Cryptology ePrint Archive: Report 2011/422

Improved Analysis of ECHO-256

Jérémy Jean and María Naya-Plasencia and Martin Schläffer

Abstract: ECHO-256 is a second-round candidate of the SHA-3 competition. It is an AES-based hash function that has attracted a lot of interest and analysis. Up to now, the best known attacks were a distinguisher on the full internal permutation and a collision on four rounds of its compression function. The latter was the best known analysis on the compression function as well as the one on the largest number of rounds so far. In this paper, we extend the compression function results to get a distinguisher on 7 out of 8 rounds using rebound techniques. We also present the first 5-round collision attack on the ECHO-256 hash function.

Category / Keywords: secret-key cryptography / hash function, cryptanalysis, rebound attack, collision attack, distinguisher

Publication Info: extended version of paper published at SAC 2011

Date: received 5 Aug 2011, last revised 5 Aug 2011

Contact author: martin schlaeffer at iaik tugraz at