Cryptology ePrint Archive: Report 2013/179

Malleable Signatures: Complex Unary Transformations and Delegatable Anonymous Credentials

Melissa Chase and Markulf Kohlweiss and Anna Lysyanskaya and Sarah Meiklejohn

Abstract: A signature scheme is malleable if, on input a message m and a signature σ, it is possible to efficiently compute a signature σ' on a related message $m' = T(m)$, for a transformation T that is allowable with respect to this signature scheme. Previous work considered various useful flavors of allowable transformations, such as quoting and sanitizing messages. In this paper, we explore a connection between malleable signatures and anonymous credentials, and give the following contributions:

-We define and construct malleable signatures for a broad category of allowable transformation classes, with security properties that are stronger than those that have been achieved previously. Our construction of malleable signatures is generically based on malleable zero-knowledge proofs, and we show how to instantiate it under the Decision Linear assumption.

-We construct delegatable anonymous credentials from signatures that are malleable with respect to an appropriate class of transformations; we also show that our construction of malleable signatures works for this class of transformations. The resulting concrete instantiation is the first to achieve security under a standard assumption (Decision Linear) while also scaling linearly with the number of delegations.

Category / Keywords: cryptographic protocols / malleability, signatures, anonymity

Date: received 29 Mar 2013

Contact author: smeiklej at cs ucsd edu