Master thesis internship: Hardware security

Countermeasures against power-off laser fault attacks

Vincent Beroulle, David Hély

Starting February 2025

1 Context of the internship

Secure circuits can be vulnerable to attacks exploiting hardware weaknesses. Active attacks involve injecting faults during runtime to extract secret data or gain unauthorized access. One approach to mitigate these threats is the integration of hardware detectors to detect or mitigate these attacks. However, previous studies have shown that power-off attacks, such as temperature manipulation when the circuits is power off, can alter the effectiveness of these detectors. New research has focused on developing self-test capabilities to detect changes in detector characteristics, such as internal frequency variations. The main goal of this internship is to prototype FPGA-based detectors with these new integrated self-testing modules and assess whether this mechanism effectively protects detectors against power-off attacks.

Objectives The detailed objectives of this internship, **which will be adapted to the candidate**, are:

- to prototype in FPGA hardware security detectors with new self-test modules,
- to realize temperature attack campaigns on FPGA prototypes to evaluate the efficiency of the self-test modules against these attacks

2 Profile of a candidate

We are looking for a motivated candidate with skills in the following areas:

- embedded systems,
- electronics/FPGA design and simulation.

Knowledge, interest or previous experience in **hardware security** would be a plus.

3 Practical information

Location The internship will take place in LCIS (Laboratoire de Conception et d'Intégration des Systèmes), Valence, France

Stipend Around 600€/month

Starting date February/March 2024

Duration 5-6 months

4 How to apply?

To apply for this internship, please send **a CV and a cover letter** to:

✉ vincent.beroulle@esisar.grenoble-inp.fr