Cryptology ePrint Archive: Report 2011/402

Formalizing Group Blind Signatures and Practical Constructions without Random Oracles

Essam Ghadafi

Abstract: In this paper, we first provide foundations for dynamic group blind signatures where we provide formal security definitions and present a security model to capture all the security properties. In doing so, we identify and address some issues which were not considered by previous constructions and (informal) security definitions.

We then present a practical scheme which has a round-optimal signing phase and yields signatures of a constant-size. Our scheme allows for members of the group to join dynamically and concurrently. The security of our scheme does not rely on any idealized assumptions.

In addition, the building blocks we present are of interest in their own right and could be used either on their own or as building blocks for other cryptographic constructions.

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

Date: received 27 Jul 2011, last revised 14 Aug 2011

Contact author: ghadafi at cs bris ac uk