Thesis subject

"Design and evaluation of countermeasures against power-off laser fault injection attacks"

Context of the PhD

All security primitives, when implemented in hardware, are subject to physical attacks. Among those, fault injection attacks consist in disturbing the operation at run-time to obtain secret data or unauthorized access. One particularly powerful technique to inject faults in a device is laser fault injection [SA02]. For instance, using an infrared laser, it is possible to alter the value stored in a flip-flop [Dut+18] or to corrupt the instructions when they are fetched from the Flash memory [Men+20].
While there are many possibilities offered by this technique, the associated so-called *attacker model* is quite restrictive. Indeed, it is necessary to have a direct access to the backside of the die to shoot the laser on it. This severely limits the applicability of the technique in a real-life attack scenario.
The aim of the ANR-POP project, in the framework of which this PhD is funded, is to study the feasibility of laser fault injection attacks on *power-off* targets. One important aspect of the project is to design countermeasures that are fully effective at detecting that a power-off attack has been carried out. This implies that the countermeasure does not need to be constantly powered on to operate, as it is the case for a BBICS[1] for example [Cha+15]. Therefore, when powered on again, the proposed sensor should indicate if the structure has been attacked or not. Beyond detection, structures which are resistant to these attacks will be studied too.

Objectives The objectives of this PhD are:

- to understand/simulate the *effect(s)* of power-off laser fault injection on hardware security primitives,
- to investigate techniques to *detect* that a power-off attack happened,
- to design hardware security primitives that are *resistant* to power-off attacks,
- to design hardware security primitives that can be *tested* on-line.

Project This PhD is funded by the ANR-POP project, which brings together four research laboratories:

- Mines Saint-Étienne,
- Laboratoire Hubert Curien,
- TIMA,
- LCIS.

Profile of a candidate

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

- microelectronics,
- embedded systems,
- digital electronics design and simulation,

Knowledge, interest or a previous experience in hardware security is a plus.
Speaking French is not mandatory to apply, but a good level of English is necessary.

[1] Bulk Built-In Current Sensors

Laboratoire TIMA
46 avenue Félix Viallet - 38031 GRENOBLE – FRANCE
Tél : 04 76 57 50 79
E-mail : tima-direction@univ-grenoble-alpes.fr
Web : http://tima.univ-grenoble-alpes.fr

TIMA Laboratory
46 avenue Félix Viallet - 38031 GRENOBLE – FRANCE
Tel: (+33) (0) 476 57 50 79
E-mail: tima-direction@univ-grenoble-alpes.fr
Website: http://tima.univ-grenoble-alpes.fr

Practical information

Location The PhD will take place in one of these two research laboratories:

- LCIS (Laboratoire de Conception et d'Intégration des Systèmes), Valence, France, in the CTSYS ("Sûreté et sécurité des systèmes embarqués et distribués") team,
- TIMA (Techniques de l'Informatique et de la Microélectronique pour l'Architecture des systèmes intégrés), Grenoble, France, in the AMfoRS ("Architectures and Methods for Resilient Systems") team.

The candidate may **choose the location that best suits them**.

Net salary 1420€/month approximately

Starting date October 2022

How to apply?

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

- vincent.beroulle@lcis.grenoble-inp.fr
- brice.colombier@grenoble-inp.fr
- giorgio.di-natale@univ-grenoble-alpes.fr
- paolo.maistri@univ-grenoble-alpes.fr
- ioana.vatajelu@univ-grenoble-alpes.fr

Diversity statement

Our team welcomes applicants with diverse backgrounds and experiences. We regard gender equality and diversity as a strength and an asset.

References

[Men+20] Alexandre Menu et al. "Single-bit Laser Fault Model in NOR Flash Memories: Analysis and Exploitation". In: *Workshop on Fault Diagnosis and Tolerance in Cryptography*. Milan, Italy: IEEE, Sept. 2020, pp. 41–48.

[Dut+18] Jean-Max Dutertre et al. "Laser Fault Injection at the CMOS 28 nm Technology Node: an Analysis of the Fault Model". In: *Workshop on Fault Diagnosis and Tolerance in Cryptography*. Amsterdam, The Netherlands: IEEE Computer Society, Sept. 2018, pp. 1–6.

[Cha+15] Clement Champeix et al. "Experimental validation of a Bulk Built-In Current Sensor for detecting laser-induced currents". In: *IEEE International On-Line Testing Symposium*. Halkidiki, Greece: IEEE, July 2015, pp. 150–155.

[SA02] Sergei P. Skorobogatov et al. "Optical Fault Induction Attacks". In: *International Workshop on Cryptographic Hardware and Embedded Systems*. Ed. by Burton S. Kaliski Jr. et al. Vol. 2523. Lecture Notes in Computer Science. Redwood Shores, CA, USA: Springer, Aug. 2002, pp. 2–12.