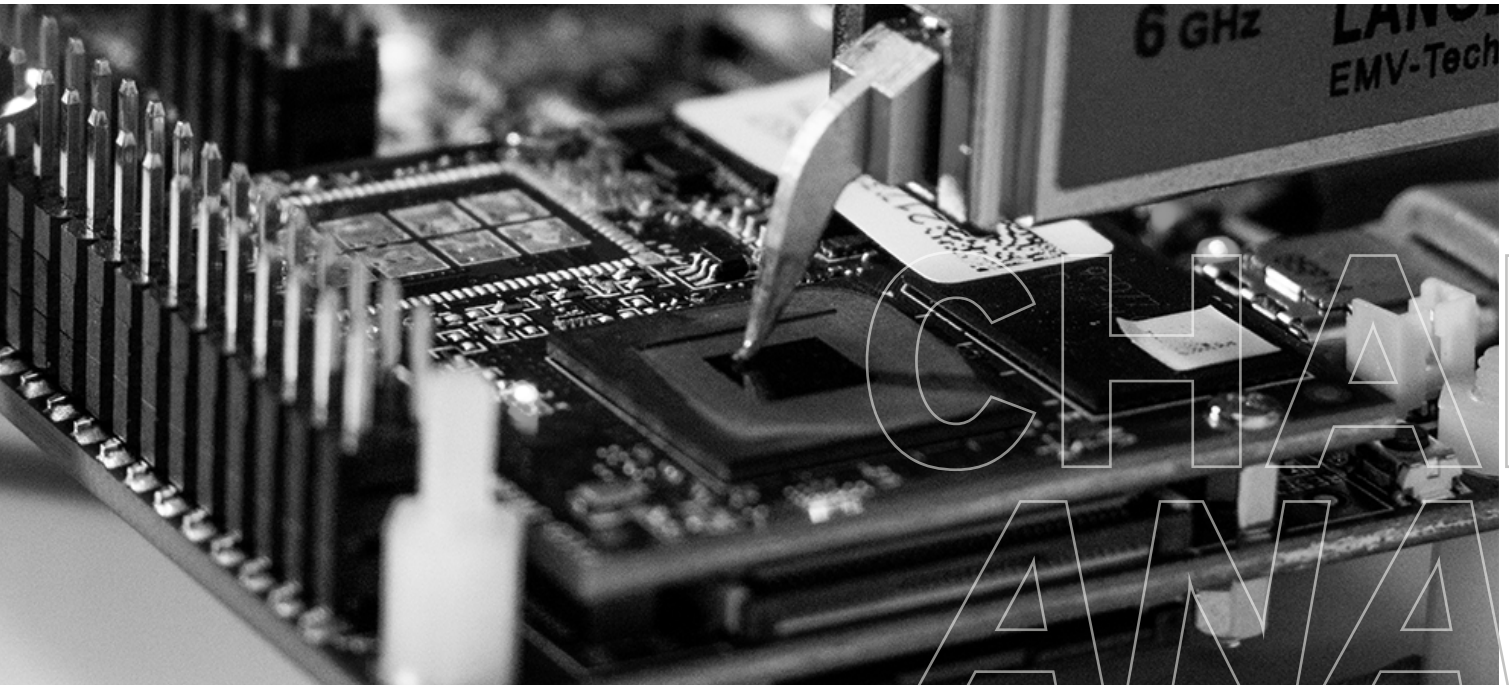
eShard

Side-Channel Analysis

A COMPLETE GUIDE OF ESHARD'S SOLUTIONS FOR SCA



SIDE CHANNEL ANALYSIS

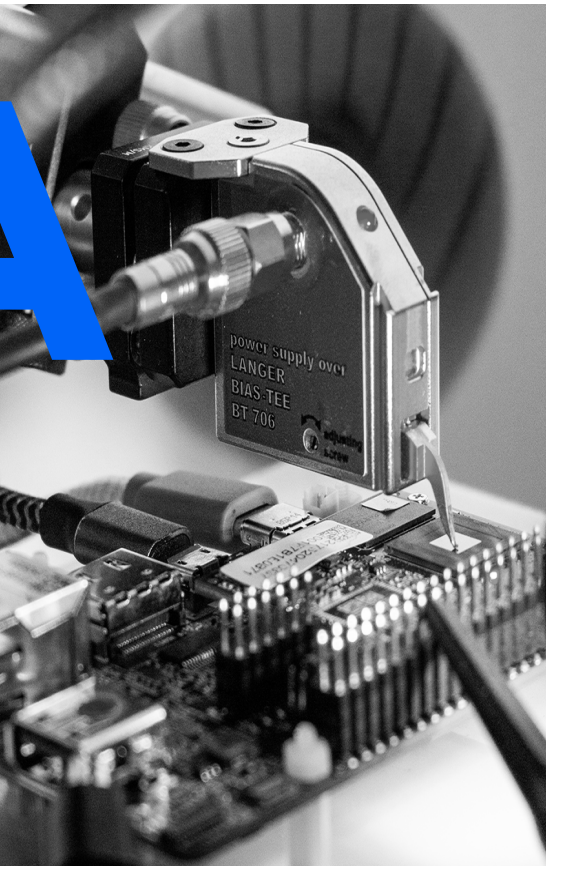
SCA

SIDE-CHANNEL ANALYSIS

An Integrated Circuit host and handles extremely valuable assets (cryptography secret keys, secrets, sensitive code,...) used for payments, access control, data protection. These assets are physically materialized into the chip itself, with more or less obfuscation layers. With the right technique (methods, tools) and enough time, it may be possible to disclose them.

The so-called Side-channel is an attack technique aiming at extracting secrets from a chip. From many observations of signals representative of the internal execution, it is possible to guess parts of the secret. Without harming the device, the SCA technique