Cryptology ePrint Archive: Report 2013/020

Aggregate and Verifiably Encrypted Signatures from Multilinear Maps Without Random Oracles

Markus Rückert and Dominique Schroeder

Abstract: Aggregate signatures provide bandwidth-saving aggregation of ordinary signatures. We present the first unrestricted instantiation in the standard model, Moreover, our construction yields a multisignature scheme where a single message is signed by a number of signers. Our second result is an application to verifiably encrypted signatures. There, signers encrypt their signature under the public key of a trusted third party and output a proof that the signature is inside. Upon dispute between signer and verifier, the trusted third party is able to recover the signature. These schemes are provably secure in the standard model.

Category / Keywords: public-key cryptography / Aggregate Signatures

Publication Info: ISA 2009

Date: received 12 Jan 2013

Contact author: schroeder at me com