Cryptology ePrint Archive: Report 2011/374

Restoring the Differential Resistance of MD6

Ethan Heilman

Abstract: These notes present new results to reestablish the differential resistance of MD6. In this paper we introduce a classification system of differential weight patterns that allows us to extend previous analysis to prove that MD6 is resistant to differential cryptanalysis. Our analysis allows us to more than double the security margin of MD6 against differential attacks.

Category / Keywords: foundations / cryptographic hash function

Publication Info: Differential Cryptanalysis, Cryptographic Hash Function, MD6, Computer Aided Proof

Date: received 10 Jul 2011, last revised 21 Sep 2011

Contact author: ethan at geographicslab org

Available formats: PDF | BibTeX Citation

Note: Added links to the source code since the source code has now been published online.

Version: 20110922:021654 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]