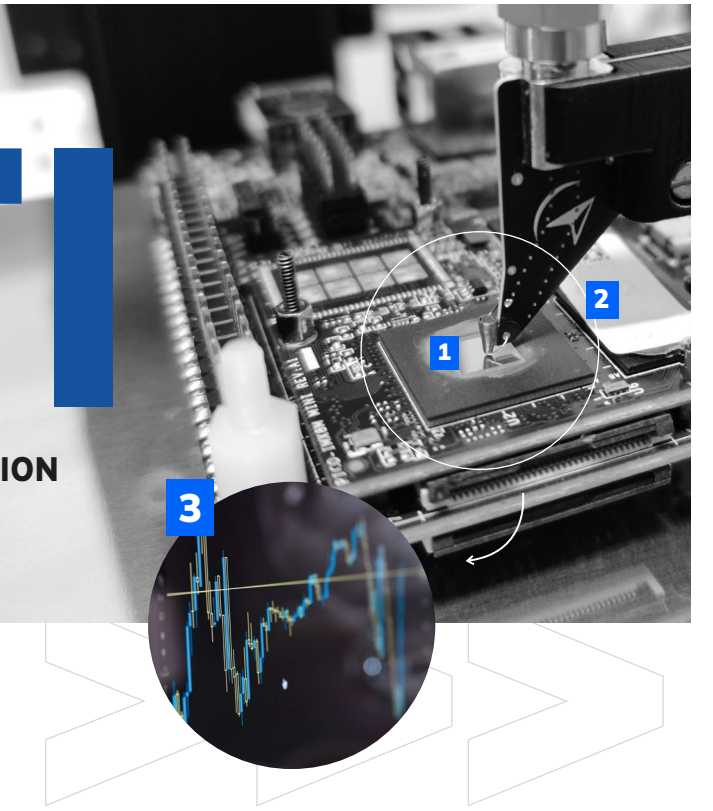
eShard

Electromagnetic Fault Injection

A COMPLETE GUIDE OF ESHARD'S SOLUTIONS FOR EMFI

EMFI

ELECTROMAGNETIC FAULT INJECTION



An Integrated Circuit hosts and handles extremely valuable assets (cryptography private keys, secrets, sensitive code,...) used for payments, access control, data protection... These assets are physically materialised into the chip itself. With the right technique (methods, tools) and enough time, it may be possible to tamper with the IC to recover the assets.

The so-called fault injections aim at inducing an exploitable logical fault by a physical disruption. It has been demonstrated that a near field EM pulse focused on a sensitive part of the die may induce such a logical fault. A non-protected device can be compromised by attackers applying Electromagnetic Fault Injection (EMFI) techniques with low cost equipment.

Mastering the EMFI technique is necessary to evaluate the efficiency of counter-measures implemented on a chip against physical perturbations and manage the risks.

KEY STEPS

1. Sample preparation: EMFI has the potential to inject a fault across the package. In some cases, a direct access to the die may be recommended for a closer access to the die.

2. Fault campaign: Injecting brief but intense near field EM pulses at different locations of the die with different fault injection parameters (pulse duration, power level...) to cause local disruptions during the logic execution and build a fault map.

3. Exploitation: Exploring and filtering faults obtained at the fault campaign step; some parameter combinations may generate exploitable logical faults. They can lead to vulnerability or secret exposure.

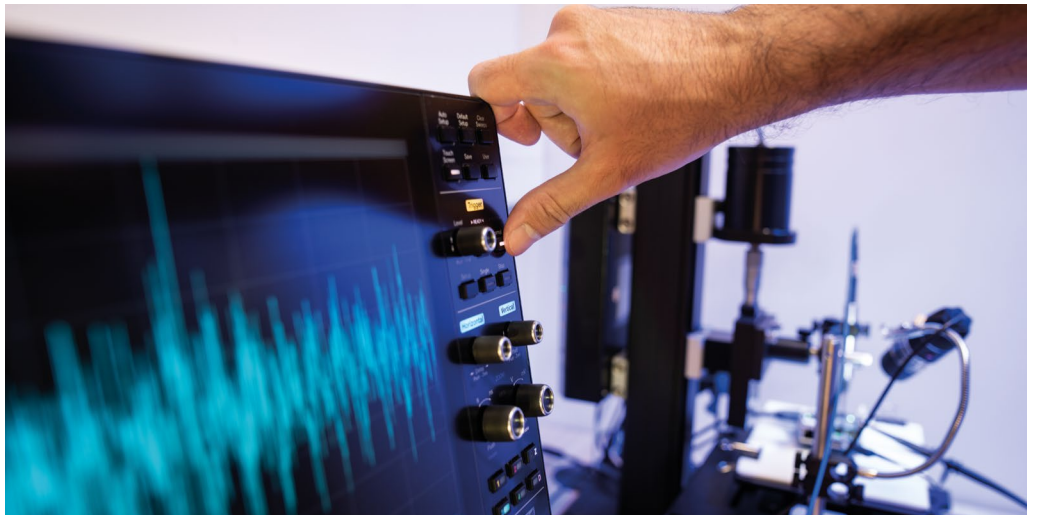
An EMFI setup can be as cheap as 5k€. With a few pieces of electronic equipment and a bit of talent an attacker can perform EMFI and compromise a non protected chip. However for chips integrating counter-measures against EMFI, a higher end setup has to be used to qualify the performance of built-in protections since the bar has been raised.

