Cryptology ePrint Archive: Report 2013/034

New Smooth Projective Hash Functions and One-Round Authenticated Key Exchange

Fabrice Ben Hamouda and Olivier Blazy and Céline Chevalier and David Pointcheval and Damien Vergnaud

Abstract: Password-Authenticated Key Exchange (PAKE) has received deep attention in the last few years, with a recent improvement by Katz-Vaikuntanathan, and their one-round protocols: the two players just have to send simultaneous flows to each other, that depend on their own passwords only, to agree on a shared high entropy secret key. To this aim, they followed the Gennaro-Lindell approach, with a new kind of Smooth-Projective Hash Functions (SPHF). They came up with the first concrete one-round PAKE, secure in the Bellare-Pointcheval-Rogaway model, but at the cost of a simulation-sound NIZK, which makes the overall construction not really efficient.

This paper follows their path with a new efficient instantiation of SPHF on Cramer-Shoup ciphertexts. It then leads to the design of the most efficient PAKE known so far: a one-round PAKE with two simultaneous flows consisting of 6 group elements each only, in any DDH-group without any pairing. We thereafter show a generic construction for SPHFs, in order to check the validity of complex relations on encrypted values. This allows to extend this work on PAKE to the more general family of protocols, termed Langage-Authenticated Key Exchange (LAKE) by Ben Hamouda-Blazy-Chevalier-Pointcheval-Vergnaud, but also to blind signatures.

Category / Keywords: Authenticated Key Exchange, Blind Signatures, Smooth Projective Hash Functions

Date: received 24 Jan 2013, last revised 15 Feb 2013

Contact author: olivier blazy at rub de

Available formats: PDF | BibTeX Citation