PostDoctoral subject

Enhancing the Security of RISC-V Microarchitectures Against Laser Fault Injection: Countermeasure Development at the RTL Level

TIMA (Grenoble INP, France)

Designing secure embedded systems is a critical challenge due to their inherently complex three-layer architecture: hardware, microarchitecture, and software. Cyber threats often exploit vulnerabilities introduced during the design phase, which remain undetected due to a lack of design tools that integrate a realistic attacker model with a holistic approach. Current tools and methods lack a deep understanding of the global system, particularly the interactions between its layers and with its environment (including attacker actions).

The TWINSEC project, which frames this research, brings together several French laboratories specializing in microarchitecture security. It focuses on a key type of attack: fault injection using lasers. Existing modeling tools are not yet capable of effectively predicting an embedded systems' resistance to such attacks, as their generality leads to excessive simulation complexity. TWINSEC proposes a more realistic attacker model to identify microarchitecture-specific vulnerabilities. This approach enables designers to develop countermeasures, integrate them into systems, and verify their effectiveness in significantly reducing—or ideally preventing—the attacker's ability to exploit vulnerabilities.

Recent works aim at building realistic fault models. Previous work [1] carried out in the LCIS and TIMA laboratories under the ANR project LIESSE provided efficient CAD tools to help circuit designers evaluate countermeasures against laser attacks early in the design process. A high-level RTL model of laser-induced faults was developed to emulate such attacks. More complex and realistic fault models have been proposed since, used to evaluate secure cryptographic implementations, and have been validated with respect to circuit layouts, quantifying its accuracy in predicting localized faults. The availability of realistic and complete fault models allows designers to propose efficient and effective countermeasures at a reasonable cost, as demonstrated in recent work [2].

The **objective** of this PostDoc is to extend this work by leveraging RTL fault models existing in the state of the art and proposed by the TwinSec project, to assess and improve the security of RISC-V microarchitectures (e.g., OpenTitan, CV32, CVA6) and their recent countermeasures (e.g., Mafia, AKHACIA). **The aim is to improve existing countermeasures or develop new ones** at design level that incorporate both hardware and software protections for embedded code, such as, for example, secure boot mechanisms.

This PostDoc will take place in TIMA Laboratory, Grenble. The candidate will strictly cooperate with other partners involved in the project, both local (CEA, LCIS, Verimag) and national. The salary will be defined according to the guidelines defined by Grenolbe INP and will depend on the experience of the candidate.

Post-Doc Profile (any of the following):

- PhD related to Electrical Engineering, Computer Science, Microelectronics, Hardware security

Skills:

- Computer Architecture
- Prototyping and Simulation of Digital Systems (FPGA & ASIC)
- Physical attacks

Location: TIMA Laboratory, Grenoble, France

Contacts: paolo.maistri@univ-grenoble-alpes.fr

To apply for this position, please send the following documents to the individuals listed above:

- Your CV
- A letter of motivation (in French or English)
- A copy of your PhD report
- Letters of recommendation

Period of application : All applications will be considered until the position is filled; PhD expected to start in November-December 2025 at the earliest.

References

[1] A. Papadimitriou and al.,Analysis of laser-induced errors: RTL fault models versus layout locality characteristics, Microprocessors and Microsystems, 2016

[2] I. Alshaer, V. Beroulle, and al. (2022): Cross-layer inference methodology for microarchitecture-aware fault models, Microelectronics Reliability, Volume 139, 2022, 114841, ISSN 0026-2714, https://doi.org/10.1016/j.microrel.2022.114841.