in the verification algorithm.

To conclude, for any fixed message m and fixed set of identities L, the distribution of $\{\cup_{i=1}^{n}\{U_i\}, V\}$ are independent and uniformly distributed no matter who is the actual signer. So we conclude that even an adversary with all the private keys corresponding to the set of identities L and unbounded computing resources has no advantage in identifying any one of the participating signers over random guessing. □

6 Extension

In this section, we explain how to extend our basic scheme into one supporting an ad-hoc access structure consisting of groups of different sizes. We employ the idea from [10], where the access structure $\mathcal{U}$ is defined as $\{\mathcal{U}_1, \mathcal{U}_2, \cdots \mathcal{U}_d\}$ (where $\mathcal{U}_i$ denotes a set of signers) and all the members of a particular set in $\mathcal{U}$ (says $\mathcal{U}_s$, where $1 \leq s \leq d$) participate in the signing. The signature can convince any one that all the members of a certain group in $\mathcal{U}$ have cooperated to give the signature, but does not know which group is signing.

6.1 Construction

The `Setup` and `Keygen` algorithm are the same as the basic scheme, except the security parameter in `Setup` should be chosen with the maximum number of subsets supported (n) in mind. Below are the descriptions of `Sign` and `Verify` algorithm.

`Sign`: Let $\mathcal{U}_s = \{ID_1, ID_2, \cdots, ID_{n_s}\}$ be the set of all identities of n_s users. They choose an access structure $\mathcal{U}$ is defined as $\{\mathcal{U}_1, \mathcal{U}_2, \cdots \mathcal{U}_d\}$ where $\mathcal{U}_s \in \mathcal{U}$. The ID-based ring signature for the access structure $\mathcal{U}$ can be generated as follows.

1. Compute $Y_i = \sum_{ID_j \in \mathcal{U}_i} (Q_{ID_j})$, $\forall i \in \{1, 2, \cdots, d\}$.
2. Choose $r_i \in_R \mathbb{Z}_q^*$, compute $U_i = r_i Y_i$ and $h_i = H_0(m||\mathcal{U}||U_i)$ $\forall i \in \{1, 2, \cdots, d\} \backslash \{s\}$.
3. Each signer $ID_{s_k} \in \mathcal{U}_s$ chooses ${r'}_{s_k} \in_R \mathbb{Z}_q^*$ and computes $U_{s_k} = r'_{s_k} Q_{ID_{s_k}}$, $\forall k \in \{1, 2, \cdots, n_s\}$.
4. Any particular signer who got the knowledge of $\cup_{s_k=1}^{n_s} \{U_{s_k}\}$ computes $U_s = \sum_{s_k=1}^{n_s} (U_{s_k}) - \sum_{i \neq s} \{(r_i + h_i) Y_i\}$ and $h_s = H_0(m||\mathcal{U}||U_s)$.
5. Each signer $ID_{s_k} \in \mathcal{U}_s$ computes $V_{s_k} = (h_s + {r'}_{s_k}) S_{ID_{s_k}}$.
6. Output the signature for m and $\mathcal{U}$ as $\sigma = \{\cup_{i=1}^{d} \{U_i\}, V = \sum_{ID_{s_k} \in \mathcal{U}_s} (V_{s_k})\}$.

`Verify`: A verifier can check the validity of a signature $\sigma = \{\cup_{i=1}^{d} \{U_i\}, V\}$ for the message m and the access structure $\mathcal{U}$ as follows.

1. Compute $h_i = H_0(m||\mathcal{U}||U_i)$ $\forall i \in \{1, 2, \cdots, d\}$.
2. Checking whether $\hat{e}\{P_{pub}, \sum_{i=1}^{d} [U_i + h_i \sum_{ID_j \in \mathcal{U}_i} (Q_{ID_j})]\} = \hat{e}(P, V)$.
3. Accept the signature if it is true, reject otherwise.

6.2 Security

The scheme's consistency and signer ambiguity can be shown in a similar manner as the cases in our basic scheme. The proof of existential unforgeability is basically the same as that of our basic scheme, due to page limit we only highlight the differences here.

