Cryptology ePrint Archive: Report 2013/145

Key Wrapping with a Fixed Permutation

Dmitry Khovratovich

Abstract: We present an efficient key wrapping scheme that uses a single wide permutation and does not rely on block ciphers. The scheme is capable of wrapping keys up to 1400 bits long and processing arbitrarily long headers. Our scheme easily delivers the security level of 128 bits or higher with the master key of the same length. The permutation can be taken from the sponge hash functions such as SHA-3 (Keccak), Quark, Photon, Spongent.

We also present a simple proof of security within the concept of Deterministic Authenticated Encryption (DAE) introduced by Rogaway and Shrimpton. We extend the setting by allowing the adversary to query the permutation and following the indifferentiability setting in the security proof of the sponge construction.

Category / Keywords: secret-key cryptography / Key wrapping, DAE, sponge, Keccak

Date: received 11 Mar 2013

Contact author: khovratovich at gmail com, dmitry khovratovich@uni lu