On the Security Models of (Threshold) Ring Signature Schemes

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. We make fine-grained distinctions on the security models for provably secure ring signature schemes. Currently there are two commonly used security models which are specified by Rivest et al. [15] and Abe et al. [1]. They offer different levels of security. In this paper, we introduce a new but compatible model whose security level can be considered to be lying in between these two commonly used models. It is important to make fine-grained distinctions on the security models because some schemes may be secure in some of the models but not in the others. In particular, we show that the bilinear map based ring signature scheme of Boneh et al. [4], which have been proven secure in the weakest model (the one specified by Rivest et al. [15]), is actually insecure in stronger models (the new model specified by us in this paper and the one specified by Abe et al. [1]). We also propose a secure modification of their scheme for each of the two stronger models. In addition, we propose a threshold ring signature scheme using bilinear maps and show its security against adaptive adversaries in the strongest model defined in this paper. Throughout the paper, we carry out all of the security analyses under the random oracle assumption.

Keywords: Ring Signature, Security Models, Anonymity, Bilinear Maps.

1 Introduction

A ring signature scheme [15, 6, 1, 4, 17, 10] allows members of a group to sign messages on behalf of the group without revealing their identities (signer anonymity). It is also not possible to decide whether two signatures have been issued by the same group member. Different from a group signature scheme [8, 7, 2], the formation of a group is spontaneous and there is no group manager to revoke the

⋆ This work was fully supported by a grant from CityU (Project No. 9040904).

C. Park and S. Chee (Eds.): ICISC 2004, LNCS 3506, pp. 204–217, 2005.

identity of the signer. That is, under the assumption that each user is already associated with a public key of some 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.

Ring signatures could be used for whistle blowing [15], anonymous membership authentication for ad hoc groups [6] and many other applications which do not want complicated group formation stage but require signer anonymity. For example, in the whistle blowing scenario, a whistleblower gives out a secret as well as a ring signature of the secret to the public. From the signature, the public can be sure that the secret is indeed given out by a group member while cannot figure out who the whistleblower is. At the same time, the whistleblower does not need any collaboration of other users who have been conscripted by him into the group of members associated with the ring signature. Hence the anonymity of the whistleblower is ensured and the public is also certain that the secret is indeed leaked by one of the group members associated with the ring signature.

In 2002, Bresson et al. [6] extended the notion of ring signature schemes to a threshold setting and proposed the first threshold ring signature scheme. Later on, some other threshold ring signature schemes [16, 13] have been proposed. A t-out-of-n threshold ring signature scheme is defined as a ring signature scheme of which at least t corresponding private keys of n public keys are needed to produce a signature. The setup-free and signer anonymity properties of a conventional ring signature scheme are preserved in the threshold setting.

1.1 Contributions

We make fine-grained distinctions on the security models for provably secure ring signature schemes. Currently there are two commonly used security models which are specified by Rivest et al. [15] and Abe et al. [1]. They offer different levels of security. In this paper, we introduce a new but compatible model. Its security level can be considered to be lying in between these two commonly used models in such a way that it captures an attack called *group-changing attack* while it does not consider another attack called *multiple-known-signature existential forgery*.

It is important to make fine-grained distinctions on the security models because some schemes may be secure in some of the models but not in the others. In particular, we show that the bilinear map based ring signature scheme of Boneh et al. [4], which have been proven secure in the weakest model (the one specified by Rivest et al. [15]), is actually insecure in stronger models (the new model specified by us in this paper and the one specified by Abe et al. [1]). We show that their scheme is susceptible to group-changing attack and multiple-known-signature existential forgery. We also propose a secure modification of their scheme for each of the two stronger models.

In addition, we propose a threshold ring signature scheme using bilinear maps and show its security against adaptive adversaries in the strongest model defined