Async2Secure

Side-Channel-Attack (SCA) Evaluation Platform

A Graphical-User-Interface (GUI) based side-channel-attack (SCA) evaluation platform to evaluate hardware security. Detect first before it is too late.

Async2Secure is dedicated to provide solutions to mitigate and evaluate hardware attacks on Integrated Circuits (IC). Our side-channel-attack (SCA) evaluation platform is an evaluation tool to quantify and qualify an Advanced Encryption Standard (AES) hardware from side-channel leakages such as power and electromagnetic (EM) parameters. Fig. 1 is a setup for our tool which accepts both measurement amd simulation data. Fig. 2 is an EM-based prototype SCA evaluation.

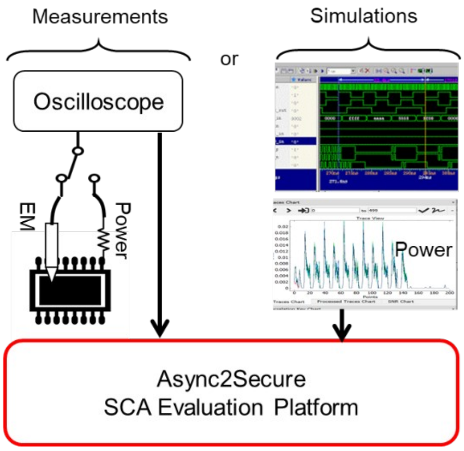

Fig. 1 A basic setup for measurements/simulations

Key Features

- Graphical-User-Interface (GUI)
- Ease of Use
- Fast analysis and pre-qualification
- Applicable to AES
- Applicable to both simulation & measurement data
- SCA for power and electromagnetic (EM) methods
- State-of-the art attacks – Correlation Power Analysis, Differential Power Analysis, and Machine Learning
- Configurable points of attack
- Configurable power models (Hamming Weight, Hamming Distance, Weight Model, Bit Model, Zero Model, etc.)
- Trace management
- Pre-analysing, pre-processing and digital signal processing features available
- Data acquisition possible
- FPGA hardware evaluation board available
- Technical support available

