# Linkable Ring Signature with Unconditional Anonymity

Joseph K. Liu, Man Ho Au, *Member, IEEE*, Willy Susilo, *Senior Member, IEEE*, Jianying Zhou

***Abstract*—In this paper, we construct a linkable ring signature scheme with unconditional anonymity. It has been regarded as an open problem in [22] since 2004 for the construction of an unconditional anonymous linkable ring signature scheme. We are the first to solve this open problem by giving a concrete instantiation, which is proven secure in the random oracle model. Our construction is even more efficient than other schemes that can only provide computational anonymity. Simultaneously, our scheme can act as an counterexample to show that Theorem 1 stated in [19] is not always true, which stated that linkable ring signature scheme cannot provide strong anonymity. Yet we prove that our scheme can achieve strong anonymity (under one of the interpretations).**

*Index Terms:* ring signature, linkable, anonymity

## I. Introduction

RING SIGNATURE. The seminal construction of ring signature scheme was proposed in [27]. Subsquently, there exist many constructions and variants of ring signature schemes that have been proposed in the literature (such as [27], [1], [37], [7], [34], [15], [14]). A ring signature allows members of a group to sign messages on behalf of the group without any necessity to reveal their identities, *i.e.*, providing signer anonymity. Additionally, it is impossible to decide whether two signatures have been issued by the same group member. In contrast to the notion of a group signature scheme (such as [9], [8], [4]), the group formation in a ring signature is spontaneous and there exists *no* group manager who is responsible for revoking the signer's identity. That is, under the assumption that each user is already associated with a public key of any standard signature scheme, a user can form a group by simply collecting the public keys of all the group members including his own. These diversion group members can be totally unaware of being conscripted into the group.

A "regular" ring signature is unlinkable. That is, no one can determine whether two ring signatures are generated by the same signer.

LINKABLE RING SIGNATURE. In 2004 [22], Liu *et al.* proposed a variant of ring signature schemes, coined as linkable ring signatures. In this notion, the identity of the signer in a ring signature remains anonymous, but two ring signatures can be linked if they are signed by the same signer. Linkable ring signatures are suitable in many different practical applications, including the following:

- Cloud Data Storage Security: Cloud computing allows data owners to remotely store their data in the cloud [32], [39], [25], [20] in order to enjoy on-demand high-quality applications and services from a shared pool of configurable computing resources. While security is one of the main concerns in the cloud data storage system, access control methodology plays an important role within the security infrastructure of the cloud computing paradigm. Ring signature provides a dynamic anonymous access control mechanism for cloud computing. The spontaneity property of ring signature makes it especially useful in the case where the access policy changes frequently. Linkable ring signature further provides enhanced security control. For example, one may limit a user to access the cloud data for a maximum number of times within a period. Normal ring signature is unable to achieve this goal since every single access is unlinkable. Instead, linkable ring signature allows the verifier to link a user for every time he accesses the system. Thus, it is possible to count the number of times a user has accessed, while preserving his anonymity.
- Ad-hoc Network Authentication: In an ad-hoc network, there is no central authority or trusted party. The formation of a group is spontaneous. Ring signature is an excellent candidate to serve as an anonymous authentication tool in an ad-hoc network environment [22]. However, sometimes a verifier may want to know whether a message is sent by the same node or not. Linkable ring signature can support this feature as required by some scenarios.
- E-voting: E-voting (e.g. [2], [11], [16]) is the digital analogy of paper voting. While there are many different approaches for e-voting, linkable ring signature is a new and efficient primitive [13] to provide robust and receipt-free e-voting system. The public verifiability, linkability and anonymous properties are the key elements to let linkable ring signature become a new advance in the research of e-voting.

### A. Computational Anonymity vs Unconditional Anonymity

The anonymity provided by ring signature schemes can be classified into two types: computational and unconditional. Computational means that the anonymity is protected under the assumption of some mathematical hard problems (e.g. discrete logarithm, RSA, factorization, computational Diffie-Hellman). If there exists an adversary who can solve the un-

Joseph K. Liu and Jianying Zhou are with Institute for Infocomm Research, Singapore; Man Ho Au and Willy Susilo are with University of Wollongong, Australia.

Willy Susilo is supported by the ARC Future Fellowship (FT0991397).

derlying hard problem *efficiently*[1], we say that the anonymity is broken. On the other hand, unconditional means that the anonymity is protected even against an unbounded adversary (with unbounded computation power and time).

Most of the traditional ring signature schemes provide unconditional anonymity [27], [1], [37], [7], [34], [21], [15], [14], [12] although some recent schemes provide only computational anonymity [28], [24], [35].

For the construction of linkable ring signatures, to the best of our knowledge, all existing schemes (e.g. [22],[30], [23],[3],[38], [29], [31], [17],[36]) only provide computational anonymity. It is also stated in [22] that to construct a linkable ring signature with unconditional anonymity is an open problem.

### B. Remarks on the Anonymity Issue raised in [19]

Jeong *et al.* [19] proposed a ring signature with *weak* linkability. In their scheme, the actual signer can *optionally* choose to be linked, or not to be linked. It is different from other traditional linkable ring signatures where the requirement to have the signer to be linked is *mandatory*. The authors also define two levels of anonymity, as quoted below:

1) Strong Anonymity:

   *Any party cannot know the actual signer of a ring signature, even if all of the private keys of the parties of the ring are known.*

2) Weak Anonymity:

   *Any party cannot know the actual signer of a ring signature, only if all of the parties of the ring do not reveal their identity.*

The authors claimed that *no* linkable ring signature (with mandatory linkability, which is also known as *Strong Linkability* in [19]), can provide strong anonymity. They proved this claim as **Theorem 1** in their paper. However, they do not provide any rigorous definition for these two levels of anonymity although they claimed that strong anonymity (as their definition) is one of the security requirements of ring signatures defined in [10], [27].

When we look into the detailed definition of anonymity given in [10], [27] and other schemes [1], [37], [7], [34], [15], [14], we find out that the definition defined in [19] is slightly different from others. For all other schemes except [19], the strongest level of anonymity is defined as

> *The probability of any unbounded adversary to know the actual signer of a ring signature is no better than random guessing.*

That is, assume there are $n$ users in the ring signature. The probability of any unbounded adversary (with unlimited computation power and time) to guess the actual signer correctly is exactly equal to $1/n$. This is also known as *Unconditional Anonymity*.

Due to the differences between these definitions and the lack of rigorous security model of anonymity, we have found out some subtleties for the **Theorem 1** in [19]. Before giving the details of these subtleties, we first try to interpret *Strong Anonymity* given by [19] in two different ways:

**Definition 1.** *Given the public keys (or identities in the case of ID-based scheme) of all parties of a ring signature, any party cannot know the actual signer even if all of the private keys* ***owned by the parties of the ring*** *are known.*

**Definition 2.** *Given the public keys (or identities in the case of ID-based scheme) of all parties of a ring signature, any party cannot know the actual signer even if all of the private keys* ***corresponding to the parties of the ring*** *are known.*

These two definitions are the same if the correspondence between private key and public key (or identity) is one-to-one. That is, given any public key (or identity), there is only one private key that corresponds to the public key (or identity). Nevertheless, there are some cases where one public key (or identity) may correspond to more than one private keys. The most common example is ID-based cryptosystem. For instance, in Boneh-Boyen-type [5], [6] or Waters-type [33] ID-based cryptosystem, any user (with one unique identity) can re-randomize his private key. In Gentry-type [18], although user cannot re-randomize his private key, the private key generator (PKG) can generate more than one private key corresponding to one identity. In this case, the private key *corresponding* to a party may not be the same as the one *owned* by that party. For example, the PKG can generate another different private key for an identity, which is different from the one actually given to this party. If a ring signature scheme is based on any of those cryptosystems, there is a difference between definition 1 and definition 2.

