Notice and Invitation

Oral Defense of Doctoral Dissertation
The Volgenau School of Engineering, George Mason University

William Diehl
Bachelor of Arts, Duke University, 1991
Master of Science, Naval Postgraduate School, 2002

Comparing Costs of Protecting Secret Key Ciphers Against Differential Power Analysis

Tuesday, 24 April 2018, 2:30 – 3:30 pm
ENGR 3507
All are invited to attend.

Committee

Dr. Kris Gaj, Chair
Dr. Jens-Peter Kaps, Committee Member
Dr. Avesta Sasan, Committee Member
Dr. Paul Ammann, Committee Member

Abstract

Secret key ciphers, including block ciphers and authenticated ciphers, are vulnerable to side-channel attacks, including differential power analysis (DPA). The Test Vector Leakage Assessment (TVLA) methodology (i.e., t-test methodology) has been used to verify improved resistance of block ciphers to DPA after application of countermeasures. However, extension of the t-test methodology to authenticated ciphers is non-trivial, since authenticated ciphers require additional input and output conditions, complex interfaces, and long test vectors interlaced with protocol necessary to describe authenticated cipher operations.

In this research we augment an existing side-channel analysis framework (FOBOS) with TVLA methodology for authenticated ciphers. We use TVLA to show that implementations in the Spartan-6 FPGA of the CAESAR Round 3 candidates ACORN, ASCON, CLOC (AES and TWINE), SILC (AES, PRESENT, and LED), JAMBU (AES and SIMON), and Ketje Jr., as well as AES-GCM, are vulnerable to 1st order DPA. We then implement versions of the above ciphers, protected against 1st order DPA, using threshold implementations. The TVLA methodology is used to verify improved resistance to 1st order DPA of the protected cipher implementations. 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 (TP), throughput-to-area (TP/A) ratio, power, and energy per bit (E/bit).

The protected cipher implementation with the lowest area, TP/A ratio, power and E/bit is ACORN, while Ketje Jr. has the highest TP, second-highest TP/A ratio, and second-highest E/bit. On average, protected cipher implementations require 3.1 times as much area, while TP and TP/A decrease by factors of 1.8 and 5.6, respectively. Power and E/bit for protected cipher implementations increase on average by a factor of 3.4 compared to their unprotected versions. Additionally, the relative ranking of the top three candidates in terms of area, TP, and TP/A, do not change between unprotected and protected implementations.