Cryptology ePrint Archive: Report 2011/074

Really fast syndrome-based hashing

Daniel J. Bernstein and Tanja Lange and Christiane Peters and Peter Schwabe

Abstract: The FSB (fast syndrome-based) hash function was submitted to the SHA-3 competition by Augot, Finiasz, Gaborit, Manuel, and Sendrier in 2008, after preliminary designs proposed in 2003, 2005, and 2007. Many FSB parameter choices were broken by Coron and Joux in 2004, Saarinen in 2007, and Fouque and Leurent in 2008, but the basic FSB idea appears to be secure, and the FSB submission remains unbroken. On the other hand, the FSB submission is also quite slow, and was not selected for the second round of the competition.

This paper introduces RFSB, an enhancement to FSB. In particular, this paper introduces the RFSB-509 compression function, RFSB with a particular set of parameters. RFSB-509, like the FSB-256 compression function, is designed to be used inside a 256-bit collision-resistant hash function: all known attack strategies cost more than 2^128 to find collisions in RFSB-509. However, RFSB-509 is an order of magnitude faster than FSB-256. On a single core of a Core 2 Quad CPU, RFSB-509 runs at 13.62 cycles/byte: faster than SHA-256, faster than 6 of the 14 second-round SHA-3 candidates, and faster than 2 of the 5 SHA-3 finalists.

Category / Keywords: secret-key cryptography / compression functions, collision resistance,

Date: received 14 Feb 2011, last revised 14 May 2011

Contact author: tanja at hyperelliptic org

Available formats: PDF | BibTeX Citation

Note: Latest version. Faster than version in Africacrypt proceedings and full bibliographic information.

Version: 20110514:173625 (All versions of this report)

Discussion forum: Show discussion | Start new discussion
