Cryptology ePrint Archive: Report 2013/217

Computing on Authenticated Data for Adjustable Predicates

Björn Deiseroth and Victoria Fehr and Marc Fischlin and Manuel Maasz and Nils Fabian Reimers and Richard Stein

Abstract: The notion of P-homomorphic signatures, introduced by Ahn et al. (TCC 2012), generalizes various approaches for public computations on authenticated data. For a given predicate P anyone can derive a signature for a message m' from the signatures of a set of messages M, as long as P(M,m')=1. This definition hence comprises notions and constructions for concrete predicates P such as homomorphic signatures and redactable signatures.

In our work we address the question of how to combine Pi-homomorphic schemes for different predicates P1,P2,... to create a richer and more flexible class of supported predicates. One approach is to statically combine schemes for predicates into new schemes for logical formulas over the predicates, such as a scheme for AND (P1 AND P2). The other approach for more flexibility is to derive schemes which allow the signer to dynamically decide which predicate to use when signing a message, instead of supporting only a single, fixed predicate.

We present two main results. One is to show that one can indeed devise solutions for the static combination for AND, and for dynamically adjustable solutions for choosing the predicate on the fly. Moreover, our constructions are practical and add only a negligible overhead. The other main result is an impossibility result for static combinations. Namely, we prove that, in contrast to the case of AND, many other formulas like the logical OR (P1 OR P2) and the NOT (NOT P) do not admit generic combinations through so-called canonical constructions. This implies that one cannot rely on general constructions in these cases, but must use other methods instead, like finding new predicate-specific solutions from scratch.

Category / Keywords: public-key cryptography / Signatures, homomorphic, redactable, predicate

Publication Info: ACNS 2013

Date: received 12 Apr 2013

Contact author: marc fischlin at gmail com