Cryptology ePrint Archive: Report 2011/270

Programmable Hash Functions and Their Applications

Dennis Hofheinz and Eike Kiltz

Abstract: We introduce a new combinatorial primitive called *programmable hash functions* (PHFs). PHFs can be used to *program* the output of a hash function such that it contains solved or unsolved discrete logarithm instances with a certain probability. This is a technique originally used for security proofs in the random oracle model. We give a variety of *standard model* realizations of PHFs (with different parameters).

The programmability makes PHFs a suitable tool to obtain black-box proofs of cryptographic protocols when considering adaptive attacks. We propose generic digital signature schemes from the strong RSA problem and from some hardness assumption on bilinear maps that can be instantiated with any PHF. Our schemes offer various improvements over known constructions. In particular, for a reasonable choice of parameters, we obtain short standard model digital signatures over bilinear maps.

Category / Keywords: public-key cryptography / hash functions, digital signatures, standard model

Publication Info: Short version appeared at Crypto 2008. This is the full version.

Date: received 27 May 2011

Contact author: Dennis Hofheinz at kit edu