The first difference is concerned with the requirement on the forger's signature. For our basic scheme, the forger should not know all the private key associated with the signature, and this happens with probability $(1-\zeta)^{n'}$, where n' represents the total number of members associated with the forged signature. For our extended scheme, the forger must not know at least one private key for all group of signers, and the corresponding probability is $(1 - \zeta^{{n_1}'})(1 - \zeta^{{n_2}'}) \cdots (1 - \zeta^{{n_d}'})$ where ${n_i}'$ is the group size of the i-th group of users. Suppose $N' = \sum_{i=1}^{d} {n_i}'$, this probability is greater than $(1 - \zeta)^{{n_1}'}(1 - \zeta)^{{n_2}'} \cdots (1 - \zeta)^{{n_d}'} = (1 - \zeta)^{N'}$. Hence the n' parameter in the proof can be replaced by N', which represents the total number of members in all d groups associated with the forged signature.

The second difference is about the solving of computational Diffie-Hellman problem. For our basic scheme, abP is computed by ${y_s}^{-1}(h_s - h'_s)^{-1}(V - V')$. For our extended scheme, $(h_s - h'_s)^{-1}(V - V')$ only gives the "private key" corresponding to $Y_s = \sum_{ID_j \in \mathcal{U}_s} (Q_{ID_j})$. To obtain abP, we should subtract other known private keys of this s-th group from this value. Suppose the unknown private key is indexed by s_k, we can compute abP by ${y_{s_k}}^{-1}\{(h_s - h'_s)^{-1}(V - V') - \sum_{ID_j \in \mathcal{U}_s \backslash \{ID_{s_k}\}} [(y_j)(bP)]\}$, where y_js can be found by looking up the list L.

7 Conclusion

For ring signature scheme to be practical, we need to eliminate the need of validity checking of the certificates and the need of registering for a certificate before getting the public key. ID-based solutions can provide these two features. Nonetheless, existing proposals of ID-based ring signature are computationally inefficient, since the number of pairing computations grows linearly with the group size. This paper closes the open problem of devising an ID-based ring signature using sublinear numbers of pairing computation. We construct an efficient ID-based ring signature which only needs two pairing computations for any group size. The proposed scheme is proven to be existential unforgeable against adaptive chosen message-and-identity attack under the random oracle model, using the forking lemma for generic ring signature schemes. Extension to support general access structure is also discussed. Future research directions include making a constant-size ID-based ring signature scheme or making the ring signature scheme works in a hierarchical setting [7, 8].

References

1. Amit K Awasthi and Sunder Lal. ID-based Ring Signature and Proxy Ring Signature Schemes from Bilinear Pairings. Cryptology ePrint Archive, Report 2004/184, 2004. Available at http://eprint.iacr.org.
2. Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In Eli Biham, editor, *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, volume 2656 of *Lecture Notes in Computer Science*, pages 416–432. Springer, 2003.
3. Dan Boneh, Ben Lynn, and Hovav Shacham. Short Signatures from the Weil Pairing. In Colin Boyd, editor, *Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings*, volume 2248 of *Lecture Notes in Computer Science*, pages 514–532. Springer, 2001.
4. Sherman S.M. Chow. Generic Multi-Designated Verifiers Signature Schemes. Manuscript.
5. Sherman S.M. Chow. Verifiable Pairing and Its Applications. In Chae Hoon Lim and Moti Yung, editors, *Information Security Applications, 5th International Workshop, WISA 2004, Revised Papers*, volume 3325 of *Lecture Notes in Computer Science*, pages 173–187, Jeju Island, Korea, August 2004. Springer-Verlag. To Appear.
6. Sherman S.M. Chow, Lucas C.K. Hui, and S.M. Yiu. Identity Based Threshold Ring Signature. In *Information Security and Cryptology - ICISC 2004, 7th International Conference Seoul, Korea, December 2-3, 2004, Revised Papers*, Lecture Notes in Computer Science, Seoul, Korea, December 2004. Springer-Verlag. Also available at Cryptology ePrint Archive, Report 2004/179.
7. Sherman S.M. Chow, Lucas C.K. Hui, S.M. Yiu, and K.P. Chow. Secure Hierarchical Identity Based Signature and its Application. In Javier Lopez, Sihan Qing, and Eiji Okamoto, editors, *Information and Communications Security, 6th International Conference, ICICS 2004, Malaga, Spain, October 27-29, 2004, Proceedings*, volume 3269 of *Lecture Notes in Computer Science*, pages 480–494, Malaga, Spain, October 2004. Springer-Verlag.
8. Sherman S.M. Chow, Tsz Hon Yuen, Lucas C.K. Hui, and S.M. Yiu. Signcryption in Hierarchical Identity Based Cryptosystem. In *Security and Privacy in the Age of Ubiquitous Computing, IFIP TC11 20^{th} International Conference on Information Security (SEC 2005), May 30 - June 1, 2005, Chiba, Japan*, IFIP Conference Proceedings. Kluwer, 2005. Also available at Cryptology ePrint Archive, Report 2004/244.
9. Ai fen Sui, Sherman S.M. Chow, Lucas C.K. Hui, S.M. Yiu, K.P. Chow, W.W. Tsang, C.F. Chong, K.H. Pun, and H.W. Chan. Separable and Anonymous Identity-Based Key Issuing without Secure Channel. Cryptology ePrint Archive, Report 2004/322, November 2004. Available at http://eprint.iacr.org.
10. Javier Herranz and Germán Sáez. New Identity-Based Ring Signature Schemes. In Javier Lopez, Sihan Qing, and Eiji Okamoto, editors, *Information and Communications Security, 6th International Conference, ICICS 2004, Malaga, Spain, October 27-29, 2004, Proceedings*, volume 3269 of *Lecture Notes in Computer Science*, pages 27–39, Malaga, Spain, October 2004. Springer-Verlag. Preliminary version available at Cryptology ePrint Archive, Report 2003/261.

