Thesis subject

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

LCIS, 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 PhD 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 a 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.

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. This model was used to evaluate secure cryptographic implementations and validated against circuit layouts, quantifying its accuracy in predicting localized faults. Ultimately, it supported the development of an RTL countermeasure for AES designs to protect against laser attacks.

The objective of this PhD is to extend this work by using RTL fault models related to laser effects to assess 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 that incorporate both hardware and software protections for embedded code, such as secure boot mechanisms while maintaining reasonable costs, as demonstrated in recent work [2].

Initially, the previously developed fault models, which were characterized by generic hardware components (registers, glue logic), will be refined to account for the effects of laser fault injection on RISC-V microarchitectures and their typical hardware protections.

This PhD will be supervised by two laboratories: LCIS (in Valence) and TIMA (in Grenoble). Both labs specialize in hardware fault simulation at the RTL level and the development of fault injection tools, ensuring a robust foundation for this research.

PhD Student Profile (any of the following):

- Master in Embedded Systems
- Master in Computer Science
- Master in Microelectronics
- Master in Cybersecurity

Skills:

- Computer Architecture
- Prototyping and Simulation of Digital Systems
- Compiler Design

Location: Grenoble INP LCIS, Valence, France

Contacts: David.hely@lcis.grenoble-inp.fr, vincent.beroulle@lcis.grenoble-inp.fr, 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 Master's transcript (M1 and M2)
- Letters of recommendation

Period of application : All applications will be considered until the position is filled; PhD expected to start in Autumn 2025.

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.