Shorter Verifier-Local Revocation Group Signatures from Bilinear Maps*

Sujing Zhou and Dongdai Lin

SKLOIS Lab, Institute of Software,
Chinese Academy of Sciences, Beijing, P.R. China
zhousujing@is.iscas.ac.cn, ddlin@is.iscas.ac.cn

Abstract. We propose a new computational complexity assumption from bilinear map, based on which we construct Verifier-Local Revocation group signatures with shorter lengths than previous ones.

Keywords: LRSW Assumption; Group Signature; Verifier-Local Revocation; Bilinear Map.

1 Introduction

Group signature [1] is motivated by enabling members of a group to sign on behalf of the group without leaking their own identities, and at the same time the signer's identity can be discovered by the group manager (GM) when a dispute occurs.

In brief, a group signature scheme is a signature scheme that has multiple secret keys corresponding to a single public key. A group signature should at least include the following five algorithms: Setup, Join, GSig, GVer and Open. Setup is executed by the group manager (GM); Join is an interactive protocol between a group member and GM or a separate issuing authority (IA); GSig is an algorithm run by any group member; any one can execute GVer to check the validity of a given group signature; Open is used by GM or a separate opening authority (OA) to find the identity of the signer given a group signature.

Various applications have been found for group signature schemes, such as anonymous authentication, internet voting and bidding. But wide implementation of group signatures in the real world has been prevented because of some factors, among which is efficient membership revocation as pointed out in [2].

Nontrivial resolutions to membership revocation have been proposed with regard to specific group signature schemes. The resolutions can be classified into two categories. One is based on *witness* [3,4,5], another is based on revocation list (RL) [6,7]. Resolutions based on witness is advantageous over the latter in that growing revocation lists are not needed to maintain, but in some applications RL based revocations are more suitable because they admit shorter signature size [8].

* Supported by 973 Project of China (No.2004CB318004), 863 Project of China (No. 2003AA144030) and NSFC90204016.

D. Pointcheval, Y. Mu, and K. Chen (Eds.): CANS 2006, LNCS 4301, pp. 126–143, 2006.

RL Based Revocation. In this category, a natural resolution is to let GM issue a revocation list of identities (public membership keys) RL, any group member proves in a zero-knowledge way that his identity hidden in the group signature is not equal to any one in RL[6]. The drawback is that signature size is linearly dependent on the size of RL.

[7] improved the above approach resulting in a scheme that signature size and computation are constant while the complexity of GVer is linearly dependent on the size of RL. In this resolution, GM publishes a RL which includes $V_i = f(pcert_i)$, i.e., evaluations of one way function f on partial certificate information $pcert_i$ which is unique to each group member. In signing a message, member i includes a random R, and $T = f'(V_i, R)$ (f' is another one way function which may equal f) in the group signature. Verifiers check if $T = f'(V_i, R)$ by trying every V_i in the current RL.

The idea of [7] is followed by [8,9] etc., and is named *verifier-local revocation* (VLR) and formalized in [8]. Nakanishi et al. [9], however, pointed out previous VLR schemes have a drawback of backward linkability, and proposed another VLR scheme based on [8] with the feature of backward unlinkability (BU), i.e., group signatures generated by the same group member is unlinkable except himself and GM, even after this member has been revoked (his/her revocation token is published).

Contributions. We propose a new computational complexity assumption from bilinear map, and a new standard signature, two new verifier-local revocation group signature, one without backward unlinkability, another with backward unlinkability, based on our assumption. The proposed group signature schemes are more efficient both in signature length and signature generation/verification than previous ones.

Organization. Our new complexity assumption and the new standard signature are described in Section 3. The proposed new group signatures from bilinear map are presented in Section 5, with corresponding security proofs provided in Appendixes.

2 Preliminaries

Suppose that $G_1 = \langle g \rangle$, $G_2 = \langle \tilde{g} \rangle$ and G_3 are multiplicative cyclic groups of prime order p, there exists an efficient non-degenerate bilinear map $e : G_1 \times G_2 \rightarrow G_3$, i.e., $e(u^a, v^b) = e(u, v)^{ab}$ for any $u \in G_1$, $v \in G_2$, $a, b \in Z_p$, and $e(g, \tilde{g}) \neq 1$.

Definition 1 (LRSW Assumption [10]). *Suppose G_1, G_2, G_3 are defined as above and generated by a setup algorithm. Let $\widetilde{X} = \tilde{g}^x$, $\widetilde{Y} = \tilde{g}^y$, $O_{x,y}(.)$ be an oracle that, on input a value $m \in Z_p^*$, outputs a triple (a, a^y, a^{x+mxy}) for a randomly chosen $a \in G_1$. Then for any probabilistic polynomial time (PPT) bounded adversary $\mathcal{A}$, the following probability is negligible:*

$$\Pr\{(p, G_1, G_2, G_3, e) \leftarrow Setup(1^k); x \xleftarrow{R} Z_p^*; y \xleftarrow{R} Z_p^*; \widetilde{X} = \tilde{g}^x; \widetilde{Y} = \tilde{g}^y;$$
$$(m, a, b, c) \leftarrow \mathcal{A}^{O_{x,y}}(g, \tilde{g}, e, \widetilde{X}, \widetilde{Y}) : m \in Z_p^* \backslash Q \wedge a \in G_1 \wedge b = a^y \wedge c = a^{x+mxy}\} < \epsilon,$$

where Q is the set of queries that $\mathcal{A}$ has made to $O_{x,y}(.)$.