may defeat non protected devices with a minimum of cost and limited efforts. This is applicable to all chips (Secure Element, SoC, FPGA, Microcontrollers) and all algorithms (AES, Elliptic Curves, ...).

Mastering the SCA technique is therefore necessary to manage the risk on chips.



WORKFLOW

1. Sample preparation: capturing the chip activity requires probing some physical signals either power fluctuations or electromagnetic activity. The setup remains simple, but the quality of the setup is essential for good measurement.

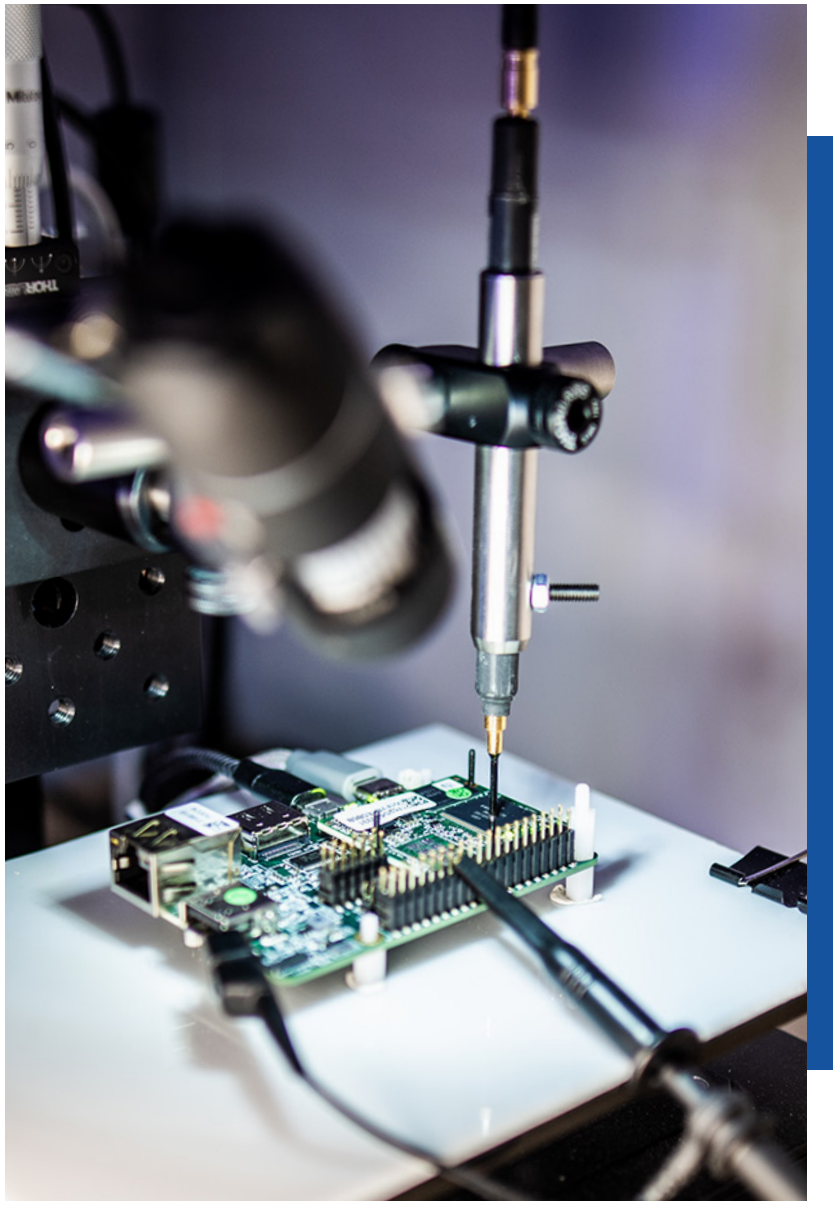
2. Experimental setup control and data acquisition: looking for useful information leakage may be tedious. Scanning multiple areas requires automation. Fast data collection is also necessary since acquiring millions to billions of cryptography iterations is common.

