Call for Side-Channel Security Evaluation Labs

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

January 18, 2022

1 Introduction

We call for groups capable and willing to serve as side-channel security evaluation labs for protected implementations of finalists in the NIST Lightweight Cryptography Standardization Process. Submitters should have access to the equipment used for side-channel leakage assessment and/or attacks, experience, and human resources necessary to perform security analysis. Suggested devices used for evaluating hardware implementations are low-cost modern FPGAs, such as Artix-7 and Spartan-7 from Xilinx, Cyclone 10 LP from Intel, and ECP5 from Lattice Semiconductor. Suggested embedded processors used for evaluating software implementations are ARM Cortex-M4F, RISC-V (e.g., RV32IMAC), Microchip 8-bit AVR, and TI MSP430. The lab can specialize in evaluating only hardware implementations, only software implementations, or both. The lab will be able to choose freely from all implementations placed in the public domain. Additionally, protected implementations may be submitted to the labs directly by their developers in a format consistent with the respective calls. Finally, labs will also be able to ask implementers for their deliverables. The developers may require a lab to keep the distribution of the source code limited to the lab personnel but may not prevent the publication of the obtained results.

2 Suggested Deliverables

Please provide one or more PDF files describing:

1. Equipment and Software Used
   (a) General type of the evaluation platform, e.g., Rambus DPA Workstation, Riscure Inspector, NewAE ChipWhisperer, SAKURA, SASEBO, FOBOS
   (b) The exact names and versions of all FPGA or embedded processor boards used to host the protected implementations (victim boards)
   (c) The exact names and versions of all FPGA and embedded processor boards used to support measurements
   (d) Oscilloscope and its major characteristics (e.g., bandwidth)
   (e) Current and electromagnetic probes
   (f) Usage of bandwidth limiters, filters, amplifiers, etc. and their specification
   (g) Are sampling clock and design-under-evaluation clock synchronized?
   (h) Names and versions of programs used for evaluating side-channel resistance.
2. Supported Leakage Assessment Methods
   (a) Type of the method, e.g., TVLA (Test Vector Leakage Assessment) a.k.a. Welch's t-test, Pearson's χ^2-test, deep learning leakage assessment (DL-LA), etc.
   (b) Approximate number of traces used in evaluations of authenticated ciphers

(c) Typical clock frequency of the device-under-evaluation

(d) Sampling frequency and resolution

(e) Graphical representation of results, e.g., TVLA graphs, χ^2 graphs, etc.

3. Supported Attacks

   (a) Types of Power Analyses, e.g., Simple Power Analysis (SPA), Differential Power Analysis (DPA), Correlation Power Analysis (CPA), Template Attacks (TA), Mutual Information Analysis (MIA), etc.

   (b) Types of Electromagnetic Analyses

   (c) Types of Fault Analyses, e.g., Differential Fault Analysis (DFA), Fault Sensitivity Attack (FSA), Differential Fault Intensity Analysis (DFIA), and Fault Behavior Analysis (FBA)

   (d) Graphical representation of results, e.g., the minimum traces to disclosure (MTD) graphs.

4. Ability to generate and publish raw measurements to be analyzed by other groups

5. Support for side-channel analysis as service, with the feedback provided to designers of protected implementations during the development process

6. Short description of the personnel and its qualifications

7. Intended period of the lab operation

8. Contact information.

We will publish a list of evaluation labs, including the received deliverables, on our ATHENa web page at `https://cryptography.gmu.edu/athena/index.php?id=LWC` by March 15th.

3 Proposed Timeline

- Call for security evaluation labs
  - First draft – December 13, 2021
  - Discussion on the `lwc-forum`
  - Final version – January 17, 2022
- Deadline for security evaluation lab specifications
  - February 28, 2022
- Security Evaluation Lab Reports
  - Preliminary version of the report – April 30, 2022
  - Final version of the report – June 30, 2022.

4 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`