### C. Our Contribution

In this paper, we first give two interpretations of Strong Anonymity defined in [19]. We find out that under one of the interpretations, Theorem 1 in [19] may not be true. We construct a linkable ring signature scheme to show that under this interpretation of strong anonymity, our scheme is still mandatory linkable (a.k.a strong linkable in [19]) which contradicts to Theorem 1 in [19]. Our scheme also solves the open problem stated in [22]. That is, our scheme provides unconditional anonymity and mandatory linkability simultaneously. All previous mandatory linkable ring signature schemes can only provide computational anonymity.

## II. Security Model

We give our security model and define relevant security notions in this section.

### A. Syntax of Linkable Ring Signature

A *linkable ring signature*, (LRS) scheme, is a tuple of five algorithms (Setup, KeyGen, Sign, Verify and Link).

- $\mathsf{param} \leftarrow \mathsf{Setup}(\lambda)$ is a probabilistic polynomial time (PPT) algorithm which, on input a security parameter $\lambda$, outputs the set of security parameters param which includes $\lambda$. We denote by $\mathcal{EID}$, $\mathcal{M}$ and $\Sigma$ the domains of event-id, messages and signatures, respectively.

[1]Usually we say that an algorithm is *efficient* if it can be run in polynomial time.

- $(sk_i, pk_i) \leftarrow \mathsf{KeyGen}(\mathsf{param})$ is a PPT algorithm which, on input a security parameter $\lambda \in \mathbb{N}$, outputs a private/public key pair $(sk_i, pk_i)$. We denote by $\mathcal{SK}$ and $\mathcal{PK}$ the domains of possible private keys and public keys, respectively.
- $\sigma \leftarrow \mathsf{Sign}(e, n, \mathcal{Y}, sk, M)$ which, on input event-id $e$, group size $n$, a set $\mathcal{Y}$ of $n$ public keys in $\mathcal{PK}$, a private key whose corresponding public key is contained in $\mathcal{Y}$, and a message $M$, produces a signature $\sigma$.
- $\mathsf{accept/reject} \leftarrow \mathsf{Verify}(e, n, \mathcal{Y}, M, \sigma)$ which, on input event-id $e$, group size $n$, a set $\mathcal{Y}$ of $n$ public keys in $\mathcal{PK}$, a message-signature pair ($M$,$\sigma$) returns accept or reject. If accept, the message-signature pair is *valid*.
- $\mathsf{linked/unlinked} \leftarrow \mathsf{Link}\ (e, n_1, n_2, \mathcal{Y}_1, \mathcal{Y}_2, M_1, M_2,, \sigma_1, \sigma_2)$ which, on input event-id $e$, group size $n_1, n_2$, two sets $\mathcal{Y}_1, \mathcal{Y}_2$ of $n_1, n_2$ public keys respectively, two valid signature and message pairs $(M_1, \sigma_1, M_2, \sigma_2)$, outputs linked or unlinked.

**Correctness.** LRS schemes must satisfy:

- (Verification Correctness.) Signatures signed according to specification are accepted during verification.
- (Linking Correctness.) If two signatures are signed for the same event according to specification, then they are linked if and only if the two signatures share a common signer.

### *B. Notions of Security of Linkable Ring Signature*

Security of LRS schemes has four aspects: unforgeability, anonymity, linkability and non-slanderability. Before giving their definition, we consider the following oracles which together model the ability of the adversaries in breaking the security of the schemes.

- $pk_i \leftarrow \mathcal{JO}(\perp)$. The *Joining Oracle*, on request, adds a new user to the system. It returns the public key $pk \in \mathcal{PK}$ of the new user.
- $sk_i \leftarrow \mathcal{CO}(pk_i)$. The *Corruption Oracle*, on input a public key $pk_i \in \mathcal{PK}$ that is a query output of $\mathcal{JO}$, returns the corresponding private key $sk_i \in \mathcal{SK}$.
- $\sigma' \leftarrow \mathcal{SO}(e, n, \mathcal{Y}, pk_\pi, M)$. The *Signing Oracle*, on input an event-id $e$, a group size $n$, a set $\mathcal{Y}$ of $n$ public keys, the public key of the signer $pk_\pi \in \mathcal{Y}$, and a message $M$, returns a valid signature $\sigma'$.

If the scheme is proven in random oracle model, a random oracle is simulated.

1) UNFORGEABILITY. Unforgeability for LRS schemes is defined in the following game between the Simulator $\mathcal{S}$ and the Adversary $\mathcal{A}$ in which $\mathcal{A}$ is given access to oracles $\mathcal{JO}$, $\mathcal{CO}$, $\mathcal{SO}$ and the random oracle:
   a) $\mathcal{S}$ generates and gives $\mathcal{A}$ the system parameters param.
   b) $\mathcal{A}$ may query the oracles according to any adaptive strategy.
   c) $\mathcal{A}$ gives $\mathcal{S}$ an event-id $e \in \mathcal{EID}$, a group size $n \in \mathbb{N}$, a set $\mathcal{Y}$ of $n$ public keys in $\mathcal{PK}$, a message $M \in \mathcal{M}$ and a signature $\sigma \in \Sigma$.

   $\mathcal{A}$ wins the game if:
   (1) $\mathsf{Verify}(e, n, \mathcal{Y}, M, \sigma)$=accept;
   (2) All of the public keys in $\mathcal{Y}$ are query outputs of $\mathcal{JO}$;
   (3) No public keys in $\mathcal{Y}$ have been input to $\mathcal{CO}$; and
   (4) $\sigma$ is not a query output of $\mathcal{SO}$.

   We denote by

$$\mathbf{Adv}_{\mathcal{A}}^{unf}(\lambda) = \Pr[\mathcal{A} \text{ wins the game }]$$

**Definition 3** (unforgeability)**.** *A LRS scheme is unforgeable if for all PPT adversary $\mathcal{A}$, $\mathbf{Adv}_{\mathcal{A}}^{unf}(\lambda)$ is negligible.*

2) UNCONDITIONAL ANONYMITY. It should not be possible for an adversary $\mathcal{A}$ to tell the public key 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.
   Specifically, unconditional anonymity for LRS schemes is defined in the following game between the Simulator $\mathcal{S}$ and the unbounded Adversary $\mathcal{A}$ in which $\mathcal{A}$ is given access to oracle $\mathcal{JO}$.
   a) $\mathcal{S}$ generates and gives $\mathcal{A}$ the system parameters param.
   b) $\mathcal{A}$ may query $\mathcal{JO}$ according to any adaptive strategy.
   c) $\mathcal{A}$ gives $\mathcal{S}$ an event-id $e \in \mathcal{EID}$, a group size $n \in \mathbb{N}$, a set $\mathcal{Y}$ of $n$ public keys in $\mathcal{PK}$ such that all of the public keys in $\mathcal{Y}$ are query outputs of $\mathcal{JO}$, a message $M \in \mathcal{M}$. Parse the set $\mathcal{Y}$ as $\{pk_1, \ldots, pk_n\}$. $\mathcal{S}$ randomly picks $\pi_R \in \{1, \ldots, n\}$ and computes $\sigma_\pi = \mathsf{Sign}(e, n, \mathcal{Y}, sk_\pi, M)$, where $sk_\pi$ is a corresponding private key of $pk_\pi$. $\sigma_\pi$ is given to $\mathcal{A}$.
   d) $\mathcal{A}$ outputs a guess $\pi' \in \{1, \ldots, n\}$.

