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 introduce a new concept in splice-and-cut attacks on hash functions, which bridges the gap between preimage attacks and a powerful method of differential cryptanalysis. The new concept is called biclique, for its system of equations resembling a complete bipartite graph. In view of the current SHA-3 competition, we apply our method to the finalist Skein and demonstrate the first attack on a 22-round version of Skein-512 in the most relevant hash function setting. Then we present the best attacks on the SHA-2 family of hash functions, breaking 45 out of the 64 rounds of SHA-256, 50 rounds of the 80 rounds of SHA-512, and many more rounds in the less relevant compression function setting.

Category / Keywords: secret-key cryptography /

Date: received 31 May 2011

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