Side-Channel Security Evaluation Lab Description

Date: 15 March 2022

This document provides a description of technical capabilities of the CESCA lab for serving as side-channel security evaluation labs for protected implementations of finalists in the NIST Lightweight Cryptography Standardization Process.

The CESCA Lab is led by prof. Lejla Batina, part of the Digital Security Group at Radboud University in the Netherlands.

1. Equipment and Software Used:

(a) General type of the evaluation platform: We have both professional grade evaluation software such as the Riscure Inspector and entry-level evaluation software Chipwhisper and private Jupyter notebook scripts;

(b) The exact names and versions of all FPGA or embedded processor boards used to host the protected implementations (victim boards):
We have several targets to choose from, among which:

- Pinata (STM32F407IGT6)
- ARM-cortex Chipwhisperers: STM32F303RDT6, STM32F405RGT6, XMEGA Chipwhisperer (XMEGA128D4 for the UFO).
- For FPGA, we will do evaluation on SAKURA board and Chipwhisperer CW305 (Artix7);

(c) The exact names and versions of all FPGA and embedded processor boards used to support Measurements:

- SAKURA-G-FPGA
- XMEGA Chipwhisperer (XMEGA128D4 for the UFO).

(d) Oscilloscope and its major characteristics (e.g., bandwidth):

- Picoscope Models 6407, 5203, 3207B, 3206D (respectively, 1GHz, 250MHz, 250MHz, 200MHz)
- LeCroy DSO Waverunner 8404M-MS (4GHz)
- LeCroy DSO Waverunner 610Zi (1GHz)
- Chipwhisperer DSO (105MHz), can be replaced with one of the above for Chipwhisperer boards;

(e) Current and electromagnetic probes:

- We have two Riscure current probes with 12V amplifiers.
- Langer probes we have:
  - Langer (ICR Near Field Microprobes) x 2
  - Langer (MFA 01 Set)
  - Langer (RF R 400-1, RF R 50-1, RF U 5-2, RF B 3-2)
  - Langer (RF U 2.5-2, RF R 0.3-3, RF B 0.3-3, LF R 400, LF U 2.5)
  - Langer(RF U 5-2)
  - Preamplifier for Near Field Probes Langer (PA 303) x
- Riscure XYZ stage for high precision probe placement;

(f) Usage of bandwidth limiters, filters, amplifiers, etc. and their specification
We have a basic range of filters, most of them are low-pass filters with cutoff frequency from 48MHz to 400MHz and a high-pass filter 290-3000MHz, but we rarely use.

(g) Are sampling clock and design-under-evaluation clock synchronized?
We don't usually synchronize with the microcontroler DUT clock. It is theoretically possible to provide an external clock but it complicates a setup and would require disabling internal PLLs and that is not always possible. Even for FPGAs we do provide the clock but we do not synchronize measurements on the clock (that is only done only of Chipwhisperer).

(h) Names and versions of programs used for evaluating side-channel resistance.:

For the implementation of (protected) algorithms software (C, assembly), hardware (VHDL) and for evaluation Riscure Inspector, personal scripts in C, Python and Matlab developed by the people doing the evaluation;

2. Supported Leakage Assessment Methods
(a) Type of the method: TVLA (Test Vector Leakage Assessment) a.k.a. Welch's t-test, Pearson's χ^2-test, deep learning leakage assessment (DL-LA);
(b) Approximate number of traces used in evaluations of authenticated ciphers
The number of traces collected for the evaluation of ciphers can vary, but we plan to measure up to 10M traces.

(c) Typical clock frequency of the device-under-evaluation
Nominal clock frequency of the Pinata is 168MHz, but for measurements it is lower and can go down to 8MHz. For Sakura we can choose between 1.5, 3, 6, 12 or 24MHz. For CW305 we can choose from 5MHz to 160MHz.

(d) Sampling frequency and resolution: we will decide depending on the target and the performed attack;
(e) Graphical representation of results, e.g., TVLA graphs, χ^2 graphs, etc.: yes, the usual types of figures we use for academic publications;

3. Supported Attacks
(a) Types of Power Analyses: Simple Power Analysis (SPA), Differential Power Analysis (DPA), Correlation Power Analysis (CPA), Template Attacks (TA);
(b) Types of Electromagnetic Analyses: DEMA;
(c) Types of Fault Analyses: e.g., Differential Fault Analysis (DFA); Fault Injection attacks;
(d) Graphical representation of results, e.g., the minimum traces to disclosure (MTD) graphs: yes;

4. Ability to generate and publish raw measurements to be analyzed by other groups
We will publish (some) of the raw traces, the decision will depend on the size of the datasets.

5. Support for side-channel analysis as service, with the feedback provided to designers of protected implementations during the development process
We will provide feedback to the designers and help improve the cryptographic implementations.

6. Short description of the personnel and its qualifications

Prof. Dr. Lejla Batina, who specializes in physical attacks and countermeasures and implementations of cryptography and has published 140 refereed papers in those areas.
Dedicated time: 0.1FTE

Dr. Ileana Buhan is an assistant professor of cryptographic who focuses on developing tools to help designers of cryptographic algorithms develop secure implementations.
Dedicated time: 0.1FTE

Dr. Łukasz Chmielewski is a Postdoc In The Digital Security group, he gained extensive experience in the area of physical security evaluating various secure devices.
Dedicated time: 0.2FTE

Léo Weissbart, PhD student, deep learning, SCA;
Dedicated time: 1FTE

Konstantina Miteloudi, PhD student, FPGA implementations, SCA;
Dedicated time: 1FTE

Asmita Adhikary, PhD student, fault injection;
Dedicated time: 1FTE

Azade Rezaeezade, PhD student, fault injection;
Dedicated time: 0.5FTE

Vahid Jahandideh, PhD student, leakage resilient ciphers and side channel analysis;
Dedicated time: 0.5FTE

Tom Stock, Cybersecurity master student;
Dedicated time: 1 FTE

Ellen Gunnarsdóttir, Cybersecurity master student;
Dedicated time: 1 FTE

7. Intended period of the lab operation

15March – 30August 2022;

8. Contact information.

Prof. dr. Lejla Batina
lejla@cs.ru.nl