   We denote by

$$\mathbf{Adv}_{\mathcal{A}}^{Anon}(\lambda) \quad = \quad |\Pr[\pi' = \pi] - \frac{1}{n}|$$

**Definition 4** (Unconditional Anonymity)**.** *A LRS scheme is unconditional anonymous if for any unbounded adversary $\mathcal{A}$, $\mathbf{Adv}_{\mathcal{A}}^{Anon}(\lambda)$ is zero.*

Note that only $\mathcal{JO}$ is given to $\mathcal{A}$. Since $\mathcal{A}$ has unbounded computation power, it can compute the corresponding private key when a public key is given. **Thus if a scheme satisfies this definition of unconditional anonymity, it also satisfies Definition 2, *i.e.,* the second interpretation of Strong Anonymity in [19].**

3) LINKABILITY.
   Linkability for LRS schemes is mandatory, that is, it should be infeasible for a signer to generate two signatures such that they are determined to be unlinked using LRS.Link. The following definition/game essentially captures a scenario that an adversary tries to generate two LRS signatures, using strictly fewer than 2 user private keys, so that these two signatures are determined to be unlinked using LRS.Link. If the LRS scheme is unforgeable (as defined above), then these signatures can only be generated if at least 2 user private keys

are known. If less than 2 user private keys are known, then there must be one common signer to both of the signatures. Therefore, this model can effectively capture the definition of linkability.

Linkability for LRS scheme is defined in the following game between the Simulator $\mathcal{S}$ and the Adversary $\mathcal{A}$ in which $\mathcal{A}$ is given access to oracles $\mathcal{JO}$, $\mathcal{CO}$, $\mathcal{SO}$ and the random oracle:

a) $\mathcal{S}$ generates and gives $\mathcal{A}$ the system parameters param.
b) $\mathcal{A}$ may query the oracles according to any adaptive strategy.
c) $\mathcal{A}$ gives $\mathcal{S}$ an event-id $e \in \mathcal{EID}$, group sizes $n_1, n_2 \in \mathbb{N}$ (w.l.o.g. we assume $n_1 \leq n_2$), sets $\mathcal{Y}_1$ and $\mathcal{Y}_2$ of public keys in $\mathcal{PK}$ of sizes $n_1$ and $n_2$ resp., messages $M_1, M_2 \in \mathcal{M}$ and signatures $\sigma_1, \sigma_2 \in \Sigma$.

$\mathcal{A}$ wins the game if

(1) All public keys in $\mathcal{Y}_1 \cup \mathcal{Y}_2$ are query outputs of $\mathcal{JO}$;
(2) Verify$(e, n_i, \mathcal{Y}_i, M_i, \sigma_i) =$ accept for $i = 1, 2$ such that $\sigma_i$ are not outputs of $\mathcal{SO}$;
(3) $\mathcal{CO}$ has been queried less than 2 times (that is, $\mathcal{A}$ can only have at most 1 user private key); and
(4) Link$(\sigma_1, \sigma_2)$= unlinked.

We denote by

$$\mathbf{Adv}_{\mathcal{A}}^{Link}(\lambda) = \Pr[\mathcal{A} \text{ wins the game }]$$

**Definition 5** (Linkability)**.** *A LRS scheme is linkable if for all PPT adversary $\mathcal{A}$, $\mathbf{Adv}_{\mathcal{A}}^{Link}$ is negligible.*

4) NON-SLANDERABILITY.

Non-slanderability ensures that no signer can generate a signature which is determined to be linked by LRS.Link with another signature which is not generated by the signer. In other words, it prevents adversaries from framing honest users.

Non-Slanderability for LRS schemes is defined in the following game between the Simulator $\mathcal{S}$ and the Adversary $\mathcal{A}$ in which $\mathcal{A}$ is given access to oracles $\mathcal{JO}$, $\mathcal{CO}$, $\mathcal{SO}$ and the random oracle:

a) $\mathcal{S}$ generates and gives $\mathcal{A}$ the system parameters param.
b) $\mathcal{A}$ may query the oracles according to any adaptive strategy.
c) $\mathcal{A}$ gives $\mathcal{S}$ an event $e$, group size $n$, a message $M$, a set of $n$ public keys $\mathcal{Y}$, the public key of an insider $pk_\pi \in \mathcal{Y}$ such that $pk_\pi$ has not been queried to $\mathcal{CO}$ or has not been included as the insider public key of any query to $\mathcal{SO}$. $\mathcal{S}$ uses the private key $sk_\pi$ corresponding to $pk_\pi$ to run Sign$(e, n, \mathcal{Y}, sk_\pi, M)$ and to produce a signatures $\sigma'$ given to $\mathcal{A}$.
d) $\mathcal{A}$ queries oracles with arbitrary interleaving. Except $pk_\pi$ cannot be queries to $\mathcal{CO}$, or included as the insider public key of any query to $\mathcal{SO}$. In particular, $\mathcal{A}$ is allowed to query any public key which is not $pk_\pi$ to $\mathcal{CO}$.
e) $\mathcal{A}$ delivers group size $n^*$, a set of $n^*$ public keys $\mathcal{Y}^*$, a message $M^*$ and a signature $\sigma^* \neq \sigma'$.

$\mathcal{A}$ wins the game if

(1) Verify$(e, n^*, \mathcal{Y}^*, M^*, \sigma^*) =$ accept;
(2) $\sigma^*$ is not an output of $\mathcal{SO}$;
(3) All of the public keys in $\mathcal{Y}^*, \mathcal{Y}$ are query outputs of $\mathcal{JO}$;
(4) $pk_\pi$ has not been queried to $\mathcal{CO}$; and
(5) Link$(\sigma^*, \sigma')$ = linked.