What makes an EMFI *successful?*

Everything lies in the ability to combine the different parameters leading to an exploitable fault: the electromagnetic pulse shape and intensity, the spot, the distance to the die... All these variables can make a big difference.

In the identification phase, when the analyst does not know the possibility of a weakness, there is a need for complex campaigns combining many parameters with many EM characteristics. Looking for the right set of parameters may be challenging without efficient automation and the ability to capture the chip reaction to faults. The main objective is to avoid any blind spot in the test coverage. While cheap setups have a small scanning area, professional equipment will do a comprehensive scan.

Key points for a successful EMFI:



EM PULSE ACCURACY IN SPACE AND TIME

EM PULSE POWER

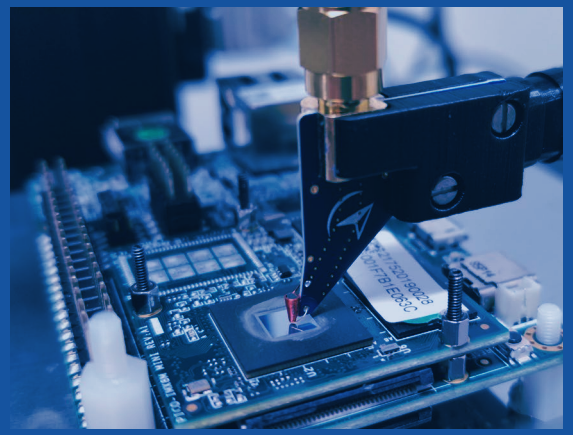
HORIZONTAL + VERTICAL POLARITY

EFFICIENT AND FLEXIBLE SCANNING ENGINE

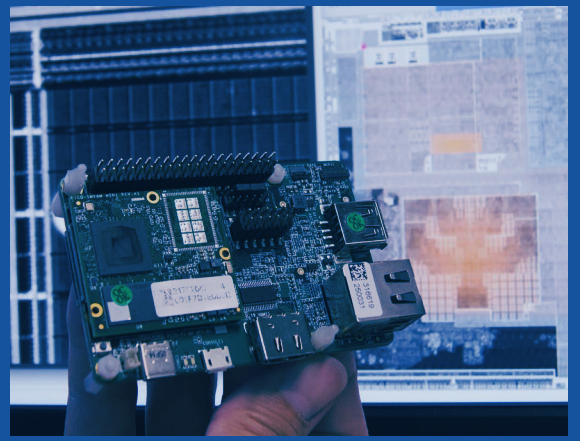
LARGE DATASET MANAGEMENT

eShard's solutions

Create or upgrade your lab with a turnkey EMFI Solution



Challenge a solution in eShard's EMFI Lab

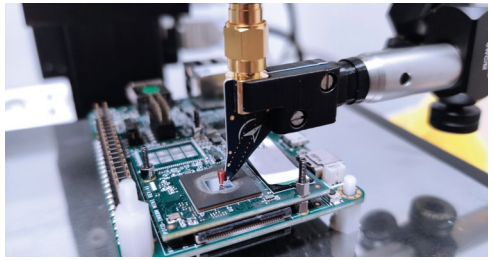


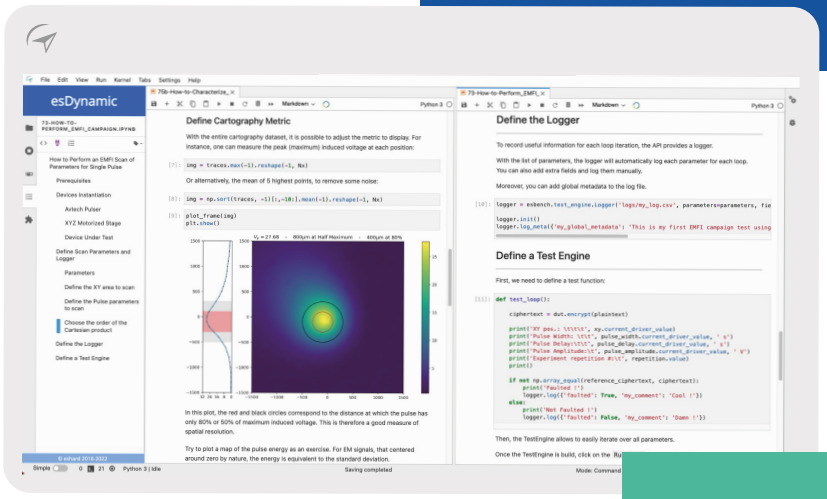
Grow your EMFI expertise

CREATE OR UPGRADE YOUR LAB WITH A

Turnkey EMFI Solution

- Experimental setup - including pulser,
- Bespoke E.M. injection probe kit,
- Data science software environment,
- Hardware equipment drivers,
- Fault campaign toolset,
- Catalogue of attacks*.





Overview of the Software Environment

*Ask our experts for the fact sheet for more technical informations.

Key differentiators:

FIELD PROVEN
Successful attacks on recent SoC and FPGA devices with large number of gates, fine geometry (10 nm scale) and high clock frequency (GHz).

FLEXIBLE
Jupyterlab interface with analysis and attack workflow scripted in Python source code.

OPEN
Integration of third-party equipment

BESPOKE
Dedicated probe and electronic design to generate consistent and accurate pulses (e.g: anti bounce system).

COLLABORATIVE
Multi-users, remote hardware control, notebook co-edition.

HIGH PERFORMANCE
High power / Low duration EM pulses, vertical and horizontal polarisation.

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

- ✔ Exploring the practicals of EMFI technique;
- ✔ Evaluating an IC against EMFI through a comprehensive scanning;
- ✔ Keeping track of results. Replaying analyses;
- ✔ Implement an end-to-end EMFI use case for stressing a specific sensitive operation.

Audience:

