Cryptology ePrint Archive: Report 2011/459

Sufficient conditions for sound hashing using a truncated permutation

Joan Daemen and Tony Dusenge and Gilles Van Assche

Abstract: In this paper we give a generic security proof for hashing modes that make use of an underlying fixed-length permutation. We formulate a set of five simple conditions, which are easy to implement and to verify, for such a hashing mode to be sound. These hashing modes include tree hashing modes and sequential hashing modes. We provide a proof that for any hashing mode satisfying the five conditions, the advantage in differentiating it from an ideal monolithic hash function is upper bounded by q^2/2^{n+1} with q the number of queries to the underlying permutation and n the length of the chaining values.

Category / Keywords: foundations / permutation-based hashing, indifferentiability, tree hashing

Date: received 22 Aug 2011

Contact author: gilles vanassche at st com