Cryptology ePrint Archive: Report 2011/286

Bicliques for Preimages: Attacks on Skein-512 and the SHA-2 family

Dmitry Khovratovich and Christian Rechberger and Alexandra Savelieva

Abstract: We present the new concept of biclique as a tool for preimage attacks, which employs many powerful techniques from differential cryptanalysis of block ciphers and hash functions.

The new tool has proved to be widely applicable by inspiring many authors to publish new results of the full versions of AES, KASUMI, IDEA, Square, and others. In this paper, we demonstrate how our concept results in the first cryptanalysis of the Skein hash function, and describe an attack on the SHA-2 hash function with more rounds than before.

Category / Keywords: secret-key cryptography /

Date: received 31 May 2011, last revised 7 Feb 2012

Contact author: khovratovich at gmail com, christian rechberger@groestl info,alexandra savelieva@gmail com

Available formats: PDF | BibTeX Citation

Version: 20120207:151720 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]