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

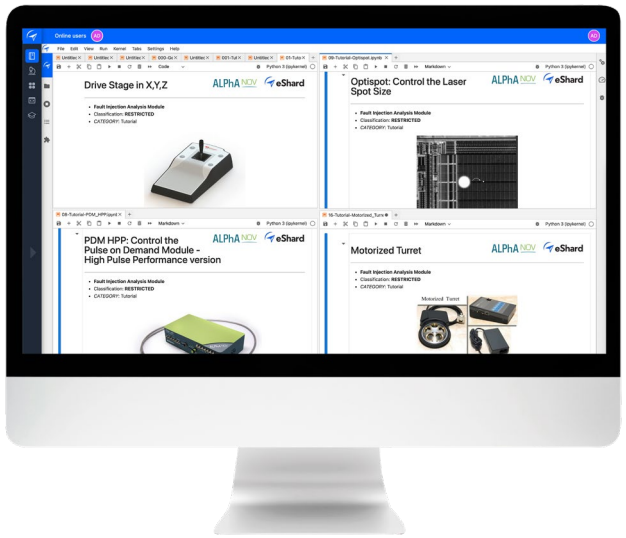
Workflow

1 integrated **workflow**

1 integrated **team**

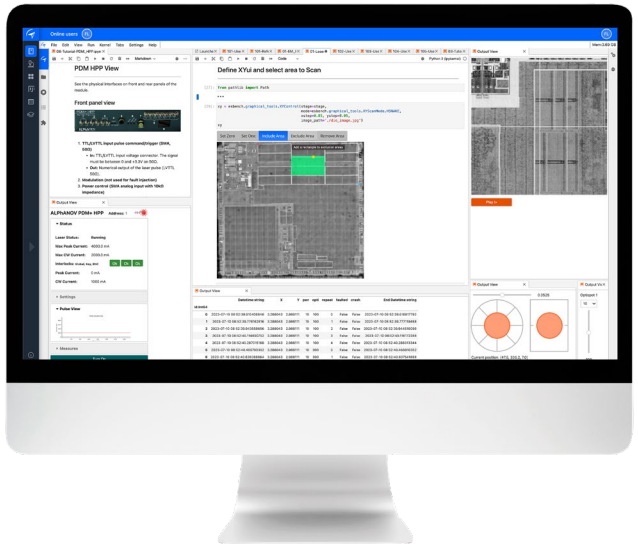
1 integrated **tool**

Fault Injection setup



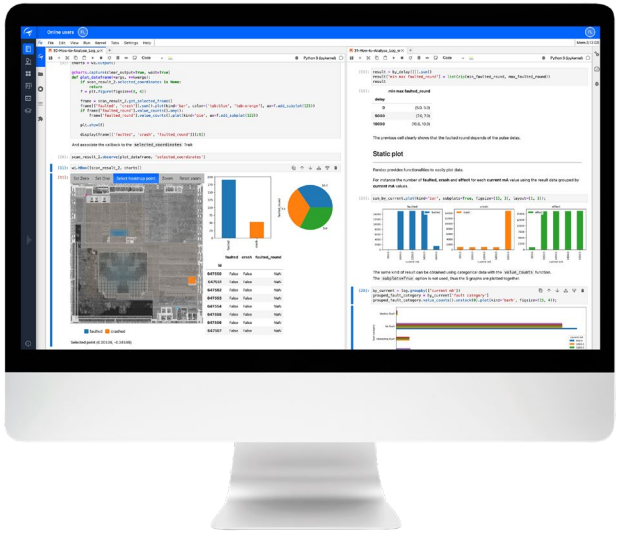
Setup your fault injection bench by controlling each equipment from the platform via API or widget. ALPhANOV equipment is ready to use. Communicate with the DUT. Manage easily any new equipment.

Fault Injection testing



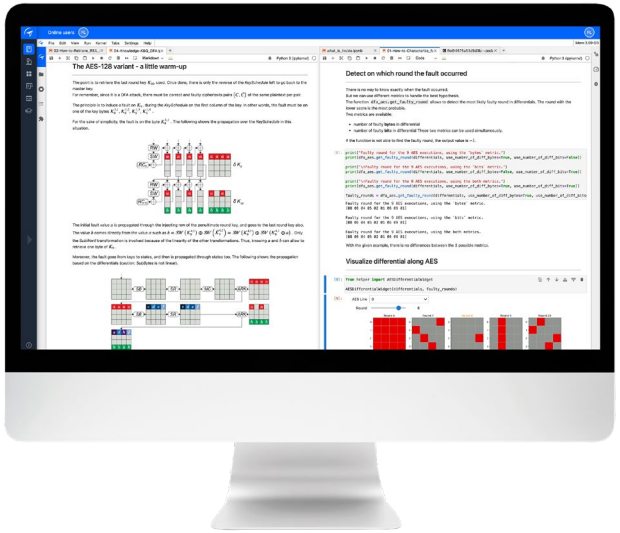
Scan the device to look for the set of parameters leading to logical faults. Create heatmaps. Launch intensive campaigns to investigate potential weaknesses in the product.

Data analysis



Classify the fault-specific outcomes. Identify the root cause of observed anomalies or unexpected behaviour. Use statistical and differential analyses to detect patterns in the acquired data.

