Application for SCA Evaluation Lab

Rishub Nagpal, Robert Primas, Stefan Mangard

February 21, 2022

Contents

This document specifies the capabilities of a potential SCA Evaluation lab at the Institute of Applied Information Processing and Communications (IAIK) at the Graz University of Technology.

Answers to specific questions:

1. Equipment and Softwaure used
   (a) NewAE Chipwhisperer
   (b) CW305, CW308T-STM32F¶
   (c) FPGA: xc7a100tftg256-2, Cortex-M4F: stm32f405, stm32f303
   (d) PicoScope 6404C. 500-Mhz bandwidth, up to 2GS/s (8-bit samples), 1GS buffersize
   (e) 10x current probes
   (f) N/A
   (g) No
   (h) SCALib v.3.4 @ `https://github.com/simple-crypto/SCALib`
2. Supported Leakage Assessment Methods
   (a) TVLA
   (b) 100k - 1 Million
   (c) 1Mhz-10MHz
   (d) 1-2GS/s with 8-bit samples
   (e) TVLA graphs
3. Supported Attacks

(a) SPA, DPA

(b) N/A

(c) N/A

(d) MTD

4. Yes

5. Yes

6. **Rishub Nagpal** - PhD Student. Primarily responsible for conducting SCA evaluations, support for designers and generation of reports.

   Robert Primas - PhD Candidate. Knowledgeable in SCA topics, published numerous articles on SCA and fault attacks. Co-designer of LWC candidate ISAP.

   Stefan Mangard - Institute Director. Subject matter expert in SCA.

7. March 1st 2022 - July 1st 2022

8. Contact: Rishub Nagpal rishub.nagpal@lamarr.at