3. Data preprocessing: data alignment, filtering and more generally speaking manipulating the signal to remove any jitter or other protection requires a flexible data processing framework to address the specifics of each attack and target.

4. Side-channel analysis: many side-channel techniques have been published. A toolbox including all these techniques must be available to address a large variety of cryptographic algorithms and implementations.

5. Data visualization: sharing the analysis flow in clear graphics helps to express a complex attack in simple terms.

A SCA setup can be relatively cheap to attack unprotected devices. Less than 1k€. A data acquisition setup, a computer and a bit of talent and SCA can disclose a secret from a non protected chip in minutes.



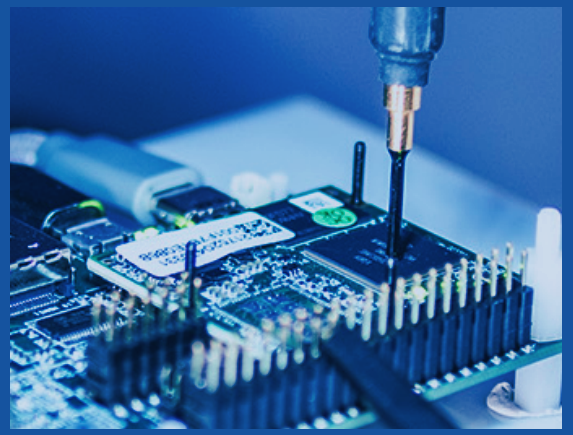
What makes a Side-Channel Analysis *successful?*

Each step of the workflow does matter: the experimental setup, the quality of the trace alignment, the ability to run efficiently heavy computation and to manipulate large amounts of data.

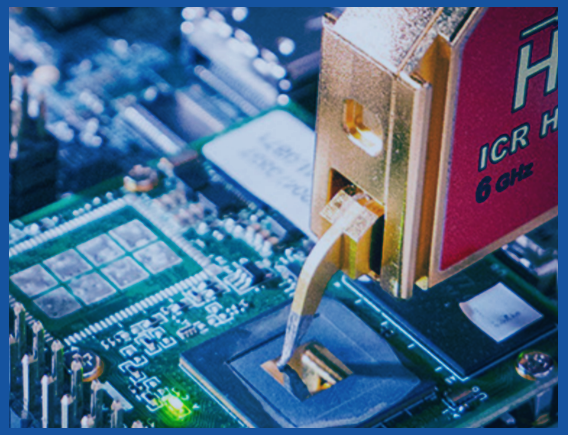
In identification, there are a lot of trial and error steps to identify the leakage area and capture meaningful information. This requires methodology, high computing power, expertise and an efficient toolchain.. This is particularly true for sophisticated attacks that are required for protected devices, such as high order or deep learning attacks.

Flexibility is equally important to performance since the experts may quickly need to apply specific processing for every cryptographic implementation they target.

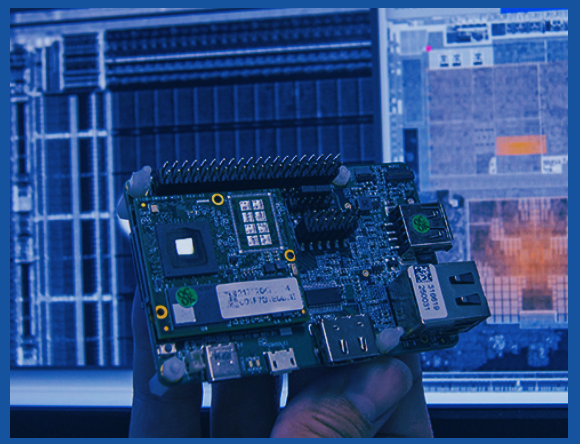
eShard's solutions



Create or upgrade your lab with a turnkey SCA Solution
(page 5)



Challenge a solution in eShard's SCA Lab
(page 9)



Grow your SCA expertise
(page 10)

CREATE OR UPGRADE YOUR LAB WITH A

Turnkey SCA Solution

- **Experimental setup** - including motorized stage, EM probe and oscilloscope;
- Data science **software environment**;
- **Side-channel library** for 1st and 2nd order attacks: (T)DES, AES, ECC, RSA, HMAC;
- Signal processing & attack analysis **toolset**: alignment, CPA, MIA, LRA, TTest, NICV;
- **Catalog of attacks** summarizing years of R&D including deep learning, scatter, lattice.

