Cryptology ePrint Archive: Report 2013/122

Practical collision attack on 40-step RIPEMD-128

Gaoli Wang

Abstract: RIPEMD-128 is an ISO/IEC standard cryptographic hash function proposed in 1996 by Dobbertin, Bosselaers and Preneel. There are two different and independent parallel lines called $line1$ operation and $line2$ operation, and each operation has 64 steps. The results of two line operations are combined at the end of every application of the compression function. In this paper, we present collision differential characteristics for both $line1$ operation and $line2$ operation by choosing a proper message difference. By using message modification technique seriously, we improve the probabilities of the differential characteristics so that we can give a collision attack on 40-step RIPEMD-128 with a complexity of 2^{35} computations.

Category / Keywords: secret-key cryptography / hash function

Date: received 28 Feb 2013

Contact author: wanggaoli at dhu edu cn