11. Fabien Laguillaumie and Damien Vergnaud. Multi-designated Verifiers Signatures. In Javier Lopez, Sihan Qing, and Eiji Okamoto, editors, *Information and Communications Security, 6th International Conference, ICICS 2004, Malaga, Spain, October 27-29, 2004, Proceedings*, volume 3269 of *Lecture Notes in Computer Science*, pages 495–507, Malaga, Spain, October 2004. Springer-Verlag.
12. Chih-Yin Lin and Tzong-Chen Wu. An Identity-based Ring Signature Scheme from Bilinear Pairings. Cryptology ePrint Archive, Report 2003/117, 2003. Available at http://eprint.iacr.org.
13. Joseph K. Liu and Duncan S. Wong. On the Security Models of (Threshold) Ring Signature Schemes. In *Information Security and Cryptology - ICISC 2004, 7th International Conference Seoul, Korea, December 2-3, 2004, Revised Papers*, Lecture Notes in Computer Science, Seoul, Korea, December 2004. Springer-Verlag.
14. Willy Susilo and Yi Mu. Non-Interactive Deniable Ring Authentication. In Jong In Lim and Dong Hoon Lee, editors, *Information Security and Cryptology - ICISC 2003, 6th International Conference Seoul, Korea, November 27-28, 2003, Revised Papers*, volume 2971 of *Lecture Notes in Computer Science*, pages 386–401, Seoul, Korea, 2004. Springer-Verlag.
15. Willy Susilo, Yi Mu, and Fangguo Zhang. Perfect Concurrent Signature Schemes. In Javier Lopez, Sihan Qing, and Eiji Okamoto, editors, *Information and Communications Security, 6th International Conference, ICICS 2004, Malaga, Spain, October 27-29, 2004, Proceedings*, volume 3269 of *Lecture Notes in Computer Science*, pages 14–26, Malaga, Spain, October 2004. Springer-Verlag.
16. Victor K. Wei. A Bilinear Spontaneous Anonymous Threshold Signature for Ad Hoc Groups. Cryptology ePrint Archive, Report 2004/039, 2004. Available at http://eprint.iacr.org.
17. Jing Xu, Zhenfeng Zhang, and Dengguo Feng. A Ring Signature Scheme Using Bilinear Pairings. In Chae Hoon Lim and Moti Yung, editors, *Information Security Applications, 5th International Workshop, WISA 2004, Revised Papers*, volume 3325 of *Lecture Notes in Computer Science*, pages 163–172, Jeju Island, Korea, August 2004. Springer-Verlag. To Appear.
18. Fangguo Zhang and Kwangjo Kim. ID-Based Blind Signature and Ring Signature from Pairings. In Yuliang Zheng, editor, *Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings*, volume 2501 of *Lecture Notes in Computer Science*, pages 533–547. Springer, 2002.
19. Fangguo Zhang, Rei Safavi-Naini, and Willy Susilo. An Efficient Signature Scheme from Bilinear Pairings and Its Application. In Feng Bao, Robert H. Deng, and Jianying Zhou, editors, *Public Key Cryptography - PKC 2004, 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004*, volume 2947 of *Lecture Notes in Computer Science*, pages 277–290. Springer, 2004.
20. Fangguo Zhang, Reihaneh Safavi-Naini, and Chih-Yin Lin. New Proxy Signature, Proxy Blind Signature and Proxy Ring Signature Schemes from Bilinear Pairings. Cryptology ePrint Archive, Report 2003/104, 2003. Available at http://eprint.iacr.org.