Short Linkable Ring Signatures Revisited

Man Ho Au[1], Sherman S.M. Chow[2], Willy Susilo[1], and Patrick P. Tsang[3]

[1] Center for Information Security Research
School of Information Technology and Computer Science
University of Wollongong, Wollongong 2522, Australia
{mhaa456, wsusilo}@uow.edu.au
[2] Department of Computer Science
Courant Institute of Mathematical Sciences
New York University, NY 10012, USA
schow@cs.nyu.edu
[3] Department of Computer Science
Dartmouth College, Hanover, NH 03755, USA
patrick@cs.dartmouth.edu

Abstract. Ring signature is a group-oriented signature in which the signer can spontaneously form a group and generate a signature such that the verifier is convinced the signature was generated by one member of the group and yet does not know who actually signed. Linkable ring signature is a variant such that two signatures can be linked if and only if they were signed by the same person.

Recently, the first short linkable ring signature has been proposed. The short signature length makes it practical all of a sudden to use linkable ring signature as a building block in various cryptographic applications. However, we observed a subtle and yet imperative blemish glossed over by their security model definition which, if not carefully understood and properly handled, could lead to unanticipated security threats.

Inspired by the recent refinement of security definitions in conventional ring signatures, we formalize a new and better security model for linkable ring signature schemes that takes into account realistic adversarial capabilities. We show that the new model is *strictly stronger* than all existing ones in the literature. Under our new model, we propose a new short linkable ring signature scheme, improved upon the existing scheme.

Keywords: ring signature, linkable ring signature, short signature.

1 Introduction

Ring signatures, introduced by Rivest, Shamir and Tauman [19], are characterized by three main properties: anonymity, spontaneity, and unlinkability. Anonymity in ring signatures means 1-out-of-n signer verifiability, which enables the signer to keep anonymous in these "rings" of diversion signers. Spontaneity is a property which makes distinction between ring signatures and group signatures [8]. In group signature schemes, there exists a trusted third party (TTP), usually known as the group manager, who handles the joining of group members

A.S. Atzeni and A. Lioy (Eds.): EuroPKI 2006, LNCS 4043, pp. 101–115, 2006.

by interacting with them. In ring signature schemes, no such trusted party exists and the rest of the $n-1$ members in the ring can be totally unaware that they have been included in the ring. Unlinkability is another notion related to privacy – two ring signatures issued by the same signer are unlinkable in any way, except the very fact that this signer appears in the rings of both ring signatures. These three properties make ring signatures widely applicable to various cryptographic schemes [2, 9, 13]. Taking the example of concurrent signatures [9, 13] which is a partial solution to the fair exchange of signatures without TTPs, anonymity provides the signer-ambiguity of signatures (before they are exchanged) and the spontaneity enables a solution without TTPs. Survey of ring signatures and related applications can be found in [12, 20].

A twist in this paradigm is linkable ring signatures [16], which make it possible to identify whether two ring signatures were actually issued by the same signer, but still impossible to identify who the signer was. This reduced level of anonymity is known as linkable-anonymity, or pseudonymity. Linkable-anonymity renders ring signatures a useful building block in various cryptographic applications with privacy concerns. In [21], applications of linkable ring signatures in e-cash, e-voting and attestation were discussed. We briefly describe the case for e-cash here. Two obvious security requirements of an e-cash system are user anonymity and the capability of detecting double spending. The anonymity set of ring signature is the set of e-coins issued by the bank thus far (i.e. each pair of keys represents a coin). When a user spends, he/she use one of the signing keys among the e-coins to sign a ring signature on a transaction transcript. Ring signatures guarantee that one e-coin honestly spent in a transaction is (computationally) indistinguishable from another, thereby protecting the anonymity of the user. Linkability comes to play in double spending detection since it is possible to tell whether or not two signatures were signed using the same key, semantically implying whether the same e-coin has been spent twice.

The efficiency of ring signatures obviously determines the efficiency (and thus practicality) of these cryptographic applications. Researches have been directed toward goals such as improving the security of the scheme (e.g. [4, 11], the running time of signature generation (e.g. [10]), or the space complexity of the signature (e.g. [14, 21]). Recently, the first *short* linkable ring signature scheme has been proposed [21]. This nice property increases the practicality of ring signature as a building block of cryptographic applications.

1.1 Our Contributions

In this work we first point out a subtle blemish in the security model for linkable ring signature in [21]. Namely their security model glossed over the existence of an empowered central authority. We discuss the possible security threats when their scheme is instantiated without carefully addressing the issue.

Secondly, we survey the literature on the security models proposed for linkable ring signatures and formalize a new one that is the *strongest* among the all. We do an in-depth comparison among the new one and existing ones, and argue the necessity of our new model by showing the fact that it takes into account