Cryptology ePrint Archive: Report 2011/342

A Domain Transformation for Structure-Preserving Signatures on Group Elements

Melissa Chase and Markulf Kohlweiss

Abstract: We present a generic transformation that allows us to use a large class of pairing-based signatures to construct schemes for signing group elements in a structure preserving way. As a result of our transformation we obtain a new efficient signature scheme for signing a vector of group elements that is based only on the well established decisional linear assumption (DLIN). Moreover, the public keys and signatures of our scheme consist of group elements only, and a signature is verified by evaluating a set of pairing-product equations. In combination with the Groth-Sahai proof system, such a signature scheme is an ideal building block for many privacy-enhancing protocols.

To do this, we start by proposing a new stateful signature scheme for signing vectors of exponents that is F-unforgeable under weak chosen message attacks. This signature scheme is of independent interest as it is compatible with Groth-Sahai proofs and secure under a computational assumption implied by DLIN. Then we give a general transformation for signing group elements based on signatures (for signing exponents) with efficient non-interactive zero-knowledge proofs. This transform also removes any dependence on state in the signature used to sign exponents. Finally, we obtain our result by instantiating this transformation with the above signature scheme and Groth-Sahai proofs.

Category / Keywords: public-key cryptography / structure preserving signatures

Date: received 23 Jun 2011

Contact author: melissac at microsoft com