Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups
(Extended Abstract)

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

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

Abstract. We present a linkable spontaneously anonymous group (LSAG) signature scheme (alternatively known as linkable ring signature scheme) satisfying the following three properties. (1) Anonymity, or signer indistinguishability. (2) Linkability: That two signatures by the same signer can be linked. (3) Spontaneity: No group secret, therefore no group manager or group secret sharing setup. We reduce the security of our scheme to well-known problems under the random oracle model. Using the scheme, we construct a new efficient one-round e-voting system which does not have a registration phase. We also present a new efficient reduction of famous rewind simulation lemma which only relies on elementary probability theory. Threshold extensions of our scheme are also presented.

1 Introduction

We present a 1-out-of-n group signature scheme which satisfy three properties: (1) Anonymity, or signer-indistinguishability. (2) Linkability: That two signatures by the same signer can be linked. (3) Spontaneity: No group secret, and thus no group manager or secret-sharing setup stage.

A 1-out-of-n group signature scheme allows any member of a group of n signers to generate a signature such that any public verifier can determine if the signature is generated by a group member. They are typically achieved by generating a group secret and then share it out using centralized methods (with group manager) or distributed methods (with a all-n-member secret sharing setup stage) [8,9,5,6].

⋆ The work described in this paper was fully supported by a grant from CityU (Project No. 7200005).

H. Wang et al. (Eds.): ACISP 2004, LNCS 3108, pp. 325–335, 2004.

In Cramer, et al. [10] and Rivest, et al. [18] a new paradigm for achieving 1-out-of-n group signature is presented. Any single user/signer can conscript the public keys of $n-1$ other users to form a group of n members. Then a signature can be generated by that single signer which can be publicly verified to be signed by one of the n group members. But the group formation and the signature generation are both *spontaneous*, meaning that no participation or even knowledge of the other $n-1$ users are needed. The 1-out-of-n signature generated this way is also anonymous (signer indistinguishable). Furthermore the anonymity is unconditional (information-theoretic) and exculpable (signer anonymous even after subpoenaing all n secret keys and all communications transcripts). Rivest, et al. [18] formalized this kind of signature to be 'Ring Signature' because their construction of the signature forms a ring structure. Some other works in the literature also call this kind of signature (with the above properties) 'Ring Signature' although some of them may not have a ring structure for their construction. In alternative terminology, we call this kind of signature 'Spontaneous Anonymous Group (SAG) Signature' as they fulfill Spontaneity, Anonymity and Group properties regardless of the construction structure.

This paradigm of SAG signature schemes have found many applications where maximum or near maximum privacy protection is needed such as whistle blowing. It has also found applications in group signatures for *ad hoc groups* where group secret setup and maintenance are too expensive due to frequent membership joins and drops. This kind of structure raises new challenges for security issues as the instance of ad hoc groups are not dependent on any particular network infrastructure. For example, a group of users who spontaneously decide to communicate some sensitive data which do not involve any trusted third party for participation while privacy need to be preserved at the same time. SAG signatures are perfectly suited to such situation due to its spontaneity property. Additional works on this topic includes [1,3,4,20,19,15].

In this paper, we present linkable SAG (LSAG) signatures. Linkability means two signatures by the same actual signer can be identified as such, but the signer remains anonymous.

There are several applications of the new LSAG signatures. (1) Linked whistle-blowing. SAG signature can be used to leak secret information [18]. However, some media or journalists may not believe what the secret leaker tells and may think that he is telling lies. They may only believe two or three different sources with the same piece of information. In this case, SAG signature cannot be used as one cannot distinguish whether two different SAG signatures are generated by the same signer or not. Instead, LSAG should be used to allow people to verify that two given signatures are in fact generated by two distinct signers. (2) A new efficient e-voting system can be built upon LSAG signatures. This new e-voting system has efficiency advantage in eliminating one of three typical phases in e-voting systems. Typical e-voting systems have three major phases: Registration, Voting, Vote Opening and Tallying Phases. Our e-voting eliminates the Registration phase, and thus achieve great efficiency and user friendliness.