We are glad to take part in the LWC standardization process as a Side-Channel Security Evaluation Lab, and we would like to evaluate no more than 5~10 both hardware and software implementations from March 15 to June 30. According to the suggested deliverables, we give some technical details of our lab.

1. Equipment and Software Used

(a) Riscure Inspector, NewAE ChipWhisperer and SAKURA are available.

(b)&(c) The test of hardware implementations could be carried out on SAKURA-G and SAKURA-X where the victim FPGA chips are SPARTAN-6 (XC6SLX75) and KINTEX-7 (XC7K160T), respectively. The software implementations could be tested on NewAE devices (STM32F3 & XMEGA). We could also test the software implementations based on our own platform on which the victim is an AVR MCU, e.g., ATmega128A.

(d) LeCroy waverunner 610Zi , Pico 3203D, Pico 5244D, Pico 6424E (with PQ265 active probe) are available.

Oscilloscope	Bandwidth	Channels	Sample Rate(2ch)	Record Length(8bit)	Resolution
610Zi	1GHz	4	20 GS/s	32MS	8-bit
3203D	50MHz	2	500MS/s	64MS	8-bit
5244D	200MHz	2	500MS/s	512MS	8/12/14//15/16-bit
6424E	500MHz	4	5 GS/s	4 GS	8/12/14-bit

(e) Langer RF2 near-field probes are available.

(f) Mini-circuit SHP and SLP serial filters that cover the frequency from 100MHz to 2GHz are available. We also have some low-noise amplifiers like ZFL-1000LN+, etc.

(g) Sampling clock and design-under-evaluation clock will be synchronized when we test on NewAE devices.

(h) The version of Inspector is 4.11. We will also mount other tests based on our scripts.

2. Supported Leakage Assessment Methods

(a) We might focus on the Welch's t-test, SNR, χ^2-test and DLLA.

(b) We could use a specific threshold value in t-test to approximate the number of traces used in an evaluation.

(c-e) We could change the clock frequency and measurement setups arbitrary if it is necessary for assessment. We could also show the graphical results. The measurement setups with most significant leakages will be chosen for the subsequent attack.

3. Supported Attacks

(a-b) We might focus on CPA, TA, MIA and deep learning-based methods [1-3] for power and electromagnetic traces.

(c)We will not conduct fault analysis.

(d)We could present the results like guess entropy and success rate in graphic.

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

We could release raw measurements on the internet.

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

We could provide feedbacks according to analysis results to designers to improve the protection.

6. Short description of the personnel and its qualifications

There are 1 professor, 1 PhD research assistant, 6 PhD students and four masters in our group. For years, our team has been working on the research of side-channel analysis and secure crypto implementation. We have made a lot of assessments by SCA on symmetric and asymmetric ciphers. Recently, we have proposed a series of deep learning-based SCA methods [1-3] that can solve the fundamental problems in

machine learning-based SCA. We are experienced in evaluating the crypto implementations with the traditional SCA methods and our new DL-based methods.

7. Intended period of the lab operation

It would take 2-3 months to finish the evaluation.

8. Contact information.

Email: dwgu@sjtu.edu.cn

References:

[1] A Nonprofiled Side-Channel Analysis Based on Variational Lower Bound Related to Mutual Information. (SCIS 2022)

[2] Pay Attention to Raw Traces: A Deep Learning Architecture for End-to-End Profiling Attacks. (TCHES 2021)

[3] Cross-Device Profiled Side-Channel Attack with Unsupervised Domain Adaptation. (TCHES 2021)