We denote by

$$\mathbf{Adv}_{\mathcal{A}}^{NS}(\lambda) = \Pr[\mathcal{A} \text{ wins the game }]$$

**Definition 6** (Non-Slanderability)**.** *A LRS scheme is* non-slanderable *if for all PPT adversary $\mathcal{A}$, $\mathbf{Adv}_{\mathcal{A}}^{NS}$ is negligible.*

## III. OUR PROPOSED LINKABLE RING SIGNATURE WITH UNCONDITIONAL ANONYMITY

### A. Construction

We give the construction of our linkable ring signatures as follows:

- Setup: Let $\mathbb{G}$ be a group of prime order $p$ such that the underlying discrete logarithm problem is intractable. Let $H : \{0,1\}^* \rightarrow \mathbb{G}$ and $H' : \{0,1\}^* \rightarrow \mathbb{Z}_p$ be two hash functions. Let $g = H(\text{“GENERATOR-g”})$ and $h = H(\text{“GENERATOR-h”})$. The public parameters are param $= (\mathbb{G}, g, h, p, H, H', \text{“GENERATOR-g”}, \text{“GENERATOR-h”})$. Note that everyone can check the correctness of the generation of $g, h$.
- KeyGen: A user randomly chooses $x, y \in_R \mathbb{Z}_p$ and computes $Z = g^x h^y$. His secret key is $sk = (x, y)$ and the corresponding public key is $pk = Z$.
- Sign: On input $(event, n, \mathcal{Y}, sk_\pi, M)$ where $event$ is the event description, $n$ is the number of users included in the ring signature, $\mathcal{Y} = \{pk_1, \ldots, pk_n\} = \{Z_1, \ldots, Z_n\}$ is the set of public keys of users in the ring, $sk_\pi$ is the secret key corresponding to the public key $pk_\pi$ such that $pk_\pi \in \mathcal{Y}$ (w.l.o.g., $\pi \in [1, n]$) and $M$ is the message to be signed, the user (with the knowledge of $sk_\pi = (x, y)$) computes the following:
  1) Compute $e = H(event)$ and $t = e^x$.
  2) Randomly generate $r_x, r_y, c_1, \ldots, c_{\pi-1}, c_{\pi+1}, \ldots, c_n \in_R \mathbb{Z}_p$ and compute
  $$K = g^{r_x} h^{r_y} \prod_{i=1, i\neq\pi}^{n} {Z_i}^{c_i}, \qquad K' = e^{r_x} t^{\sum_{i=1, i\neq\pi}^{n} c_i}$$
  3) Find $c_\pi$ such that
  $$c_1 + \ldots + c_n \bmod p = H'\big(\mathcal{Y} || event || t || M || K || K'\big)$$
  4) Compute
  $$\tilde{x} = r_x - c_\pi x \bmod p, \qquad \tilde{y} = r_y - c_\pi y \bmod p$$
  5) Output the signature $\sigma = (t, \tilde{x}, \tilde{y}, c_1, \ldots, c_n)$.

- Verify: On input $(event, \mathcal{Y}, M, \sigma)$, first compute $e = H(event)$ and

$$c_0 = H'\Big(\mathcal{Y}||event||t||M||g^{\tilde{x}}h^{\tilde{y}}\prod_{i=1}^{n} {Z_i}^{c_i}||e^{\tilde{x}}t^{\sum_{i=1}^{n} c_i}\Big)$$

Then check whether

$$\sum_{i=1}^{n} c_i \bmod p = c_0$$

Output accept if it is equal. Otherwise output reject.
- Link: On input two signatures $\sigma_1 = (t_1, \cdot)$, $\sigma_2 = (t_2, \cdot)$, two messages $M_1, M_2$, and an event description $event$, first check whether two signatures are valid. If yes, output link if $t_1 = t_2$ and output unlink otherwise.

### B. Security Analysis

We first give a description of the computational assumption on which the security of our system relies on.

*Computational Assumption:* To prove the security of our scheme, we assume the following mathematical problem is hard: the discrete logarithm problem (DLP). It is described as follow.

**Definition 7** (Discrete Logarithm (DL) Assumption)**.** *For any probabilistic polynomial time algorithm $\mathcal{A}$, the probability that $\Pr[\mathcal{A}(g, g^a) = a]$ is negligible, where $g, g^a \in_R \mathbb{G}$.*

We first prove our scheme is unforgeable, by the following theorem:

**Theorem 1** (**Unforgeability**)**.** *Our linkable ring signature scheme is unforgeable in the random oracle model, if DLP is hard.*

*Proof:* Setup: Given $n$ DL problem instances $(X_1, \ldots, X_n)$ and a generator $g \in \mathbb{G}$, $\mathcal{B}$ is asked to output at least one $x_i \in \mathbb{Z}_p$ such that $X_i = g^{x_i}$ where $i \in [1, n]$. $\mathcal{B}$ chooses $x' \in_R \mathbb{Z}_p$ and sets $h = g^{x'}$. $\mathcal{B}$ also chooses $y_i \in_R \mathbb{Z}_p$ and sets $Z_i = X_i h^{y_i}$ for all $i \in [1, n]$.

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

- *Random Oracle H*: For query input "GENERATOR-g", $\mathcal{B}$ returns $g$. For For query input "GENERATOR-h", $\mathcal{B}$ returns $h$. For other query, $\mathcal{B}$ randomly picks $\lambda \in_R \mathbb{Z}_p$ and returns $g^{\lambda}$.
- *Random Oracle H'*: $\mathcal{B}$ randomly picks $\alpha \in_R \mathbb{Z}_p$ and returns provided that the value has not been assigned.
- *Joining Oracle $\mathcal{JO}$*: Assume $\mathcal{A}$ can only query $\mathcal{JO}$ for a maximum $n'$ times, where $n' \geq n$. $\mathcal{B}$ randomly chooses a subset $\mathcal{I}_n$ containing $n$ indexes. $\mathcal{B}$ assigns $Z_i$ for $i \in [1, n]$ to these $n$ indexes. W.l.o.g., we use $1, \ldots, n$ to denote these indexes (in which $\mathcal{B}$ does not know the corresponding private key) while $n+1, \ldots, n'$ to denote the other indexes. For the other $n' - n$ indexes, $\mathcal{B}$ generates the public key and private key pair according to the algorithm. Upon the $j$-th query, $\mathcal{B}$ returns the corresponding public key.
- *Corruption Oracle $\mathcal{CO}$*: On input a public key $pk$ which is an output from $\mathcal{JO}$, $\mathcal{B}$ checks whether it is corresponding to the subset $\mathcal{I}_n$. If yes, $\mathcal{B}$ halts. Otherwise, $\mathcal{B}$ outputs the corresponding private key.
- *Signing Oracle $\mathcal{SO}$*: On input a signing query for event $event$, a set of public key $\mathcal{Y} = \{Z_1, \ldots, Z_n\}$, the public key for the signer $Z_\pi$ where $\pi \in [1, n]$, and a message $M$, $\mathcal{B}$ simulates as follow:
  1) If the query of $H(event)$ has not been made, carry out the $H$-query of $event$ as described above. Set $e$ to $H(event)$. Note that $\mathcal{B}$ knowns the discrete-log, denoted by $\lambda$, of $e$ to the base $g$. That is, $e = g^{\lambda}$.
  2) If $Z_\pi$ is not corresponding to any element in the set $\mathcal{I}_n$, $\mathcal{B}$ knows the private key and computes the signature according to the algorithm. Otherwise, w.l.o.g, we let $Z_\pi$ be the $\pi$-th index from the $\mathcal{JO}$. $\mathcal{B}$ sets $t = {X_\pi}^{\lambda}$.
  3) $\mathcal{B}$ randomly chooses $\tilde{x}, \tilde{y} \in \mathbb{Z}_p$ and $c_i \in_R \mathbb{Z}_p$ for all $i \in [1, n]$ and set the $H'$ oracle output of

$$H'\Big(\mathcal{Y}||event||t||M||g^{\tilde{x}}h^{\tilde{y}}\prod_{i=1}^{n} {Z_i}^{c_i}||e^{\tilde{x}}t^{\sum_{i=1}^{n} c_i}\Big)$$

  to $\sum_{i=1}^{n} c_i \bmod p$. If collision occurs, that is, the value $\sum_{i=1}^{n} c_i \bmod p$ has already been assigned to some $H'$ query, repeats this step.
  4) $\mathcal{B}$ returns the signature $\sigma = (t, \tilde{x}, \tilde{y}, c_1, \ldots, c_n)$.