Key differentiators:

FIELD PROVEN

Successful multi millions traces attacks on recent SoC, Secure Element, FPGA devices with many gates, fine geometry (10 nm scale) and high clock frequency (GHz).

SCALABLE

Ideal for intensive and efficient computation leveraging GPU or distributed computing architectures.

FLEXIBLE

Ideal framework to manage trace alignment or filtering by cascading customized signal processing operations (peak to peak, pattern detection, ...)

COLLABORATIVE

Multi-users, one unique data centre, remote hardware control, notebook co-edition.

OPEN

Smooth integration of third party equipment, develop or install your own library, customize the function selection, the targeted value or algorithms.

IT AGNOSTIC

esDynamic software framework deployable on workstation, server, cloud, computer clusters, data-centres.

With such a solution, you can empower your experts in:

- ✓ Scanning a chip and qualifying the leakage areas;
- ✓ Running the whole side-channel workflow to stress a specific implementation;
- ✓ Building the internal expertise by selecting or developing a set of attacks;
- ✓ Undertaking research work to push the side-channel boundaries.

Audience: Semiconductor companies with IC security expertise, Secure products OEM and system vendors, Governmental agencies, Evaluation laboratories, Research centres in IC security.

Unlock the full potential of your analysis with Expertise Modules

Unique catalogue of attacks and techniques in Side-Channel

SIDE-CHANNEL ADVANCED

Knowledge: attack catalogue targeting public key algorithms (ECC, RSA)
Knowledge: High order attack sophisticated attacks
Knowledge: Lattice techniques

DEEP LEARNING SCA

Library: Dedicated to SCA leveraging Pytorch and Tensorflow
Knowledge: Using DL framework and deep learning applied to SCA
Use cases on ASCAD or LedgerCTF

SCATTER ATTACKS

Library for efficient Scatter implementation
Knowledge: Principle 1st and 2nd order
Use cases on AES and ECC

SIDE-CHANNEL ON POST QUANTUM CRYPTOGRAPHY

Knowledge: Understanding Kyber and Dilithium
Knowledge: Side-channel attacks on Kyber and Dilithium
Use cases on chosen implementations

Ask our experts for detailed documentation about expertise modules and the fact sheet for more technical informations: contact@eshard.com

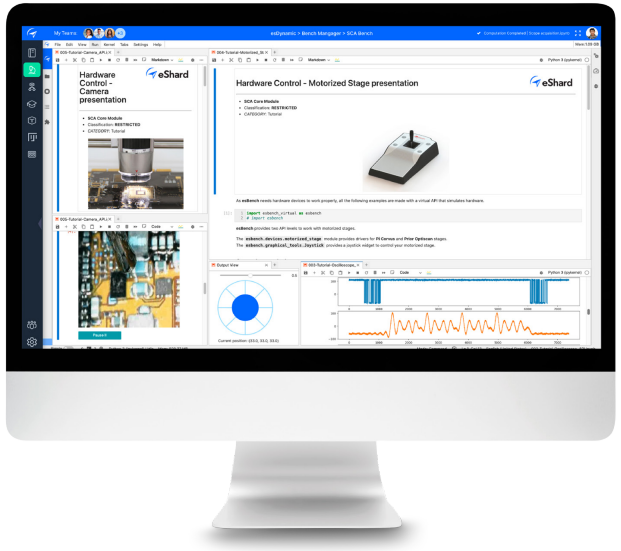
Workflow

1 integrated **workflow**

1 integrated **team**

1 integrated **tool**

Acquisition

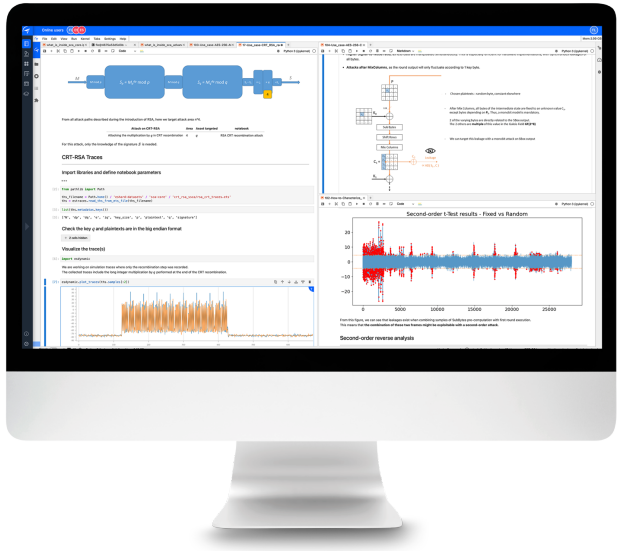


Instrument the device under test (DUT), the digital oscilloscope, the xyz stage and use power or electromagnetic probes to automate side-channel signals capture while the DUT performs a cryptographic or another operation of interest.