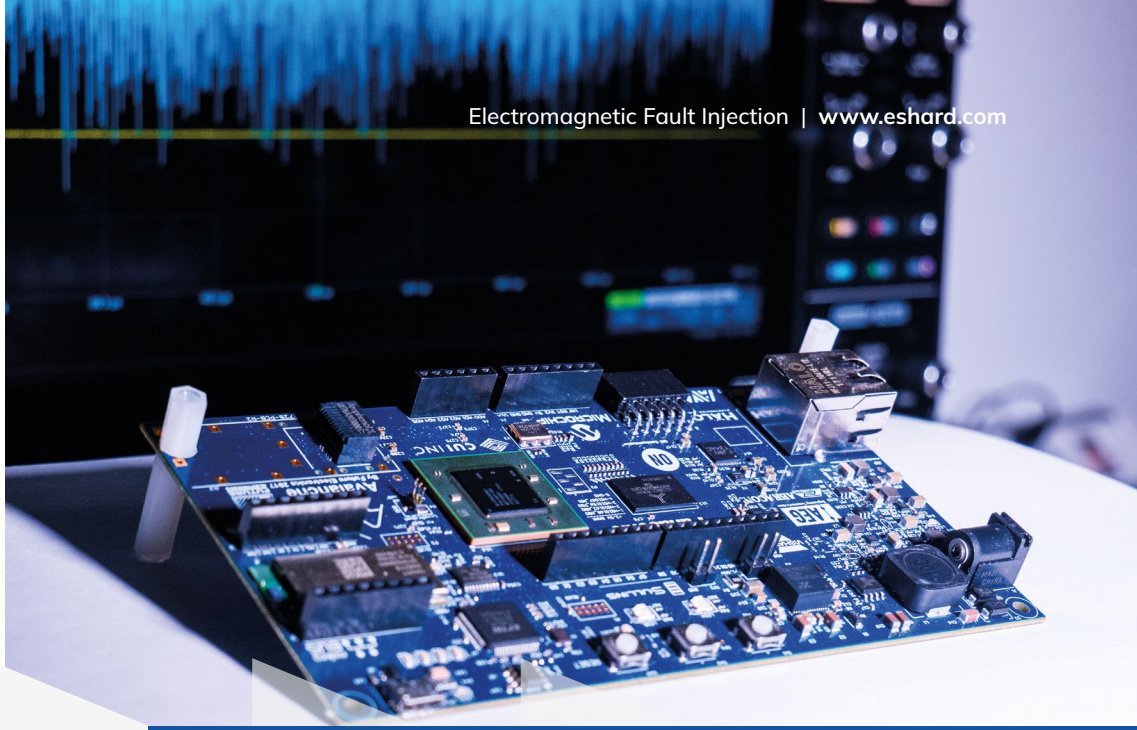
Exploitation



Combine your knowledge of the target with the identified faulty outcomes that qualify for differential fault analysis on symmetric and asymmetric cryptographic primitives.

Complete and Efficient Hardware Security Testing.

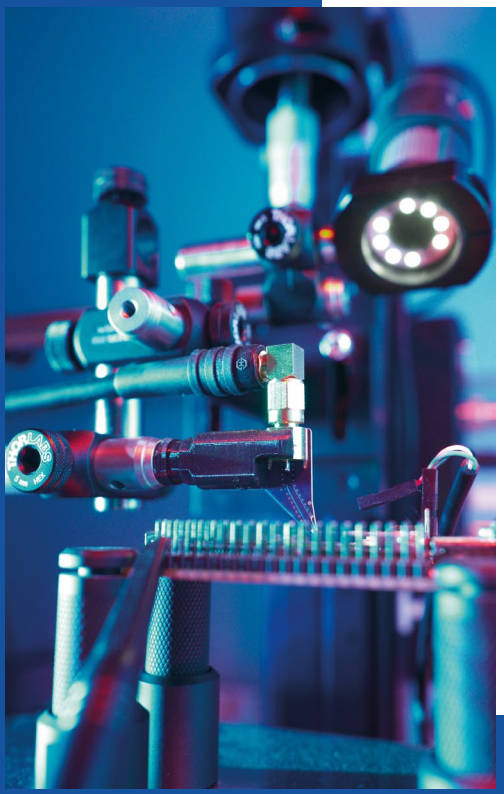
Ask for your free trial



CHALLENGE A SOLUTION IN ESHARD'S

EMFI Lab

For any industry and governmental and academic institution that needs to outsource a hardware product evaluation with EMFI for lack of expertise or resource reasons.



TESTING LAB

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

LONG TRACK RECORD

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

COLLABORATIVE

With continuous project scope review and adjustments. Resulting notebooks can be replayed in your lab premises for further analyses.

GROW YOUR

Expertise

WITH STARTER KITS

REALISTIC

Done on recent microcontrollers and complex SoC targets, not outdated chips.

PROGRESSIVE

Step-by-step learning from dataset acquisition to exploitation.

PRACTICAL

Real EMFI use cases.

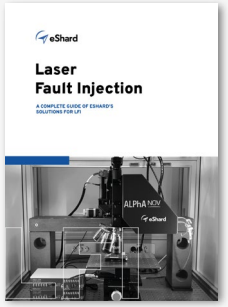