$\mathcal{A}$ cannot distinguish between $\mathcal{B}$'s simulation and real life.

Output: For one successful simulation, suppose the forgery of $\mathcal{A}$ is $\sigma^1 = (t^1, \tilde{x}^1, \tilde{y}^1, c_1^1, \ldots, c_{n"}^1)$ on an event $event$ and a set of public key $\mathcal{Y}$" such that it is a subset of those public key with corresponding indexes in $\mathcal{I}_n$. W.l.o.g, we let $n" = n$. By the assumption of random oracle model, $\mathcal{A}$ has a query $H(event)$ which is denoted by $e$ and query $H'(\mathcal{Y}"||event||t||M||K||K')$ where

$$K = g^{\tilde{x}^1}h^{\tilde{y}^1}\prod_{i=1}^{n} {Z_i}^{c_i^1} \qquad \text{and} \qquad K' = e^{\tilde{x}^1}{t^1}^{\sum_{i=1}^{n} c_i^1}.$$

Let $K = g^{\beta}h^{\beta'}$ for some $\beta, \beta' \in \mathbb{Z}_p$. Suppose this is done at the $\ell$-th query of $H'$ and $\mathcal{B}$ returns $c_0^1$. Since $c_0^1 = c_1^1 + \cdots + c_n^1 \bmod p$ and by the assumption of random oracle model, at least one $c_i^1$, $1 \leq i \leq n$, is determined after $c_0^1$ is returned by $\mathcal{B}$. In the best case where there is only one $c_i^1$ which is not determined at $\ell$-th query, one rewind allows $\mathcal{B}$ to find out the secret $x_i$ (since $\mathcal{B}$ knows the corresponding $y_i$). In the worst case, that is, all $n$ $c_i^1$'s, $1 \leq i \leq n$, are not determined at $\ell$-th $H'$ query, $\mathcal{B}$ rewinds with the same input tape for $\mathcal{A}$ and answers all queries consistently until the $\ell$-th $H'$ query. For $i$-th rewind at the $\ell$-th $H'$ query, $c_0^i$ is randomly picked in $\mathbb{Z}_p$ and returned. $\mathcal{B}$ conducts the process above until $n$ simulations of $\mathcal{A}$ have completed. Suppose all the $n$ simulations are successful, $\mathcal{A}$ produces altogether $n$ forgeries $(t^i, \tilde{x}^i, \tilde{y}^i, c_1^i, \ldots, c_n^i)$ for all $i \in [1, n]$. Since $c_0^i \neq c_0^j$ for any $i \neq j$, $i, j \in \{1, \ldots, n\}$, there are $n$ distinct linear equations:

$$\beta = \tilde{x}^i + c_1^i x_1 + \cdots + c_n^i x_n$$

for $i = 1, \ldots, n$. Hence up to $n$ $x_i$ can be obtained.

Analysis: The running time of $\mathcal{B}$ is at most $n\tau$ where $\tau$ is the running time for $\mathcal{A}$. $\mathcal{B}$ succeeds if all the $n$ simulations of

$\mathcal{A}$ are successful. By the forking lemma [26], the chance of each successful rewind simulation is at least $\epsilon/4$ where $\epsilon$ is the probability that $\mathcal{A}$ successfully forges a signature. Hence the successful chance of $\mathcal{B}$ is at least $(\epsilon/4)^n$. ■

Then we prove our scheme is unconditional anonymous.

**Theorem 2** (**Anonymity**). *Our linkable ring signature scheme is unconditional anonymous.*

*Proof:* For each $\mathcal{JO}$ query, a value $Z = g^x h^y$ is returned for some randomly generated pair $(x, y)$. The challenge signature is created using the key of a random signer in the set of the ring. In the following, we are going to show the advantage of the adversary is 0 in an information-theoretic manner. The proof is divided into three parts. Firstly, we show that given a signature $\sigma = (t, \tilde{x}, \tilde{y}, c_1, \ldots, c_n)$ for a ring of public keys $(Z_1, \ldots, Z_n)$ on message $M$ and event $event$, there exists a corresponding private key $(x_\pi, y_\pi)$ **for each possible public key** $Z_\pi$, for any $\pi \in \{1, \ldots, n\}$, that can produce the linking tag $t$. That is, $t = H(event)^{x_\pi}$. In the following, we use $e$ to denote the value of $H(event)$. Secondly, we show that given such a private key $(x_\pi, y_\pi)$, there exists a tuple of values $(r_{x_\pi}, r_{y_\pi})$ such that $\sigma$ is created with the private key $(x_\pi, y_\pi)$ using randomness $(r_{x_\pi}, r_{y_\pi})$. Finally, we show that for any value of $\pi \in \{1, \ldots, n\}$, the distribution of the tuple $(x_\pi, y_\pi, r_{x_\pi}, r_{y_\pi})$ defined in part one and two of the proof is identical. In other words, in the view of the adversary, the signature $\sigma$ is independent to the value $\pi$, the index of the actual signer. Thus, we can safely conclude that even an unbounded adversary cannot output the value $\pi$ with probability better than random guessing.

- (Part I.) Let $x, \ell$ be the values such that $t = e^x$ and $g = h^\ell$. Further, let $Z_i = h^{z_i}$ for $i = 1$ to $n$. For each $\pi \in \{1, \ldots, n\}$, consider the values
$$x_\pi = x \bmod p$$
$$y_\pi = z_\pi - x_\pi \ell \bmod p.$$
Obviously, $(x_\pi, y_\pi)$ is a private key corresponding to the public key $Z_\pi$ (since $Z_\pi = h^{z_\pi} = h^{x_\pi \ell + y_\pi} = g^{x_\pi} h^{y_\pi}$) and that $t = e^x = e^{x_\pi}$.
- (Part II.) For each possible $(x_\pi, y_\pi)$ defined in Part I, consider the values
$$r_{x_\pi} := \tilde{x} + c_\pi x_\pi \bmod p$$
$$r_{y_\pi} := \tilde{y} + c_\pi y_\pi \bmod p.$$
It can be seen that $\sigma$ is created by the private key $(x_\pi, y_\pi)$ using the randomness $(r_{x_\pi}, r_{y_\pi})$, for any $\pi \in \{1, \ldots, n\}$.
- (Part III.) It is straightforward to show the distributions of $(x_\pi, y_\pi, r_{x_\pi}, r_{y_\pi})$ for each possible value $\pi$ are identical and that it adheres to the distribution to a signature created by the signer with public key $Z_\pi$.

In other words, the signature $\sigma$ can be created by any signer equipped with private key $(x_\pi, y_\pi)$ for any $\pi \in \{1, \ldots, n\}$ using randomness $(r_{x_\pi}, r_{y_\pi})$. Even if the unbounded adversary can compute all the values $(x_\pi, y_\pi, r_{x_\pi}, r_{y_\pi})$ for all $\pi = 1$ to $n$, it still cannot guess who the actual signer is.

