# Linkable Ring Signatures: Security Models and New Schemes

## (Extended Abstract)

Joseph K. Liu[1] and Duncan S. Wong[2,⋆]

[1] Department of Information Engineering,
The Chinese University of Hong Kong, Shatin, Hong Kong
ksliu@ie.cuhk.edu.hk
[2] Department of Computer Science,
City University of Hong Kong, Kowloon, Hong Kong
duncan@cityu.edu.hk

**Abstract.** A ring signature scheme is a group signature scheme but with no group manager to setup a group or revoke a signer's identity. The formation of a group is spontaneous in the way that diversion group members can be totally unaware of being conscripted to the group. It allows members of a group to sign messages on the group's behalf such that the resulting signature does not reveal their identity (anonymity). The notion of linkable ring signature, introduced by Liu, et al. [10], also provides signer anonymity, but at the same time, allows anyone to determine whether two signatures have been issued by the same group member (linkability). In this paper, we enhance the security model of [10] for capturing new and practical attacking scenarios. We also propose two polynomial-structured linkable ring signature schemes. Both schemes are given strong security evidence by providing proofs under the random oracle model.

## 1 Introduction

A group signature scheme [7, 6, 2] allows members of a group to sign messages on behalf of the group without revealing the identity of the signer (anonymity). It is also not possible to decide whether two signatures have been issued by the same group member (unlinkability). Only a designated group manager which also maintains the group membership can revoke the authorship of signatures. For anyone else, signatures are anonymous and unlinkable.

A ring signature scheme [13, 5, 1, 4, 8] can be considered as a group signature scheme without a group manager. The formation of a group is spontaneous. That is, under the assumption that each user is already associated with the public key

⋆ The work described in this paper was supported by a grant from the Research Grants Council of the Hong Kong Special Administrative Region, China (Project No. 9040904 (RGC Ref. No. CityU 1161/04E )).

O. Gervasi et al. (Eds.): ICCSA 2005, LNCS 3481, pp. 614–623, 2005.

of some standard signature scheme, a user (group creator) can spontaneously create a group by collecting the public keys of some other users and his own public key. The diversion group members (i.e. those users whose public keys are included in the group by the group creator) can be totally unaware of being conscripted into the group. Similar to group signature schemes, ring signature schemes are also anonymous and unlinkable. But also unlike group signature schemes, ring signature schemes do not have any group manager to revoke the anonymity of a signature or maintain the group membership.

A linkable ring signature scheme, introduced by Liu, et al. [10], is a ring signature scheme that provides signer anonymity but at the same time allows one to determine whether two signatures have been issued by the same group member. Linkable ring signature schemes can be used for constructing efficient e-voting systems [10]. To cast a vote, a voter generates a linkable ring signature for his vote. Anonymity is maintained and linkability helps detect double voting if a voter casts two votes. In addition, linkable ring signatures eliminate the involvement of voters in the registration phase of each voting event and at the same time prevent information leak on which voters have cast votes and which voters have not.

We enhance the security model of [10] by providing a stronger notion of signer anonymity and redefining linkability. The new security model captures new and practical attacking scenarios, and properties more thoroughly.

In this paper, we use an approach based on the proof of knowledge system called Witness Indistinguishable Proof of Equality of a Discrete Logarithm to construct two linkable ring signature schemes. We also discuss a subtlely on linkability between these two schemes. For both of the schemes proposed in this paper, we give strong evidence of their security by providing security proofs in our enhanced security model under the random oracle model [3].

The paper is organized as follows. In Sec. 2, a linkable ring signature scheme and a security model are defined. In Sec. 3, the basic techniques of our constructions are described and two polynomial-structured linkable ring signature schemes are proposed. In Sec. 4, we conclude the paper. There are several appendices at the end of the paper containing the proofs of the theorems stated in the paper body.

## 2 Linkable Ring Signature Schemes

A linkable ring signature scheme is a quadruple $(Gen, Sig, Ver, Link)$.

- $(x, y) \leftarrow Gen(1^k)$ is a probabilistic algorithm which takes security parameter $k$ and outputs private key $x$ and public key $y$.
- $\sigma \leftarrow Sig(1^k, 1^n, x, L, m)$ is a probabilistic algorithm which takes security parameter $k$, group size $n$, private key $x$, a list $L$ of $n$ public keys which includes the one corresponding to $x$ and message $m$, produces a signature $\sigma$.
- $1/0 \leftarrow Ver(1^k, 1^n, L, m, \sigma)$ is a boolean algorithm which accepts as inputs security parameter $k$, group size $n$, a list $L$ of $n$ public keys, message $m$ and