Dynamic Fully Anonymous Short Group Signatures

Cécile Delerablée[1] and David Pointcheval[2]

[1] France Telecom Division R&D, Issy-les-Moulineaux, France
cecile.delerablee@orange-ftgroup.com
[2] CNRS-ENS, Paris, France
david.pointcheval@ens.fr

Abstract. Group signatures allow members to sign on behalf of a group. Recently, several schemes have been proposed, in order to provide more *efficient* and *shorter* group signatures. However, this should be performed achieving a strong security level. To this aim, a formal security model has been proposed by Bellare, Shi and Zang, including both dynamic groups and concurrent join. Unfortunately, very few schemes satisfy all the requirements, and namely the shortest ones needed to weaken the anonymity notion.

We present an extremely short dynamic group signature scheme, with concurrent join, provably secure in this model. It achieves stronger security notions than BBS, and namely the full anonymity, while still shorter. The proofs hold under the q-SDH and the XDH assumptions, in the random oracle model.

1 Introduction

Group signature schemes (thereafter denoted GSS) have been introduced by Chaum and van Heyst [12], in order to provide revocable anonymity to the signer, who is allowed to sign on behalf of a group. In such a scheme, an authority is able, in exceptional cases, to "open" any group signature, and thus recover the actual signer. Properties of group signature schemes make them very important cryptographic tools, with lots of applications (voting, bidding, *anonymous attestation*).

For many years, several GSS have been introduced, and namely the famous ACJT [1], which was the first provably secure coalition-resistant scheme, under the Strong RSA and DDH assumptions. More recently, Boneh, Boyen and Shacham (BBS) [6], and Camenisch and Lysyanskaya [11], proposed very efficient group signature schemes using bilinear maps. The former provides very short group signatures. Independently, Nguyen and Safavi-Naini (NS) [19] also proposed another group signature scheme using bilinear maps. Note that all these schemes were analyzed in the random oracle model [3].

Bellare, Micciancio and Warinschi (BMW) [2] gave formal definitions of the security properties of group signatures, and proposed the first scheme provably secure in the standard model (while totally unpractical). Independently, Kiayias

P.Q. Nguyen (Ed.): VIETCRYPT 2006, LNCS 4341, pp. 193–210, 2006.

and Yung [16] (and later [17]), also defined a security model. Bellare, Shi and Zhang (BSZ) [4] extended the BMW model to the case of dynamic groups. Unforgeability and anonymity are indeed crucial security notions, but they should be guaranteed even if the adversary is allowed to play various attack games: adaptively open signatures, join any user of his choice (dynamic group [4]), possibly concurrently (concurrent join [17]).

However, in several schemes, this model has been "weakened", to obtain better efficiency, or to fit with the actually achieved security notions, as done in BBS with CPA-full-anonymity, a weaker version of anonymity where the adversary is not allowed to open signatures when trying to break the anonymity notion. Very recently, Boyen and Waters [8] proposed the first *efficient* GSS that is provably secure without random oracles, but with an important loss of efficiency. Indeed, the length of group signatures grows according to the number of users, and the group public key too.

1.1 Motivations and Related Work

Recently, several schemes have been proposed, in order to reduce the computational cost and the size of group signatures. In particular, BBS [6] is the most efficient one, and provides the shortest signatures so far. But they are still quite large if one compares to short classical signatures [7], and very short group signatures would be of great interest too.

Furthermore, the security level provided by BBS signatures does not fit in the security models proposed by Bellare et al. [2,4]. Namely, *anonymity* is no longer formally guaranteed as soon as one signature is open. However, such an opening process is expected to happen, hence the importance of anonymity as defined in [2]: it must be guaranteed, even if the adversary can see/ask for several openings. Moreover, *non-frameability*, as defined in BSZ is not guaranteed, because the group manager is able to sign on behalf of any group member. However, the authors suggest a possible way to fix this security problem, what we exploited, as explained below. In NS [19], the (full) anonymity is guaranteed, but the computational cost and the size of the group signatures are larger, compared to BBS. Furthermore, while NS claims to be in the BSZ security model, an adaptive access to the join oracle is not properly dealt in the security proofs, and namely for the traceability.

Adaptive, together with concurrent join is specifically considered by Kiayias and Yung [17]. It is indeed a very attractive property since it allows for several users to register at the same time, which could not be avoided (without a drastic efficiency reduction) in many applications (Internet-based for example) However, their scheme provides quite long signatures, with quite high computational cost.

A weakness in the BSZ model is the lack of revocation procedure. They gave some reasons for that, however, revocation of group members is usually a major issue in practice, one has to deal with for an actual scheme.