Cryptology ePrint Archive: Report 2011/499

Duplexing the sponge: single-pass authenticated encryption and other applications

Guido Bertoni and Joan Daemen and Michaël Peeters and Gilles Van Assche

Abstract: This paper proposes a novel construction, called duplex, closely related to the sponge construction, that accepts message blocks to be hashed and, at no extra cost, provides digests on the input blocks received so far. It can be proven equivalent to a cascade of sponge functions and hence inherits its security against single-stage generic attacks. The main application proposed here is an authenticated encryption mode based on the duplex construction. This mode is efficient, namely, enciphering and authenticating together require only a single call to the underlying permutation per block, and is readily usable in, e.g., key wrapping. Furthermore, it is the first mode of this kind to be directly based on a permutation instead of a block cipher and to natively support intermediate tags. The duplex construction can be used to efficiently realize other modes, such as a reseedable pseudo-random bit sequence generators and a sponge variant that overwrites part of the state with the input block rather than to XOR it in.

Category / Keywords: foundations / sponge functions, duplex construction, authenticated encryption, key wrapping, provable security, pseudo-random bit sequence generator, Keccak

Publication Info: Extended version of the paper to appear in SAC 2011

Date: received 14 Sep 2011

Contact author: gilles vanassche at st com

Available formats: PDF | BibTeX Citation

Version: 20110918:014604 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]