Cryptology ePrint Archive: Report 2011/037

Higher-Order Differential Attack on Reduced SHA-256

Mario Lamberger and Florian Mendel

Abstract: In this work, we study the application of higher-order differential attacks on hash functions. We show a second-order differential attack on the SHA-256 compression function reduced to 46 out of 64 steps. We implemented the attack and give the result in Table 1. The best attack so far (in a different attack model) with practical complexity was for 33 steps of the compression function.

Category / Keywords: hash functions, higher-order differentials, non-randomness, boomerang attack, SHA-256

Date: received 20 Jan 2011

Contact author: florian mendel at iaik tugraz at

Available formats: PDF | BibTeX Citation

Version: 20110121:040754 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]