GMU Side-Channel Security Evaluation Lab Proposal (Hardware implementations)

Cryptographic Engineering Research Group, George Mason University, U.S.A.

March 17, 2022

1 Introduction

This document describes the equipment, software, and methods we would like to use for our side-channel security evaluation lab. These capabilities will be committed to evaluate the side-channel security of NIST LWC finalists.

2 Equipment and Software Used

We plan to use our FOBOS3 side-channel platform with NewAE ChipWhisperer CW305 target board.

- **Target board:** 2× NewAE CW305, which is based on Xilinx Artix-7 xc7a100tftg256-3 FPGA.
- **Control board:** 2× FOBOS3 control boards. The control board is based on the PYNQ-Z1 board, which includes a Xilinx Zynq-7020 system-on-chip. This board provides communication to target and ADC measurements among other features.
- **Oscilloscope:** We have two options to collect data; an oscilloscope and an ADC:
  - Picotech Picoscope 5244D which has 200 MHz bandwidth, a maximum sampling rate of 1G, 500M, 125M, 125M and 62.5 Sample/sec, for resolutions of 8, 12, 14, 15, and 16-bit , respectively.
  - The FOBOS3 shield's OpenADC with 40 MHz bandwidth, a maximum sampling rate of 100M Sample /sec, and 10-bit resolution.

  The target and sampling clocks are synchronized when FOBOS3 shield's ADC is used.
- **Power measurement:** The NewAE CW305 target collects voltage drop across a 0.1-ohm onboard shunt resistor. We plan to use the onboard 20 dB amplifier to amplify the signal before measurement.
- **Software:** FOBOS3 Python-based analysis scripts will be used for leakage assessment.

3 Supported Leakage Assessment Methods

We support test vector leakage assessment (TVLA) using t-test. We plan to collect around 10 million traces per test and run targets at around 10 MHz.

TVLA graphs showing t-values vs. samples and maximum t-value vs. the number of traces analyzed will be provided. We are able to provide the results online for analysis by other teams.

4 Short description of the personnel and its qualifications

- Kamyar Mohajerani; experienced in secure implementation, evaluation, and benchmarking of cryptography.
- Abubakr Abdulgadir; experienced in secure implementation and evaluation of cryptography and side-channel setups.
- Jens-Peter Kaps; co-director of the Cryptographic Engineering Research Group (CERG).
- Kris Gaj; co-director of the Cryptographic Engineering Research Group (CERG).

5 Intended period of the lab operation

We plan to run the lab until the final report is produced.

6 Contact Information

Jens-Peter Kaps and Kris Gaj
Cryptographic Engineering Research Group
George Mason University
jkaps@gmu.edu , kgaj@gmu.edu
https://cryptography.gmu.edu