Cryptology ePrint Archive: Report 2013/130

Blank Digital Signatures

Christian Hanser and Daniel Slamanig

Abstract: In this paper we present a novel type of digital signatures, which we call blank digital signatures. The basic idea behind this scheme is that an originator can define and sign a message template, describing fixed parts of a message as well as multiple choices for exchangeable parts of a message. One may think of a form with blank fields, where for such fields the originator specifies all the allowed strings to choose from. Then, a proxy is given the power to sign an instantiation of the template signed by the originator by using some secret information. By an instantiation, the proxy commits to one allowed choice per blank field in the template. The resulting message signature can be publicly verified under the originator's and the proxy's signature verification keys. Thereby, no verifying party except the originator and the proxy learn anything about the ``unused'' choices from the message template given a message signature. Consequently, the template is hidden from verifiers.

We discuss several applications, provide a formal definition of blank digital signature schemes and introduce a security model. Furthermore, we provide an efficient construction of such a blank digital signature scheme from any secure digital signature scheme, pairing-friendly elliptic curves and polynomial commitments, which we prove secure in our model. We also provide a detailed efficiency analysis of our proposed construction supporting its practicality. Finally, we outline several open issues and extensions for future work.

Category / Keywords: public-key cryptography / Digital signature scheme, blank digital signatures, elliptic curves, pairings, polynomial commitments

Publication Info: revised version of paper to appear at AsiaCCS 2013

Date: received 5 Mar 2013, last revised 23 May 2013

Contact author: christian hanser at iaik tugraz at