An Implementation and Experimental Evaluation of Hardware Accelerated Ciphers in All-Programmable SoCs

Title	An Implementation and Experimental Evaluation of Hardware Accelerated Ciphers in All-Programmable SoCs
Publication Type	Conference Paper
Year of Publication	2017
Authors	Cowart, R., Coe, D., Kulick, J., Milenkovi?, A.
Conference Name	Proceedings of the SouthEast Conference
Publisher	ACM
Conference Location	New York, NY, USA
ISBN Number	978-1-4503-5024-2
Keywords	AES, FPGAs, hardware acceleration, IP cores, Metrics, OpenSSL, pubcrawl, security metrics

Abstract

The protection of confidential information has become very important with the increase of data sharing and storage on public domains. Data confidentiality is accomplished through the use of ciphers that encrypt and decrypt the data to impede unauthorized access. Emerging heterogeneous platforms provide an ideal environment to use hardware acceleration to improve application performance. In this paper, we explore the performance benefits of an AES hardware accelerator versus the software implementation for multiple cipher modes on the Zynq 7000 All-Programmable System-on-a-Chip (SoC). The accelerator is implemented on the FPGA fabric of the SoC and utilizes DMA for interfacing to the CPU. File encryption and decryption of varying file sizes are used as the workload, with execution time and throughput as the metrics for comparing the performance of the hardware and software implementations. The performance evaluations show that the accelerated AES operations achieve a speedup of 7 times relative to its software implementation and throughput upwards of 350 MB/s for the counter cipher mode, and modest improvements for other cipher modes.

URL	https://dl.acm.org/citation.cfm?doid=3077286.3077297

DOI 10.1145/3077286.3077297
Citation Key cowart_implementation_2017

AES FPGAs hardware acceleration IP cores Metrics OpenSSL pubcrawl Security Metrics