Separable Linkable Threshold Ring Signatures

Patrick P. Tsang[1], Victor K. Wei[1], Tony K. Chan[1], Man Ho Au[1], Joseph K. Liu[1], and Duncan S. Wong[2]

[1] Department of Information Engineering,
The Chinese University of Hong Kong,
Shatin, Hong Kong
{pktsang3, kwwei, klchan3, mhau3, ksliu9}@ie.cuhk.edu.hk
[2] Department of Computer Science,
The City University of Hong Kong,
Hong Kong
duncan@cityu.edu.hk

Abstract. A ring signature scheme is a group signature scheme with no group manager to setup a group or revoke a signer. A linkable ring signature, introduced by Liu, et al. [20], additionally allows anyone to determine if two ring signatures are signed by the same group member (a.k.a. they are *linked*). In this paper, we present the first separable linkable ring signature scheme, which also supports an efficient thresholding option. We also present the security model and reduce the security of our scheme to well-known hardness assumptions. In particular, we introduce the security notions of *accusatory linkability* and *non-slanderability* to linkable ring signatures. Our scheme supports "event-oriented" linking. Applications to such linking criterion is discussed.

1 Introduction

Ring Signatures. A ring signature scheme [22] is a group signature scheme [10, 2] with no group manager to setup a group or revoke a signer's identity. Formation of a group is *spontaneous* in a way that diversion group members can be totally unaware of being conscripted to the group. It allows members to *anonymously* sign messages on behalf of their group. Applications include leaking secrets [22] and anonymous identification/authentication for ad hoc groups [6, 13].

Threshold Ring Signatures. Threshold cryptography [12] allows n parties to share the ability to perform a cryptographic operation (e.g., creating a digital signature). Any d parties can perform the operation jointly, whereas it is infeasible for at most $d-1$ to do so. In a (d, n)-threshold ring signature scheme, the generation of a ring signature for a group of n members requires the involvement of at least d members/signers, and yet the signature reveals nothing about the identities of the signers. Schemes in the literature include [6, 19, 24].

Linkable Ring Signatures. The notion of linkable ring signatures was introduced by Liu, et al. [20]. They are ring signatures, but with added linkability: such signatures allow anyone to determine if two signatures are signed by the same

A. Canteaut and K. Viswanathan (Eds.): INDOCRYPT 2004, LNCS 3348, pp. 384–398, 2004.

group member (in which case the two signatures are said to be "*linked*"). If a user signs only once on behalf of a group, the user still enjoys anonymity similar to that in conventional ring signature schemes. If the user signs multiple times, anyone can tell that these signatures have been generated by the same group member. Applications include leaking sequences of secrets and e-voting [20].

Linkable Threshold Ring Signatures. In [20], a (d, n)-threshold extension to its original linkable ring signature scheme is constructed by concatenating d linkable ring signatures. We note that the construction, though simple and trivial, is not efficient. In particular, the space and time complexities are both $O(dn)$. We give in this paper a construction with time and space complexities both being $O(n)$.

Separability. In [8], Camenisch, et. al. diversified the concept of separability of cryptographic protocols into *perfect separability*, *strong separability* and *weak separability* when describing the users' ability to choose their own cryptographic primitive and system parameters. Separability is of particular importance for ring signature schemes as there is no group manager to coordinate the choice of signature primitive and system parameters for each user. For instance, a ring signature scheme that is only weak separable is not practical at all as it is unlikely to have all group members using the same primitive, system parameters and security parameters. The RSA implementation of [22, 1, 19, 24, 20] are strongly separable while the DL implementation of [1, 19, 20] are only weakly separable.

Event-Oriented Linkability. In [20], one can tell if two ring signatures are linked or not if and only if they are signed on behalf of the same group of members. We call this "*group-oriented*" linkability. We present a new linking criterion that we call "*event-oriented*" linkability in which one can tell if two signatures are linked if and only if they are signed for the same event, despite the fact that they may be signed on behalf of different groups. Event-oriented linkable ring signatures are comparatively more flexible in application. E.g., group settings keep changing frequently in ad-hoc group and most of the ring signatures are signed on behalf of different groups, thus render group-oriented linkability virtually useless. Consider another scenario: The CEOs of a company vote for business decisions. Using linkable ring signatures, they can vote anonymously by ring-signing their votes. However, as the group is fixed throughout the polls, votes among polls can be linked by anybody and information can be derived which means anonymity is in jeopardy. This can be prevented when an event-oriented scheme is used.

1.1 Contributions

Our main contributions include:

- We give the first separable linkable ring signature. It also the first linkable ring signature of the CDS-type ([11]).
- We present a security model for linkable threshold ring signature, and reduce the security of our scheme to well-known hard problem assumptions.
- Our scheme supports bandwidth-efficient threshold signing. The signature size in [20] is $O(dn)$ while ours is $O(n)$, where n is the number of users