Cryptology ePrint Archive: Report 2011/420

Unaligned Rebound Attack - Application to Keccak

Alexandre Duc, Jian Guo, Thomas Peyrin, Lei Wei

Abstract: We analyze the internal permutations of Keccak, one of the NIST SHA-3 competition finalists, in regard to differential properties. By carefully studying the elements composing those permutations, we are able to derive most of the best known differential paths for up to 5 rounds. We use these differential paths in a rebound attack setting and adapt this powerful freedom degrees utilization in order to derive distinguishers for up to 8 rounds of the internal permutations of the submitted version of Keccak. The complexity of the 8 round distinguisher is $2^{491.47}$. Our results have been implemented and verified experimentally on a small version of Keccak. This is currently the best known differential attack against the internal permutations of Keccak.

Category / Keywords: secret-key cryptography / Keccak, SHA-3, hash function, differential cryptanalysis, rebound attack

Date: received 3 Aug 2011, last revised 10 Nov 2011

Contact author: alexandre duc at epfl ch, ntu guo@gmail com, thomas peyrin@gmail com, wl@pmail ntu edu sg