Cryptology ePrint Archive: Report 2011/623

Indifferentiability of the Hash Algorithm BLAKE

Donghoon Chang and Mridul Nandi and Moti Yung

Abstract: The hash algorithm BLAKE, one of the SHA-3 finalists, was designed by Aumasson, Henzen, Meier, and Phan. Unlike other SHA-3 finalists, there is no known indifferentiable security proof on BLAKE. In this paper, we provide the indifferentiable security proof on BLAKE with the bound O(\delta^2/2^{n-3}), where \delta is the total number of blocks of queries, and n is the hash output size.

Category / Keywords: hash function

Date: received 18 Nov 2011, last revised 18 Nov 2011

Contact author: pointchang at gmail com