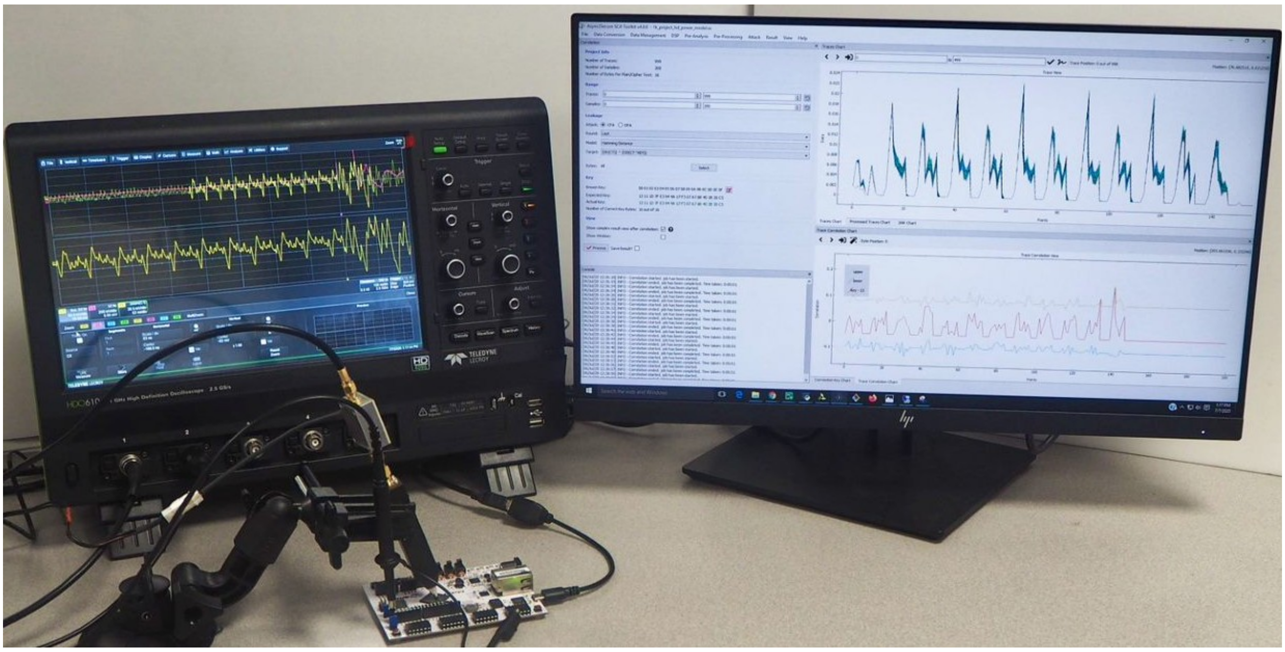

Fig. 2: An FPGA prototype SCA evaluation using our SCA evaluation platform

Our SCA evaluation platform is based on Python. The system requirements for our platform are listed in Table I. The platform will be installed at a local computer, and we adopt a web-based licensing access to enable the tool.

Table I
System Requirements

No	Item	Requirement
1	Operating system	▪ Windows 10 ▪ Linux (tested on Ubuntu 18.04 LTS and 20.04 LTS)
2	Disk	400MB for a typical installation
3	RAM	Minimum 8GB (16GB recommended)
4	GPU	Yes, if machine learning option is added
5	Internet access	Needed, for licensing

We offer three different packages, as depicted in Table II, for different users. The basic package is mainly for students/beginners to learn the principle/concepts of SCA. The advanced package is mainly for users who would like to have relatively comprehensive SCA evaluations on their hardware for pre-qualification. The professional package is mainly for users who would like to have all-rounded SCA evaluations on their hardware for complete pre-qualification.

We would also offer databases (power and EM traces) for evaluation. We would also offer various FPGA evaluation boards (and interface modules) that are linked to our SCA evaluation platform for SCAs. Automatic data acquisition between an oscilloscope and our platform could be setup upon request.

Table II
The different packages for our SCA evaluation platform

No	Features	Basic	Advanced	Professional
1	Software Basic Features			
	- Graphic User Interface	Yes	Yes	Yes
	- Trace Limit	limited	unlimited	unlimited
2	Data Management Features			
	- select, delete, split	Yes	Yes	Yes
3	Digital Signal Processing Features			
	- Moving average	Yes	Yes	Yes
	- Frequency transformation (for Frequency Attack)	No	Yes	Yes
4	Pre-analysing Features			
	- Signal-to-noise (SNR) analysis	No	Yes	Yes
	- SNR analysis for mask	No	Yes	Yes
5	Pre-processing Features			
	- Trace alignment/resynchronization	No	Yes	Yes
	- Trace re-transformation	No	No	Yes
	- Normalization	No	Yes	Yes
6	Attack Models			
	- First round/last Round (on AES)	Yes	Yes	Yes
	- CPA with Hamming Distance (HD) & Hamming Weight (HW)	Yes	Yes	Yes
	- CPA with bit-wise HW, Weight, Zero-Value	No	Yes	Yes
	- Basic DPA	Yes	Yes	Yes
	- Advanced DPA	No	Yes	Yes
	- 2nd order CPA (HD, HD, bit-wise HW, Weight, Zero-Value)	No	No	Yes
	- 2nd order CPA parameters (Absolute Difference, Difference, Sum, Square of Sum, Product)	No	No	Yes
	- Machine Learning	No	No	Yes
7	Result Display			
	- Correct/Wrong key display, time-domain result display, minimum-to-disclosure display	Yes	Yes	Yes

For more information, visit http://Async2Secure.com

Async2Secure Pte Ltd, TCH TechCentre #05-07, 71, Toh Guan Road East, Singapore 608598
Contact: contact@async2secure.com