Evaluation of DPA Protected Implementations of CAESAR Finalists ACORN and Ascon and other Candidates

William Diehl, Abubakr Abdulgadir, Farnoud Farahmand, Kris Gaj, and Jens-Peter Kaps
George Mason University, Fairfax, USA

Abstract

The Competition for Authenticated Encryption, Security, Applicability, and Robustness (CAESAR) seeks to identify a portfolio of authenticated ciphers that offer advantages over AES-GCM, and are suitable for widespread adoption based on three use cases: lightweight, high-speed, and defense in depth. In March 2018, ACORN and Ascon were selected as CAESAR contest finalists for the use case for lightweight applications, i.e., candidate ciphers that exhibit good performance in resource-challenged devices, such as small FPGAs or ASICs, and have natural side-channel resistance. In this presentation we present our latest results of our unprotected and side-channel resistant FPGA implementations of ACORN and Ascon as well as several other candidates, namely CLOC (AES and TWINE), SILC (AES, PRESENT, and LED), JAMBU (AES and SIMON), Ketje Jr., and AES-GCM. We demonstrate a methodology for analyzing a large group of authenticated ciphers for vulnerabilities to power analysis side-channel attack, and evaluation of the effectiveness of countermeasures. We use the Test Vector Leakage Assessment (TVLA) methodology using Welch's t-test, and upgrade the Flexible Open-source workBench fOr Side-channel analysis (FOBOS), to perform t-tests on authenticated ciphers. The FOBOS interface with the victim cipher implementation is standardized by leveraging the CAESAR Hardware Applications Programming Interface (API) for Authenticated Ciphers, which was adopted by the CAESAR committee in May 2016. Additionally, the use of the Development Package for the CAESAR Hardware API facilitates a repeatable and exportable test methodology for all CAESAR candidates. Finally, we benchmark unprotected and protected cipher implementations in the Spartan-6 FPGA, and compare the costs of 1st order DPA protection in terms of area, frequency, throughput, throughput-to-area (TP/A) ratio, power, and energy per bit. Based on our evaluation of ciphers using TVLA, our unprotected serial implementation of ACORN is close to having "natural side-channel resistance."