Data processing

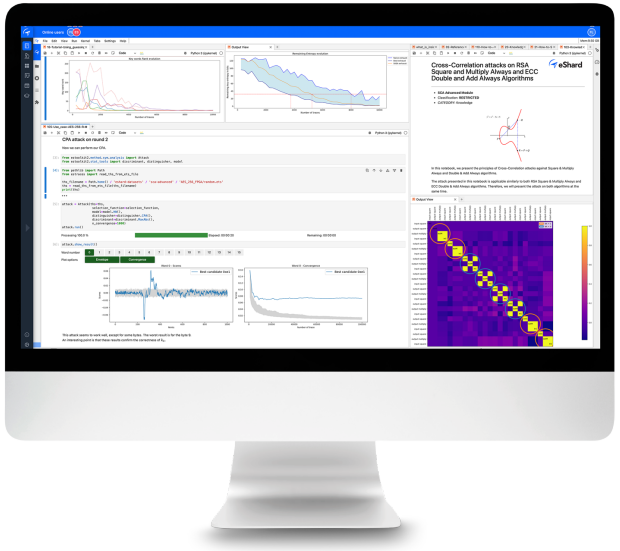
Apply techniques such as signal filtering, pattern and peak detection to remove noise and to align the acquired data traces. The insight widget is a powerful observation tool for visual inspection even in case of very large traces.

Data analysis



Analyse data using statistical methods like the t-Test to detect side-channel leakage and point of interest. Dedicated leaked analysis campaigns can be built for different targeted algorithms, either symmetric or asymmetric.

Exploitation



Exploit the side-channel information by using many statistical distinguishers, such as CPA, DPA, MIA, LRA. Use first order or high order advanced techniques to recover the secrets from many algorithms. Apply techniques such as guessing entropy for disclosing the full secret key.

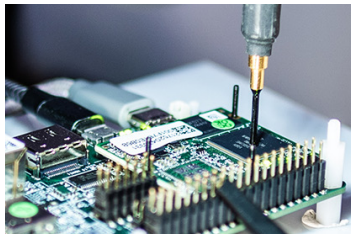
Complete and Efficient Hardware Security Testing.

Request a demo

CHALLENGE A SOLUTION IN
ESHARD & **ALPHANOV**'S

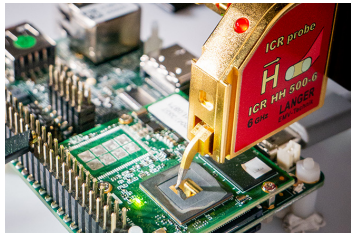
SCA Lab

Key differentiators:



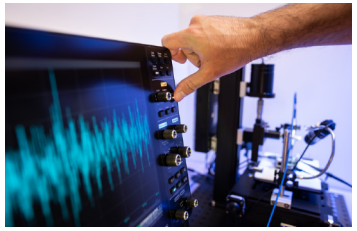
LONG TRACK RECORD

Hands-on experience on different chip technologies: Secure elements, SoC, ASIC and FPGA.



TESTING LAB

High end and efficient testing lab based on eShard's SCA solution.



COLLABORATIVE

Continuous project scope review and adjustment. Resulting notebooks can be replayed in your lab premises for further analyses.

Audience: Any industry and governmental and academic institution that needs to outsource a hardware product evaluation with Laser FI for lack of expertise or resource reasons.

GROW YOUR

Expertise

WITH ESCOACHING

- Setup the laser bench and learn about safety procedures
- Characterize a chip susceptibility to laser pulse and launch a test campaign
- Implement a practical laser fault injection from back to back

AND WITH

STARTER KITS

Laser Fault Injection implemented on a complex and not outdated SoC: a hardware-based cryptography engine.

Know-how material implements the workflow: from the lab setup, the fault campaign to the secret key extraction.

Ideal as a training material, an internal benchmark or a showcase.

Audience: Hardware security analysts who want to learn practical knowledge about Laser FI or increase their competencies in this field.

eShard

Get in touch

www.eshard.com

contact@eshard.com

/company/eshard

@eshard