Cryptology ePrint Archive: Report 2011/078

A Low-Area Unified Hardware Architecture for the AES and the Cryptographic Hash Function ECHO

Jean-Luc Beuchat and Eiji Okamoto and Teppei Yamazaki

Abstract: We propose a compact coprocessor for the AES (encryption, decryption, and key expansion) and the cryptographic hash function ECHO on Virtex-\$5\$ and Virtex-\$6\$ FPGAs. Our architecture is built around a \$8\$-bit datapath. The Arithmetic and Logic Unit performs a single instruction that allows for implementing AES encryption, AES decryption, AES key expansion, and ECHO at all levels of security. Thanks to a careful organization of AES and ECHO internal states in the register file, we manage to generate all read and write addresses by means of a modulo-\$16\$ counter and a modulo-\$256\$ counter. A fully autonomous implementation of ECHO and AES on a Virtex-\$5\$ FPGA requires \$193\$ slices and a single \$36\$k memory block, and achieves competitive throughputs. Assuming that the security guarantees of ECHO are at least as good as the ones of the SHA-\$3\$ finalists BLAKE and Keccak, our results show that ECHO is a better candidate for low-area cryptographic coprocessors. Furthermore, the design strategy described in this work can be applied to combine the AES and the SHA-\$3\$ finalist {G}r{\o}stl.

Category / Keywords: implementation / AES, ECHO, hash functions, implementation, SHA-3

Date: received 14 Feb 2011, last revised 22 May 2011

Contact author: jeanluc beuchat at gmail com

Available formats: PDF | BibTeX Citation

Version: 20110523:053753 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]