Hardware Security and Cryptographic Processor Lab

Tsinghua University, Beijing

March 2022

Equipment and Software

SCA boards

- Sakura-X: Xilinx Kintex-7 -- 2 pcs
- Sakura-G: Xilinx Spartan-6 LX75 -- 3 pcs
  Accessory: YKC-1000 pre-amplifier set -- 1 pce

Other FPGA boards

- Xilinx ZCU106: Zynq UltraScale+ MPSoC -- 2 pcs
- Xilinx Nexys A7-100T: Xilinx Artix-7 XC7A100T -- 10 pcs
- Intel: CYCLONE IV EP4CE10 FPGA Development Board -- 5 pcs

Other MCU boards

- STM32f303 -- 2 pcs
- STM32f407 -- 2 pcs
- ARM cortex-3 -- 2 pcs

Oscilloscope and Logic Analyzer

- Teledyne LeCroy: WaveRunner8404M (MaxBand - 4 GHz, MaxSampRate - 20 GS/s, MemDepth - 64 Mpts/C) -- 1 pce
- DSLogic: U3Pro32 (MaxSampRate - 1GHz, MaxSampDepth - 16G stream) -- 1 pce

Supported Leakage Assessment Methods and Attacks

Supported Leakage Assessment Methods

- NICV, TVLA (t-test, Chi-Squared test)
- Acquisition campaign up to 1,000,000 traces or more
- Typical DUT clock: 5 MHz to 800 MHz

Supported Attacks

- SPA, DPA, CPA, MIA, TA, LRA, etc.
- Same graphical representations:
  - minimum traces to disclosure (MTD)
  - global success rate (GSR)

- partial success rate (PSR)
- partial guessing entropy (PGE)

Sharing of Measurements

- FTP Server
- SVN Server
- SQL server

Telemeeting Software

- Zoom
- VooV

Personnel

- Prof. Leibo Liu, head of Hardware Security and Cryptographic Processor Lab
- Wenping Zhu, Senior Engineer
- Shuying Yin, Senior Engineer
- Bohan Yang, Postdoctoral Researcher
- Cankun Zhao, PhD Student
- Shuohang Peng, Master Student

Lab Available From March 15 to June 30

Contact: bohanyang@tsinghua.edu.cn