We are using the fact a public key in our construction corresponds to multiple secret keys. For each public key, there exists a unique corresponding private key that would match with the given linking tag in the signature.

Note that this case explains why our scheme is *unconditional anonymous*, which induces Definition 2 (our second interpretation of Strong Anonymity). However, our scheme cannot achieve the anonymity for Definition 1. That is, if the adversary knows the private keys *owned by the parties*, it can compute the actual signer easily. ■

Now we prove our scheme is linkable.

**Theorem 3** (**Linkability**). *Our linkable ring signature scheme is linkable in the random oracle mode, if DLP is hard.*

*Proof:* We try to derive some contradictions based on the assumption that if $\mathcal{A}$ can produce two valid signatures that are unlinked with just one private key. We use the same setting as the proof in Theorem 1, except that we use $n - 1$ DLP problem instances. Simulator $\mathcal{B}$ generates the remaining user private key and public key pair according to the algorithm. Thus it knows the private key of this user, denoted by $\pi$ where $\pi \in [1, n]$. This private key is given to the adversary $\mathcal{A}$ during its query to the $\mathcal{CO}$, which is the only private key that $\mathcal{A}$ is allowed to have.

We first prove the following lemma:

**Lemma 1.** *If an adversary $\mathcal{A}$ knowns only one private key $sk_\pi = (x_\pi, y_\pi)$, $\pi \in [1, n]$ and produces a valid signature $\sigma = (t, \tilde{x}, \tilde{y}, c_1, \ldots, c_n)$ for an event $event$, then $t = H(event)^{x_\pi}$ provided that DLP is hard, in the random oracle model.*

*Proof*: We use standard proof-of-knowledge proving technique in the random oracle model. Suppose $\mathcal{A}$ produces a valid signature $\sigma^1 = (t, \tilde{x}^1, \tilde{y}^1, c_1^1, \ldots, c_n^1)$ where $t = H(event)^{\hat{x}}$ for some $\hat{x} \in \mathbb{Z}_p$ for the first run. Then rewind $\mathcal{A}$ with a different value for the random oracle $H'$, to obtain a second signature $\sigma^2 = (t, \tilde{x}^2, \tilde{y}^2, c_1^2, \ldots, c_n^2)$. Note that the following elements are fixed during both runs: the list of public keys $\mathcal{Y}$, the event description $event$, the message $M$, $\alpha, \alpha', \lambda, \hat{x} \in \mathbb{Z}_p$ where the random oracle query $H'$ for input

$$H'\big(\mathcal{Y}||event||H(event)^{\hat{x}}||M||g^\alpha h^{\alpha'}||H(event)^\lambda\big)$$

gives two different outputs $c_0^1, c_0^2$ for two different runs. From these two signatures, we have the following equations:

$$\begin{aligned} c_0^1 &= c_1^1 + \cdots + c_n^1 \\ c_0^2 &= c_1^2 + \cdots + c_n^2 \\ \alpha &= \tilde{x}^1 + x_1 c_1^1 + \cdots + x_n c_n^1 \\ &= \tilde{x}^2 + x_1 c_1^2 + \cdots + x_n c_n^2 \qquad (1) \\ \lambda &= \tilde{x}^1 + \hat{x} c_0^1 \;=\; \tilde{x}^2 + \hat{x} c_0^2 \qquad (2) \end{aligned}$$

We evaluate the possible values of $\hat{x}$ for enabling $\mathcal{A}$ to generate two such sequences by having only one private key $(x_\pi, y_\pi)$. We divide into two cases:

1) Case 1: Suppose all $c_i^1 = c_i^2$ except when $i = j$ for some $j \in [1, n]$. From equation (1) and (2), since $c_j^1 \neq c_j^2$, hence $\tilde{x}_1 \neq \tilde{x}_2$. Then we have
$$\frac{\tilde{x}_1 - \tilde{x}_2}{c_j^2 - c_j^1} = x_j \qquad \text{from equation (1)},$$

$$\frac{\tilde{x}_1 - \tilde{x}_2}{c_0^2 - c_0^1} = \frac{\tilde{x}_1 - \tilde{x}_2}{c_j^2 - c_j^1} = \hat{x} \qquad \text{from equation (2)}$$

That is, $x_j = \hat{x}$ which is known by $\mathcal{A}$. Since $\mathcal{A}$ is assumed to know only one private key, we have $j = \pi$.

2) Case 2: Suppose all $c_i^1 \neq c_i^2$ except when $i \in \{j_1, j_2\}$ for some $j_1, j_2 \in [1, n]$. We have $c_{j_1}^1 \neq c_{j_1}^2$, $c_{j_2}^1 \neq c_{j_2}^2$ and $\tilde{x}^1 \neq \tilde{x}^2$. From equation (1), we have

$$\tilde{x}^1 + x_{j_1} c_{j_1}^1 + x_{j_2} c_{j_2}^1 = \tilde{x}^2 + x_{j_1} c_{j_1}^1 + x_{j_2} c_{j_2}^2$$

If $\pi \in \{j_1, j_2\}$, then $\mathcal{A}$ knows both $x_{j_1}$ and $x_{j_2}$ which contradicts to our assumption that $\mathcal{A}$ knows only one private key. If $\pi \notin \{j_1, j_2\}$, $\mathcal{A}$ obtains the following relation:

$$x_{j_1} + x_{j_2}\phi_2 = \phi_1$$

where

$$\phi_2 = \frac{c_{j_2}^1 - c_{j_2}^2}{c_{j_1}^1 - c_{j_1}^2} \qquad \text{and} \qquad \phi_1 = \frac{\tilde{x}^2 - \tilde{x}^1}{c_{j_1}^1 - c_{j_1}^2}.$$

This implies that $\mathcal{A}$ can solve the following problem: Given $Y_1, Y_2 \in \mathbb{G}$, find $\phi_1, \phi_2 \in \mathbb{Z}_p$ such that $Y_1 \cdot Y_2^{\phi_2} = g^{\phi_1}$. This is hard if $Y_1, Y_2$ are independently and randomly generated. One can show that the problem is computationally equivalent to DLP. We omit the details here. Since suppose DLP is hard, this case should not exist.

The same argument can be generalized to have three of more $c_i^1$ be not equal to the corresponding $c_i^2$.

Concluding, only case 1 is possible. That is, if $\mathcal{A}$ only knowns one private key $(x_\pi, y_\pi)$, we have $t = H(event)^{x_\pi}$. □

If $\mathcal{A}$ produces two valid signatures such that they are unlinkable, that is, $t^1 \neq t^2$ where $t^1$ and $t^2$ are the linking tags, we have $t^1 = e^{x_{\pi_1}}$ and $t^2 = e^{x_{\pi_2}}$ where $e = H(event)$. From **Lemma** 1, $\mathcal{A}$ must know $x_{\pi_1}$ and $x_{\pi_2}$. It contradicts to the assumption that $\mathcal{A}$ only knows one private key. ■

Finally we prove our scheme is non-slanderable.

