Cryptology ePrint Archive: Report 2011/363

Dynamic Group Blind Signatures

Essam Ghadafi

Abstract: Group signatures provide authenticity of a message while maintaining singer's privacy. A blind signature on the other hand allows a user to obtain a signature while maintaining the privacy of the message. Group blind signatures combine properties of both group signatures and blind signatures and therefore offer a stronger notion of anonymity where both the message to be signed and the identity of the signer remain anonymous. Group blind signatures have many useful applications in practice; including multi-authority e-voting systems and distributed e-cash systems.

In this paper, we first present a formalized security model for dynamic group blind signatures and then we propose a new group blind signature scheme which has a round-optimal signing protocol and yet does not rely on random oracles which is to the best of our knowledge the first scheme with such properties. Most of the previous schemes in the literature require either lengthy (many-round) signing protocols and/or random oracles to prove their security. Our scheme also allows for concurrent joining and yields signatures of a constant-size. In addition, the new variant of the Camenisch-Lysyanskaya signature scheme which we introduce and use for the joining protocol is of interest in its own right and could be used either on its own to sign group elements or as a building block for other cryptographic constructions.

Category / Keywords: public-key cryptography/ Group Signatures, lind Signatures, Group Blind Signatures, Security Model

Date: received 5 Jul 2011, last revised 19 Jul 2011, withdrawn 24 Jul 2011

Contact author: ghadafi at cs bris ac uk

Available formats: (-- withdrawn --)

Note: Under update. Will be available shortly.

Version: 20110724:090614 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]