Audience: For Hardware Security Analysts who want to learn practical knowledge about EMFI or increase their competencies in this field.

Book a demo with our experts

We would like to know more about your business and projects in order to present you a more in-depth view of our solutions, tailored to your needs.

Click or scan to be redirected to the form.

Learn more about our other solutions for Integrated Circuits Security:



LASER FAULT INJECTION

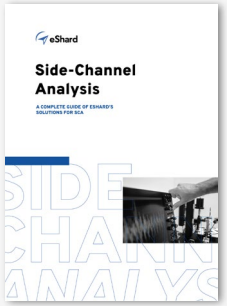
In partnership with ALPhANOV, our solution allows the implementation of laser fault injections at the state-of-the-art.

Learn more.

FIRMWARE SECURITY

Assess the security of firmware of IoT devices against logical and physical attacks.

Learn more.



SIDE-CHANNEL ANALYSIS

Our solution includes hardware, software, training for experts in cryptography and physical attacks on hardware products.

Learn more.

eShard

Get in touch

www.eshard.com

contact@eshard.com

/showcase/ic-eshard

@eshard

France HQ
Bâtiment GIENAH
11 avenue de Canteranne
33600 Pessac, France

France R&D
7 rue Gaston de Flotte
13012 Marseille, France

Germany
eShard GmbH
Beethovenallee 21
53173 Bonn