**Theorem 4** (**Non-Slanderability**). *Our linkable ring signature scheme is non-slanderable in the random oracle mode, if DLP is hard.*

*Proof:* $\mathcal{A}$ can query any oracle except that it cannot submit a chosen pubic key $pk_\pi$ to the $\mathcal{CO}$. It then gives $\mathcal{B}$ $pk_\pi$, a list of public key $\mathcal{Y}$ (w.l.o.g, we have $|\mathcal{Y}| = n$) such that $pk_\pi \in \mathcal{Y}$, a message $M$ and an event description $event$. In return, simulator $\mathcal{B}$ generates a signature $\sigma = (t, \cdot)$ using $sk_\pi$, the corresponding secret key of $pk_\pi$ and gives it back to $\mathcal{A}$. $\mathcal{A}$ continues to query various oracles, except that it is not allowed to submit $pk_\pi$ to $\mathcal{CO}$.

Suppose $\mathcal{A}$ produces another valid signature $\sigma^* = (t^*, \cdot)$ such that it is not an output from $\mathcal{SO}$ and it is linkable to $\sigma$. Since they are linkable, we have $t^* = t$. From **Lemma** 1, the signer must have the knowledge of $x_{\pi'}$ where $t^* = t = H(event)^{x_{\pi'}}$ and $\pi' \in [1, n]$. Since $\mathcal{B}$ uses private key $sk_\pi$ to generate $\sigma$, we have $\pi = \pi'$. That is, $\mathcal{A}$ must know $sk_\pi$ to generate $\sigma^*$ (as the corresponding linking tag $t^* = H(event)^{x_\pi}$), which contradicts to the assumption that $\mathcal{A}$ is not allowed to query $pk_\pi$ for $\mathcal{CO}$. ■

Our scheme achieves all security requirement of a linkable ring signature (our mandatory linkability is known as strong linkability in [19]), yet it provides unconditional anonymity. Hence it can act as an counterexample to show that under one of the interpretations of *Strong Anonymity* (Definition 2), Theorem 1 in [19] is not always true.

### C. Efficiency and Comparison

Let $n$ be the number of parties in the ring. We compare our scheme with other linkable ring signature schemes in Table I. We can see that our scheme is very efficient for both signing and verification. We do not require any pairing operations, while the number of exponentiation and multi-bases exponentiation operation is constant.

## IV. Conclusion

In this paper, we have shown that it is possible to have a linkable ring signature scheme with unconditional anonymity. To construct a linkable ring signature scheme with unconditional anonymity was considered as an open problem in [22]. All existing schemes can only provide computational anonymity. We solve this open problem by giving a concrete construction in the random oracle model. Our scheme is also very efficient and practical.

Simultaneously, our scheme can act as an counterexample to show that the Theorem 1 stated in [19] is not always true. That theorem stated that mandatory linkable ring signature cannot provide strong anonymity. However, we have proven that our scheme can provide strong anonymity under one of the interpretations.

The security of our scheme relies on random oracle model. We regard as an open problem to construct a scheme with unconditional anonymity in the standard model. Another interesting open problem is to shorten the size of the signature. The ideal case is to have a signature size independent to the number of users in the ring.

## References


[1] M. Abe, M. Ohkubo, and K. Suzuki. 1-out-of-n Signatures from a Variety of Keys. In *ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 415–432. Springer, 2002.

[2] N. R. Adam. A new dynamic voting algorithm for distributed database systems. *IEEE Trans. Knowl. Data Eng.*, 6(3):470–478, 1994.

[3] M. H. Au, S. S. M. Chow, W. Susilo, and P. P. Tsang. Short linkable ring signatures revisited. In *EuroPKI*, volume 4043 of *Lecture Notes in Computer Science*, pages 101–115. Springer, 2006.

[4] M. Bellare, D. Micciancio, and B. Warinschi. Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions. In *EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 614–629. Springer, 2003.

[5] D. Boneh and X. Boyen. Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In *EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 223–238. Springer, 2004.

[6] D. Boneh and X. Boyen. Secure Identity Based Encryption Without Random Oracles. In *CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 443–459. Springer, 2004.

[7] D. Boneh, C. Gentry, B. Lynn, and H. Shacham. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In *EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 416–432. Springer, 2003.

TABLE I: Comparison of $(1, n)$-Linkable Ring Signatures

| Scheme | Signature Size | Anonymity | Model | Linking | Sign Computation[a] | Verify Computation[a] |
|---|---|---|---|---|---|---|
| Liu *et al.* [22] | $O(n)$ | computational | ROM | compulsory | $3E + 2(n-1)M$ | $2nM$ |
| Tsang and Wei [30] | $O(1)$ | computational | ROM | compulsory | $(2+n)E + 7M$ | $7M$ |
| Liu and Wong [23] | $O(n)$ | computational | ROM | compulsory | $E + 2M$ | $2M$ |
| Au *et al.* [3] | $O(1)$ | computational | ROM | compulsory | $(2+n)E + 7M$ | $7M$ |
| Zheng *et al.* [38] | $O(n)$ | computational | ROM | compulsory | $(14n+2)$ seq. op.[b] | $(14n+2)$ seq. op.[b] |
| Tsang *et al.* [29], [31] | $O(n)$ | computational | ROM | compulsory | $2(n+1)E$ $+2(n-1)M$ ([31]) $(n+4)E$ $+4nM$ ([29]) | $3nM$ ([31]) $5nM$ ([29]) |
| Fujisaki [17] | $O(\sqrt{n})$ | computational | standard | compulsory | $(6+13\sqrt{n})E$ $+(5+n+2\sqrt{n})M$ $+2\sqrt{n}P + \mathsf{OTS}$ | $nM$ $+(8+2n+12\sqrt{n})P$ $+\mathsf{OTV}$ |
| Yuen *et al.* [36] | $O(\sqrt{n})$ | computational | standard | compulsory | $(8+4\sqrt{n})E+$ $(4+2\sqrt{n})M + \mathsf{OTS}$ | $2E + 8(1+$ $\sqrt{n})P + 1 + \mathsf{OTV}$ |
| Jeong *et al.* [19] | $O(n)$ | unconditional | ROM | optional | $2E + (n-1)M$ | $(n+1)M$ |
| Our Scheme | $O(n)$ | unconditional | ROM | compulsory | $E + 2M$ | $2M$ |

[a] When we come across the computation of sign and verify, we use $E$ to represent an exponentiation, $M$ to represent a multi-bases exponentiation which is equal to the cost of approximate 1.3 exponentiation, $P$ to represent a pairing, $\mathsf{OTS}$ to represent a one-time signature signing and $\mathsf{OTV}$ to represent a one-time signature verification.

[b] The scheme in [38] relies on Linear Feedback Shift Register (LFSR) and the computations are sequence operations.


[8] J. Camenisch and M. Stadler. Efficient Group Signature Schemes for Large Groups (Extended Abstract). In *CRYPTO 97*, volume 1294 of *Lecture Notes in Computer Science*, pages 410–424. Springer, 1997.

[9] D. Chaum and E. van Heyst. Group signatures. In *EUROCRYPT*, volume 547 of *Lecture Notes in Computer Science*, pages 257–265. Springer, 1991.

[10] L. Chen and T. P. Pedersen. New group signature schemes (extended abstract). In *EUROCRYPT*, volume 950 of *Lecture Notes in Computer Science*, pages 171–181. Springer, 1994.

[11] L. Chen and N. Tokuda. Stability analysis of regional and national voting schemes by a continuous model. *IEEE Trans. Knowl. Data Eng.*, 15(4):1037–1042, 2003.

[12] S. S. Chow, J. K. Liu, V. K. Wei, and T. H. Yuen. Ring Signatures without Random Oracles. In *ASIACCS 06*, pages 297–302. ACM Press, 2006.

