Cryptology ePrint Archive: Report 2011/635

Groestl Tweaks and their Effect on FPGA Results

Marcin Rogawski and Kris Gaj

Abstract: In January 2011, Groestl team published tweaks to their specification of Groestl. In this paper, we investigate the influence of these tweaks on the Groestl performance in hardware. The results indicate that the performance penalty in terms of the throughput to area ratio depends strongly on the architecture used. This penalty is smaller in case of architecture in which permutations P and Q are implemented using two independent units.

Category / Keywords: implementation / SHA-3, hash functions, hardware, FPGA

Date: received 25 Nov 2011

Contact author: kgaj at gmu edu