# Cryptology ePrint Archive: Report 2013/113

### Compact Hardware Implementations of ChaCha, BLAKE, Threefish, and Skein on FPGA

*Nuray At and Jean-Luc Beuchat and Eiji Okamoto and Ismail San and Teppei Yamazaki*

**Abstract:** The cryptographic hash functions BLAKE and Skein are built from the ChaCha stream cipher and the tweakable Threefish block cipher, respectively. Interestingly enough, they are based on the same arithmetic operations, and the same design philosophy allows one to design lightweight coprocessors for hashing and encryption. The key element of our approach is to take advantage of the parallelism of the algorithms to deeply pipeline our Arithmetic an Logic Units, and to avoid data dependencies by interleaving independent tasks. We show for instance that a fully autonomous implementation of BLAKE and ChaCha on a Xilinx Virtex-6 device occupies 144 slices and three memory blocks, and achieves competitive throughputs. In order to offer the same features, a coprocessor implementing Skein and Threefish requires a substantial higher slice count.

**Category / Keywords:** implementation /

**Date:** received 25 Feb 2013, last revised 3 Mar 2013

**Contact author:** jeanluc beuchat at gmail com

**Available formats:** PDF | BibTeX Citation

**Version:** 20130303:144456 (All versions of this report)

**Discussion forum:** Show discussion | Start new discussion

---

[ Cryptology ePrint archive ]