[13] S. S. M. Chow, J. K. Liu, and D. S. Wong. Robust receipt-free election system with ballot secrecy and verifiability. In *NDSS*. The Internet Society, 2008.

[14] 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, 2005. Also available at Cryptology ePrint Archive, Report 2004/327.

[15] Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup. Anonymous Identification in Ad Hoc Groups. In *EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 609–626. Springer, 2004.

[16] Q. Feng, Y. L. Sun, L. Liu, Y. Yang, and Y. Dai. Voting systems with trust mechanisms in cyberspace: Vulnerabilities and defenses. *IEEE Trans. Knowl. Data Eng.*, 22(12):1766–1780, 2010.

[17] E. Fujisaki. Sub-linear size traceable ring signatures without random oracles. In *CT-RSA 2011*, volume 6558 of *Lecture Notes in Computer Science*, pages 393–415. Springer, 2011.

[18] C. Gentry. Practical identity-based encryption without random oracles. In *EUROCRYPT 2006*, volume 4404 of *Lecture Notes in Computer Science*, pages 445–464. Springer, 2006.

[19] I. R. Jeong, J. O. Kwon, and D. H. Lee. Ring signature with weak linkability and its applications. *IEEE Trans. Knowl. Data Eng.*, 20(8):1145–1148, 2008.

[20] V. Kantere, D. Dash, G. François, S. Kyriakopoulou, and A. Ailamaki. Optimal service pricing for a cloud cache. *IEEE Trans. Knowl. Data Eng.*, 23(9):1345–1358, 2011.

[21] J. K. Liu, V. K. Wei, and D. S. Wong. A separable threshold ring signature scheme. In *ICISC 2003*, volume 2971 of *Lecture Notes in Computer Science*, pages 352–369. Springer, 2003.

[22] J. K. Liu, V. K. Wei, and D. S. Wong. Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups (Extended Abstract). In *ACISP*, volume 3108 of *Lecture Notes in Computer Science*. Springer, 2004.

[23] J. K. Liu and D. S. Wong. Linkable ring signatures: Security models and new schemes. In *ICCSA (2)*, volume 3481 of *Lecture Notes in Computer Science*, pages 614–623. Springer, 2005.

[24] J. K. Liu, T. H. Yuen, and J. Zhou. Forward secure ring signature without random oracles. In *ICICS*, volume 7043 of *Lecture Notes in Computer Science*, pages 1–14. Springer, 2011.

[25] S. Meng, L. Liu, and T. Wang. State monitoring in cloud datacenters. *IEEE Trans. Knowl. Data Eng.*, 23(9):1328–1344, 2011.

[26] D. Pointcheval and J. Stern. Security proofs for signature schemes. In *EUROCRYPT*, volume 1070 of *Lecture Notes in Computer Science*, pages 387–398. Springer, 1996.

[27] R. L. Rivest, A. Shamir, and Y. Tauman. How to Leak a Secret. In *ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 552–565. Springer, 2001.

[28] H. Shacham and B. Waters. Efficient ring signatures without random oracles. In *Public Key Cryptography*, volume 4450 of *Lecture Notes in Computer Science*, pages 166–180. Springer, 2007.

[29] P. P. Tsang, M. H. Au, J. K. Liu, W. Susilo, and D. S. Wong. A suite of non-pairing id-based threshold ring signature schemes with different levels of anonymity. In *ProvSec 2010*, volume 6402 of *Lecture Notes in Computer Science*, pages 166–183. Springer, 2010.

[30] P. P. Tsang and V. K. Wei. Short linkable ring signatures for e-voting, e-cash and attestation. In *ISPEC 2005*, volume 3439 of *Lecture Notes in Computer Science*, pages 48–60. Springer, 2005.

[31] P. P. Tsang, V. K. Wei, T. K. Chan, M. H. Au, J. K. Liu, and D. S. Wong. Separable linkable threshold ring signatures. In *INDOCRYPT 2004*, Lecture Notes in Computer Science, pages 384–398. Springer, 2004.

[32] C. Wang, K. Ren, W. Lou, and J. Li. Toward publicly auditable secure cloud data storage services. *IEEE Network*, 24(4):19–24, 2010.

[33] B. Waters. Efficient Identity-Based Encryption Without Random Oracles. In *EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 114–127. Springer, 2005.

[34] 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 *ICICS 2003*, volume 2836 of *Lecture Notes in Computer Science*, pages 34–46. Springer, 2003.

[35] T. H. Yuen, J. K. Liu, M. H. Au, W. Susilo, and J. Zhou. Threshold Ring Signatures without Random Oracles. In *ASIACCS 2011*, pages 261–267. ACM Press, 2011.

[36] T. H. Yuen, J. K. Liu, M. H. Au, W. Susilo, and J. Zhou. Efficient linkable and/or threshold ring signature without random oracles. To Appear, Computer Journal, 2012.

[37] F. Zhang and K. Kim. ID-Based Blind Signature and Ring Signature from Pairings. In *ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 533–547. Springer, 2002.

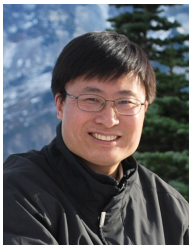
[38] D. Zheng, X. Li, K. Chen, and J. Li. Linkable ring signatures from linear feedback shift register. In *EUC Workshops*, volume 4809 of *Lecture Notes in Computer Science*, pages 716–727. Springer, 2007.

[39] L. Zhou, V. Varadharajan, and M. Hitchens. Enforcing role-based access control for secure data storage in the cloud. *Comput. J.*, 54(10):1675–1687, 2011.

**Joseph K. Liu** received the PhD degree in information engineering from the Chinese University of Hong Kong in July 2004, speciallizing in cryptographic protocols for securing wireless networks, privacy, authentication and provable security. He is now a research scientist in the Cryptography and Security Department at the Institute for Infocomm Research, Singapore. His current technical focus is particularly lightweight cryptography, wireless security, security in smart grid system and cloud computing environment.

**Man Ho Au** received his PhD degree from the University of Wollongong in 2009. He is currently an associate lecturer in the School of Computer Science and Software Engineering, University of Wollongong. His research interests include information security, privacy and cryptography. He has published over 40 referred research papers at international conferences and has served as a workshop chair, programme committee member, organizing committee member or publication chair for around 10 international conferences. He is a member of IEEE, starting from 2012.

**Willy Susilo** received a Ph.D. in Computer Science from University of Wollongong, Australia. He is a Professor at the School of Computer Science and Software Engineering and the director of Centre for Computer and Information Security Research (CCISR) at the University of Wollongong. He is currently holding the prestigious ARC Future Fellow awarded by the Australian Research Council (ARC). His main research interests include cryptography and information security. His main contribution is in the area of digital signature schemes. He has served as a program committee member in dozens of international conferences. He has published numerous publications in the area of digital signature schemes and encryption schemes. He is a senior member of IEEE, starting from 2001.



**Jianying Zhou** is a senior scientist at Institute for Infocomm Research, and heads the Network Security Lab. He received PhD in Information Security from University of London in 1997. His research interests are in computer and network security, mobile and wireless communications security. He is a co-founder and steering committee member of International Conference on Applied Cryptography and Network Security (ACNS).