Laser Fault Injection Applied to Reverse Engineering of Memories

Description

Digital systems are now deeply integrated into our daily lives and essential to the functioning of our society. In these systems, memories play a crucial role in storing and manipulating secrets such as cryptographic keys, bootloaders, or proprietary codes. It is also through memories that configuration options, such as debugging modes and access privileges, are stored. A wide variety of memories exists: non-volatile memories (NVM) such as FLASH, MRAM, FUSES, and ROM, and volatile memories such as SRAM and DRAM. To ensure the security of systems, it is imperative to understand the organization of memories and master state-of-the-art methods for extracting or modifying their content.

The main objective of this thesis is to study the security of memories against laser disturbances. Laser fault injection attacks have been known since the early 2000s [1] and are now widely implemented in security characterizations and evaluation schemes. The effect of faults on volatile [2] or non-volatile [3] memories has been extensively studied. This thesis will address the problem from the perspective of reverse engineering by investigating how can laser injections be used to retrieve the organization of a memory and extract and/or modify its content.

The first axis of work will study the so-called "Thermal Laser Stimulation" (TLS) approaches, which allow information to be extracted passively from a memory. Compared to existing studies [4], we will study the effect of the type of technological node and its size. We will particularly seek to determine if the precision is sufficient to implement TLS attacks on a 22nm FDSOI technology.

The second axis of work will use laser techniques for the reverse engineering of a memory architecture. Those research will focus on understanding the organization of data, identifying the parameters of error detection and correction codes, and analyzing countermeasures. More generally, it will help in understanding the memory, in preliminary analyses to other more specific analysis techniques.

Practical Information

The PhD will take place at CEA-LETI in France, in Grenoble, within the Security Testing and Tools Laboratory (LTSO). The LTSO is a team of approximately 15 security experts and several PhD students. The laboratory specializes in security testing of products and the development of tools for vulnerability research. The laboratory has state-of-the-art equipment for laser fault injection and TLS, which will be used throughout the PhD work.

The PhD will be supervised by Thomas Hiscock, Simon Pontié, Maxime Lecomte and directed by Jessy Cledière.

Start date: September-December 2025

If you are interested, please send your resumé to Thomas Hiscock (thomas.hiscock@cea.fr) and Jessy Cledière (jessy.clediere@cea.fr)

Bibliography

[1] S. P. Skorobogatov and R. J. Anderson, “Optical Fault Induction Attacks,” in *Cryptographic Hardware and Embedded Systems - CHES 2002*, B. S. Kaliski, çetin K. Koç, and C. Paar, Eds., Berlin, Heidelberg: Springer, 2003, pp. 2–12. doi: 10.1007/3-540-36400-5_2.

[2] A. Sarafianos, C. Roscian, J.-M. Dutertre, M. Lisart, and A. Tria, “Electrical modeling of the photoelectric effect induced by a pulsed laser applied to an SRAM cell,” *Microelectronics Reliability*, vol. 53, no. 9, pp. 1300–1305, Sep. 2013, doi: 10.1016/j.microrel.2013.07.125.

[3] B. Colombier, A. Menu, J.-M. Dutertre, P.-A. Moëllic, J.-B. Rigaud, and J.-L. Danger, “Laser-induced Single-bit Faults in Flash Memory: Instructions Corruption on a 32-bit Microcontroller,” in *2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, May 2019, pp. 1–10. doi: 10.1109/HST.2019.8741030.

[4] H. Lohrke, S. Tajik, T. Krachenfels, C. Boit, and J.-P. Seifert, “Key Extraction Using Thermal Laser Stimulation: A Case Study on Xilinx Ultrascale FPGAs,” *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 573–595, Aug. 2018, doi: 10.13154/tches.v2018.i3.573-595.